Reti Avanzate e Sicurezza dei Dati, A.A. 2017–2018

Seconda prova parziale — temi e correzione

Mauro Brunato

Lonedì 4 giugno 2018

Contenuti

- Testi dei temi d'esame
- Traccia della soluzione dei primi due esercizi del Tema 1
- Risposte corrette e commentate alle domande dell'ultimo esercizio
- Griglie di correzione dei temi

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Tema 1

Lunedì 4 giugno 2018

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 13$ e sul generatore $g = 7$.

1.1) Supponendo che Alice scelga il valore segreto $a = 10$ e Bob il valore $b = 5$, descrivere lo scambio di informazioni che avviene fra i due interlocutori.

1.2) Calcolare la chiave condivisa K utilizzando la formula più conveniente fra quella usata da Alice e quella usata da Bob.

Esercizio 2

Il server web di Alice dispone di un sistema di login basato su username e password; per comodità, assumiamo che le password siano stringhe di bit.
Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile: si assuma che utilizzi una stringa casuale di 64 bit.
Il server applica alle password degli utenti una funzione hash crittografica H che genera un valore a 30 bit. In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 30 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.

Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H, ma che sappia che Bob utilizza una password di 64 bit. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login verso il server ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password, portandola a 128 bit casuali.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash in locale (nel computer di Charlie) richieda un miliardesimo di secondo.
Le risposte alle domande 2.1 e 2.2 cambiano?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Quale, tra i seguenti, è un possibile problema del protocollo Diffie-Hellman?
   (a) La possibilità di un attacco Man-in-the-Middle.
   (b) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (c) La lentezza in rapporto ai cifrari a chiave condivisa.
2. Alice e Bob avviano una sessione Diffie-Hellman; per decifrare la chiave di sessione, Charlie (in ascolto sul canale ma non in grado di interferire) deve...
   (a) ...risolvere un problema di logaritmo discreto.
   (b) ...fattorizzare un grande prodotto di numeri primi.
   (c) ...trovare una collisione in un valore hash crittografico.
3. Quale, tra i seguenti, è un possibile problema del cifrario RSA?
   (a) La possibilità di un attacco Man-in-the-Middle.
   (b) La lentezza in rapporto ai cifrari a chiave condivisa.
   (c) La difficoltà di trovare numeri primi di dimensioni sufficienti.
4. Quale proprietà caratterizza i cifrari a flusso?
   (a) Sono necessariamente interattivi.
   (b) Combinano i dati da cifrare con un flusso potenzialmente infinito di dati (pseudo-) casuali.
   (c) Non richiedono che gli interlocutori abbiano concordato e condiviso una chiave.
5. Quale delle seguenti proprietà **non** è posseduta da nessuna funzione hash crittografica?
   (a) La suriettività.
   (b) La resistenza agli attacchi di preimmagine e di collisione.
   (c) L'iniettività.
6. Quale delle seguenti proprietà è necessaria per una funzione di cifratura?
   (a) La suriettività.
   (b) L'iniettività.
   (c) La resistenza agli attacchi di preimmagine e di collisione.
7. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (b) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (c) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
8. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) Il common name del richiedente.
   (b) La chiave pubblica del richiedente.
   (c) La chiave privata del richiedente.
9. Un certificato di firma digitale solitamente accompagna...
   (a) ...una chiave di sessione, e ne garantisce l'autenticità.
   (b) ...una chiave privata, e garantisce l'identità del possessore della corrispondente chiave pubblica.
   (c) ...una chiave pubblica, e garantisce l'identità del possessore della corrispondente chiave privata.
10. Quale delle seguenti proprietà è necessaria affinché una funzione hash sia crittograficamente sicura?
    (a) La resistenza agli attacchi di preimmagine e di collisione.
    (b) L'iniettività.
    (c) La suriettività.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Tema 2

Lunedì 4 giugno 2018

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 11$ e sul generatore $g = 7$.

1.1) Supponendo che Alice scelga il valore segreto $a = 8$ e Bob il valore $b = 4$, descrivere lo scambio di informazioni che avviene fra i due interlocutori.

1.2) Calcolare la chiave condivisa K utilizzando la formula più conveniente fra quella usata da Alice e quella usata da Bob.

Esercizio 2

Il server web di Alice dispone di un sistema di login basato su username e password; per comodità, assumiamo che le password siano stringhe di bit.
Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile: si assuma che utilizzi una stringa casuale di 64 bit.
Il server applica alle password degli utenti una funzione hash crittografica H che genera un valore a 28 bit. In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 28 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.

Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H, ma che sappia che Bob utilizza una password di 64 bit. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login verso il server ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password, portandola a 128 bit casuali.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash in locale (nel computer di Charlie) richieda un miliardesimo di secondo.
Le risposte alle domande 2.1 e 2.2 cambiano?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Un certificato di firma digitale solitamente accompagna...
   (a) ...una chiave pubblica, e garantisce l'identità del possessore della corrispondente chiave privata.
   (b) ...una chiave privata, e garantisce l'identità del possessore della corrispondente chiave pubblica.
   (c) ...una chiave di sessione, e ne garantisce l'autenticità.
2. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (b) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (c) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
3. Alice e Bob avviano una sessione Diffie-Hellman; per decifrare la chiave di sessione, Charlie (in ascolto sul canale ma non in grado di interferire) deve...
   (a) ...trovare una collisione in un valore hash crittografico.
   (b) ...risolvere un problema di logaritmo discreto.
   (c) ...fattorizzare un grande prodotto di numeri primi.
4. Quale delle seguenti proprietà **non** è posseduta da nessuna funzione hash crittografica?
   (a) La resistenza agli attacchi di preimmagine e di collisione.
   (b) La suriettività.
   (c) L'iniettività.
5. Quale delle seguenti proprietà è necessaria per una funzione di cifratura?
   (a) La suriettività.
   (b) L'iniettività.
   (c) La resistenza agli attacchi di preimmagine e di collisione.
6. Quale, tra i seguenti, è un possibile problema del protocollo Diffie-Hellman?
   (a) La lentezza in rapporto ai cifrari a chiave condivisa.
   (b) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (c) La possibilità di un attacco Man-in-the-Middle.
7. Quale, tra i seguenti, è un possibile problema del cifrario RSA?
   (a) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (b) La lentezza in rapporto ai cifrari a chiave condivisa.
   (c) La possibilità di un attacco Man-in-the-Middle.
8. Quale proprietà caratterizza i cifrari a flusso?
   (a) Sono necessariamente interattivi.
   (b) Non richiedono che gli interlocutori abbiano concordato e condiviso una chiave.
   (c) Combinano i dati da cifrare con un flusso potenzialmente infinito di dati (pseudo-) casuali.
9. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave privata del richiedente.
   (b) La chiave pubblica del richiedente.
   (c) Il common name del richiedente.
10. Quale delle seguenti proprietà è necessaria affinché una funzione hash sia crittograficamente sicura?
    (a) La suriettività.
    (b) L'iniettività.
    (c) La resistenza agli attacchi di preimmagine e di collisione.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Tema 3

Lunedì 4 giugno 2018

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 11$ e sul generatore $g = 7$.

1.1) Supponendo che Alice scelga il valore segreto $a = 9$ e Bob il valore $b = 4$, descrivere lo scambio di informazioni che avviene fra i due interlocutori.

1.2) Calcolare la chiave condivisa K utilizzando la formula più conveniente fra quella usata da Alice e quella usata da Bob.

Esercizio 2

Il server web di Alice dispone di un sistema di login basato su username e password; per comodità, assumiamo che le password siano stringhe di bit.
Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile: si assuma che utilizzi una stringa casuale di 64 bit.
Il server applica alle password degli utenti una funzione hash crittografica H che genera un valore a 30 bit. In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 30 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.

Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H, ma che sappia che Bob utilizza una password di 64 bit. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login verso il server ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password, portandola a 128 bit casuali.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash in locale (nel computer di Charlie) richieda un miliardesimo di secondo.
Le risposte alle domande 2.1 e 2.2 cambiano?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Quale delle seguenti proprietà è necessaria per una funzione di cifratura?
   (a) L'iniettività.
   (b) La resistenza agli attacchi di preimmagine e di collisione.
   (c) La suriettività.
2. Quale, tra i seguenti, è un possibile problema del protocollo Diffie-Hellman?
   (a) La lentezza in rapporto ai cifrari a chiave condivisa.
   (b) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (c) La possibilità di un attacco Man-in-the-Middle.
3. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave privata del richiedente.
   (b) La chiave pubblica del richiedente.
   (c) Il common name del richiedente.
4. Un certificato di firma digitale solitamente accompagna...
   (a) ...una chiave privata, e garantisce l'identità del possessore della corrispondente chiave pubblica.
   (b) ...una chiave di sessione, e ne garantisce l'autenticità.
   (c) ...una chiave pubblica, e garantisce l'identità del possessore della corrispondente chiave privata.
5. Quale delle seguenti proprietà **non** è posseduta da nessuna funzione hash crittografica?
   (a) La suriettività.
   (b) L'iniettività.
   (c) La resistenza agli attacchi di preimmagine e di collisione.
6. Quale delle seguenti proprietà è necessaria affinché una funzione hash sia crittograficamente sicura?
   (a) La resistenza agli attacchi di preimmagine e di collisione.
   (b) L'iniettività.
   (c) La suriettività.
7. Quale proprietà caratterizza i cifrari a flusso?
   (a) Combinano i dati da cifrare con un flusso potenzialmente infinito di dati (pseudo-) casuali.
   (b) Sono necessariamente interattivi.
   (c) Non richiedono che gli interlocutori abbiano concordato e condiviso una chiave.
8. Quale, tra i seguenti, è un possibile problema del cifrario RSA?
   (a) La possibilità di un attacco Man-in-the-Middle.
   (b) La lentezza in rapporto ai cifrari a chiave condivisa.
   (c) La difficoltà di trovare numeri primi di dimensioni sufficienti.
9. Alice e Bob avviano una sessione Diffie-Hellman; per decifrare la chiave di sessione, Charlie (in ascolto sul canale ma non in grado di interferire) deve...
   (a) ...fattorizzare un grande prodotto di numeri primi.
   (b) ...risolvere un problema di logaritmo discreto.
   (c) ...trovare una collisione in un valore hash crittografico.
10. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
    (a) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
    (b) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
    (c) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Tema 4

Lunedì 4 giugno 2018

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 13$ e sul generatore $g = 7$.

1.1) Supponendo che Alice scelga il valore segreto $a = 10$ e Bob il valore $b = 2$, descrivere lo scambio di informazioni che avviene fra i due interlocutori.

1.2) Calcolare la chiave condivisa K utilizzando la formula più conveniente fra quella usata da Alice e quella usata da Bob.

Esercizio 2

Il server web di Alice dispone di un sistema di login basato su username e password; per comodità, assumiamo che le password siano stringhe di bit.
Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile: si assuma che utilizzi una stringa casuale di 64 bit.
Il server applica alle password degli utenti una funzione hash crittografica H che genera un valore a 32 bit. In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 32 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.

Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H, ma che sappia che Bob utilizza una password di 64 bit. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login verso il server ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password, portandola a 128 bit casuali.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash in locale (nel computer di Charlie) richieda un miliardesimo di secondo.
Le risposte alle domande 2.1 e 2.2 cambiano?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Quale proprietà caratterizza i cifrari a flusso?
   (a) Sono necessariamente interattivi.
   (b) Combinano i dati da cifrare con un flusso potenzialmente infinito di dati (pseudo-) casuali.
   (c) Non richiedono che gli interlocutori abbiano concordato e condiviso una chiave.
2. Alice e Bob avviano una sessione Diffie-Hellman; per decifrare la chiave di sessione, Charlie (in ascolto sul canale ma non in grado di interferire) deve...
   (a) ... fattorizzare un grande prodotto di numeri primi.
   (b) ... trovare una collisione in un valore hash crittografico.
   (c) ... risolvere un problema di logaritmo discreto.
3. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (b) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (c) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
4. Quale delle seguenti proprietà è necessaria per una funzione di cifratura?
   (a) La resistenza agli attacchi di preimmagine e di collisione.
   (b) La suriettività.
   (c) L'iniettività.
5. Quale, tra i seguenti, è un possibile problema del cifrario RSA?
   (a) La possibilità di un attacco Man-in-the-Middle.
   (b) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (c) La lentezza in rapporto ai cifrari a chiave condivisa.
6. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave privata del richiedente.
   (b) Il common name del richiedente.
   (c) La chiave pubblica del richiedente.
7. Quale, tra i seguenti, è un possibile problema del protocollo Diffie-Hellman?
   (a) La possibilità di un attacco Man-in-the-Middle.
   (b) La lentezza in rapporto ai cifrari a chiave condivisa.
   (c) La difficoltà di trovare numeri primi di dimensioni sufficienti.
8. Quale delle seguenti proprietà **non** è posseduta da nessuna funzione hash crittografica?
   (a) La suriettività.
   (b) L'iniettività.
   (c) La resistenza agli attacchi di preimmagine e di collisione.
9. Un certificato di firma digitale solitamente accompagna...
   (a) ... una chiave privata, e garantisce l'identità del possessore della corrispondente chiave pubblica.
   (b) ... una chiave pubblica, e garantisce l'identità del possessore della corrispondente chiave privata.
   (c) ... una chiave di sessione, e ne garantisce l'autenticità.
10. Quale delle seguenti proprietà è necessaria affinché una funzione hash sia crittograficamente sicura?
    (a) L'iniettività.
    (b) La suriettività.
    (c) La resistenza agli attacchi di preimmagine e di collisione.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Tema 5

Lunedì 4 giugno 2018

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 11$ e sul generatore $g = 8$.

1.1) Supponendo che Alice scelga il valore segreto $a = 7$ e Bob il valore $b = 2$, descrivere lo scambio di informazioni che avviene fra i due interlocutori.

1.2) Calcolare la chiave condivisa K utilizzando la formula più conveniente fra quella usata da Alice e quella usata da Bob.

Esercizio 2

Il server web di Alice dispone di un sistema di login basato su username e password; per comodità, assumiamo che le password siano stringhe di bit.
Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile: si assuma che utilizzi una stringa casuale di 64 bit.
Il server applica alle password degli utenti una funzione hash crittografica H che genera un valore a 30 bit. In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 30 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.

Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H, ma che sappia che Bob utilizza una password di 64 bit. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login verso il server ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password, portandola a 128 bit casuali.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash in locale (nel computer di Charlie) richieda un miliardesimo di secondo.
Le risposte alle domande 2.1 e 2.2 cambiano?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) Il common name del richiedente.
   (b) La chiave pubblica del richiedente.
   (c) La chiave privata del richiedente.
2. Quale, tra i seguenti, è un possibile problema del cifrario RSA?
   (a) La lentezza in rapporto ai cifrari a chiave condivisa.
   (b) La possibilità di un attacco Man-in-the-Middle.
   (c) La difficoltà di trovare numeri primi di dimensioni sufficienti.
3. Quale delle seguenti proprietà è necessaria per una funzione di cifratura?
   (a) L'iniettività.
   (b) La suriettività.
   (c) La resistenza agli attacchi di preimmagine e di collisione.
4. Quale proprietà caratterizza i cifrari a flusso?
   (a) Non richiedono che gli interlocutori abbiano concordato e condiviso una chiave.
   (b) Combinano i dati da cifrare con un flusso potenzialmente infinito di dati (pseudo-) casuali.
   (c) Sono necessariamente interattivi.
5. Quale, tra i seguenti, è un possibile problema del protocollo Diffie-Hellman?
   (a) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (b) La lentezza in rapporto ai cifrari a chiave condivisa.
   (c) La possibilità di un attacco Man-in-the-Middle.
6. Alice e Bob avviano una sessione Diffie-Hellman; per decifrare la chiave di sessione, Charlie (in ascolto sul canale ma non in grado di interferire) deve...
   (a) ... fattorizzare un grande prodotto di numeri primi.
   (b) ... trovare una collisione in un valore hash crittografico.
   (c) ... risolvere un problema di logaritmo discreto.
7. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (b) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (c) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
8. Quale delle seguenti proprietà è necessaria affinché una funzione hash sia crittograficamente sicura?
   (a) La resistenza agli attacchi di preimmagine e di collisione.
   (b) L'iniettività.
   (c) La suriettività.
9. Quale delle seguenti proprietà **non** è posseduta da nessuna funzione hash crittografica?
   (a) La suriettività.
   (b) L'iniettività.
   (c) La resistenza agli attacchi di preimmagine e di collisione.
10. Un certificato di firma digitale solitamente accompagna...
    (a) ... una chiave di sessione, e ne garantisce l'autenticità.
    (b) ... una chiave privata, e garantisce l'identità del possessore della corrispondente chiave pubblica.
    (c) ... una chiave pubblica, e garantisce l'identità del possessore della corrispondente chiave privata.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Tema 6

Lunedì 4 giugno 2018

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 11$ e sul generatore $g = 7$.

1.1) Supponendo che Alice scelga il valore segreto $a = 7$ e Bob il valore $b = 3$, descrivere lo scambio di informazioni che avviene fra i due interlocutori.

1.2) Calcolare la chiave condivisa K utilizzando la formula più conveniente fra quella usata da Alice e quella usata da Bob.

Esercizio 2

Il server web di Alice dispone di un sistema di login basato su username e password; per comodità, assumiamo che le password siano stringhe di bit.
Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile: si assuma che utilizzi una stringa casuale di 64 bit.
Il server applica alle password degli utenti una funzione hash crittografica H che genera un valore a 32 bit. In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 32 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.

Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H, ma che sappia che Bob utilizza una password di 64 bit. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login verso il server ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password, portandola a 128 bit casuali.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash in locale (nel computer di Charlie) richieda un miliardesimo di secondo.
Le risposte alle domande 2.1 e 2.2 cambiano?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Quale proprietà caratterizza i cifrari a flusso?
   (a) Sono necessariamente interattivi.
   (b) Non richiedono che gli interlocutori abbiano concordato e condiviso una chiave.
   (c) Combinano i dati da cifrare con un flusso potenzialmente infinito di dati (pseudo-) casuali.
2. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (b) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (c) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
3. Un certificato di firma digitale solitamente accompagna...
   (a) ...una chiave pubblica, e garantisce l'identità del possessore della corrispondente chiave privata.
   (b) ...una chiave privata, e garantisce l'identità del possessore della corrispondente chiave pubblica.
   (c) ...una chiave di sessione, e ne garantisce l'autenticità.
4. Alice e Bob avviano una sessione Diffie-Hellman; per decifrare la chiave di sessione, Charlie (in ascolto sul canale ma non in grado di interferire) deve...
   (a) ...trovare una collisione in un valore hash crittografico.
   (b) ...fattorizzare un grande prodotto di numeri primi.
   (c) ...risolvere un problema di logaritmo discreto.
5. Quale delle seguenti proprietà è necessaria affinché una funzione hash sia crittograficamente sicura?
   (a) La resistenza agli attacchi di preimmagine e di collisione.
   (b) L'iniettività.
   (c) La suriettività.
6. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave privata del richiedente.
   (b) La chiave pubblica del richiedente.
   (c) Il common name del richiedente.
7. Quale delle seguenti proprietà **non** è posseduta da nessuna funzione hash crittografica?
   (a) L'iniettività.
   (b) La suriettività.
   (c) La resistenza agli attacchi di preimmagine e di collisione.
8. Quale, tra i seguenti, è un possibile problema del protocollo Diffie-Hellman?
   (a) La possibilità di un attacco Man-in-the-Middle.
   (b) La lentezza in rapporto ai cifrari a chiave condivisa.
   (c) La difficoltà di trovare numeri primi di dimensioni sufficienti.
9. Quale, tra i seguenti, è un possibile problema del cifrario RSA?
   (a) La possibilità di un attacco Man-in-the-Middle.
   (b) La lentezza in rapporto ai cifrari a chiave condivisa.
   (c) La difficoltà di trovare numeri primi di dimensioni sufficienti.
10. Quale delle seguenti proprietà è necessaria per una funzione di cifratura?
    (a) La resistenza agli attacchi di preimmagine e di collisione.
    (b) La suriettività.
    (c) L'iniettività.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Tema 7

Lunedì 4 giugno 2018

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 13$ e sul generatore $g = 7$.

1.1) Supponendo che Alice scelga il valore segreto $a = 10$ e Bob il valore $b = 2$, descrivere lo scambio di informazioni che avviene fra i due interlocutori.

1.2) Calcolare la chiave condivisa K utilizzando la formula più conveniente fra quella usata da Alice e quella usata da Bob.

Esercizio 2

Il server web di Alice dispone di un sistema di login basato su username e password; per comodità, assumiamo che le password siano stringhe di bit.
Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile: si assuma che utilizzi una stringa casuale di 64 bit.
Il server applica alle password degli utenti una funzione hash crittografica H che genera un valore a 30 bit. In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 30 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.

Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H, ma che sappia che Bob utilizza una password di 64 bit. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login verso il server ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password, portandola a 128 bit casuali.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash in locale (nel computer di Charlie) richieda un miliardesimo di secondo.
Le risposte alle domande 2.1 e 2.2 cambiano?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Quale delle seguenti proprietà è necessaria affinché una funzione hash sia crittograficamente sicura?
   (a) La suriettività.
   (b) La resistenza agli attacchi di preimmagine e di collisione.
   (c) L'iniettività.
2. Quale delle seguenti proprietà **non** è posseduta da nessuna funzione hash crittografica?
   (a) La suriettività.
   (b) L'iniettività.
   (c) La resistenza agli attacchi di preimmagine e di collisione.
3. Quale proprietà caratterizza i cifrari a flusso?
   (a) Non richiedono che gli interlocutori abbiano concordato e condiviso una chiave.
   (b) Sono necessariamente interattivi.
   (c) Combinano i dati da cifrare con un flusso potenzialmente infinito di dati (pseudo-) casuali.
4. Un certificato di firma digitale solitamente accompagna...
   (a) ...una chiave pubblica, e garantisce l'identità del possessore della corrispondente chiave privata.
   (b) ...una chiave di sessione, e ne garantisce l'autenticità.
   (c) ...una chiave privata, e garantisce l'identità del possessore della corrispondente chiave pubblica.
5. Alice e Bob avviano una sessione Diffie-Hellman; per decifrare la chiave di sessione, Charlie (in ascolto sul canale ma non in grado di interferire) deve...
   (a) ...trovare una collisione in un valore hash crittografico.
   (b) ...fattorizzare un grande prodotto di numeri primi.
   (c) ...risolvere un problema di logaritmo discreto.
6. Quale, tra i seguenti, è un possibile problema del protocollo Diffie-Hellman?
   (a) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (b) La possibilità di un attacco Man-in-the-Middle.
   (c) La lentezza in rapporto ai cifrari a chiave condivisa.
7. Quale, tra i seguenti, è un possibile problema del cifrario RSA?
   (a) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (b) La possibilità di un attacco Man-in-the-Middle.
   (c) La lentezza in rapporto ai cifrari a chiave condivisa.
8. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) Il common name del richiedente.
   (b) La chiave pubblica del richiedente.
   (c) La chiave privata del richiedente.
9. Quale delle seguenti proprietà è necessaria per una funzione di cifratura?
   (a) La suriettività.
   (b) La resistenza agli attacchi di preimmagine e di collisione.
   (c) L'iniettività.
10. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
    (a) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
    (b) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
    (c) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Tema 8

Lunedì 4 giugno 2018

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 13$ e sul generatore $g = 6$.

1.1) Supponendo che Alice scelga il valore segreto $a = 10$ e Bob il valore $b = 2$, descrivere lo scambio di informazioni che avviene fra i due interlocutori.

1.2) Calcolare la chiave condivisa K utilizzando la formula più conveniente fra quella usata da Alice e quella usata da Bob.

Esercizio 2

Il server web di Alice dispone di un sistema di login basato su username e password; per comodità, assumiamo che le password siano stringhe di bit.
Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile: si assuma che utilizzi una stringa casuale di 64 bit.
Il server applica alle password degli utenti una funzione hash crittografica H che genera un valore a 30 bit. In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 30 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.

Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H, ma che sappia che Bob utilizza una password di 64 bit. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login verso il server ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password, portandola a 128 bit casuali.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash in locale (nel computer di Charlie) richieda un miliardesimo di secondo.
Le risposte alle domande 2.1 e 2.2 cambiano?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Quale, tra i seguenti, è un possibile problema del cifrario RSA?
   (a) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (b) La lentezza in rapporto ai cifrari a chiave condivisa.
   (c) La possibilità di un attacco Man-in-the-Middle.
2. Alice e Bob avviano una sessione Diffie-Hellman; per decifrare la chiave di sessione, Charlie (in ascolto sul canale ma non in grado di interferire) deve...
   (a) ...trovare una collisione in un valore hash crittografico.
   (b) ...fattorizzare un grande prodotto di numeri primi.
   (c) ...risolvere un problema di logaritmo discreto.
3. Quale delle seguenti proprietà è necessaria per una funzione di cifratura?
   (a) La suriettività.
   (b) L'iniettività.
   (c) La resistenza agli attacchi di preimmagine e di collisione.
4. Quale delle seguenti proprietà **non** è posseduta da nessuna funzione hash crittografica?
   (a) La suriettività.
   (b) La resistenza agli attacchi di preimmagine e di collisione.
   (c) L'iniettività.
5. Quale, tra i seguenti, è un possibile problema del protocollo Diffie-Hellman?
   (a) La possibilità di un attacco Man-in-the-Middle.
   (b) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (c) La lentezza in rapporto ai cifrari a chiave condivisa.
6. Un certificato di firma digitale solitamente accompagna...
   (a) ...una chiave di sessione, e ne garantisce l'autenticità.
   (b) ...una chiave pubblica, e garantisce l'identità del possessore della corrispondente chiave privata.
   (c) ...una chiave privata, e garantisce l'identità del possessore della corrispondente chiave pubblica.
7. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (b) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (c) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
8. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave pubblica del richiedente.
   (b) Il common name del richiedente.
   (c) La chiave privata del richiedente.
9. Quale delle seguenti proprietà è necessaria affinché una funzione hash sia crittograficamente sicura?
   (a) L'iniettività.
   (b) La resistenza agli attacchi di preimmagine e di collisione.
   (c) La suriettività.
10. Quale proprietà caratterizza i cifrari a flusso?
    (a) Non richiedono che gli interlocutori abbiano concordato e condiviso una chiave.
    (b) Combinano i dati da cifrare con un flusso potenzialmente infinito di dati (pseudo-) casuali.
    (c) Sono necessariamente interattivi.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Tema 9

Lunedì 4 giugno 2018

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 11$ e sul generatore $g = 6$.

1.1) Supponendo che Alice scelga il valore segreto $a = 9$ e Bob il valore $b = 5$, descrivere lo scambio di informazioni che avviene fra i due interlocutori.

1.2) Calcolare la chiave condivisa K utilizzando la formula più conveniente fra quella usata da Alice e quella usata da Bob.

Esercizio 2

Il server web di Alice dispone di un sistema di login basato su username e password; per comodità, assumiamo che le password siano stringhe di bit.
Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile: si assuma che utilizzi una stringa casuale di 64 bit.
Il server applica alle password degli utenti una funzione hash crittografica H che genera un valore a 30 bit. In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 30 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.

Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H, ma che sappia che Bob utilizza una password di 64 bit. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login verso il server ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password, portandola a 128 bit casuali.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash in locale (nel computer di Charlie) richieda un miliardesimo di secondo.
Le risposte alle domande 2.1 e 2.2 cambiano?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) Il common name del richiedente.
   (b) La chiave privata del richiedente.
   (c) La chiave pubblica del richiedente.
2. Quale delle seguenti proprietà è necessaria affinché una funzione hash sia crittograficamente sicura?
   (a) La resistenza agli attacchi di preimmagine e di collisione.
   (b) L'iniettività.
   (c) La suriettività.
3. Alice e Bob avviano una sessione Diffie-Hellman; per decifrare la chiave di sessione, Charlie (in ascolto sul canale ma non in grado di interferire) deve...
   (a) ...fattorizzare un grande prodotto di numeri primi.
   (b) ...risolvere un problema di logaritmo discreto.
   (c) ...trovare una collisione in un valore hash crittografico.
4. Quale delle seguenti proprietà **non** è posseduta da nessuna funzione hash crittografica?
   (a) La resistenza agli attacchi di preimmagine e di collisione.
   (b) L'iniettività.
   (c) La suriettività.
5. Quale, tra i seguenti, è un possibile problema del protocollo Diffie-Hellman?
   (a) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (b) La lentezza in rapporto ai cifrari a chiave condivisa.
   (c) La possibilità di un attacco Man-in-the-Middle.
6. Quale delle seguenti proprietà è necessaria per una funzione di cifratura?
   (a) La resistenza agli attacchi di preimmagine e di collisione.
   (b) L'iniettività.
   (c) La suriettività.
7. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (b) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (c) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
8. Quale, tra i seguenti, è un possibile problema del cifrario RSA?
   (a) La possibilità di un attacco Man-in-the-Middle.
   (b) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (c) La lentezza in rapporto ai cifrari a chiave condivisa.
9. Quale proprietà caratterizza i cifrari a flusso?
   (a) Combinano i dati da cifrare con un flusso potenzialmente infinito di dati (pseudo-) casuali.
   (b) Non richiedono che gli interlocutori abbiano concordato e condiviso una chiave.
   (c) Sono necessariamente interattivi.
10. Un certificato di firma digitale solitamente accompagna...
    (a) ...una chiave di sessione, e ne garantisce l'autenticità.
    (b) ...una chiave privata, e garantisce l'identità del possessore della corrispondente chiave pubblica.
    (c) ...una chiave pubblica, e garantisce l'identità del possessore della corrispondente chiave privata.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Tema 10

Lunedì 4 giugno 2018

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 11$ e sul generatore $g = 8$.

1.1) Supponendo che Alice scelga il valore segreto $a = 9$ e Bob il valore $b = 4$, descrivere lo scambio di informazioni che avviene fra i due interlocutori.

1.2) Calcolare la chiave condivisa K utilizzando la formula più conveniente fra quella usata da Alice e quella usata da Bob.

Esercizio 2

Il server web di Alice dispone di un sistema di login basato su username e password; per comodità, assumiamo che le password siano stringhe di bit.
Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile: si assuma che utilizzi una stringa casuale di 64 bit.
Il server applica alle password degli utenti una funzione hash crittografica H che genera un valore a 24 bit. In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 24 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.

Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H, ma che sappia che Bob utilizza una password di 64 bit. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login verso il server ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password, portandola a 128 bit casuali.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash in locale (nel computer di Charlie) richieda un miliardesimo di secondo.
Le risposte alle domande 2.1 e 2.2 cambiano?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Quale proprietà caratterizza i cifrari a flusso?
   (a) Combinano i dati da cifrare con un flusso potenzialmente infinito di dati (pseudo-) casuali.
   (b) Non richiedono che gli interlocutori abbiano concordato e condiviso una chiave.
   (c) Sono necessariamente interattivi.
2. Quale delle seguenti proprietà è necessaria per una funzione di cifratura?
   (a) La resistenza agli attacchi di preimmagine e di collisione.
   (b) L'iniettività.
   (c) La suriettività.
3. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (b) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (c) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
4. Quale, tra i seguenti, è un possibile problema del cifrario RSA?
   (a) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (b) La lentezza in rapporto ai cifrari a chiave condivisa.
   (c) La possibilità di un attacco Man-in-the-Middle.
5. Un certificato di firma digitale solitamente accompagna...
   (a) ...una chiave privata, e garantisce l'identità del possessore della corrispondente chiave pubblica.
   (b) ...una chiave di sessione, e ne garantisce l'autenticità.
   (c) ...una chiave pubblica, e garantisce l'identità del possessore della corrispondente chiave privata.
6. Quale delle seguenti proprietà è necessaria affinché una funzione hash sia crittograficamente sicura?
   (a) La suriettività.
   (b) L'iniettività.
   (c) La resistenza agli attacchi di preimmagine e di collisione.
7. Quale delle seguenti proprietà **non** è posseduta da nessuna funzione hash crittografica?
   (a) La resistenza agli attacchi di preimmagine e di collisione.
   (b) L'iniettività.
   (c) La suriettività.
8. Alice e Bob avviano una sessione Diffie-Hellman; per decifrare la chiave di sessione, Charlie (in ascolto sul canale ma non in grado di interferire) deve...
   (a) ...fattorizzare un grande prodotto di numeri primi.
   (b) ...trovare una collisione in un valore hash crittografico.
   (c) ...risolvere un problema di logaritmo discreto.
9. Quale, tra i seguenti, è un possibile problema del protocollo Diffie-Hellman?
   (a) La possibilità di un attacco Man-in-the-Middle.
   (b) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (c) La lentezza in rapporto ai cifrari a chiave condivisa.
10. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
    (a) Il common name del richiedente.
    (b) La chiave privata del richiedente.
    (c) La chiave pubblica del richiedente.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Tema 11

Lunedì 4 giugno 2018

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 13$ e sul generatore $g = 6$.

1.1) Supponendo che Alice scelga il valore segreto $a = 9$ e Bob il valore $b = 5$, descrivere lo scambio di informazioni che avviene fra i due interlocutori.

1.2) Calcolare la chiave condivisa K utilizzando la formula più conveniente fra quella usata da Alice e quella usata da Bob.

Esercizio 2

Il server web di Alice dispone di un sistema di login basato su username e password; per comodità, assumiamo che le password siano stringhe di bit.
Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile: si assuma che utilizzi una stringa casuale di 64 bit.
Il server applica alle password degli utenti una funzione hash crittografica H che genera un valore a 30 bit. In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 30 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.

Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H, ma che sappia che Bob utilizza una password di 64 bit. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login verso il server ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password, portandola a 128 bit casuali.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash in locale (nel computer di Charlie) richieda un miliardesimo di secondo.
Le risposte alle domande 2.1 e 2.2 cambiano?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Quale proprietà caratterizza i cifrari a flusso?
   (a) Combinano i dati da cifrare con un flusso potenzialmente infinito di dati (pseudo-) casuali.
   (b) Sono necessariamente interattivi.
   (c) Non richiedono che gli interlocutori abbiano concordato e condiviso una chiave.
2. Quale delle seguenti proprietà è necessaria affinché una funzione hash sia crittograficamente sicura?
   (a) La resistenza agli attacchi di preimmagine e di collisione.
   (b) La suriettività.
   (c) L'iniettività.
3. Quale, tra i seguenti, è un possibile problema del cifrario RSA?
   (a) La possibilità di un attacco Man-in-the-Middle.
   (b) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (c) La lentezza in rapporto ai cifrari a chiave condivisa.
4. Alice e Bob avviano una sessione Diffie-Hellman; per decifrare la chiave di sessione, Charlie (in ascolto sul canale ma non in grado di interferire) deve...
   (a) ...trovare una collisione in un valore hash crittografico.
   (b) ...fattorizzare un grande prodotto di numeri primi.
   (c) ...risolvere un problema di logaritmo discreto.
5. Quale delle seguenti proprietà è necessaria per una funzione di cifratura?
   (a) La suriettività.
   (b) L'iniettività.
   (c) La resistenza agli attacchi di preimmagine e di collisione.
6. Quale delle seguenti proprietà **non** è posseduta da nessuna funzione hash crittografica?
   (a) La resistenza agli attacchi di preimmagine e di collisione.
   (b) La suriettività.
   (c) L'iniettività.
7. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave pubblica del richiedente.
   (b) La chiave privata del richiedente.
   (c) Il common name del richiedente.
8. Quale, tra i seguenti, è un possibile problema del protocollo Diffie-Hellman?
   (a) La possibilità di un attacco Man-in-the-Middle.
   (b) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (c) La lentezza in rapporto ai cifrari a chiave condivisa.
9. Un certificato di firma digitale solitamente accompagna...
   (a) ...una chiave privata, e garantisce l'identità del possessore della corrispondente chiave pubblica.
   (b) ...una chiave pubblica, e garantisce l'identità del possessore della corrispondente chiave privata.
   (c) ...una chiave di sessione, e ne garantisce l'autenticità.
10. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
    (a) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
    (b) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
    (c) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Tema 12

Lunedì 4 giugno 2018

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 11$ e sul generatore $g = 6$.

1.1) Supponendo che Alice scelga il valore segreto $a = 9$ e Bob il valore $b = 2$, descrivere lo scambio di informazioni che avviene fra i due interlocutori.

1.2) Calcolare la chiave condivisa K utilizzando la formula più conveniente fra quella usata da Alice e quella usata da Bob.

Esercizio 2

Il server web di Alice dispone di un sistema di login basato su username e password; per comodità, assumiamo che le password siano stringhe di bit.
Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile: si assuma che utilizzi una stringa casuale di 64 bit.
Il server applica alle password degli utenti una funzione hash crittografica H che genera un valore a 24 bit. In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 24 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.

Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H, ma che sappia che Bob utilizza una password di 64 bit. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login verso il server ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password, portandola a 128 bit casuali.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash in locale (nel computer di Charlie) richieda un miliardesimo di secondo.
Le risposte alle domande 2.1 e 2.2 cambiano?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Quale delle seguenti proprietà **non** è posseduta da nessuna funzione hash crittografica?
   (a) La resistenza agli attacchi di preimmagine e di collisione.
   (b) L'iniettività.
   (c) La suriettività.
2. Quale, tra i seguenti, è un possibile problema del cifrario RSA?
   (a) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (b) La possibilità di un attacco Man-in-the-Middle.
   (c) La lentezza in rapporto ai cifrari a chiave condivisa.
3. Un certificato di firma digitale solitamente accompagna...
   (a) ...una chiave di sessione, e ne garantisce l'autenticità.
   (b) ...una chiave pubblica, e garantisce l'identità del possessore della corrispondente chiave privata.
   (c) ...una chiave privata, e garantisce l'identità del possessore della corrispondente chiave pubblica.
4. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (b) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (c) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
5. Quale delle seguenti proprietà è necessaria affinché una funzione hash sia crittograficamente sicura?
   (a) La resistenza agli attacchi di preimmagine e di collisione.
   (b) La suriettività.
   (c) L'iniettività.
6. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) Il common name del richiedente.
   (b) La chiave pubblica del richiedente.
   (c) La chiave privata del richiedente.
7. Quale delle seguenti proprietà è necessaria per una funzione di cifratura?
   (a) La suriettività.
   (b) La resistenza agli attacchi di preimmagine e di collisione.
   (c) L'iniettività.
8. Quale proprietà caratterizza i cifrari a flusso?
   (a) Non richiedono che gli interlocutori abbiano concordato e condiviso una chiave.
   (b) Combinano i dati da cifrare con un flusso potenzialmente infinito di dati (pseudo-) casuali.
   (c) Sono necessariamente interattivi.
9. Quale, tra i seguenti, è un possibile problema del protocollo Diffie-Hellman?
   (a) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (b) La possibilità di un attacco Man-in-the-Middle.
   (c) La lentezza in rapporto ai cifrari a chiave condivisa.
10. Alice e Bob avviano una sessione Diffie-Hellman; per decifrare la chiave di sessione, Charlie (in ascolto sul canale ma non in grado di interferire) deve...
    (a) ...fattorizzare un grande prodotto di numeri primi.
    (b) ...risolvere un problema di logaritmo discreto.
    (c) ...trovare una collisione in un valore hash crittografico.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Tema 13

Lunedì 4 giugno 2018

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 11$ e sul generatore $g = 7$.

1.1) Supponendo che Alice scelga il valore segreto $a = 9$ e Bob il valore $b = 3$, descrivere lo scambio di informazioni che avviene fra i due interlocutori.

1.2) Calcolare la chiave condivisa K utilizzando la formula più conveniente fra quella usata da Alice e quella usata da Bob.

Esercizio 2

Il server web di Alice dispone di un sistema di login basato su username e password; per comodità, assumiamo che le password siano stringhe di bit.
Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile: si assuma che utilizzi una stringa casuale di 64 bit.
Il server applica alle password degli utenti una funzione hash crittografica H che genera un valore a 32 bit. In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 32 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.

Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H, ma che sappia che Bob utilizza una password di 64 bit. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login verso il server ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password, portandola a 128 bit casuali.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash in locale (nel computer di Charlie) richieda un miliardesimo di secondo.
Le risposte alle domande 2.1 e 2.2 cambiano?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Quale delle seguenti proprietà è necessaria affinché una funzione hash sia crittograficamente sicura?
   (a) La suriettività.
   (b) La resistenza agli attacchi di preimmagine e di collisione.
   (c) L'iniettività.
2. Quale delle seguenti proprietà **non** è posseduta da nessuna funzione hash crittografica?
   (a) L'iniettività.
   (b) La suriettività.
   (c) La resistenza agli attacchi di preimmagine e di collisione.
3. Quale delle seguenti proprietà è necessaria per una funzione di cifratura?
   (a) La suriettività.
   (b) L'iniettività.
   (c) La resistenza agli attacchi di preimmagine e di collisione.
4. Un certificato di firma digitale solitamente accompagna...
   (a) ... una chiave di sessione, e ne garantisce l'autenticità.
   (b) ... una chiave pubblica, e garantisce l'identità del possessore della corrispondente chiave privata.
   (c) ... una chiave privata, e garantisce l'identità del possessore della corrispondente chiave pubblica.
5. Quale, tra i seguenti, è un possibile problema del protocollo Diffie-Hellman?
   (a) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (b) La possibilità di un attacco Man-in-the-Middle.
   (c) La lentezza in rapporto ai cifrari a chiave condivisa.
6. Quale, tra i seguenti, è un possibile problema del cifrario RSA?
   (a) La lentezza in rapporto ai cifrari a chiave condivisa.
   (b) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (c) La possibilità di un attacco Man-in-the-Middle.
7. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (b) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (c) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
8. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave pubblica del richiedente.
   (b) Il common name del richiedente.
   (c) La chiave privata del richiedente.
9. Alice e Bob avviano una sessione Diffie-Hellman; per decifrare la chiave di sessione, Charlie (in ascolto sul canale ma non in grado di interferire) deve...
   (a) ... trovare una collisione in un valore hash crittografico.
   (b) ... risolvere un problema di logaritmo discreto.
   (c) ... fattorizzare un grande prodotto di numeri primi.
10. Quale proprietà caratterizza i cifrari a flusso?
    (a) Non richiedono che gli interlocutori abbiano concordato e condiviso una chiave.
    (b) Combinano i dati da cifrare con un flusso potenzialmente infinito di dati (pseudo-) casuali.
    (c) Sono necessariamente interattivi.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Tema 14

Lunedì 4 giugno 2018

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 13$ e sul generatore $g = 6$.

1.1) Supponendo che Alice scelga il valore segreto $a = 10$ e Bob il valore $b = 5$, descrivere lo scambio di informazioni che avviene fra i due interlocutori.

1.2) Calcolare la chiave condivisa K utilizzando la formula più conveniente fra quella usata da Alice e quella usata da Bob.

Esercizio 2

Il server web di Alice dispone di un sistema di login basato su username e password; per comodità, assumiamo che le password siano stringhe di bit.
Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile: si assuma che utilizzi una stringa casuale di 64 bit.
Il server applica alle password degli utenti una funzione hash crittografica H che genera un valore a 30 bit. In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 30 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.

Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H, ma che sappia che Bob utilizza una password di 64 bit. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login verso il server ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password, portandola a 128 bit casuali.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash in locale (nel computer di Charlie) richieda un miliardesimo di secondo.
Le risposte alle domande 2.1 e 2.2 cambiano?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (b) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (c) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
2. Quale delle seguenti proprietà è necessaria affinché una funzione hash sia crittograficamente sicura?
   (a) La resistenza agli attacchi di preimmagine e di collisione.
   (b) La suriettività.
   (c) L'iniettività.
3. Un certificato di firma digitale solitamente accompagna...
   (a) ...una chiave pubblica, e garantisce l'identità del possessore della corrispondente chiave privata.
   (b) ...una chiave privata, e garantisce l'identità del possessore della corrispondente chiave pubblica.
   (c) ...una chiave di sessione, e ne garantisce l'autenticità.
4. Quale, tra i seguenti, è un possibile problema del cifrario RSA?
   (a) La possibilità di un attacco Man-in-the-Middle.
   (b) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (c) La lentezza in rapporto ai cifrari a chiave condivisa.
5. Quale delle seguenti proprietà **non** è posseduta da nessuna funzione hash crittografica?
   (a) La resistenza agli attacchi di preimmagine e di collisione.
   (b) La suriettività.
   (c) L'iniettività.
6. Alice e Bob avviano una sessione Diffie-Hellman; per decifrare la chiave di sessione, Charlie (in ascolto sul canale ma non in grado di interferire) deve...
   (a) ...trovare una collisione in un valore hash crittografico.
   (b) ...fattorizzare un grande prodotto di numeri primi.
   (c) ...risolvere un problema di logaritmo discreto.
7. Quale, tra i seguenti, è un possibile problema del protocollo Diffie-Hellman?
   (a) La possibilità di un attacco Man-in-the-Middle.
   (b) La lentezza in rapporto ai cifrari a chiave condivisa.
   (c) La difficoltà di trovare numeri primi di dimensioni sufficienti.
8. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave pubblica del richiedente.
   (b) Il common name del richiedente.
   (c) La chiave privata del richiedente.
9. Quale proprietà caratterizza i cifrari a flusso?
   (a) Non richiedono che gli interlocutori abbiano concordato e condiviso una chiave.
   (b) Sono necessariamente interattivi.
   (c) Combinano i dati da cifrare con un flusso potenzialmente infinito di dati (pseudo-) casuali.
10. Quale delle seguenti proprietà è necessaria per una funzione di cifratura?
    (a) L'iniettività.
    (b) La resistenza agli attacchi di preimmagine e di collisione.
    (c) La suriettività.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Tema 15

Lunedì 4 giugno 2018

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 11$ e sul generatore $g = 6$.

1.1) Supponendo che Alice scelga il valore segreto $a = 8$ e Bob il valore $b = 4$, descrivere lo scambio di informazioni che avviene fra i due interlocutori.

1.2) Calcolare la chiave condivisa K utilizzando la formula più conveniente fra quella usata da Alice e quella usata da Bob.

Esercizio 2

Il server web di Alice dispone di un sistema di login basato su username e password; per comodità, assumiamo che le password siano stringhe di bit.
Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile: si assuma che utilizzi una stringa casuale di 64 bit.
Il server applica alle password degli utenti una funzione hash crittografica H che genera un valore a 32 bit. In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 32 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.

Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H, ma che sappia che Bob utilizza una password di 64 bit. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login verso il server ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password, portandola a 128 bit casuali.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash in locale (nel computer di Charlie) richieda un miliardesimo di secondo.
Le risposte alle domande 2.1 e 2.2 cambiano?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (b) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (c) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
2. Quale delle seguenti proprietà è necessaria affinché una funzione hash sia crittograficamente sicura?
   (a) La resistenza agli attacchi di preimmagine e di collisione.
   (b) L'iniettività.
   (c) La suriettività.
3. Quale, tra i seguenti, è un possibile problema del protocollo Diffie-Hellman?
   (a) La possibilità di un attacco Man-in-the-Middle.
   (b) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (c) La lentezza in rapporto ai cifrari a chiave condivisa.
4. Quale, tra i seguenti, è un possibile problema del cifrario RSA?
   (a) La possibilità di un attacco Man-in-the-Middle.
   (b) La lentezza in rapporto ai cifrari a chiave condivisa.
   (c) La difficoltà di trovare numeri primi di dimensioni sufficienti.
5. Quale delle seguenti proprietà è necessaria per una funzione di cifratura?
   (a) L'iniettività.
   (b) La suriettività.
   (c) La resistenza agli attacchi di preimmagine e di collisione.
6. Alice e Bob avviano una sessione Diffie-Hellman; per decifrare la chiave di sessione, Charlie (in ascolto sul canale ma non in grado di interferire) deve...
   (a) ...fattorizzare un grande prodotto di numeri primi.
   (b) ...risolvere un problema di logaritmo discreto.
   (c) ...trovare una collisione in un valore hash crittografico.
7. Un certificato di firma digitale solitamente accompagna...
   (a) ...una chiave pubblica, e garantisce l'identità del possessore della corrispondente chiave privata.
   (b) ...una chiave di sessione, e ne garantisce l'autenticità.
   (c) ...una chiave privata, e garantisce l'identità del possessore della corrispondente chiave pubblica.
8. Quale delle seguenti proprietà **non** è posseduta da nessuna funzione hash crittografica?
   (a) L'iniettività.
   (b) La suriettività.
   (c) La resistenza agli attacchi di preimmagine e di collisione.
9. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave privata del richiedente.
   (b) Il common name del richiedente.
   (c) La chiave pubblica del richiedente.
10. Quale proprietà caratterizza i cifrari a flusso?
    (a) Combinano i dati da cifrare con un flusso potenzialmente infinito di dati (pseudo-) casuali.
    (b) Non richiedono che gli interlocutori abbiano concordato e condiviso una chiave.
    (c) Sono necessariamente interattivi.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Tema 16

Lunedì 4 giugno 2018

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 11$ e sul generatore $g = 7$.

1.1) Supponendo che Alice scelga il valore segreto $a = 9$ e Bob il valore $b = 4$, descrivere lo scambio di informazioni che avviene fra i due interlocutori.

1.2) Calcolare la chiave condivisa K utilizzando la formula più conveniente fra quella usata da Alice e quella usata da Bob.

Esercizio 2

Il server web di Alice dispone di un sistema di login basato su username e password; per comodità, assumiamo che le password siano stringhe di bit.
Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile: si assuma che utilizzi una stringa casuale di 64 bit.
Il server applica alle password degli utenti una funzione hash crittografica H che genera un valore a 30 bit. In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 30 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.

Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H, ma che sappia che Bob utilizza una password di 64 bit. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login verso il server ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password, portandola a 128 bit casuali.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash in locale (nel computer di Charlie) richieda un miliardesimo di secondo.
Le risposte alle domande 2.1 e 2.2 cambiano?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (b) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (c) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
2. Quale delle seguenti proprietà è necessaria affinché una funzione hash sia crittograficamente sicura?
   (a) La resistenza agli attacchi di preimmagine e di collisione.
   (b) La suriettività.
   (c) L'iniettività.
3. Quale, tra i seguenti, è un possibile problema del protocollo Diffie-Hellman?
   (a) La possibilità di un attacco Man-in-the-Middle.
   (b) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (c) La lentezza in rapporto ai cifrari a chiave condivisa.
4. Alice e Bob avviano una sessione Diffie-Hellman; per decifrare la chiave di sessione, Charlie (in ascolto sul canale ma non in grado di interferire) deve...
   (a) ...trovare una collisione in un valore hash crittografico.
   (b) ...risolvere un problema di logaritmo discreto.
   (c) ...fattorizzare un grande prodotto di numeri primi.
5. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) Il common name del richiedente.
   (b) La chiave privata del richiedente.
   (c) La chiave pubblica del richiedente.
6. Quale, tra i seguenti, è un possibile problema del cifrario RSA?
   (a) La lentezza in rapporto ai cifrari a chiave condivisa.
   (b) La possibilità di un attacco Man-in-the-Middle.
   (c) La difficoltà di trovare numeri primi di dimensioni sufficienti.
7. Un certificato di firma digitale solitamente accompagna...
   (a) ...una chiave pubblica, e garantisce l'identità del possessore della corrispondente chiave privata.
   (b) ...una chiave privata, e garantisce l'identità del possessore della corrispondente chiave pubblica.
   (c) ...una chiave di sessione, e ne garantisce l'autenticità.
8. Quale delle seguenti proprietà è necessaria per una funzione di cifratura?
   (a) La suriettività.
   (b) La resistenza agli attacchi di preimmagine e di collisione.
   (c) L'iniettività.
9. Quale proprietà caratterizza i cifrari a flusso?
   (a) Sono necessariamente interattivi.
   (b) Combinano i dati da cifrare con un flusso potenzialmente infinito di dati (pseudo-) casuali.
   (c) Non richiedono che gli interlocutori abbiano concordato e condiviso una chiave.
10. Quale delle seguenti proprietà **non** è posseduta da nessuna funzione hash crittografica?
    (a) La suriettività.
    (b) L'iniettività.
    (c) La resistenza agli attacchi di preimmagine e di collisione.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Tema 17

Lunedì 4 giugno 2018

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 13$ e sul generatore $g = 6$.

1.1) Supponendo che Alice scelga il valore segreto $a = 10$ e Bob il valore $b = 2$, descrivere lo scambio di informazioni che avviene fra i due interlocutori.

1.2) Calcolare la chiave condivisa K utilizzando la formula più conveniente fra quella usata da Alice e quella usata da Bob.

Esercizio 2

Il server web di Alice dispone di un sistema di login basato su username e password; per comodità, assumiamo che le password siano stringhe di bit.
Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile: si assuma che utilizzi una stringa casuale di 64 bit.
Il server applica alle password degli utenti una funzione hash crittografica H che genera un valore a 28 bit. In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 28 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.

Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H, ma che sappia che Bob utilizza una password di 64 bit. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login verso il server ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password, portandola a 128 bit casuali.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash in locale (nel computer di Charlie) richieda un miliardesimo di secondo.
Le risposte alle domande 2.1 e 2.2 cambiano?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Quale proprietà caratterizza i cifrari a flusso?
   (a) Non richiedono che gli interlocutori abbiano concordato e condiviso una chiave.
   (b) Combinano i dati da cifrare con un flusso potenzialmente infinito di dati (pseudo-) casuali.
   (c) Sono necessariamente interattivi.
2. Quale delle seguenti proprietà **non** è posseduta da nessuna funzione hash crittografica?
   (a) La resistenza agli attacchi di preimmagine e di collisione.
   (b) La suriettività.
   (c) L'iniettività.
3. Un certificato di firma digitale solitamente accompagna...
   (a) ...una chiave di sessione, e ne garantisce l'autenticità.
   (b) ...una chiave pubblica, e garantisce l'identità del possessore della corrispondente chiave privata.
   (c) ...una chiave privata, e garantisce l'identità del possessore della corrispondente chiave pubblica.
4. Quale delle seguenti proprietà è necessaria affinché una funzione hash sia crittograficamente sicura?
   (a) La suriettività.
   (b) L'iniettività.
   (c) La resistenza agli attacchi di preimmagine e di collisione.
5. Quale, tra i seguenti, è un possibile problema del protocollo Diffie-Hellman?
   (a) La possibilità di un attacco Man-in-the-Middle.
   (b) La lentezza in rapporto ai cifrari a chiave condivisa.
   (c) La difficoltà di trovare numeri primi di dimensioni sufficienti.
6. Quale delle seguenti proprietà è necessaria per una funzione di cifratura?
   (a) La resistenza agli attacchi di preimmagine e di collisione.
   (b) L'iniettività.
   (c) La suriettività.
7. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (b) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (c) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
8. Alice e Bob avviano una sessione Diffie-Hellman; per decifrare la chiave di sessione, Charlie (in ascolto sul canale ma non in grado di interferire) deve...
   (a) ...risolvere un problema di logaritmo discreto.
   (b) ...fattorizzare un grande prodotto di numeri primi.
   (c) ...trovare una collisione in un valore hash crittografico.
9. Quale, tra i seguenti, è un possibile problema del cifrario RSA?
   (a) La possibilità di un attacco Man-in-the-Middle.
   (b) La lentezza in rapporto ai cifrari a chiave condivisa.
   (c) La difficoltà di trovare numeri primi di dimensioni sufficienti.
10. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
    (a) Il common name del richiedente.
    (b) La chiave privata del richiedente.
    (c) La chiave pubblica del richiedente.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Tema 18

Lunedì 4 giugno 2018

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 11$ e sul generatore $g = 8$.

1.1) Supponendo che Alice scelga il valore segreto $a = 7$ e Bob il valore $b = 3$, descrivere lo scambio di informazioni che avviene fra i due interlocutori.

1.2) Calcolare la chiave condivisa K utilizzando la formula più conveniente fra quella usata da Alice e quella usata da Bob.

Esercizio 2

Il server web di Alice dispone di un sistema di login basato su username e password; per comodità, assumiamo che le password siano stringhe di bit.
Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile: si assuma che utilizzi una stringa casuale di 64 bit.
Il server applica alle password degli utenti una funzione hash crittografica H che genera un valore a 30 bit. In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 30 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.

Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H, ma che sappia che Bob utilizza una password di 64 bit. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login verso il server ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password, portandola a 128 bit casuali.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash in locale (nel computer di Charlie) richieda un miliardesimo di secondo.
Le risposte alle domande 2.1 e 2.2 cambiano?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Alice e Bob avviano una sessione Diffie-Hellman; per decifrare la chiave di sessione, Charlie (in ascolto sul canale ma non in grado di interferire) deve...
   (a) ...trovare una collisione in un valore hash crittografico.
   (b) ...risolvere un problema di logaritmo discreto.
   (c) ...fattorizzare un grande prodotto di numeri primi.
2. Quale delle seguenti proprietà è necessaria affinché una funzione hash sia crittograficamente sicura?
   (a) La suriettività.
   (b) La resistenza agli attacchi di preimmagine e di collisione.
   (c) L'iniettività.
3. Quale, tra i seguenti, è un possibile problema del cifrario RSA?
   (a) La lentezza in rapporto ai cifrari a chiave condivisa.
   (b) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (c) La possibilità di un attacco Man-in-the-Middle.
4. Quale, tra i seguenti, è un possibile problema del protocollo Diffie-Hellman?
   (a) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (b) La lentezza in rapporto ai cifrari a chiave condivisa.
   (c) La possibilità di un attacco Man-in-the-Middle.
5. Un certificato di firma digitale solitamente accompagna...
   (a) ...una chiave privata, e garantisce l'identità del possessore della corrispondente chiave pubblica.
   (b) ...una chiave pubblica, e garantisce l'identità del possessore della corrispondente chiave privata.
   (c) ...una chiave di sessione, e ne garantisce l'autenticità.
6. Quale proprietà caratterizza i cifrari a flusso?
   (a) Sono necessariamente interattivi.
   (b) Combinano i dati da cifrare con un flusso potenzialmente infinito di dati (pseudo-) casuali.
   (c) Non richiedono che gli interlocutori abbiano concordato e condiviso una chiave.
7. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (b) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (c) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
8. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave privata del richiedente.
   (b) La chiave pubblica del richiedente.
   (c) Il common name del richiedente.
9. Quale delle seguenti proprietà è necessaria per una funzione di cifratura?
   (a) La resistenza agli attacchi di preimmagine e di collisione.
   (b) La suriettività.
   (c) L'iniettività.
10. Quale delle seguenti proprietà **non** è posseduta da nessuna funzione hash crittografica?
    (a) La resistenza agli attacchi di preimmagine e di collisione.
    (b) L'iniettività.
    (c) La suriettività.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Tema 19

Lunedì 4 giugno 2018

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 11$ e sul generatore $g = 6$.

1.1) Supponendo che Alice scelga il valore segreto $a = 8$ e Bob il valore $b = 2$, descrivere lo scambio di informazioni che avviene fra i due interlocutori.

1.2) Calcolare la chiave condivisa K utilizzando la formula più conveniente fra quella usata da Alice e quella usata da Bob.

Esercizio 2

Il server web di Alice dispone di un sistema di login basato su username e password; per comodità, assumiamo che le password siano stringhe di bit.
Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile: si assuma che utilizzi una stringa casuale di 64 bit.
Il server applica alle password degli utenti una funzione hash crittografica H che genera un valore a 32 bit. In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 32 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.

Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H, ma che sappia che Bob utilizza una password di 64 bit. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login verso il server ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password, portandola a 128 bit casuali.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash in locale (nel computer di Charlie) richieda un miliardesimo di secondo.
Le risposte alle domande 2.1 e 2.2 cambiano?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Alice e Bob avviano una sessione Diffie-Hellman; per decifrare la chiave di sessione, Charlie (in ascolto sul canale ma non in grado di interferire) deve...
   (a) ...fattorizzare un grande prodotto di numeri primi.
   (b) ...risolvere un problema di logaritmo discreto.
   (c) ...trovare una collisione in un valore hash crittografico.
2. Quale, tra i seguenti, è un possibile problema del cifrario RSA?
   (a) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (b) La possibilità di un attacco Man-in-the-Middle.
   (c) La lentezza in rapporto ai cifrari a chiave condivisa.
3. Quale, tra i seguenti, è un possibile problema del protocollo Diffie-Hellman?
   (a) La possibilità di un attacco Man-in-the-Middle.
   (b) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (c) La lentezza in rapporto ai cifrari a chiave condivisa.
4. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (b) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (c) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
5. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) Il common name del richiedente.
   (b) La chiave pubblica del richiedente.
   (c) La chiave privata del richiedente.
6. Un certificato di firma digitale solitamente accompagna...
   (a) ...una chiave di sessione, e ne garantisce l'autenticità.
   (b) ...una chiave privata, e garantisce l'identità del possessore della corrispondente chiave pubblica.
   (c) ...una chiave pubblica, e garantisce l'identità del possessore della corrispondente chiave privata.
7. Quale delle seguenti proprietà è necessaria per una funzione di cifratura?
   (a) L'iniettività.
   (b) La resistenza agli attacchi di preimmagine e di collisione.
   (c) La suriettività.
8. Quale delle seguenti proprietà **non** è posseduta da nessuna funzione hash crittografica?
   (a) La suriettività.
   (b) L'iniettività.
   (c) La resistenza agli attacchi di preimmagine e di collisione.
9. Quale delle seguenti proprietà è necessaria affinché una funzione hash sia crittograficamente sicura?
   (a) L'iniettività.
   (b) La suriettività.
   (c) La resistenza agli attacchi di preimmagine e di collisione.
10. Quale proprietà caratterizza i cifrari a flusso?
    (a) Sono necessariamente interattivi.
    (b) Non richiedono che gli interlocutori abbiano concordato e condiviso una chiave.
    (c) Combinano i dati da cifrare con un flusso potenzialmente infinito di dati (pseudo-) casuali.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Tema 20

Lunedì 4 giugno 2018

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 11$ e sul generatore $g = 6$.

1.1) Supponendo che Alice scelga il valore segreto $a = 7$ e Bob il valore $b = 2$, descrivere lo scambio di informazioni che avviene fra i due interlocutori.

1.2) Calcolare la chiave condivisa K utilizzando la formula più conveniente fra quella usata da Alice e quella usata da Bob.

Esercizio 2

Il server web di Alice dispone di un sistema di login basato su username e password; per comodità, assumiamo che le password siano stringhe di bit.
Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile: si assuma che utilizzi una stringa casuale di 64 bit.
Il server applica alle password degli utenti una funzione hash crittografica H che genera un valore a 32 bit. In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 32 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.

Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H, ma che sappia che Bob utilizza una password di 64 bit. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login verso il server ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password, portandola a 128 bit casuali.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash in locale (nel computer di Charlie) richieda un miliardesimo di secondo.
Le risposte alle domande 2.1 e 2.2 cambiano?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) Il common name del richiedente.
   (b) La chiave privata del richiedente.
   (c) La chiave pubblica del richiedente.
2. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (b) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (c) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
3. Quale delle seguenti proprietà è necessaria per una funzione di cifratura?
   (a) La resistenza agli attacchi di preimmagine e di collisione.
   (b) La suriettività.
   (c) L'iniettività.
4. Quale delle seguenti proprietà **non** è posseduta da nessuna funzione hash crittografica?
   (a) La resistenza agli attacchi di preimmagine e di collisione.
   (b) L'iniettività.
   (c) La suriettività.
5. Quale, tra i seguenti, è un possibile problema del protocollo Diffie-Hellman?
   (a) La lentezza in rapporto ai cifrari a chiave condivisa.
   (b) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (c) La possibilità di un attacco Man-in-the-Middle.
6. Quale proprietà caratterizza i cifrari a flusso?
   (a) Combinano i dati da cifrare con un flusso potenzialmente infinito di dati (pseudo-) casuali.
   (b) Non richiedono che gli interlocutori abbiano concordato e condiviso una chiave.
   (c) Sono necessariamente interattivi.
7. Quale, tra i seguenti, è un possibile problema del cifrario RSA?
   (a) La lentezza in rapporto ai cifrari a chiave condivisa.
   (b) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (c) La possibilità di un attacco Man-in-the-Middle.
8. Quale delle seguenti proprietà è necessaria affinché una funzione hash sia crittograficamente sicura?
   (a) La suriettività.
   (b) L'iniettività.
   (c) La resistenza agli attacchi di preimmagine e di collisione.
9. Un certificato di firma digitale solitamente accompagna...
   (a) ...una chiave di sessione, e ne garantisce l'autenticità.
   (b) ...una chiave privata, e garantisce l'identità del possessore della corrispondente chiave pubblica.
   (c) ...una chiave pubblica, e garantisce l'identità del possessore della corrispondente chiave privata.
10. Alice e Bob avviano una sessione Diffie-Hellman; per decifrare la chiave di sessione, Charlie (in ascolto sul canale ma non in grado di interferire) deve...
    (a) ...fattorizzare un grande prodotto di numeri primi.
    (b) ...risolvere un problema di logaritmo discreto.
    (c) ...trovare una collisione in un valore hash crittografico.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Tema 21

Lunedì 4 giugno 2018

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 13$ e sul generatore $g = 7$.

1.1) Supponendo che Alice scelga il valore segreto $a = 10$ e Bob il valore $b = 3$, descrivere lo scambio di informazioni che avviene fra i due interlocutori.

1.2) Calcolare la chiave condivisa K utilizzando la formula più conveniente fra quella usata da Alice e quella usata da Bob.

Esercizio 2

Il server web di Alice dispone di un sistema di login basato su username e password; per comodità, assumiamo che le password siano stringhe di bit.
Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile: si assuma che utilizzi una stringa casuale di 64 bit.
Il server applica alle password degli utenti una funzione hash crittografica H che genera un valore a 24 bit. In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 24 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.

Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H, ma che sappia che Bob utilizza una password di 64 bit. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login verso il server ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password, portandola a 128 bit casuali.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash in locale (nel computer di Charlie) richieda un miliardesimo di secondo.
Le risposte alle domande 2.1 e 2.2 cambiano?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) Il common name del richiedente.
   (b) La chiave pubblica del richiedente.
   (c) La chiave privata del richiedente.
2. Quale proprietà caratterizza i cifrari a flusso?
   (a) Non richiedono che gli interlocutori abbiano concordato e condiviso una chiave.
   (b) Sono necessariamente interattivi.
   (c) Combinano i dati da cifrare con un flusso potenzialmente infinito di dati (pseudo-) casuali.
3. Alice e Bob avviano una sessione Diffie-Hellman; per decifrare la chiave di sessione, Charlie (in ascolto sul canale ma non in grado di interferire) deve...
   (a) ...fattorizzare un grande prodotto di numeri primi.
   (b) ...trovare una collisione in un valore hash crittografico.
   (c) ...risolvere un problema di logaritmo discreto.
4. Quale, tra i seguenti, è un possibile problema del cifrario RSA?
   (a) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (b) La possibilità di un attacco Man-in-the-Middle.
   (c) La lentezza in rapporto ai cifrari a chiave condivisa.
5. Un certificato di firma digitale solitamente accompagna...
   (a) ...una chiave di sessione, e ne garantisce l'autenticità.
   (b) ...una chiave privata, e garantisce l'identità del possessore della corrispondente chiave pubblica.
   (c) ...una chiave pubblica, e garantisce l'identità del possessore della corrispondente chiave privata.
6. Quale delle seguenti proprietà è necessaria per una funzione di cifratura?
   (a) La suriettività.
   (b) L'iniettività.
   (c) La resistenza agli attacchi di preimmagine e di collisione.
7. Quale, tra i seguenti, è un possibile problema del protocollo Diffie-Hellman?
   (a) La lentezza in rapporto ai cifrari a chiave condivisa.
   (b) La possibilità di un attacco Man-in-the-Middle.
   (c) La difficoltà di trovare numeri primi di dimensioni sufficienti.
8. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (b) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (c) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
9. Quale delle seguenti proprietà è necessaria affinché una funzione hash sia crittograficamente sicura?
   (a) La suriettività.
   (b) L'iniettività.
   (c) La resistenza agli attacchi di preimmagine e di collisione.
10. Quale delle seguenti proprietà **non** è posseduta da nessuna funzione hash crittografica?
    (a) L'iniettività.
    (b) La resistenza agli attacchi di preimmagine e di collisione.
    (c) La suriettività.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Tema 22

Lunedì 4 giugno 2018

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 13$ e sul generatore $g = 7$.

1.1) Supponendo che Alice scelga il valore segreto $a = 10$ e Bob il valore $b = 4$, descrivere lo scambio di informazioni che avviene fra i due interlocutori.

1.2) Calcolare la chiave condivisa K utilizzando la formula più conveniente fra quella usata da Alice e quella usata da Bob.

Esercizio 2

Il server web di Alice dispone di un sistema di login basato su username e password; per comodità, assumiamo che le password siano stringhe di bit.
Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile: si assuma che utilizzi una stringa casuale di 64 bit.
Il server applica alle password degli utenti una funzione hash crittografica H che genera un valore a 30 bit. In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 30 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.

Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H, ma che sappia che Bob utilizza una password di 64 bit. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login verso il server ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password, portandola a 128 bit casuali.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash in locale (nel computer di Charlie) richieda un miliardesimo di secondo.
Le risposte alle domande 2.1 e 2.2 cambiano?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Quale delle seguenti proprietà è necessaria per una funzione di cifratura?
   (a) La resistenza agli attacchi di preimmagine e di collisione.
   (b) L'iniettività.
   (c) La suriettività.
2. Quale proprietà caratterizza i cifrari a flusso?
   (a) Combinano i dati da cifrare con un flusso potenzialmente infinito di dati (pseudo-) casuali.
   (b) Non richiedono che gli interlocutori abbiano concordato e condiviso una chiave.
   (c) Sono necessariamente interattivi.
3. Quale delle seguenti proprietà **non** è posseduta da nessuna funzione hash crittografica?
   (a) La resistenza agli attacchi di preimmagine e di collisione.
   (b) L'iniettività.
   (c) La suriettività.
4. Un certificato di firma digitale solitamente accompagna...
   (a) ...una chiave privata, e garantisce l'identità del possessore della corrispondente chiave pubblica.
   (b) ...una chiave pubblica, e garantisce l'identità del possessore della corrispondente chiave privata.
   (c) ...una chiave di sessione, e ne garantisce l'autenticità.
5. Quale, tra i seguenti, è un possibile problema del protocollo Diffie-Hellman?
   (a) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (b) La lentezza in rapporto ai cifrari a chiave condivisa.
   (c) La possibilità di un attacco Man-in-the-Middle.
6. Alice e Bob avviano una sessione Diffie-Hellman; per decifrare la chiave di sessione, Charlie (in ascolto sul canale ma non in grado di interferire) deve...
   (a) ...trovare una collisione in un valore hash crittografico.
   (b) ...fattorizzare un grande prodotto di numeri primi.
   (c) ...risolvere un problema di logaritmo discreto.
7. Quale, tra i seguenti, è un possibile problema del cifrario RSA?
   (a) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (b) La possibilità di un attacco Man-in-the-Middle.
   (c) La lentezza in rapporto ai cifrari a chiave condivisa.
8. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (b) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (c) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
9. Quale delle seguenti proprietà è necessaria affinché una funzione hash sia crittograficamente sicura?
   (a) La suriettività.
   (b) L'iniettività.
   (c) La resistenza agli attacchi di preimmagine e di collisione.
10. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
    (a) La chiave privata del richiedente.
    (b) Il common name del richiedente.
    (c) La chiave pubblica del richiedente.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Tema 23

Lunedì 4 giugno 2018

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 11$ e sul generatore $g = 7$.

1.1) Supponendo che Alice scelga il valore segreto $a = 8$ e Bob il valore $b = 4$, descrivere lo scambio di informazioni che avviene fra i due interlocutori.

1.2) Calcolare la chiave condivisa K utilizzando la formula più conveniente fra quella usata da Alice e quella usata da Bob.

Esercizio 2

Il server web di Alice dispone di un sistema di login basato su username e password; per comodità, assumiamo che le password siano stringhe di bit.
Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile: si assuma che utilizzi una stringa casuale di 64 bit.
Il server applica alle password degli utenti una funzione hash crittografica H che genera un valore a 32 bit. In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 32 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.

Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H, ma che sappia che Bob utilizza una password di 64 bit. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login verso il server ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password, portandola a 128 bit casuali.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash in locale (nel computer di Charlie) richieda un miliardesimo di secondo.
Le risposte alle domande 2.1 e 2.2 cambiano?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Quale delle seguenti proprietà è necessaria per una funzione di cifratura?
   (a) L'iniettività.
   (b) La suriettività.
   (c) La resistenza agli attacchi di preimmagine e di collisione.
2. Quale, tra i seguenti, è un possibile problema del cifrario RSA?
   (a) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (b) La lentezza in rapporto ai cifrari a chiave condivisa.
   (c) La possibilità di un attacco Man-in-the-Middle.
3. Un certificato di firma digitale solitamente accompagna...
   (a) ...una chiave privata, e garantisce l'identità del possessore della corrispondente chiave pubblica.
   (b) ...una chiave di sessione, e ne garantisce l'autenticità.
   (c) ...una chiave pubblica, e garantisce l'identità del possessore della corrispondente chiave privata.
4. Quale, tra i seguenti, è un possibile problema del protocollo Diffie-Hellman?
   (a) La possibilità di un attacco Man-in-the-Middle.
   (b) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (c) La lentezza in rapporto ai cifrari a chiave condivisa.
5. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (b) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (c) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
6. Alice e Bob avviano una sessione Diffie-Hellman; per decifrare la chiave di sessione, Charlie (in ascolto sul canale ma non in grado di interferire) deve...
   (a) ...trovare una collisione in un valore hash crittografico.
   (b) ...fattorizzare un grande prodotto di numeri primi.
   (c) ...risolvere un problema di logaritmo discreto.
7. Quale delle seguenti proprietà **non** è posseduta da nessuna funzione hash crittografica?
   (a) La resistenza agli attacchi di preimmagine e di collisione.
   (b) L'iniettività.
   (c) La suriettività.
8. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave privata del richiedente.
   (b) La chiave pubblica del richiedente.
   (c) Il common name del richiedente.
9. Quale proprietà caratterizza i cifrari a flusso?
   (a) Non richiedono che gli interlocutori abbiano concordato e condiviso una chiave.
   (b) Sono necessariamente interattivi.
   (c) Combinano i dati da cifrare con un flusso potenzialmente infinito di dati (pseudo-) casuali.
10. Quale delle seguenti proprietà è necessaria affinché una funzione hash sia crittograficamente sicura?
    (a) La resistenza agli attacchi di preimmagine e di collisione.
    (b) L'iniettività.
    (c) La suriettività.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Tema 24

Lunedì 4 giugno 2018

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 11$ e sul generatore $g = 6$.

1.1) Supponendo che Alice scelga il valore segreto $a = 8$ e Bob il valore $b = 4$, descrivere lo scambio di informazioni che avviene fra i due interlocutori.

1.2) Calcolare la chiave condivisa K utilizzando la formula più conveniente fra quella usata da Alice e quella usata da Bob.

Esercizio 2

Il server web di Alice dispone di un sistema di login basato su username e password; per comodità, assumiamo che le password siano stringhe di bit.
Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile: si assuma che utilizzi una stringa casuale di 64 bit.
Il server applica alle password degli utenti una funzione hash crittografica H che genera un valore a 30 bit. In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 30 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.

Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H, ma che sappia che Bob utilizza una password di 64 bit. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login verso il server ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password, portandola a 128 bit casuali.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash in locale (nel computer di Charlie) richieda un miliardesimo di secondo.
Le risposte alle domande 2.1 e 2.2 cambiano?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Quale, tra i seguenti, è un possibile problema del protocollo Diffie-Hellman?
   (a) La lentezza in rapporto ai cifrari a chiave condivisa.
   (b) La possibilità di un attacco Man-in-the-Middle.
   (c) La difficoltà di trovare numeri primi di dimensioni sufficienti.
2. Quale, tra i seguenti, è un possibile problema del cifrario RSA?
   (a) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (b) La possibilità di un attacco Man-in-the-Middle.
   (c) La lentezza in rapporto ai cifrari a chiave condivisa.
3. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave pubblica del richiedente.
   (b) La chiave privata del richiedente.
   (c) Il common name del richiedente.
4. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (b) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (c) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
5. Un certificato di firma digitale solitamente accompagna...
   (a) ...una chiave pubblica, e garantisce l'identità del possessore della corrispondente chiave privata.
   (b) ...una chiave di sessione, e ne garantisce l'autenticità.
   (c) ...una chiave privata, e garantisce l'identità del possessore della corrispondente chiave pubblica.
6. Quale delle seguenti proprietà è necessaria per una funzione di cifratura?
   (a) La resistenza agli attacchi di preimmagine e di collisione.
   (b) L'iniettività.
   (c) La suriettività.
7. Quale delle seguenti proprietà **non** è posseduta da nessuna funzione hash crittografica?
   (a) La resistenza agli attacchi di preimmagine e di collisione.
   (b) L'iniettività.
   (c) La suriettività.
8. Quale proprietà caratterizza i cifrari a flusso?
   (a) Sono necessariamente interattivi.
   (b) Combinano i dati da cifrare con un flusso potenzialmente infinito di dati (pseudo-) casuali.
   (c) Non richiedono che gli interlocutori abbiano concordato e condiviso una chiave.
9. Alice e Bob avviano una sessione Diffie-Hellman; per decifrare la chiave di sessione, Charlie (in ascolto sul canale ma non in grado di interferire) deve...
   (a) ...fattorizzare un grande prodotto di numeri primi.
   (b) ...trovare una collisione in un valore hash crittografico.
   (c) ...risolvere un problema di logaritmo discreto.
10. Quale delle seguenti proprietà è necessaria affinché una funzione hash sia crittograficamente sicura?
    (a) La suriettività.
    (b) L'iniettività.
    (c) La resistenza agli attacchi di preimmagine e di collisione.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Tema 25

Lunedì 4 giugno 2018

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 11$ e sul generatore $g = 6$.

1.1) Supponendo che Alice scelga il valore segreto $a = 9$ e Bob il valore $b = 4$, descrivere lo scambio di informazioni che avviene fra i due interlocutori.

1.2) Calcolare la chiave condivisa K utilizzando la formula più conveniente fra quella usata da Alice e quella usata da Bob.

Esercizio 2

Il server web di Alice dispone di un sistema di login basato su username e password; per comodità, assumiamo che le password siano stringhe di bit.
Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile: si assuma che utilizzi una stringa casuale di 64 bit.
Il server applica alle password degli utenti una funzione hash crittografica H che genera un valore a 26 bit. In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 26 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.

Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H, ma che sappia che Bob utilizza una password di 64 bit. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login verso il server ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password, portandola a 128 bit casuali.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash in locale (nel computer di Charlie) richieda un miliardesimo di secondo.
Le risposte alle domande 2.1 e 2.2 cambiano?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Quale delle seguenti proprietà **non** è posseduta da nessuna funzione hash crittografica?
   (a) La suriettività.
   (b) La resistenza agli attacchi di preimmagine e di collisione.
   (c) L'iniettività.
2. Quale, tra i seguenti, è un possibile problema del cifrario RSA?
   (a) La possibilità di un attacco Man-in-the-Middle.
   (b) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (c) La lentezza in rapporto ai cifrari a chiave condivisa.
3. Un certificato di firma digitale solitamente accompagna...
   (a) ...una chiave di sessione, e ne garantisce l'autenticità.
   (b) ...una chiave pubblica, e garantisce l'identità del possessore della corrispondente chiave privata.
   (c) ...una chiave privata, e garantisce l'identità del possessore della corrispondente chiave pubblica.
4. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (b) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (c) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
5. Alice e Bob avviano una sessione Diffie-Hellman; per decifrare la chiave di sessione, Charlie (in ascolto sul canale ma non in grado di interferire) deve...
   (a) ...trovare una collisione in un valore hash crittografico.
   (b) ...risolvere un problema di logaritmo discreto.
   (c) ...fattorizzare un grande prodotto di numeri primi.
6. Quale delle seguenti proprietà è necessaria per una funzione di cifratura?
   (a) L'iniettività.
   (b) La suriettività.
   (c) La resistenza agli attacchi di preimmagine e di collisione.
7. Quale delle seguenti proprietà è necessaria affinché una funzione hash sia crittograficamente sicura?
   (a) La resistenza agli attacchi di preimmagine e di collisione.
   (b) L'iniettività.
   (c) La suriettività.
8. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave pubblica del richiedente.
   (b) La chiave privata del richiedente.
   (c) Il common name del richiedente.
9. Quale, tra i seguenti, è un possibile problema del protocollo Diffie-Hellman?
   (a) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (b) La lentezza in rapporto ai cifrari a chiave condivisa.
   (c) La possibilità di un attacco Man-in-the-Middle.
10. Quale proprietà caratterizza i cifrari a flusso?
    (a) Sono necessariamente interattivi.
    (b) Non richiedono che gli interlocutori abbiano concordato e condiviso una chiave.
    (c) Combinano i dati da cifrare con un flusso potenzialmente infinito di dati (pseudo-) casuali.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Tema 26

Lunedì 4 giugno 2018

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 11$ e sul generatore $g = 6$.

1.1) Supponendo che Alice scelga il valore segreto $a = 8$ e Bob il valore $b = 4$, descrivere lo scambio di informazioni che avviene fra i due interlocutori.

1.2) Calcolare la chiave condivisa K utilizzando la formula più conveniente fra quella usata da Alice e quella usata da Bob.

Esercizio 2

Il server web di Alice dispone di un sistema di login basato su username e password; per comodità, assumiamo che le password siano stringhe di bit.
Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile: si assuma che utilizzi una stringa casuale di 64 bit.
Il server applica alle password degli utenti una funzione hash crittografica H che genera un valore a 30 bit. In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 30 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.

Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H, ma che sappia che Bob utilizza una password di 64 bit. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login verso il server ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password, portandola a 128 bit casuali.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash in locale (nel computer di Charlie) richieda un miliardesimo di secondo.
Le risposte alle domande 2.1 e 2.2 cambiano?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Un certificato di firma digitale solitamente accompagna...
   (a) ...una chiave di sessione, e ne garantisce l'autenticità.
   (b) ...una chiave pubblica, e garantisce l'identità del possessore della corrispondente chiave privata.
   (c) ...una chiave privata, e garantisce l'identità del possessore della corrispondente chiave pubblica.
2. Quale proprietà caratterizza i cifrari a flusso?
   (a) Non richiedono che gli interlocutori abbiano concordato e condiviso una chiave.
   (b) Combinano i dati da cifrare con un flusso potenzialmente infinito di dati (pseudo-) casuali.
   (c) Sono necessariamente interattivi.
3. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave privata del richiedente.
   (b) La chiave pubblica del richiedente.
   (c) Il common name del richiedente.
4. Alice e Bob avviano una sessione Diffie-Hellman; per decifrare la chiave di sessione, Charlie (in ascolto sul canale ma non in grado di interferire) deve...
   (a) ...risolvere un problema di logaritmo discreto.
   (b) ...fattorizzare un grande prodotto di numeri primi.
   (c) ...trovare una collisione in un valore hash crittografico.
5. Quale delle seguenti proprietà è necessaria per una funzione di cifratura?
   (a) L'iniettività.
   (b) La suriettività.
   (c) La resistenza agli attacchi di preimmagine e di collisione.
6. Quale delle seguenti proprietà è necessaria affinché una funzione hash sia crittograficamente sicura?
   (a) La resistenza agli attacchi di preimmagine e di collisione.
   (b) La suriettività.
   (c) L'iniettività.
7. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (b) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (c) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
8. Quale, tra i seguenti, è un possibile problema del cifrario RSA?
   (a) La possibilità di un attacco Man-in-the-Middle.
   (b) La lentezza in rapporto ai cifrari a chiave condivisa.
   (c) La difficoltà di trovare numeri primi di dimensioni sufficienti.
9. Quale, tra i seguenti, è un possibile problema del protocollo Diffie-Hellman?
   (a) La possibilità di un attacco Man-in-the-Middle.
   (b) La lentezza in rapporto ai cifrari a chiave condivisa.
   (c) La difficoltà di trovare numeri primi di dimensioni sufficienti.
10. Quale delle seguenti proprietà **non** è posseduta da nessuna funzione hash crittografica?
    (a) La suriettività.
    (b) La resistenza agli attacchi di preimmagine e di collisione.
    (c) L'iniettività.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Tema 27

Lunedì 4 giugno 2018

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 11$ e sul generatore $g = 6$.

1.1) Supponendo che Alice scelga il valore segreto $a = 9$ e Bob il valore $b = 5$, descrivere lo scambio di informazioni che avviene fra i due interlocutori.

1.2) Calcolare la chiave condivisa K utilizzando la formula più conveniente fra quella usata da Alice e quella usata da Bob.

Esercizio 2

Il server web di Alice dispone di un sistema di login basato su username e password; per comodità, assumiamo che le password siano stringhe di bit.
Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile: si assuma che utilizzi una stringa casuale di 64 bit.
Il server applica alle password degli utenti una funzione hash crittografica H che genera un valore a 30 bit. In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 30 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.

Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H, ma che sappia che Bob utilizza una password di 64 bit. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login verso il server ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password, portandola a 128 bit casuali.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash in locale (nel computer di Charlie) richieda un miliardesimo di secondo.
Le risposte alle domande 2.1 e 2.2 cambiano?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Quale, tra i seguenti, è un possibile problema del cifrario RSA?
   (a) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (b) La possibilità di un attacco Man-in-the-Middle.
   (c) La lentezza in rapporto ai cifrari a chiave condivisa.
2. Quale delle seguenti proprietà **non** è posseduta da nessuna funzione hash crittografica?
   (a) La suriettività.
   (b) L'iniettività.
   (c) La resistenza agli attacchi di preimmagine e di collisione.
3. Quale, tra i seguenti, è un possibile problema del protocollo Diffie-Hellman?
   (a) La possibilità di un attacco Man-in-the-Middle.
   (b) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (c) La lentezza in rapporto ai cifrari a chiave condivisa.
4. Quale delle seguenti proprietà è necessaria affinché una funzione hash sia crittograficamente sicura?
   (a) L'iniettività.
   (b) La resistenza agli attacchi di preimmagine e di collisione.
   (c) La suriettività.
5. Quale delle seguenti proprietà è necessaria per una funzione di cifratura?
   (a) La resistenza agli attacchi di preimmagine e di collisione.
   (b) La suriettività.
   (c) L'iniettività.
6. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (b) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (c) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
7. Alice e Bob avviano una sessione Diffie-Hellman; per decifrare la chiave di sessione, Charlie (in ascolto sul canale ma non in grado di interferire) deve...
   (a) ...trovare una collisione in un valore hash crittografico.
   (b) ...fattorizzare un grande prodotto di numeri primi.
   (c) ...risolvere un problema di logaritmo discreto.
8. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave privata del richiedente.
   (b) Il common name del richiedente.
   (c) La chiave pubblica del richiedente.
9. Quale proprietà caratterizza i cifrari a flusso?
   (a) Combinano i dati da cifrare con un flusso potenzialmente infinito di dati (pseudo-) casuali.
   (b) Non richiedono che gli interlocutori abbiano concordato e condiviso una chiave.
   (c) Sono necessariamente interattivi.
10. Un certificato di firma digitale solitamente accompagna...
    (a) ...una chiave di sessione, e ne garantisce l'autenticità.
    (b) ...una chiave privata, e garantisce l'identità del possessore della corrispondente chiave pubblica.
    (c) ...una chiave pubblica, e garantisce l'identità del possessore della corrispondente chiave privata.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Tema 28

Lunedì 4 giugno 2018

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 13$ e sul generatore $g = 6$.

1.1) Supponendo che Alice scelga il valore segreto $a = 11$ e Bob il valore $b = 5$, descrivere lo scambio di informazioni che avviene fra i due interlocutori.

1.2) Calcolare la chiave condivisa K utilizzando la formula più conveniente fra quella usata da Alice e quella usata da Bob.

Esercizio 2

Il server web di Alice dispone di un sistema di login basato su username e password; per comodità, assumiamo che le password siano stringhe di bit.
Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile: si assuma che utilizzi una stringa casuale di 64 bit.
Il server applica alle password degli utenti una funzione hash crittografica H che genera un valore a 26 bit. In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 26 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.

Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H, ma che sappia che Bob utilizza una password di 64 bit. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login verso il server ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password, portandola a 128 bit casuali.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash in locale (nel computer di Charlie) richieda un miliardesimo di secondo.
Le risposte alle domande 2.1 e 2.2 cambiano?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Quale, tra i seguenti, è un possibile problema del protocollo Diffie-Hellman?
   (a) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (b) La lentezza in rapporto ai cifrari a chiave condivisa.
   (c) La possibilità di un attacco Man-in-the-Middle.
2. Quale delle seguenti proprietà è necessaria affinché una funzione hash sia crittograficamente sicura?
   (a) La suriettività.
   (b) La resistenza agli attacchi di preimmagine e di collisione.
   (c) L'iniettività.
3. Quale, tra i seguenti, è un possibile problema del cifrario RSA?
   (a) La lentezza in rapporto ai cifrari a chiave condivisa.
   (b) La possibilità di un attacco Man-in-the-Middle.
   (c) La difficoltà di trovare numeri primi di dimensioni sufficienti.
4. Quale proprietà caratterizza i cifrari a flusso?
   (a) Sono necessariamente interattivi.
   (b) Combinano i dati da cifrare con un flusso potenzialmente infinito di dati (pseudo-) casuali.
   (c) Non richiedono che gli interlocutori abbiano concordato e condiviso una chiave.
5. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (b) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (c) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
6. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) Il common name del richiedente.
   (b) La chiave privata del richiedente.
   (c) La chiave pubblica del richiedente.
7. Quale delle seguenti proprietà è necessaria per una funzione di cifratura?
   (a) La suriettività.
   (b) L'iniettività.
   (c) La resistenza agli attacchi di preimmagine e di collisione.
8. Un certificato di firma digitale solitamente accompagna...
   (a) ...una chiave pubblica, e garantisce l'identità del possessore della corrispondente chiave privata.
   (b) ...una chiave privata, e garantisce l'identità del possessore della corrispondente chiave pubblica.
   (c) ...una chiave di sessione, e ne garantisce l'autenticità.
9. Quale delle seguenti proprietà **non** è posseduta da nessuna funzione hash crittografica?
   (a) La resistenza agli attacchi di preimmagine e di collisione.
   (b) L'iniettività.
   (c) La suriettività.
10. Alice e Bob avviano una sessione Diffie-Hellman; per decifrare la chiave di sessione, Charlie (in ascolto sul canale ma non in grado di interferire) deve...
    (a) ...fattorizzare un grande prodotto di numeri primi.
    (b) ...trovare una collisione in un valore hash crittografico.
    (c) ...risolvere un problema di logaritmo discreto.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Tema 29

Lunedì 4 giugno 2018

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 11$ e sul generatore $g = 7$.

1.1) Supponendo che Alice scelga il valore segreto $a = 8$ e Bob il valore $b = 3$, descrivere lo scambio di informazioni che avviene fra i due interlocutori.

1.2) Calcolare la chiave condivisa K utilizzando la formula più conveniente fra quella usata da Alice e quella usata da Bob.

Esercizio 2

Il server web di Alice dispone di un sistema di login basato su username e password; per comodità, assumiamo che le password siano stringhe di bit.
Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile: si assuma che utilizzi una stringa casuale di 64 bit.
Il server applica alle password degli utenti una funzione hash crittografica H che genera un valore a 24 bit. In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 24 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.

Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H, ma che sappia che Bob utilizza una password di 64 bit. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login verso il server ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password, portandola a 128 bit casuali.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash in locale (nel computer di Charlie) richieda un miliardesimo di secondo.
Le risposte alle domande 2.1 e 2.2 cambiano?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Quale delle seguenti proprietà è necessaria affinché una funzione hash sia crittograficamente sicura?
   (a) L'iniettività.
   (b) La resistenza agli attacchi di preimmagine e di collisione.
   (c) La suriettività.
2. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave privata del richiedente.
   (b) La chiave pubblica del richiedente.
   (c) Il common name del richiedente.
3. Quale delle seguenti proprietà è necessaria per una funzione di cifratura?
   (a) La suriettività.
   (b) L'iniettività.
   (c) La resistenza agli attacchi di preimmagine e di collisione.
4. Quale proprietà caratterizza i cifrari a flusso?
   (a) Sono necessariamente interattivi.
   (b) Non richiedono che gli interlocutori abbiano concordato e condiviso una chiave.
   (c) Combinano i dati da cifrare con un flusso potenzialmente infinito di dati (pseudo-) casuali.
5. Alice e Bob avviano una sessione Diffie-Hellman; per decifrare la chiave di sessione, Charlie (in ascolto sul canale ma non in grado di interferire) deve...
   (a) ...fattorizzare un grande prodotto di numeri primi.
   (b) ...risolvere un problema di logaritmo discreto.
   (c) ...trovare una collisione in un valore hash crittografico.
6. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (b) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (c) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
7. Un certificato di firma digitale solitamente accompagna...
   (a) ...una chiave pubblica, e garantisce l'identità del possessore della corrispondente chiave privata.
   (b) ...una chiave privata, e garantisce l'identità del possessore della corrispondente chiave pubblica.
   (c) ...una chiave di sessione, e ne garantisce l'autenticità.
8. Quale, tra i seguenti, è un possibile problema del cifrario RSA?
   (a) La possibilità di un attacco Man-in-the-Middle.
   (b) La lentezza in rapporto ai cifrari a chiave condivisa.
   (c) La difficoltà di trovare numeri primi di dimensioni sufficienti.
9. Quale, tra i seguenti, è un possibile problema del protocollo Diffie-Hellman?
   (a) La possibilità di un attacco Man-in-the-Middle.
   (b) La lentezza in rapporto ai cifrari a chiave condivisa.
   (c) La difficoltà di trovare numeri primi di dimensioni sufficienti.
10. Quale delle seguenti proprietà **non** è posseduta da nessuna funzione hash crittografica?
    (a) La suriettività.
    (b) L'iniettività.
    (c) La resistenza agli attacchi di preimmagine e di collisione.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Tema 30

Lunedì 4 giugno 2018

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 11$ e sul generatore $g = 6$.

1.1) Supponendo che Alice scelga il valore segreto $a = 9$ e Bob il valore $b = 2$, descrivere lo scambio di informazioni che avviene fra i due interlocutori.

1.2) Calcolare la chiave condivisa K utilizzando la formula più conveniente fra quella usata da Alice e quella usata da Bob.

Esercizio 2

Il server web di Alice dispone di un sistema di login basato su username e password; per comodità, assumiamo che le password siano stringhe di bit.
Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile: si assuma che utilizzi una stringa casuale di 64 bit.
Il server applica alle password degli utenti una funzione hash crittografica H che genera un valore a 30 bit. In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 30 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.

Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H, ma che sappia che Bob utilizza una password di 64 bit. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login verso il server ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password, portandola a 128 bit casuali.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash in locale (nel computer di Charlie) richieda un miliardesimo di secondo.
Le risposte alle domande 2.1 e 2.2 cambiano?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave pubblica del richiedente.
   (b) Il common name del richiedente.
   (c) La chiave privata del richiedente.
2. Alice e Bob avviano una sessione Diffie-Hellman; per decifrare la chiave di sessione, Charlie (in ascolto sul canale ma non in grado di interferire) deve...
   (a) ... fattorizzare un grande prodotto di numeri primi.
   (b) ... risolvere un problema di logaritmo discreto.
   (c) ... trovare una collisione in un valore hash crittografico.
3. Quale delle seguenti proprietà **non** è posseduta da nessuna funzione hash crittografica?
   (a) La resistenza agli attacchi di preimmagine e di collisione.
   (b) La suriettività.
   (c) L'iniettività.
4. Un certificato di firma digitale solitamente accompagna...
   (a) ... una chiave privata, e garantisce l'identità del possessore della corrispondente chiave pubblica.
   (b) ... una chiave di sessione, e ne garantisce l'autenticità.
   (c) ... una chiave pubblica, e garantisce l'identità del possessore della corrispondente chiave privata.
5. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (b) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (c) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
6. Quale proprietà caratterizza i cifrari a flusso?
   (a) Sono necessariamente interattivi.
   (b) Combinano i dati da cifrare con un flusso potenzialmente infinito di dati (pseudo-) casuali.
   (c) Non richiedono che gli interlocutori abbiano concordato e condiviso una chiave.
7. Quale delle seguenti proprietà è necessaria per una funzione di cifratura?
   (a) La resistenza agli attacchi di preimmagine e di collisione.
   (b) La suriettività.
   (c) L'iniettività.
8. Quale, tra i seguenti, è un possibile problema del protocollo Diffie-Hellman?
   (a) La possibilità di un attacco Man-in-the-Middle.
   (b) La lentezza in rapporto ai cifrari a chiave condivisa.
   (c) La difficoltà di trovare numeri primi di dimensioni sufficienti.
9. Quale delle seguenti proprietà è necessaria affinché una funzione hash sia crittograficamente sicura?
   (a) La suriettività.
   (b) La resistenza agli attacchi di preimmagine e di collisione.
   (c) L'iniettività.
10. Quale, tra i seguenti, è un possibile problema del cifrario RSA?
    (a) La possibilità di un attacco Man-in-the-Middle.
    (b) La difficoltà di trovare numeri primi di dimensioni sufficienti.
    (c) La lentezza in rapporto ai cifrari a chiave condivisa.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Tema 31

Lunedì 4 giugno 2018

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 11$ e sul generatore $g = 8$.

1.1) Supponendo che Alice scelga il valore segreto $a = 9$ e Bob il valore $b = 4$, descrivere lo scambio di informazioni che avviene fra i due interlocutori.

1.2) Calcolare la chiave condivisa K utilizzando la formula più conveniente fra quella usata da Alice e quella usata da Bob.

Esercizio 2

Il server web di Alice dispone di un sistema di login basato su username e password; per comodità, assumiamo che le password siano stringhe di bit.
Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile: si assuma che utilizzi una stringa casuale di 64 bit.
Il server applica alle password degli utenti una funzione hash crittografica H che genera un valore a 30 bit. In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 30 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.

Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H, ma che sappia che Bob utilizza una password di 64 bit. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login verso il server ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password, portandola a 128 bit casuali.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash in locale (nel computer di Charlie) richieda un miliardesimo di secondo.
Le risposte alle domande 2.1 e 2.2 cambiano?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Quale delle seguenti proprietà è necessaria per una funzione di cifratura?
   (a) La suriettività.
   (b) L'iniettività.
   (c) La resistenza agli attacchi di preimmagine e di collisione.
2. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (b) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (c) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
3. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave privata del richiedente.
   (b) Il common name del richiedente.
   (c) La chiave pubblica del richiedente.
4. Quale proprietà caratterizza i cifrari a flusso?
   (a) Combinano i dati da cifrare con un flusso potenzialmente infinito di dati (pseudo-) casuali.
   (b) Non richiedono che gli interlocutori abbiano concordato e condiviso una chiave.
   (c) Sono necessariamente interattivi.
5. Quale, tra i seguenti, è un possibile problema del protocollo Diffie-Hellman?
   (a) La lentezza in rapporto ai cifrari a chiave condivisa.
   (b) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (c) La possibilità di un attacco Man-in-the-Middle.
6. Quale delle seguenti proprietà **non** è posseduta da nessuna funzione hash crittografica?
   (a) La resistenza agli attacchi di preimmagine e di collisione.
   (b) La suriettività.
   (c) L'iniettività.
7. Alice e Bob avviano una sessione Diffie-Hellman; per decifrare la chiave di sessione, Charlie (in ascolto sul canale ma non in grado di interferire) deve...
   (a) ...fattorizzare un grande prodotto di numeri primi.
   (b) ...risolvere un problema di logaritmo discreto.
   (c) ...trovare una collisione in un valore hash crittografico.
8. Quale delle seguenti proprietà è necessaria affinché una funzione hash sia crittograficamente sicura?
   (a) La suriettività.
   (b) La resistenza agli attacchi di preimmagine e di collisione.
   (c) L'iniettività.
9. Un certificato di firma digitale solitamente accompagna...
   (a) ...una chiave di sessione, e ne garantisce l'autenticità.
   (b) ...una chiave privata, e garantisce l'identità del possessore della corrispondente chiave pubblica.
   (c) ...una chiave pubblica, e garantisce l'identità del possessore della corrispondente chiave privata.
10. Quale, tra i seguenti, è un possibile problema del cifrario RSA?
    (a) La difficoltà di trovare numeri primi di dimensioni sufficienti.
    (b) La lentezza in rapporto ai cifrari a chiave condivisa.
    (c) La possibilità di un attacco Man-in-the-Middle.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Tema 32

Lunedì 4 giugno 2018

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 11$ e sul generatore $g = 8$.

1.1) Supponendo che Alice scelga il valore segreto $a = 9$ e Bob il valore $b = 4$, descrivere lo scambio di informazioni che avviene fra i due interlocutori.

1.2) Calcolare la chiave condivisa K utilizzando la formula più conveniente fra quella usata da Alice e quella usata da Bob.

Esercizio 2

Il server web di Alice dispone di un sistema di login basato su username e password; per comodità, assumiamo che le password siano stringhe di bit.
Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile: si assuma che utilizzi una stringa casuale di 64 bit.
Il server applica alle password degli utenti una funzione hash crittografica H che genera un valore a 24 bit. In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 24 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.

Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H, ma che sappia che Bob utilizza una password di 64 bit. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login verso il server ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password, portandola a 128 bit casuali.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash in locale (nel computer di Charlie) richieda un miliardesimo di secondo.
Le risposte alle domande 2.1 e 2.2 cambiano?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Quale delle seguenti proprietà **non** è posseduta da nessuna funzione hash crittografica?
   (a) La resistenza agli attacchi di preimmagine e di collisione.
   (b) La suriettività.
   (c) L'iniettività.
2. Un certificato di firma digitale solitamente accompagna...
   (a) ...una chiave privata, e garantisce l'identità del possessore della corrispondente chiave pubblica.
   (b) ...una chiave pubblica, e garantisce l'identità del possessore della corrispondente chiave privata.
   (c) ...una chiave di sessione, e ne garantisce l'autenticità.
3. Quale proprietà caratterizza i cifrari a flusso?
   (a) Combinano i dati da cifrare con un flusso potenzialmente infinito di dati (pseudo-) casuali.
   (b) Non richiedono che gli interlocutori abbiano concordato e condiviso una chiave.
   (c) Sono necessariamente interattivi.
4. Alice e Bob avviano una sessione Diffie-Hellman; per decifrare la chiave di sessione, Charlie (in ascolto sul canale ma non in grado di interferire) deve...
   (a) ...trovare una collisione in un valore hash crittografico.
   (b) ...risolvere un problema di logaritmo discreto.
   (c) ...fattorizzare un grande prodotto di numeri primi.
5. Quale delle seguenti proprietà è necessaria per una funzione di cifratura?
   (a) La suriettività.
   (b) La resistenza agli attacchi di preimmagine e di collisione.
   (c) L'iniettività.
6. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (b) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (c) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
7. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave pubblica del richiedente.
   (b) La chiave privata del richiedente.
   (c) Il common name del richiedente.
8. Quale, tra i seguenti, è un possibile problema del cifrario RSA?
   (a) La possibilità di un attacco Man-in-the-Middle.
   (b) La lentezza in rapporto ai cifrari a chiave condivisa.
   (c) La difficoltà di trovare numeri primi di dimensioni sufficienti.
9. Quale, tra i seguenti, è un possibile problema del protocollo Diffie-Hellman?
   (a) La lentezza in rapporto ai cifrari a chiave condivisa.
   (b) La possibilità di un attacco Man-in-the-Middle.
   (c) La difficoltà di trovare numeri primi di dimensioni sufficienti.
10. Quale delle seguenti proprietà è necessaria affinché una funzione hash sia crittograficamente sicura?
    (a) La resistenza agli attacchi di preimmagine e di collisione.
    (b) La suriettività.
    (c) L'iniettività.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Tema 33

Lunedì 4 giugno 2018

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 13$ e sul generatore $g = 7$.

1.1) Supponendo che Alice scelga il valore segreto $a = 10$ e Bob il valore $b = 4$, descrivere lo scambio di informazioni che avviene fra i due interlocutori.

1.2) Calcolare la chiave condivisa K utilizzando la formula più conveniente fra quella usata da Alice e quella usata da Bob.

Esercizio 2

Il server web di Alice dispone di un sistema di login basato su username e password; per comodità, assumiamo che le password siano stringhe di bit.
Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile: si assuma che utilizzi una stringa casuale di 64 bit.
Il server applica alle password degli utenti una funzione hash crittografica H che genera un valore a 28 bit. In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 28 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.

Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H, ma che sappia che Bob utilizza una password di 64 bit. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login verso il server ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password, portandola a 128 bit casuali.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash in locale (nel computer di Charlie) richieda un miliardesimo di secondo.
Le risposte alle domande 2.1 e 2.2 cambiano?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Quale, tra i seguenti, è un possibile problema del protocollo Diffie-Hellman?
   (a) La lentezza in rapporto ai cifrari a chiave condivisa.
   (b) La possibilità di un attacco Man-in-the-Middle.
   (c) La difficoltà di trovare numeri primi di dimensioni sufficienti.
2. Quale delle seguenti proprietà **non** è posseduta da nessuna funzione hash crittografica?
   (a) La resistenza agli attacchi di preimmagine e di collisione.
   (b) La suriettività.
   (c) L'iniettività.
3. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (b) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (c) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
4. Quale, tra i seguenti, è un possibile problema del cifrario RSA?
   (a) La possibilità di un attacco Man-in-the-Middle.
   (b) La lentezza in rapporto ai cifrari a chiave condivisa.
   (c) La difficoltà di trovare numeri primi di dimensioni sufficienti.
5. Un certificato di firma digitale solitamente accompagna...
   (a) ...una chiave di sessione, e ne garantisce l'autenticità.
   (b) ...una chiave pubblica, e garantisce l'identità del possessore della corrispondente chiave privata.
   (c) ...una chiave privata, e garantisce l'identità del possessore della corrispondente chiave pubblica.
6. Quale delle seguenti proprietà è necessaria affinché una funzione hash sia crittograficamente sicura?
   (a) La resistenza agli attacchi di preimmagine e di collisione.
   (b) L'iniettività.
   (c) La suriettività.
7. Quale proprietà caratterizza i cifrari a flusso?
   (a) Non richiedono che gli interlocutori abbiano concordato e condiviso una chiave.
   (b) Combinano i dati da cifrare con un flusso potenzialmente infinito di dati (pseudo-) casuali.
   (c) Sono necessariamente interattivi.
8. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) Il common name del richiedente.
   (b) La chiave privata del richiedente.
   (c) La chiave pubblica del richiedente.
9. Quale delle seguenti proprietà è necessaria per una funzione di cifratura?
   (a) La suriettività.
   (b) L'iniettività.
   (c) La resistenza agli attacchi di preimmagine e di collisione.
10. Alice e Bob avviano una sessione Diffie-Hellman; per decifrare la chiave di sessione, Charlie (in ascolto sul canale ma non in grado di interferire) deve...
    (a) ...fattorizzare un grande prodotto di numeri primi.
    (b) ...trovare una collisione in un valore hash crittografico.
    (c) ...risolvere un problema di logaritmo discreto.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Tema 34

Lunedì 4 giugno 2018

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 13$ e sul generatore $g = 7$.

1.1) Supponendo che Alice scelga il valore segreto $a = 10$ e Bob il valore $b = 3$, descrivere lo scambio di informazioni che avviene fra i due interlocutori.

1.2) Calcolare la chiave condivisa K utilizzando la formula più conveniente fra quella usata da Alice e quella usata da Bob.

Esercizio 2

Il server web di Alice dispone di un sistema di login basato su username e password; per comodità, assumiamo che le password siano stringhe di bit.
Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile: si assuma che utilizzi una stringa casuale di 64 bit.
Il server applica alle password degli utenti una funzione hash crittografica H che genera un valore a 32 bit. In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 32 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.

Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H, ma che sappia che Bob utilizza una password di 64 bit. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login verso il server ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password, portandola a 128 bit casuali.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash in locale (nel computer di Charlie) richieda un miliardesimo di secondo.
Le risposte alle domande 2.1 e 2.2 cambiano?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Alice e Bob avviano una sessione Diffie-Hellman; per decifrare la chiave di sessione, Charlie (in ascolto sul canale ma non in grado di interferire) deve...
   (a) ...risolvere un problema di logaritmo discreto.
   (b) ...trovare una collisione in un valore hash crittografico.
   (c) ...fattorizzare un grande prodotto di numeri primi.
2. Quale delle seguenti proprietà è necessaria per una funzione di cifratura?
   (a) La resistenza agli attacchi di preimmagine e di collisione.
   (b) L'iniettività.
   (c) La suriettività.
3. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave privata del richiedente.
   (b) Il common name del richiedente.
   (c) La chiave pubblica del richiedente.
4. Quale, tra i seguenti, è un possibile problema del protocollo Diffie-Hellman?
   (a) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (b) La lentezza in rapporto ai cifrari a chiave condivisa.
   (c) La possibilità di un attacco Man-in-the-Middle.
5. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (b) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (c) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
6. Quale proprietà caratterizza i cifrari a flusso?
   (a) Combinano i dati da cifrare con un flusso potenzialmente infinito di dati (pseudo-) casuali.
   (b) Sono necessariamente interattivi.
   (c) Non richiedono che gli interlocutori abbiano concordato e condiviso una chiave.
7. Un certificato di firma digitale solitamente accompagna...
   (a) ...una chiave di sessione, e ne garantisce l'autenticità.
   (b) ...una chiave privata, e garantisce l'identità del possessore della corrispondente chiave pubblica.
   (c) ...una chiave pubblica, e garantisce l'identità del possessore della corrispondente chiave privata.
8. Quale delle seguenti proprietà **non** è posseduta da nessuna funzione hash crittografica?
   (a) La suriettività.
   (b) L'iniettività.
   (c) La resistenza agli attacchi di preimmagine e di collisione.
9. Quale, tra i seguenti, è un possibile problema del cifrario RSA?
   (a) La possibilità di un attacco Man-in-the-Middle.
   (b) La lentezza in rapporto ai cifrari a chiave condivisa.
   (c) La difficoltà di trovare numeri primi di dimensioni sufficienti.
10. Quale delle seguenti proprietà è necessaria affinché una funzione hash sia crittograficamente sicura?
    (a) L'iniettività.
    (b) La suriettività.
    (c) La resistenza agli attacchi di preimmagine e di collisione.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Tema 35

Lunedì 4 giugno 2018

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 13$ e sul generatore $g = 6$.

1.1) Supponendo che Alice scelga il valore segreto $a = 10$ e Bob il valore $b = 2$, descrivere lo scambio di informazioni che avviene fra i due interlocutori.

1.2) Calcolare la chiave condivisa K utilizzando la formula più conveniente fra quella usata da Alice e quella usata da Bob.

Esercizio 2

Il server web di Alice dispone di un sistema di login basato su username e password; per comodità, assumiamo che le password siano stringhe di bit.
Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile: si assuma che utilizzi una stringa casuale di 64 bit.
Il server applica alle password degli utenti una funzione hash crittografica H che genera un valore a 26 bit. In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 26 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.

Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H, ma che sappia che Bob utilizza una password di 64 bit. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login verso il server ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password, portandola a 128 bit casuali.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash in locale (nel computer di Charlie) richieda un miliardesimo di secondo.
Le risposte alle domande 2.1 e 2.2 cambiano?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Quale proprietà caratterizza i cifrari a flusso?
   (a) Combinano i dati da cifrare con un flusso potenzialmente infinito di dati (pseudo-) casuali.
   (b) Sono necessariamente interattivi.
   (c) Non richiedono che gli interlocutori abbiano concordato e condiviso una chiave.
2. Quale, tra i seguenti, è un possibile problema del cifrario RSA?
   (a) La possibilità di un attacco Man-in-the-Middle.
   (b) La lentezza in rapporto ai cifrari a chiave condivisa.
   (c) La difficoltà di trovare numeri primi di dimensioni sufficienti.
3. Quale delle seguenti proprietà è necessaria affinché una funzione hash sia crittograficamente sicura?
   (a) La resistenza agli attacchi di preimmagine e di collisione.
   (b) La suriettività.
   (c) L'iniettività.
4. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (b) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (c) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
5. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave privata del richiedente.
   (b) Il common name del richiedente.
   (c) La chiave pubblica del richiedente.
6. Quale, tra i seguenti, è un possibile problema del protocollo Diffie-Hellman?
   (a) La possibilità di un attacco Man-in-the-Middle.
   (b) La lentezza in rapporto ai cifrari a chiave condivisa.
   (c) La difficoltà di trovare numeri primi di dimensioni sufficienti.
7. Quale delle seguenti proprietà è necessaria per una funzione di cifratura?
   (a) La suriettività.
   (b) La resistenza agli attacchi di preimmagine e di collisione.
   (c) L'iniettività.
8. Alice e Bob avviano una sessione Diffie-Hellman; per decifrare la chiave di sessione, Charlie (in ascolto sul canale ma non in grado di interferire) deve...
   (a) ... fattorizzare un grande prodotto di numeri primi.
   (b) ... trovare una collisione in un valore hash crittografico.
   (c) ... risolvere un problema di logaritmo discreto.
9. Un certificato di firma digitale solitamente accompagna...
   (a) ... una chiave di sessione, e ne garantisce l'autenticità.
   (b) ... una chiave pubblica, e garantisce l'identità del possessore della corrispondente chiave privata.
   (c) ... una chiave privata, e garantisce l'identità del possessore della corrispondente chiave pubblica.
10. Quale delle seguenti proprietà **non** è posseduta da nessuna funzione hash crittografica?
    (a) L'iniettività.
    (b) La resistenza agli attacchi di preimmagine e di collisione.
    (c) La suriettività.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Tema 36

Lunedì 4 giugno 2018

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 11$ e sul generatore $g = 8$.

1.1) Supponendo che Alice scelga il valore segreto $a = 9$ e Bob il valore $b = 4$, descrivere lo scambio di informazioni che avviene fra i due interlocutori.

1.2) Calcolare la chiave condivisa K utilizzando la formula più conveniente fra quella usata da Alice e quella usata da Bob.

Esercizio 2

Il server web di Alice dispone di un sistema di login basato su username e password; per comodità, assumiamo che le password siano stringhe di bit.
Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile: si assuma che utilizzi una stringa casuale di 64 bit.
Il server applica alle password degli utenti una funzione hash crittografica H che genera un valore a 30 bit. In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 30 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.

Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H, ma che sappia che Bob utilizza una password di 64 bit. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login verso il server ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password, portandola a 128 bit casuali.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash in locale (nel computer di Charlie) richieda un miliardesimo di secondo.
Le risposte alle domande 2.1 e 2.2 cambiano?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Alice e Bob avviano una sessione Diffie-Hellman; per decifrare la chiave di sessione, Charlie (in ascolto sul canale ma non in grado di interferire) deve...
   (a) ...trovare una collisione in un valore hash crittografico.
   (b) ...risolvere un problema di logaritmo discreto.
   (c) ...fattorizzare un grande prodotto di numeri primi.
2. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (b) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (c) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
3. Quale, tra i seguenti, è un possibile problema del protocollo Diffie-Hellman?
   (a) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (b) La possibilità di un attacco Man-in-the-Middle.
   (c) La lentezza in rapporto ai cifrari a chiave condivisa.
4. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave privata del richiedente.
   (b) La chiave pubblica del richiedente.
   (c) Il common name del richiedente.
5. Quale proprietà caratterizza i cifrari a flusso?
   (a) Non richiedono che gli interlocutori abbiano concordato e condiviso una chiave.
   (b) Combinano i dati da cifrare con un flusso potenzialmente infinito di dati (pseudo-) casuali.
   (c) Sono necessariamente interattivi.
6. Un certificato di firma digitale solitamente accompagna...
   (a) ...una chiave privata, e garantisce l'identità del possessore della corrispondente chiave pubblica.
   (b) ...una chiave pubblica, e garantisce l'identità del possessore della corrispondente chiave privata.
   (c) ...una chiave di sessione, e ne garantisce l'autenticità.
7. Quale delle seguenti proprietà è necessaria per una funzione di cifratura?
   (a) La suriettività.
   (b) L'iniettività.
   (c) La resistenza agli attacchi di preimmagine e di collisione.
8. Quale, tra i seguenti, è un possibile problema del cifrario RSA?
   (a) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (b) La lentezza in rapporto ai cifrari a chiave condivisa.
   (c) La possibilità di un attacco Man-in-the-Middle.
9. Quale delle seguenti proprietà **non** è posseduta da nessuna funzione hash crittografica?
   (a) La suriettività.
   (b) L'iniettività.
   (c) La resistenza agli attacchi di preimmagine e di collisione.
10. Quale delle seguenti proprietà è necessaria affinché una funzione hash sia crittograficamente sicura?
    (a) La resistenza agli attacchi di preimmagine e di collisione.
    (b) La suriettività.
    (c) L'iniettività.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Tema 37

Lunedì 4 giugno 2018

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 11$ e sul generatore $g = 6$.

1.1) Supponendo che Alice scelga il valore segreto $a = 9$ e Bob il valore $b = 4$, descrivere lo scambio di informazioni che avviene fra i due interlocutori.

1.2) Calcolare la chiave condivisa K utilizzando la formula più conveniente fra quella usata da Alice e quella usata da Bob.

Esercizio 2

Il server web di Alice dispone di un sistema di login basato su username e password; per comodità, assumiamo che le password siano stringhe di bit.
Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile: si assuma che utilizzi una stringa casuale di 64 bit.
Il server applica alle password degli utenti una funzione hash crittografica H che genera un valore a 26 bit. In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 26 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.

Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H, ma che sappia che Bob utilizza una password di 64 bit. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login verso il server ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password, portandola a 128 bit casuali.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash in locale (nel computer di Charlie) richieda un miliardesimo di secondo.
Le risposte alle domande 2.1 e 2.2 cambiano?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (b) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (c) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
2. Quale delle seguenti proprietà è necessaria per una funzione di cifratura?
   (a) La suriettività.
   (b) L'iniettività.
   (c) La resistenza agli attacchi di preimmagine e di collisione.
3. Quale delle seguenti proprietà è necessaria affinché una funzione hash sia crittograficamente sicura?
   (a) La suriettività.
   (b) La resistenza agli attacchi di preimmagine e di collisione.
   (c) L'iniettività.
4. Quale proprietà caratterizza i cifrari a flusso?
   (a) Sono necessariamente interattivi.
   (b) Non richiedono che gli interlocutori abbiano concordato e condiviso una chiave.
   (c) Combinano i dati da cifrare con un flusso potenzialmente infinito di dati (pseudo-) casuali.
5. Quale, tra i seguenti, è un possibile problema del cifrario RSA?
   (a) La possibilità di un attacco Man-in-the-Middle.
   (b) La lentezza in rapporto ai cifrari a chiave condivisa.
   (c) La difficoltà di trovare numeri primi di dimensioni sufficienti.
6. Quale, tra i seguenti, è un possibile problema del protocollo Diffie-Hellman?
   (a) La possibilità di un attacco Man-in-the-Middle.
   (b) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (c) La lentezza in rapporto ai cifrari a chiave condivisa.
7. Quale delle seguenti proprietà **non** è posseduta da nessuna funzione hash crittografica?
   (a) La resistenza agli attacchi di preimmagine e di collisione.
   (b) La suriettività.
   (c) L'iniettività.
8. Alice e Bob avviano una sessione Diffie-Hellman; per decifrare la chiave di sessione, Charlie (in ascolto sul canale ma non in grado di interferire) deve...
   (a) ...risolvere un problema di logaritmo discreto.
   (b) ...trovare una collisione in un valore hash crittografico.
   (c) ...fattorizzare un grande prodotto di numeri primi.
9. Un certificato di firma digitale solitamente accompagna...
   (a) ...una chiave pubblica, e garantisce l'identità del possessore della corrispondente chiave privata.
   (b) ...una chiave privata, e garantisce l'identità del possessore della corrispondente chiave pubblica.
   (c) ...una chiave di sessione, e ne garantisce l'autenticità.
10. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
    (a) La chiave privata del richiedente.
    (b) La chiave pubblica del richiedente.
    (c) Il common name del richiedente.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Tema 38

Lunedì 4 giugno 2018

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 11$ e sul generatore $g = 6$.

1.1) Supponendo che Alice scelga il valore segreto $a = 7$ e Bob il valore $b = 2$, descrivere lo scambio di informazioni che avviene fra i due interlocutori.

1.2) Calcolare la chiave condivisa K utilizzando la formula più conveniente fra quella usata da Alice e quella usata da Bob.

Esercizio 2

Il server web di Alice dispone di un sistema di login basato su username e password; per comodità, assumiamo che le password siano stringhe di bit.
Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile: si assuma che utilizzi una stringa casuale di 64 bit.
Il server applica alle password degli utenti una funzione hash crittografica H che genera un valore a 26 bit. In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 26 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.

Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H, ma che sappia che Bob utilizza una password di 64 bit. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login verso il server ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password, portandola a 128 bit casuali.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash in locale (nel computer di Charlie) richieda un miliardesimo di secondo.
Le risposte alle domande 2.1 e 2.2 cambiano?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Un certificato di firma digitale solitamente accompagna...
   (a) ...una chiave di sessione, e ne garantisce l'autenticità.
   (b) ...una chiave privata, e garantisce l'identità del possessore della corrispondente chiave pubblica.
   (c) ...una chiave pubblica, e garantisce l'identità del possessore della corrispondente chiave privata.
2. Quale proprietà caratterizza i cifrari a flusso?
   (a) Non richiedono che gli interlocutori abbiano concordato e condiviso una chiave.
   (b) Sono necessariamente interattivi.
   (c) Combinano i dati da cifrare con un flusso potenzialmente infinito di dati (pseudo-) casuali.
3. Quale delle seguenti proprietà **non** è posseduta da nessuna funzione hash crittografica?
   (a) L'iniettività.
   (b) La resistenza agli attacchi di preimmagine e di collisione.
   (c) La suriettività.
4. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (b) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (c) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
5. Quale, tra i seguenti, è un possibile problema del cifrario RSA?
   (a) La possibilità di un attacco Man-in-the-Middle.
   (b) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (c) La lentezza in rapporto ai cifrari a chiave condivisa.
6. Quale delle seguenti proprietà è necessaria per una funzione di cifratura?
   (a) La suriettività.
   (b) La resistenza agli attacchi di preimmagine e di collisione.
   (c) L'iniettività.
7. Quale, tra i seguenti, è un possibile problema del protocollo Diffie-Hellman?
   (a) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (b) La possibilità di un attacco Man-in-the-Middle.
   (c) La lentezza in rapporto ai cifrari a chiave condivisa.
8. Quale delle seguenti proprietà è necessaria affinché una funzione hash sia crittograficamente sicura?
   (a) L'iniettività.
   (b) La suriettività.
   (c) La resistenza agli attacchi di preimmagine e di collisione.
9. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave privata del richiedente.
   (b) La chiave pubblica del richiedente.
   (c) Il common name del richiedente.
10. Alice e Bob avviano una sessione Diffie-Hellman; per decifrare la chiave di sessione, Charlie (in ascolto sul canale ma non in grado di interferire) deve...
    (a) ...trovare una collisione in un valore hash crittografico.
    (b) ...fattorizzare un grande prodotto di numeri primi.
    (c) ...risolvere un problema di logaritmo discreto.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Tema 39

Lunedì 4 giugno 2018

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 11$ e sul generatore $g = 6$.

1.1) Supponendo che Alice scelga il valore segreto $a = 8$ e Bob il valore $b = 4$, descrivere lo scambio di informazioni che avviene fra i due interlocutori.

1.2) Calcolare la chiave condivisa K utilizzando la formula più conveniente fra quella usata da Alice e quella usata da Bob.

Esercizio 2

Il server web di Alice dispone di un sistema di login basato su username e password; per comodità, assumiamo che le password siano stringhe di bit.
Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile: si assuma che utilizzi una stringa casuale di 64 bit.
Il server applica alle password degli utenti una funzione hash crittografica H che genera un valore a 28 bit. In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 28 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.

Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H, ma che sappia che Bob utilizza una password di 64 bit. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login verso il server ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password, portandola a 128 bit casuali.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash in locale (nel computer di Charlie) richieda un miliardesimo di secondo.
Le risposte alle domande 2.1 e 2.2 cambiano?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Quale delle seguenti proprietà **non** è posseduta da nessuna funzione hash crittografica?
   (a) L'iniettività.
   (b) La resistenza agli attacchi di preimmagine e di collisione.
   (c) La suriettività.
2. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (b) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (c) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
3. Quale, tra i seguenti, è un possibile problema del cifrario RSA?
   (a) La possibilità di un attacco Man-in-the-Middle.
   (b) La lentezza in rapporto ai cifrari a chiave condivisa.
   (c) La difficoltà di trovare numeri primi di dimensioni sufficienti.
4. Quale delle seguenti proprietà è necessaria affinché una funzione hash sia crittograficamente sicura?
   (a) La suriettività.
   (b) La resistenza agli attacchi di preimmagine e di collisione.
   (c) L'iniettività.
5. Quale proprietà caratterizza i cifrari a flusso?
   (a) Combinano i dati da cifrare con un flusso potenzialmente infinito di dati (pseudo-) casuali.
   (b) Non richiedono che gli interlocutori abbiano concordato e condiviso una chiave.
   (c) Sono necessariamente interattivi.
6. Quale, tra i seguenti, è un possibile problema del protocollo Diffie-Hellman?
   (a) La lentezza in rapporto ai cifrari a chiave condivisa.
   (b) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (c) La possibilità di un attacco Man-in-the-Middle.
7. Un certificato di firma digitale solitamente accompagna...
   (a) ...una chiave di sessione, e ne garantisce l'autenticità.
   (b) ...una chiave pubblica, e garantisce l'identità del possessore della corrispondente chiave privata.
   (c) ...una chiave privata, e garantisce l'identità del possessore della corrispondente chiave pubblica.
8. Alice e Bob avviano una sessione Diffie-Hellman; per decifrare la chiave di sessione, Charlie (in ascolto sul canale ma non in grado di interferire) deve...
   (a) ...fattorizzare un grande prodotto di numeri primi.
   (b) ...trovare una collisione in un valore hash crittografico.
   (c) ...risolvere un problema di logaritmo discreto.
9. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) Il common name del richiedente.
   (b) La chiave pubblica del richiedente.
   (c) La chiave privata del richiedente.
10. Quale delle seguenti proprietà è necessaria per una funzione di cifratura?
    (a) L'iniettività.
    (b) La suriettività.
    (c) La resistenza agli attacchi di preimmagine e di collisione.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Tema 40

Lunedì 4 giugno 2018

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 11$ e sul generatore $g = 8$.

1.1) Supponendo che Alice scelga il valore segreto $a = 8$ e Bob il valore $b = 4$, descrivere lo scambio di informazioni che avviene fra i due interlocutori.

1.2) Calcolare la chiave condivisa K utilizzando la formula più conveniente fra quella usata da Alice e quella usata da Bob.

Esercizio 2

Il server web di Alice dispone di un sistema di login basato su username e password; per comodità, assumiamo che le password siano stringhe di bit.
Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile: si assuma che utilizzi una stringa casuale di 64 bit.
Il server applica alle password degli utenti una funzione hash crittografica H che genera un valore a 32 bit. In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 32 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.

Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H, ma che sappia che Bob utilizza una password di 64 bit. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login verso il server ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password, portandola a 128 bit casuali.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash in locale (nel computer di Charlie) richieda un miliardesimo di secondo.
Le risposte alle domande 2.1 e 2.2 cambiano?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Quale delle seguenti proprietà **non** è posseduta da nessuna funzione hash crittografica?
   (a) La suriettività.
   (b) L'iniettività.
   (c) La resistenza agli attacchi di preimmagine e di collisione.
2. Alice e Bob avviano una sessione Diffie-Hellman; per decifrare la chiave di sessione, Charlie (in ascolto sul canale ma non in grado di interferire) deve...
   (a) ...fattorizzare un grande prodotto di numeri primi.
   (b) ...trovare una collisione in un valore hash crittografico.
   (c) ...risolvere un problema di logaritmo discreto.
3. Quale delle seguenti proprietà è necessaria affinché una funzione hash sia crittograficamente sicura?
   (a) L'iniettività.
   (b) La resistenza agli attacchi di preimmagine e di collisione.
   (c) La suriettività.
4. Quale delle seguenti proprietà è necessaria per una funzione di cifratura?
   (a) La suriettività.
   (b) L'iniettività.
   (c) La resistenza agli attacchi di preimmagine e di collisione.
5. Un certificato di firma digitale solitamente accompagna...
   (a) ...una chiave privata, e garantisce l'identità del possessore della corrispondente chiave pubblica.
   (b) ...una chiave di sessione, e ne garantisce l'autenticità.
   (c) ...una chiave pubblica, e garantisce l'identità del possessore della corrispondente chiave privata.
6. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) Il common name del richiedente.
   (b) La chiave privata del richiedente.
   (c) La chiave pubblica del richiedente.
7. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (b) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (c) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
8. Quale, tra i seguenti, è un possibile problema del protocollo Diffie-Hellman?
   (a) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (b) La possibilità di un attacco Man-in-the-Middle.
   (c) La lentezza in rapporto ai cifrari a chiave condivisa.
9. Quale proprietà caratterizza i cifrari a flusso?
   (a) Sono necessariamente interattivi.
   (b) Combinano i dati da cifrare con un flusso potenzialmente infinito di dati (pseudo-) casuali.
   (c) Non richiedono che gli interlocutori abbiano concordato e condiviso una chiave.
10. Quale, tra i seguenti, è un possibile problema del cifrario RSA?
    (a) La possibilità di un attacco Man-in-the-Middle.
    (b) La lentezza in rapporto ai cifrari a chiave condivisa.
    (c) La difficoltà di trovare numeri primi di dimensioni sufficienti.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Tema 41

Lunedì 4 giugno 2018

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 13$ e sul generatore $g = 6$.

1.1) Supponendo che Alice scelga il valore segreto $a = 10$ e Bob il valore $b = 3$, descrivere lo scambio di informazioni che avviene fra i due interlocutori.

1.2) Calcolare la chiave condivisa K utilizzando la formula più conveniente fra quella usata da Alice e quella usata da Bob.

Esercizio 2

Il server web di Alice dispone di un sistema di login basato su username e password; per comodità, assumiamo che le password siano stringhe di bit.
Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile: si assuma che utilizzi una stringa casuale di 64 bit.
Il server applica alle password degli utenti una funzione hash crittografica H che genera un valore a 28 bit. In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 28 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.

Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H, ma che sappia che Bob utilizza una password di 64 bit. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login verso il server ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password, portandola a 128 bit casuali.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash in locale (nel computer di Charlie) richieda un miliardesimo di secondo.
Le risposte alle domande 2.1 e 2.2 cambiano?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Quale delle seguenti proprietà è necessaria affinché una funzione hash sia crittograficamente sicura?
   (a) La suriettività.
   (b) La resistenza agli attacchi di preimmagine e di collisione.
   (c) L'iniettività.
2. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (b) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (c) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
3. Quale delle seguenti proprietà è necessaria per una funzione di cifratura?
   (a) La resistenza agli attacchi di preimmagine e di collisione.
   (b) L'iniettività.
   (c) La suriettività.
4. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave pubblica del richiedente.
   (b) La chiave privata del richiedente.
   (c) Il common name del richiedente.
5. Quale proprietà caratterizza i cifrari a flusso?
   (a) Sono necessariamente interattivi.
   (b) Combinano i dati da cifrare con un flusso potenzialmente infinito di dati (pseudo-) casuali.
   (c) Non richiedono che gli interlocutori abbiano concordato e condiviso una chiave.
6. Quale, tra i seguenti, è un possibile problema del protocollo Diffie-Hellman?
   (a) La lentezza in rapporto ai cifrari a chiave condivisa.
   (b) La possibilità di un attacco Man-in-the-Middle.
   (c) La difficoltà di trovare numeri primi di dimensioni sufficienti.
7. Quale, tra i seguenti, è un possibile problema del cifrario RSA?
   (a) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (b) La lentezza in rapporto ai cifrari a chiave condivisa.
   (c) La possibilità di un attacco Man-in-the-Middle.
8. Quale delle seguenti proprietà **non** è posseduta da nessuna funzione hash crittografica?
   (a) La resistenza agli attacchi di preimmagine e di collisione.
   (b) La suriettività.
   (c) L'iniettività.
9. Un certificato di firma digitale solitamente accompagna...
   (a) ...una chiave privata, e garantisce l'identità del possessore della corrispondente chiave pubblica.
   (b) ...una chiave pubblica, e garantisce l'identità del possessore della corrispondente chiave privata.
   (c) ...una chiave di sessione, e ne garantisce l'autenticità.
10. Alice e Bob avviano una sessione Diffie-Hellman; per decifrare la chiave di sessione, Charlie (in ascolto sul canale ma non in grado di interferire) deve...
    (a) ...trovare una collisione in un valore hash crittografico.
    (b) ...risolvere un problema di logaritmo discreto.
    (c) ...fattorizzare un grande prodotto di numeri primi.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Tema 42

Lunedì 4 giugno 2018

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 11$ e sul generatore $g = 8$.

1.1) Supponendo che Alice scelga il valore segreto $a = 7$ e Bob il valore $b = 3$, descrivere lo scambio di informazioni che avviene fra i due interlocutori.

1.2) Calcolare la chiave condivisa K utilizzando la formula più conveniente fra quella usata da Alice e quella usata da Bob.

Esercizio 2

Il server web di Alice dispone di un sistema di login basato su username e password; per comodità, assumiamo che le password siano stringhe di bit.
Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile: si assuma che utilizzi una stringa casuale di 64 bit.
Il server applica alle password degli utenti una funzione hash crittografica H che genera un valore a 28 bit. In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 28 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.

Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H, ma che sappia che Bob utilizza una password di 64 bit. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login verso il server ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password, portandola a 128 bit casuali.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash in locale (nel computer di Charlie) richieda un miliardesimo di secondo.
Le risposte alle domande 2.1 e 2.2 cambiano?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Un certificato di firma digitale solitamente accompagna...
   (a) ...una chiave pubblica, e garantisce l'identità del possessore della corrispondente chiave privata.
   (b) ...una chiave di sessione, e ne garantisce l'autenticità.
   (c) ...una chiave privata, e garantisce l'identità del possessore della corrispondente chiave pubblica.
2. Alice e Bob avviano una sessione Diffie-Hellman; per decifrare la chiave di sessione, Charlie (in ascolto sul canale ma non in grado di interferire) deve...
   (a) ...trovare una collisione in un valore hash crittografico.
   (b) ...risolvere un problema di logaritmo discreto.
   (c) ...fattorizzare un grande prodotto di numeri primi.
3. Quale, tra i seguenti, è un possibile problema del protocollo Diffie-Hellman?
   (a) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (b) La lentezza in rapporto ai cifrari a chiave condivisa.
   (c) La possibilità di un attacco Man-in-the-Middle.
4. Quale proprietà caratterizza i cifrari a flusso?
   (a) Non richiedono che gli interlocutori abbiano concordato e condiviso una chiave.
   (b) Sono necessariamente interattivi.
   (c) Combinano i dati da cifrare con un flusso potenzialmente infinito di dati (pseudo-) casuali.
5. Quale, tra i seguenti, è un possibile problema del cifrario RSA?
   (a) La possibilità di un attacco Man-in-the-Middle.
   (b) La lentezza in rapporto ai cifrari a chiave condivisa.
   (c) La difficoltà di trovare numeri primi di dimensioni sufficienti.
6. Quale delle seguenti proprietà è necessaria per una funzione di cifratura?
   (a) L'iniettività.
   (b) La suriettività.
   (c) La resistenza agli attacchi di preimmagine e di collisione.
7. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (b) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (c) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
8. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave privata del richiedente.
   (b) Il common name del richiedente.
   (c) La chiave pubblica del richiedente.
9. Quale delle seguenti proprietà **non** è posseduta da nessuna funzione hash crittografica?
   (a) La resistenza agli attacchi di preimmagine e di collisione.
   (b) La suriettività.
   (c) L'iniettività.
10. Quale delle seguenti proprietà è necessaria affinché una funzione hash sia crittograficamente sicura?
    (a) L'iniettività.
    (b) La resistenza agli attacchi di preimmagine e di collisione.
    (c) La suriettività.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Tema 43

Lunedì 4 giugno 2018

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 11$ e sul generatore $g = 7$.

1.1) Supponendo che Alice scelga il valore segreto $a = 9$ e Bob il valore $b = 4$, descrivere lo scambio di informazioni che avviene fra i due interlocutori.

1.2) Calcolare la chiave condivisa K utilizzando la formula più conveniente fra quella usata da Alice e quella usata da Bob.

Esercizio 2

Il server web di Alice dispone di un sistema di login basato su username e password; per comodità, assumiamo che le password siano stringhe di bit.
Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile: si assuma che utilizzi una stringa casuale di 64 bit.
Il server applica alle password degli utenti una funzione hash crittografica H che genera un valore a 28 bit. In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 28 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.

Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H, ma che sappia che Bob utilizza una password di 64 bit. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login verso il server ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password, portandola a 128 bit casuali.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash in locale (nel computer di Charlie) richieda un miliardesimo di secondo.
Le risposte alle domande 2.1 e 2.2 cambiano?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave privata del richiedente.
   (b) Il common name del richiedente.
   (c) La chiave pubblica del richiedente.
2. Quale, tra i seguenti, è un possibile problema del cifrario RSA?
   (a) La lentezza in rapporto ai cifrari a chiave condivisa.
   (b) La possibilità di un attacco Man-in-the-Middle.
   (c) La difficoltà di trovare numeri primi di dimensioni sufficienti.
3. Quale delle seguenti proprietà **non** è posseduta da nessuna funzione hash crittografica?
   (a) L'iniettività.
   (b) La resistenza agli attacchi di preimmagine e di collisione.
   (c) La suriettività.
4. Un certificato di firma digitale solitamente accompagna...
   (a) ...una chiave di sessione, e ne garantisce l'autenticità.
   (b) ...una chiave pubblica, e garantisce l'identità del possessore della corrispondente chiave privata.
   (c) ...una chiave privata, e garantisce l'identità del possessore della corrispondente chiave pubblica.
5. Quale delle seguenti proprietà è necessaria affinché una funzione hash sia crittograficamente sicura?
   (a) L'iniettività.
   (b) La suriettività.
   (c) La resistenza agli attacchi di preimmagine e di collisione.
6. Alice e Bob avviano una sessione Diffie-Hellman; per decifrare la chiave di sessione, Charlie (in ascolto sul canale ma non in grado di interferire) deve...
   (a) ...fattorizzare un grande prodotto di numeri primi.
   (b) ...trovare una collisione in un valore hash crittografico.
   (c) ...risolvere un problema di logaritmo discreto.
7. Quale proprietà caratterizza i cifrari a flusso?
   (a) Non richiedono che gli interlocutori abbiano concordato e condiviso una chiave.
   (b) Sono necessariamente interattivi.
   (c) Combinano i dati da cifrare con un flusso potenzialmente infinito di dati (pseudo-) casuali.
8. Quale delle seguenti proprietà è necessaria per una funzione di cifratura?
   (a) L'iniettività.
   (b) La resistenza agli attacchi di preimmagine e di collisione.
   (c) La suriettività.
9. Quale, tra i seguenti, è un possibile problema del protocollo Diffie-Hellman?
   (a) La possibilità di un attacco Man-in-the-Middle.
   (b) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (c) La lentezza in rapporto ai cifrari a chiave condivisa.
10. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
    (a) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
    (b) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
    (c) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Tema 44

Lunedì 4 giugno 2018

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 11$ e sul generatore $g = 7$.

1.1) Supponendo che Alice scelga il valore segreto $a = 9$ e Bob il valore $b = 3$, descrivere lo scambio di informazioni che avviene fra i due interlocutori.

1.2) Calcolare la chiave condivisa K utilizzando la formula più conveniente fra quella usata da Alice e quella usata da Bob.

Esercizio 2

Il server web di Alice dispone di un sistema di login basato su username e password; per comodità, assumiamo che le password siano stringhe di bit.
Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile: si assuma che utilizzi una stringa casuale di 64 bit.
Il server applica alle password degli utenti una funzione hash crittografica H che genera un valore a 24 bit. In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 24 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.

Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H, ma che sappia che Bob utilizza una password di 64 bit. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login verso il server ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password, portandola a 128 bit casuali.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash in locale (nel computer di Charlie) richieda un miliardesimo di secondo.
Le risposte alle domande 2.1 e 2.2 cambiano?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) Il common name del richiedente.
   (b) La chiave pubblica del richiedente.
   (c) La chiave privata del richiedente.
2. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (b) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (c) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
3. Alice e Bob avviano una sessione Diffie-Hellman; per decifrare la chiave di sessione, Charlie (in ascolto sul canale ma non in grado di interferire) deve...
   (a) ...risolvere un problema di logaritmo discreto.
   (b) ...fattorizzare un grande prodotto di numeri primi.
   (c) ...trovare una collisione in un valore hash crittografico.
4. Quale delle seguenti proprietà **non** è posseduta da nessuna funzione hash crittografica?
   (a) L'iniettività.
   (b) La resistenza agli attacchi di preimmagine e di collisione.
   (c) La suriettività.
5. Quale, tra i seguenti, è un possibile problema del protocollo Diffie-Hellman?
   (a) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (b) La possibilità di un attacco Man-in-the-Middle.
   (c) La lentezza in rapporto ai cifrari a chiave condivisa.
6. Quale proprietà caratterizza i cifrari a flusso?
   (a) Non richiedono che gli interlocutori abbiano concordato e condiviso una chiave.
   (b) Sono necessariamente interattivi.
   (c) Combinano i dati da cifrare con un flusso potenzialmente infinito di dati (pseudo-) casuali.
7. Un certificato di firma digitale solitamente accompagna...
   (a) ...una chiave pubblica, e garantisce l'identità del possessore della corrispondente chiave privata.
   (b) ...una chiave privata, e garantisce l'identità del possessore della corrispondente chiave pubblica.
   (c) ...una chiave di sessione, e ne garantisce l'autenticità.
8. Quale delle seguenti proprietà è necessaria affinché una funzione hash sia crittograficamente sicura?
   (a) La suriettività.
   (b) La resistenza agli attacchi di preimmagine e di collisione.
   (c) L'iniettività.
9. Quale, tra i seguenti, è un possibile problema del cifrario RSA?
   (a) La possibilità di un attacco Man-in-the-Middle.
   (b) La lentezza in rapporto ai cifrari a chiave condivisa.
   (c) La difficoltà di trovare numeri primi di dimensioni sufficienti.
10. Quale delle seguenti proprietà è necessaria per una funzione di cifratura?
    (a) La resistenza agli attacchi di preimmagine e di collisione.
    (b) La suriettività.
    (c) L'iniettività.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Tema 45

Lunedì 4 giugno 2018

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 11$ e sul generatore $g = 8$.

1.1) Supponendo che Alice scelga il valore segreto $a = 7$ e Bob il valore $b = 4$, descrivere lo scambio di informazioni che avviene fra i due interlocutori.

1.2) Calcolare la chiave condivisa K utilizzando la formula più conveniente fra quella usata da Alice e quella usata da Bob.

Esercizio 2

Il server web di Alice dispone di un sistema di login basato su username e password; per comodità, assumiamo che le password siano stringhe di bit.
Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile: si assuma che utilizzi una stringa casuale di 64 bit.
Il server applica alle password degli utenti una funzione hash crittografica H che genera un valore a 32 bit. In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 32 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.

Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H, ma che sappia che Bob utilizza una password di 64 bit. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login verso il server ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password, portandola a 128 bit casuali.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash in locale (nel computer di Charlie) richieda un miliardesimo di secondo.
Le risposte alle domande 2.1 e 2.2 cambiano?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Alice e Bob avviano una sessione Diffie-Hellman; per decifrare la chiave di sessione, Charlie (in ascolto sul canale ma non in grado di interferire) deve...
   (a) ...fattorizzare un grande prodotto di numeri primi.
   (b) ...trovare una collisione in un valore hash crittografico.
   (c) ...risolvere un problema di logaritmo discreto.
2. Quale, tra i seguenti, è un possibile problema del protocollo Diffie-Hellman?
   (a) La possibilità di un attacco Man-in-the-Middle.
   (b) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (c) La lentezza in rapporto ai cifrari a chiave condivisa.
3. Quale delle seguenti proprietà è necessaria per una funzione di cifratura?
   (a) La resistenza agli attacchi di preimmagine e di collisione.
   (b) L'iniettività.
   (c) La suriettività.
4. Quale, tra i seguenti, è un possibile problema del cifrario RSA?
   (a) La lentezza in rapporto ai cifrari a chiave condivisa.
   (b) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (c) La possibilità di un attacco Man-in-the-Middle.
5. Un certificato di firma digitale solitamente accompagna...
   (a) ...una chiave pubblica, e garantisce l'identità del possessore della corrispondente chiave privata.
   (b) ...una chiave di sessione, e ne garantisce l'autenticità.
   (c) ...una chiave privata, e garantisce l'identità del possessore della corrispondente chiave pubblica.
6. Quale delle seguenti proprietà è necessaria affinché una funzione hash sia crittograficamente sicura?
   (a) La suriettività.
   (b) La resistenza agli attacchi di preimmagine e di collisione.
   (c) L'iniettività.
7. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (b) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (c) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
8. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave pubblica del richiedente.
   (b) Il common name del richiedente.
   (c) La chiave privata del richiedente.
9. Quale proprietà caratterizza i cifrari a flusso?
   (a) Combinano i dati da cifrare con un flusso potenzialmente infinito di dati (pseudo-) casuali.
   (b) Non richiedono che gli interlocutori abbiano concordato e condiviso una chiave.
   (c) Sono necessariamente interattivi.
10. Quale delle seguenti proprietà **non** è posseduta da nessuna funzione hash crittografica?
    (a) La suriettività.
    (b) L'iniettività.
    (c) La resistenza agli attacchi di preimmagine e di collisione.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Tema 46

Lunedì 4 giugno 2018

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 11$ e sul generatore $g = 8$.

1.1) Supponendo che Alice scelga il valore segreto $a = 7$ e Bob il valore $b = 2$, descrivere lo scambio di informazioni che avviene fra i due interlocutori.

1.2) Calcolare la chiave condivisa K utilizzando la formula più conveniente fra quella usata da Alice e quella usata da Bob.

Esercizio 2

Il server web di Alice dispone di un sistema di login basato su username e password; per comodità, assumiamo che le password siano stringhe di bit.
Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile: si assuma che utilizzi una stringa casuale di 64 bit.
Il server applica alle password degli utenti una funzione hash crittografica H che genera un valore a 32 bit. In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 32 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.

Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H, ma che sappia che Bob utilizza una password di 64 bit. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login verso il server ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password, portandola a 128 bit casuali.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash in locale (nel computer di Charlie) richieda un miliardesimo di secondo.
Le risposte alle domande 2.1 e 2.2 cambiano?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Alice e Bob avviano una sessione Diffie-Hellman; per decifrare la chiave di sessione, Charlie (in ascolto sul canale ma non in grado di interferire) deve...
   (a) ...fattorizzare un grande prodotto di numeri primi.
   (b) ...risolvere un problema di logaritmo discreto.
   (c) ...trovare una collisione in un valore hash crittografico.
2. Quale delle seguenti proprietà è necessaria per una funzione di cifratura?
   (a) La resistenza agli attacchi di preimmagine e di collisione.
   (b) La suriettività.
   (c) L'iniettività.
3. Quale delle seguenti proprietà è necessaria affinché una funzione hash sia crittograficamente sicura?
   (a) La resistenza agli attacchi di preimmagine e di collisione.
   (b) L'iniettività.
   (c) La suriettività.
4. Quale delle seguenti proprietà **non** è posseduta da nessuna funzione hash crittografica?
   (a) La suriettività.
   (b) La resistenza agli attacchi di preimmagine e di collisione.
   (c) L'iniettività.
5. Quale, tra i seguenti, è un possibile problema del protocollo Diffie-Hellman?
   (a) La possibilità di un attacco Man-in-the-Middle.
   (b) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (c) La lentezza in rapporto ai cifrari a chiave condivisa.
6. Un certificato di firma digitale solitamente accompagna...
   (a) ...una chiave di sessione, e ne garantisce l'autenticità.
   (b) ...una chiave privata, e garantisce l'identità del possessore della corrispondente chiave pubblica.
   (c) ...una chiave pubblica, e garantisce l'identità del possessore della corrispondente chiave privata.
7. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave pubblica del richiedente.
   (b) La chiave privata del richiedente.
   (c) Il common name del richiedente.
8. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (b) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (c) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
9. Quale, tra i seguenti, è un possibile problema del cifrario RSA?
   (a) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (b) La lentezza in rapporto ai cifrari a chiave condivisa.
   (c) La possibilità di un attacco Man-in-the-Middle.
10. Quale proprietà caratterizza i cifrari a flusso?
    (a) Sono necessariamente interattivi.
    (b) Non richiedono che gli interlocutori abbiano concordato e condiviso una chiave.
    (c) Combinano i dati da cifrare con un flusso potenzialmente infinito di dati (pseudo-) casuali.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Tema 47

Lunedì 4 giugno 2018

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 11$ e sul generatore $g = 8$.

1.1) Supponendo che Alice scelga il valore segreto $a = 9$ e Bob il valore $b = 4$, descrivere lo scambio di informazioni che avviene fra i due interlocutori.

1.2) Calcolare la chiave condivisa K utilizzando la formula più conveniente fra quella usata da Alice e quella usata da Bob.

Esercizio 2

Il server web di Alice dispone di un sistema di login basato su username e password; per comodità, assumiamo che le password siano stringhe di bit.
Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile: si assuma che utilizzi una stringa casuale di 64 bit.
Il server applica alle password degli utenti una funzione hash crittografica H che genera un valore a 30 bit. In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 30 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.

Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H, ma che sappia che Bob utilizza una password di 64 bit. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login verso il server ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password, portandola a 128 bit casuali.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash in locale (nel computer di Charlie) richieda un miliardesimo di secondo.
Le risposte alle domande 2.1 e 2.2 cambiano?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) Il common name del richiedente.
   (b) La chiave pubblica del richiedente.
   (c) La chiave privata del richiedente.
2. Quale, tra i seguenti, è un possibile problema del cifrario RSA?
   (a) La possibilità di un attacco Man-in-the-Middle.
   (b) La lentezza in rapporto ai cifrari a chiave condivisa.
   (c) La difficoltà di trovare numeri primi di dimensioni sufficienti.
3. Quale delle seguenti proprietà è necessaria per una funzione di cifratura?
   (a) L'iniettività.
   (b) La resistenza agli attacchi di preimmagine e di collisione.
   (c) La suriettività.
4. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (b) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (c) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
5. Quale proprietà caratterizza i cifrari a flusso?
   (a) Sono necessariamente interattivi.
   (b) Combinano i dati da cifrare con un flusso potenzialmente infinito di dati (pseudo-) casuali.
   (c) Non richiedono che gli interlocutori abbiano concordato e condiviso una chiave.
6. Quale delle seguenti proprietà è necessaria affinché una funzione hash sia crittograficamente sicura?
   (a) La resistenza agli attacchi di preimmagine e di collisione.
   (b) L'iniettività.
   (c) La suriettività.
7. Quale delle seguenti proprietà **non** è posseduta da nessuna funzione hash crittografica?
   (a) La suriettività.
   (b) La resistenza agli attacchi di preimmagine e di collisione.
   (c) L'iniettività.
8. Alice e Bob avviano una sessione Diffie-Hellman; per decifrare la chiave di sessione, Charlie (in ascolto sul canale ma non in grado di interferire) deve...
   (a) ...risolvere un problema di logaritmo discreto.
   (b) ...fattorizzare un grande prodotto di numeri primi.
   (c) ...trovare una collisione in un valore hash crittografico.
9. Quale, tra i seguenti, è un possibile problema del protocollo Diffie-Hellman?
   (a) La possibilità di un attacco Man-in-the-Middle.
   (b) La lentezza in rapporto ai cifrari a chiave condivisa.
   (c) La difficoltà di trovare numeri primi di dimensioni sufficienti.
10. Un certificato di firma digitale solitamente accompagna...
    (a) ...una chiave pubblica, e garantisce l'identità del possessore della corrispondente chiave privata.
    (b) ...una chiave di sessione, e ne garantisce l'autenticità.
    (c) ...una chiave privata, e garantisce l'identità del possessore della corrispondente chiave pubblica.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Tema 48

Lunedì 4 giugno 2018

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 11$ e sul generatore $g = 6$.

1.1) Supponendo che Alice scelga il valore segreto $a = 9$ e Bob il valore $b = 2$, descrivere lo scambio di informazioni che avviene fra i due interlocutori.

1.2) Calcolare la chiave condivisa K utilizzando la formula più conveniente fra quella usata da Alice e quella usata da Bob.

Esercizio 2

Il server web di Alice dispone di un sistema di login basato su username e password; per comodità, assumiamo che le password siano stringhe di bit.
Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile: si assuma che utilizzi una stringa casuale di 64 bit.
Il server applica alle password degli utenti una funzione hash crittografica H che genera un valore a 32 bit. In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 32 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.

Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H, ma che sappia che Bob utilizza una password di 64 bit. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login verso il server ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password, portandola a 128 bit casuali.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash in locale (nel computer di Charlie) richieda un miliardesimo di secondo.
Le risposte alle domande 2.1 e 2.2 cambiano?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Quale proprietà caratterizza i cifrari a flusso?
   (a) Combinano i dati da cifrare con un flusso potenzialmente infinito di dati (pseudo-) casuali.
   (b) Sono necessariamente interattivi.
   (c) Non richiedono che gli interlocutori abbiano concordato e condiviso una chiave.
2. Quale, tra i seguenti, è un possibile problema del cifrario RSA?
   (a) La lentezza in rapporto ai cifrari a chiave condivisa.
   (b) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (c) La possibilità di un attacco Man-in-the-Middle.
3. Quale delle seguenti proprietà è necessaria affinché una funzione hash sia crittograficamente sicura?
   (a) La suriettività.
   (b) L'iniettività.
   (c) La resistenza agli attacchi di preimmagine e di collisione.
4. Quale, tra i seguenti, è un possibile problema del protocollo Diffie-Hellman?
   (a) La possibilità di un attacco Man-in-the-Middle.
   (b) La lentezza in rapporto ai cifrari a chiave condivisa.
   (c) La difficoltà di trovare numeri primi di dimensioni sufficienti.
5. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (b) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (c) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
6. Quale delle seguenti proprietà **non** è posseduta da nessuna funzione hash crittografica?
   (a) L'iniettività.
   (b) La resistenza agli attacchi di preimmagine e di collisione.
   (c) La suriettività.
7. Un certificato di firma digitale solitamente accompagna...
   (a) ...una chiave privata, e garantisce l'identità del possessore della corrispondente chiave pubblica.
   (b) ...una chiave di sessione, e ne garantisce l'autenticità.
   (c) ...una chiave pubblica, e garantisce l'identità del possessore della corrispondente chiave privata.
8. Alice e Bob avviano una sessione Diffie-Hellman; per decifrare la chiave di sessione, Charlie (in ascolto sul canale ma non in grado di interferire) deve...
   (a) ...trovare una collisione in un valore hash crittografico.
   (b) ...fattorizzare un grande prodotto di numeri primi.
   (c) ...risolvere un problema di logaritmo discreto.
9. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave pubblica del richiedente.
   (b) Il common name del richiedente.
   (c) La chiave privata del richiedente.
10. Quale delle seguenti proprietà è necessaria per una funzione di cifratura?
    (a) L'iniettività.
    (b) La suriettività.
    (c) La resistenza agli attacchi di preimmagine e di collisione.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Tema 49

Lunedì 4 giugno 2018

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 13$ e sul generatore $g = 6$.

1.1) Supponendo che Alice scelga il valore segreto $a = 10$ e Bob il valore $b = 5$, descrivere lo scambio di informazioni che avviene fra i due interlocutori.

1.2) Calcolare la chiave condivisa K utilizzando la formula più conveniente fra quella usata da Alice e quella usata da Bob.

Esercizio 2

Il server web di Alice dispone di un sistema di login basato su username e password; per comodità, assumiamo che le password siano stringhe di bit.
Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile: si assuma che utilizzi una stringa casuale di 64 bit.
Il server applica alle password degli utenti una funzione hash crittografica H che genera un valore a 32 bit. In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 32 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.

Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H, ma che sappia che Bob utilizza una password di 64 bit. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login verso il server ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password, portandola a 128 bit casuali.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash in locale (nel computer di Charlie) richieda un miliardesimo di secondo.
Le risposte alle domande 2.1 e 2.2 cambiano?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Quale delle seguenti proprietà è necessaria affinché una funzione hash sia crittograficamente sicura?
   (a) La suriettività.
   (b) L'iniettività.
   (c) La resistenza agli attacchi di preimmagine e di collisione.
2. Quale delle seguenti proprietà è necessaria per una funzione di cifratura?
   (a) La resistenza agli attacchi di preimmagine e di collisione.
   (b) L'iniettività.
   (c) La suriettività.
3. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave pubblica del richiedente.
   (b) La chiave privata del richiedente.
   (c) Il common name del richiedente.
4. Quale, tra i seguenti, è un possibile problema del cifrario RSA?
   (a) La possibilità di un attacco Man-in-the-Middle.
   (b) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (c) La lentezza in rapporto ai cifrari a chiave condivisa.
5. Quale proprietà caratterizza i cifrari a flusso?
   (a) Combinano i dati da cifrare con un flusso potenzialmente infinito di dati (pseudo-) casuali.
   (b) Non richiedono che gli interlocutori abbiano concordato e condiviso una chiave.
   (c) Sono necessariamente interattivi.
6. Un certificato di firma digitale solitamente accompagna...
   (a) ...una chiave di sessione, e ne garantisce l'autenticità.
   (b) ...una chiave privata, e garantisce l'identità del possessore della corrispondente chiave pubblica.
   (c) ...una chiave pubblica, e garantisce l'identità del possessore della corrispondente chiave privata.
7. Quale, tra i seguenti, è un possibile problema del protocollo Diffie-Hellman?
   (a) La lentezza in rapporto ai cifrari a chiave condivisa.
   (b) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (c) La possibilità di un attacco Man-in-the-Middle.
8. Quale delle seguenti proprietà **non** è posseduta da nessuna funzione hash crittografica?
   (a) La resistenza agli attacchi di preimmagine e di collisione.
   (b) La suriettività.
   (c) L'iniettività.
9. Alice e Bob avviano una sessione Diffie-Hellman; per decifrare la chiave di sessione, Charlie (in ascolto sul canale ma non in grado di interferire) deve...
   (a) ...fattorizzare un grande prodotto di numeri primi.
   (b) ...risolvere un problema di logaritmo discreto.
   (c) ...trovare una collisione in un valore hash crittografico.
10. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
    (a) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
    (b) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
    (c) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Tema 50

Lunedì 4 giugno 2018

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 13$ e sul generatore $g = 7$.

1.1) Supponendo che Alice scelga il valore segreto $a = 11$ e Bob il valore $b = 2$, descrivere lo scambio di informazioni che avviene fra i due interlocutori.

1.2) Calcolare la chiave condivisa K utilizzando la formula più conveniente fra quella usata da Alice e quella usata da Bob.

Esercizio 2

Il server web di Alice dispone di un sistema di login basato su username e password; per comodità, assumiamo che le password siano stringhe di bit.
Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile: si assuma che utilizzi una stringa casuale di 64 bit.
Il server applica alle password degli utenti una funzione hash crittografica H che genera un valore a 28 bit. In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 28 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.

Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H, ma che sappia che Bob utilizza una password di 64 bit. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login verso il server ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password, portandola a 128 bit casuali.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash in locale (nel computer di Charlie) richieda un miliardesimo di secondo.
Le risposte alle domande 2.1 e 2.2 cambiano?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (b) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (c) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
2. Quale delle seguenti proprietà è necessaria affinché una funzione hash sia crittograficamente sicura?
   (a) La resistenza agli attacchi di preimmagine e di collisione.
   (b) L'iniettività.
   (c) La suriettività.
3. Quale proprietà caratterizza i cifrari a flusso?
   (a) Combinano i dati da cifrare con un flusso potenzialmente infinito di dati (pseudo-) casuali.
   (b) Sono necessariamente interattivi.
   (c) Non richiedono che gli interlocutori abbiano concordato e condiviso una chiave.
4. Quale, tra i seguenti, è un possibile problema del protocollo Diffie-Hellman?
   (a) La lentezza in rapporto ai cifrari a chiave condivisa.
   (b) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (c) La possibilità di un attacco Man-in-the-Middle.
5. Quale delle seguenti proprietà **non** è posseduta da nessuna funzione hash crittografica?
   (a) La suriettività.
   (b) La resistenza agli attacchi di preimmagine e di collisione.
   (c) L'iniettività.
6. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave privata del richiedente.
   (b) Il common name del richiedente.
   (c) La chiave pubblica del richiedente.
7. Alice e Bob avviano una sessione Diffie-Hellman; per decifrare la chiave di sessione, Charlie (in ascolto sul canale ma non in grado di interferire) deve...
   (a) ... trovare una collisione in un valore hash crittografico.
   (b) ... fattorizzare un grande prodotto di numeri primi.
   (c) ... risolvere un problema di logaritmo discreto.
8. Quale, tra i seguenti, è un possibile problema del cifrario RSA?
   (a) La possibilità di un attacco Man-in-the-Middle.
   (b) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (c) La lentezza in rapporto ai cifrari a chiave condivisa.
9. Quale delle seguenti proprietà è necessaria per una funzione di cifratura?
   (a) La resistenza agli attacchi di preimmagine e di collisione.
   (b) L'iniettività.
   (c) La suriettività.
10. Un certificato di firma digitale solitamente accompagna...
    (a) ... una chiave privata, e garantisce l'identità del possessore della corrispondente chiave pubblica.
    (b) ... una chiave di sessione, e ne garantisce l'autenticità.
    (c) ... una chiave pubblica, e garantisce l'identità del possessore della corrispondente chiave privata.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Tema 51

Lunedì 4 giugno 2018

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 13$ e sul generatore $g = 6$.

1.1) Supponendo che Alice scelga il valore segreto $a = 10$ e Bob il valore $b = 3$, descrivere lo scambio di informazioni che avviene fra i due interlocutori.

1.2) Calcolare la chiave condivisa K utilizzando la formula più conveniente fra quella usata da Alice e quella usata da Bob.

Esercizio 2

Il server web di Alice dispone di un sistema di login basato su username e password; per comodità, assumiamo che le password siano stringhe di bit.
Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile: si assuma che utilizzi una stringa casuale di 64 bit.
Il server applica alle password degli utenti una funzione hash crittografica H che genera un valore a 30 bit. In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 30 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.

Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H, ma che sappia che Bob utilizza una password di 64 bit. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login verso il server ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password, portandola a 128 bit casuali.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash in locale (nel computer di Charlie) richieda un miliardesimo di secondo.
Le risposte alle domande 2.1 e 2.2 cambiano?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Quale, tra i seguenti, è un possibile problema del protocollo Diffie-Hellman?
   (a) La possibilità di un attacco Man-in-the-Middle.
   (b) La lentezza in rapporto ai cifrari a chiave condivisa.
   (c) La difficoltà di trovare numeri primi di dimensioni sufficienti.
2. Un certificato di firma digitale solitamente accompagna...
   (a) ...una chiave privata, e garantisce l'identità del possessore della corrispondente chiave pubblica.
   (b) ...una chiave pubblica, e garantisce l'identità del possessore della corrispondente chiave privata.
   (c) ...una chiave di sessione, e ne garantisce l'autenticità.
3. Quale delle seguenti proprietà **non** è posseduta da nessuna funzione hash crittografica?
   (a) La suriettività.
   (b) La resistenza agli attacchi di preimmagine e di collisione.
   (c) L'iniettività.
4. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave pubblica del richiedente.
   (b) La chiave privata del richiedente.
   (c) Il common name del richiedente.
5. Quale proprietà caratterizza i cifrari a flusso?
   (a) Non richiedono che gli interlocutori abbiano concordato e condiviso una chiave.
   (b) Sono necessariamente interattivi.
   (c) Combinano i dati da cifrare con un flusso potenzialmente infinito di dati (pseudo-) casuali.
6. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (b) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (c) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
7. Quale delle seguenti proprietà è necessaria per una funzione di cifratura?
   (a) L'iniettività.
   (b) La suriettività.
   (c) La resistenza agli attacchi di preimmagine e di collisione.
8. Quale, tra i seguenti, è un possibile problema del cifrario RSA?
   (a) La possibilità di un attacco Man-in-the-Middle.
   (b) La lentezza in rapporto ai cifrari a chiave condivisa.
   (c) La difficoltà di trovare numeri primi di dimensioni sufficienti.
9. Quale delle seguenti proprietà è necessaria affinché una funzione hash sia crittograficamente sicura?
   (a) La resistenza agli attacchi di preimmagine e di collisione.
   (b) La suriettività.
   (c) L'iniettività.
10. Alice e Bob avviano una sessione Diffie-Hellman; per decifrare la chiave di sessione, Charlie (in ascolto sul canale ma non in grado di interferire) deve...
    (a) ...risolvere un problema di logaritmo discreto.
    (b) ...fattorizzare un grande prodotto di numeri primi.
    (c) ...trovare una collisione in un valore hash crittografico.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Tema 52

Lunedì 4 giugno 2018

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 13$ e sul generatore $g = 7$.

1.1) Supponendo che Alice scelga il valore segreto $a = 11$ e Bob il valore $b = 5$, descrivere lo scambio di informazioni che avviene fra i due interlocutori.

1.2) Calcolare la chiave condivisa K utilizzando la formula più conveniente fra quella usata da Alice e quella usata da Bob.

Esercizio 2

Il server web di Alice dispone di un sistema di login basato su username e password; per comodità, assumiamo che le password siano stringhe di bit.
Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile: si assuma che utilizzi una stringa casuale di 64 bit.
Il server applica alle password degli utenti una funzione hash crittografica H che genera un valore a 24 bit. In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 24 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.

Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H, ma che sappia che Bob utilizza una password di 64 bit. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login verso il server ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password, portandola a 128 bit casuali.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash in locale (nel computer di Charlie) richieda un miliardesimo di secondo.
Le risposte alle domande 2.1 e 2.2 cambiano?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Alice e Bob avviano una sessione Diffie-Hellman; per decifrare la chiave di sessione, Charlie (in ascolto sul canale ma non in grado di interferire) deve...
   (a) ...risolvere un problema di logaritmo discreto.
   (b) ...fattorizzare un grande prodotto di numeri primi.
   (c) ...trovare una collisione in un valore hash crittografico.
2. Quale proprietà caratterizza i cifrari a flusso?
   (a) Combinano i dati da cifrare con un flusso potenzialmente infinito di dati (pseudo-) casuali.
   (b) Non richiedono che gli interlocutori abbiano concordato e condiviso una chiave.
   (c) Sono necessariamente interattivi.
3. Un certificato di firma digitale solitamente accompagna...
   (a) ...una chiave pubblica, e garantisce l'identità del possessore della corrispondente chiave privata.
   (b) ...una chiave privata, e garantisce l'identità del possessore della corrispondente chiave pubblica.
   (c) ...una chiave di sessione, e ne garantisce l'autenticità.
4. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave pubblica del richiedente.
   (b) Il common name del richiedente.
   (c) La chiave privata del richiedente.
5. Quale, tra i seguenti, è un possibile problema del cifrario RSA?
   (a) La lentezza in rapporto ai cifrari a chiave condivisa.
   (b) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (c) La possibilità di un attacco Man-in-the-Middle.
6. Quale, tra i seguenti, è un possibile problema del protocollo Diffie-Hellman?
   (a) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (b) La lentezza in rapporto ai cifrari a chiave condivisa.
   (c) La possibilità di un attacco Man-in-the-Middle.
7. Quale delle seguenti proprietà è necessaria affinché una funzione hash sia crittograficamente sicura?
   (a) La suriettività.
   (b) L'iniettività.
   (c) La resistenza agli attacchi di preimmagine e di collisione.
8. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (b) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (c) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
9. Quale delle seguenti proprietà **non** è posseduta da nessuna funzione hash crittografica?
   (a) L'iniettività.
   (b) La resistenza agli attacchi di preimmagine e di collisione.
   (c) La suriettività.
10. Quale delle seguenti proprietà è necessaria per una funzione di cifratura?
    (a) La suriettività.
    (b) La resistenza agli attacchi di preimmagine e di collisione.
    (c) L'iniettività.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Tema 53

Lunedì 4 giugno 2018

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 11$ e sul generatore $g = 8$.

1.1) Supponendo che Alice scelga il valore segreto $a = 7$ e Bob il valore $b = 2$, descrivere lo scambio di informazioni che avviene fra i due interlocutori.

1.2) Calcolare la chiave condivisa K utilizzando la formula più conveniente fra quella usata da Alice e quella usata da Bob.

Esercizio 2

Il server web di Alice dispone di un sistema di login basato su username e password; per comodità, assumiamo che le password siano stringhe di bit.
Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile: si assuma che utilizzi una stringa casuale di 64 bit.
Il server applica alle password degli utenti una funzione hash crittografica H che genera un valore a 28 bit. In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 28 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.

Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H, ma che sappia che Bob utilizza una password di 64 bit. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login verso il server ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password, portandola a 128 bit casuali.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash in locale (nel computer di Charlie) richieda un miliardesimo di secondo.
Le risposte alle domande 2.1 e 2.2 cambiano?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Quale delle seguenti proprietà è necessaria per una funzione di cifratura?
   (a) La suriettività.
   (b) La resistenza agli attacchi di preimmagine e di collisione.
   (c) L'iniettività.
2. Quale proprietà caratterizza i cifrari a flusso?
   (a) Non richiedono che gli interlocutori abbiano concordato e condiviso una chiave.
   (b) Sono necessariamente interattivi.
   (c) Combinano i dati da cifrare con un flusso potenzialmente infinito di dati (pseudo-) casuali.
3. Alice e Bob avviano una sessione Diffie-Hellman; per decifrare la chiave di sessione, Charlie (in ascolto sul canale ma non in grado di interferire) deve...
   (a) ...trovare una collisione in un valore hash crittografico.
   (b) ...fattorizzare un grande prodotto di numeri primi.
   (c) ...risolvere un problema di logaritmo discreto.
4. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (b) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (c) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
5. Quale, tra i seguenti, è un possibile problema del cifrario RSA?
   (a) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (b) La lentezza in rapporto ai cifrari a chiave condivisa.
   (c) La possibilità di un attacco Man-in-the-Middle.
6. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave pubblica del richiedente.
   (b) Il common name del richiedente.
   (c) La chiave privata del richiedente.
7. Quale, tra i seguenti, è un possibile problema del protocollo Diffie-Hellman?
   (a) La lentezza in rapporto ai cifrari a chiave condivisa.
   (b) La possibilità di un attacco Man-in-the-Middle.
   (c) La difficoltà di trovare numeri primi di dimensioni sufficienti.
8. Un certificato di firma digitale solitamente accompagna...
   (a) ...una chiave pubblica, e garantisce l'identità del possessore della corrispondente chiave privata.
   (b) ...una chiave di sessione, e ne garantisce l'autenticità.
   (c) ...una chiave privata, e garantisce l'identità del possessore della corrispondente chiave pubblica.
9. Quale delle seguenti proprietà **non** è posseduta da nessuna funzione hash crittografica?
   (a) L'iniettività.
   (b) La resistenza agli attacchi di preimmagine e di collisione.
   (c) La suriettività.
10. Quale delle seguenti proprietà è necessaria affinché una funzione hash sia crittograficamente sicura?
    (a) La suriettività.
    (b) L'iniettività.
    (c) La resistenza agli attacchi di preimmagine e di collisione.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Tema 54

Lunedì 4 giugno 2018

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 13$ e sul generatore $g = 7$.

1.1) Supponendo che Alice scelga il valore segreto $a = 10$ e Bob il valore $b = 4$, descrivere lo scambio di informazioni che avviene fra i due interlocutori.

1.2) Calcolare la chiave condivisa K utilizzando la formula più conveniente fra quella usata da Alice e quella usata da Bob.

Esercizio 2

Il server web di Alice dispone di un sistema di login basato su username e password; per comodità, assumiamo che le password siano stringhe di bit.
Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile: si assuma che utilizzi una stringa casuale di 64 bit.
Il server applica alle password degli utenti una funzione hash crittografica H che genera un valore a 30 bit. In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 30 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.

Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H, ma che sappia che Bob utilizza una password di 64 bit. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login verso il server ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password, portandola a 128 bit casuali.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash in locale (nel computer di Charlie) richieda un miliardesimo di secondo.
Le risposte alle domande 2.1 e 2.2 cambiano?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (b) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (c) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
2. Quale delle seguenti proprietà è necessaria per una funzione di cifratura?
   (a) L'iniettività.
   (b) La suriettività.
   (c) La resistenza agli attacchi di preimmagine e di collisione.
3. Alice e Bob avviano una sessione Diffie-Hellman; per decifrare la chiave di sessione, Charlie (in ascolto sul canale ma non in grado di interferire) deve...
   (a) ...fattorizzare un grande prodotto di numeri primi.
   (b) ...trovare una collisione in un valore hash crittografico.
   (c) ...risolvere un problema di logaritmo discreto.
4. Quale delle seguenti proprietà è necessaria affinché una funzione hash sia crittograficamente sicura?
   (a) La resistenza agli attacchi di preimmagine e di collisione.
   (b) La suriettività.
   (c) L'iniettività.
5. Quale delle seguenti proprietà **non** è posseduta da nessuna funzione hash crittografica?
   (a) La suriettività.
   (b) La resistenza agli attacchi di preimmagine e di collisione.
   (c) L'iniettività.
6. Quale, tra i seguenti, è un possibile problema del protocollo Diffie-Hellman?
   (a) La possibilità di un attacco Man-in-the-Middle.
   (b) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (c) La lentezza in rapporto ai cifrari a chiave condivisa.
7. Quale, tra i seguenti, è un possibile problema del cifrario RSA?
   (a) La possibilità di un attacco Man-in-the-Middle.
   (b) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (c) La lentezza in rapporto ai cifrari a chiave condivisa.
8. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) Il common name del richiedente.
   (b) La chiave pubblica del richiedente.
   (c) La chiave privata del richiedente.
9. Un certificato di firma digitale solitamente accompagna...
   (a) ...una chiave di sessione, e ne garantisce l'autenticità.
   (b) ...una chiave privata, e garantisce l'identità del possessore della corrispondente chiave pubblica.
   (c) ...una chiave pubblica, e garantisce l'identità del possessore della corrispondente chiave privata.
10. Quale proprietà caratterizza i cifrari a flusso?
    (a) Combinano i dati da cifrare con un flusso potenzialmente infinito di dati (pseudo-) casuali.
    (b) Non richiedono che gli interlocutori abbiano concordato e condiviso una chiave.
    (c) Sono necessariamente interattivi.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Tema 55

Lunedì 4 giugno 2018

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 11$ e sul generatore $g = 8$.

1.1) Supponendo che Alice scelga il valore segreto $a = 7$ e Bob il valore $b = 4$, descrivere lo scambio di informazioni che avviene fra i due interlocutori.

1.2) Calcolare la chiave condivisa K utilizzando la formula più conveniente fra quella usata da Alice e quella usata da Bob.

Esercizio 2

Il server web di Alice dispone di un sistema di login basato su username e password; per comodità, assumiamo che le password siano stringhe di bit.
Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile: si assuma che utilizzi una stringa casuale di 64 bit.
Il server applica alle password degli utenti una funzione hash crittografica H che genera un valore a 28 bit. In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 28 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.

Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H, ma che sappia che Bob utilizza una password di 64 bit. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login verso il server ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password, portandola a 128 bit casuali.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash in locale (nel computer di Charlie) richieda un miliardesimo di secondo.
Le risposte alle domande 2.1 e 2.2 cambiano?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Un certificato di firma digitale solitamente accompagna...
   (a) ...una chiave pubblica, e garantisce l'identità del possessore della corrispondente chiave privata.
   (b) ...una chiave di sessione, e ne garantisce l'autenticità.
   (c) ...una chiave privata, e garantisce l'identità del possessore della corrispondente chiave pubblica.
2. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave pubblica del richiedente.
   (b) La chiave privata del richiedente.
   (c) Il common name del richiedente.
3. Quale, tra i seguenti, è un possibile problema del cifrario RSA?
   (a) La lentezza in rapporto ai cifrari a chiave condivisa.
   (b) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (c) La possibilità di un attacco Man-in-the-Middle.
4. Quale delle seguenti proprietà è necessaria affinché una funzione hash sia crittograficamente sicura?
   (a) L'iniettività.
   (b) La suriettività.
   (c) La resistenza agli attacchi di preimmagine e di collisione.
5. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (b) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (c) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
6. Quale, tra i seguenti, è un possibile problema del protocollo Diffie-Hellman?
   (a) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (b) La lentezza in rapporto ai cifrari a chiave condivisa.
   (c) La possibilità di un attacco Man-in-the-Middle.
7. Quale delle seguenti proprietà **non** è posseduta da nessuna funzione hash crittografica?
   (a) L'iniettività.
   (b) La resistenza agli attacchi di preimmagine e di collisione.
   (c) La suriettività.
8. Quale proprietà caratterizza i cifrari a flusso?
   (a) Non richiedono che gli interlocutori abbiano concordato e condiviso una chiave.
   (b) Sono necessariamente interattivi.
   (c) Combinano i dati da cifrare con un flusso potenzialmente infinito di dati (pseudo-) casuali.
9. Quale delle seguenti proprietà è necessaria per una funzione di cifratura?
   (a) L'iniettività.
   (b) La resistenza agli attacchi di preimmagine e di collisione.
   (c) La suriettività.
10. Alice e Bob avviano una sessione Diffie-Hellman; per decifrare la chiave di sessione, Charlie (in ascolto sul canale ma non in grado di interferire) deve...
    (a) ...risolvere un problema di logaritmo discreto.
    (b) ...trovare una collisione in un valore hash crittografico.
    (c) ...fattorizzare un grande prodotto di numeri primi.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Tema 56

Lunedì 4 giugno 2018

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 13$ e sul generatore $g = 6$.

1.1) Supponendo che Alice scelga il valore segreto $a = 9$ e Bob il valore $b = 5$, descrivere lo scambio di informazioni che avviene fra i due interlocutori.

1.2) Calcolare la chiave condivisa K utilizzando la formula più conveniente fra quella usata da Alice e quella usata da Bob.

Esercizio 2

Il server web di Alice dispone di un sistema di login basato su username e password; per comodità, assumiamo che le password siano stringhe di bit.
Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile: si assuma che utilizzi una stringa casuale di 64 bit.
Il server applica alle password degli utenti una funzione hash crittografica H che genera un valore a 30 bit. In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 30 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.

Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H, ma che sappia che Bob utilizza una password di 64 bit. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login verso il server ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password, portandola a 128 bit casuali.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash in locale (nel computer di Charlie) richieda un miliardesimo di secondo.
Le risposte alle domande 2.1 e 2.2 cambiano?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Quale delle seguenti proprietà è necessaria affinché una funzione hash sia crittograficamente sicura?
   (a) L'iniettività.
   (b) La suriettività.
   (c) La resistenza agli attacchi di preimmagine e di collisione.
2. Quale delle seguenti proprietà **non** è posseduta da nessuna funzione hash crittografica?
   (a) La resistenza agli attacchi di preimmagine e di collisione.
   (b) L'iniettività.
   (c) La suriettività.
3. Alice e Bob avviano una sessione Diffie-Hellman; per decifrare la chiave di sessione, Charlie (in ascolto sul canale ma non in grado di interferire) deve...
   (a) ...risolvere un problema di logaritmo discreto.
   (b) ...trovare una collisione in un valore hash crittografico.
   (c) ...fattorizzare un grande prodotto di numeri primi.
4. Un certificato di firma digitale solitamente accompagna...
   (a) ...una chiave di sessione, e ne garantisce l'autenticità.
   (b) ...una chiave privata, e garantisce l'identità del possessore della corrispondente chiave pubblica.
   (c) ...una chiave pubblica, e garantisce l'identità del possessore della corrispondente chiave privata.
5. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave pubblica del richiedente.
   (b) Il common name del richiedente.
   (c) La chiave privata del richiedente.
6. Quale, tra i seguenti, è un possibile problema del protocollo Diffie-Hellman?
   (a) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (b) La lentezza in rapporto ai cifrari a chiave condivisa.
   (c) La possibilità di un attacco Man-in-the-Middle.
7. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (b) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (c) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
8. Quale, tra i seguenti, è un possibile problema del cifrario RSA?
   (a) La possibilità di un attacco Man-in-the-Middle.
   (b) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (c) La lentezza in rapporto ai cifrari a chiave condivisa.
9. Quale proprietà caratterizza i cifrari a flusso?
   (a) Non richiedono che gli interlocutori abbiano concordato e condiviso una chiave.
   (b) Combinano i dati da cifrare con un flusso potenzialmente infinito di dati (pseudo-) casuali.
   (c) Sono necessariamente interattivi.
10. Quale delle seguenti proprietà è necessaria per una funzione di cifratura?
    (a) L'iniettività.
    (b) La suriettività.
    (c) La resistenza agli attacchi di preimmagine e di collisione.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Tema 57

Lunedì 4 giugno 2018

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 13$ e sul generatore $g = 7$.

1.1) Supponendo che Alice scelga il valore segreto $a = 10$ e Bob il valore $b = 4$, descrivere lo scambio di informazioni che avviene fra i due interlocutori.

1.2) Calcolare la chiave condivisa K utilizzando la formula più conveniente fra quella usata da Alice e quella usata da Bob.

Esercizio 2

Il server web di Alice dispone di un sistema di login basato su username e password; per comodità, assumiamo che le password siano stringhe di bit.
Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile: si assuma che utilizzi una stringa casuale di 64 bit.
Il server applica alle password degli utenti una funzione hash crittografica H che genera un valore a 30 bit. In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 30 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.

Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H, ma che sappia che Bob utilizza una password di 64 bit. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login verso il server ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password, portandola a 128 bit casuali.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash in locale (nel computer di Charlie) richieda un miliardesimo di secondo.
Le risposte alle domande 2.1 e 2.2 cambiano?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (b) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (c) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
2. Quale, tra i seguenti, è un possibile problema del cifrario RSA?
   (a) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (b) La possibilità di un attacco Man-in-the-Middle.
   (c) La lentezza in rapporto ai cifrari a chiave condivisa.
3. Alice e Bob avviano una sessione Diffie-Hellman; per decifrare la chiave di sessione, Charlie (in ascolto sul canale ma non in grado di interferire) deve...
   (a) ...risolvere un problema di logaritmo discreto.
   (b) ...trovare una collisione in un valore hash crittografico.
   (c) ...fattorizzare un grande prodotto di numeri primi.
4. Un certificato di firma digitale solitamente accompagna...
   (a) ...una chiave privata, e garantisce l'identità del possessore della corrispondente chiave pubblica.
   (b) ...una chiave di sessione, e ne garantisce l'autenticità.
   (c) ...una chiave pubblica, e garantisce l'identità del possessore della corrispondente chiave privata.
5. Quale proprietà caratterizza i cifrari a flusso?
   (a) Combinano i dati da cifrare con un flusso potenzialmente infinito di dati (pseudo-) casuali.
   (b) Sono necessariamente interattivi.
   (c) Non richiedono che gli interlocutori abbiano concordato e condiviso una chiave.
6. Quale delle seguenti proprietà è necessaria per una funzione di cifratura?
   (a) L'iniettività.
   (b) La resistenza agli attacchi di preimmagine e di collisione.
   (c) La suriettività.
7. Quale delle seguenti proprietà **non** è posseduta da nessuna funzione hash crittografica?
   (a) La resistenza agli attacchi di preimmagine e di collisione.
   (b) La suriettività.
   (c) L'iniettività.
8. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) Il common name del richiedente.
   (b) La chiave privata del richiedente.
   (c) La chiave pubblica del richiedente.
9. Quale, tra i seguenti, è un possibile problema del protocollo Diffie-Hellman?
   (a) La lentezza in rapporto ai cifrari a chiave condivisa.
   (b) La possibilità di un attacco Man-in-the-Middle.
   (c) La difficoltà di trovare numeri primi di dimensioni sufficienti.
10. Quale delle seguenti proprietà è necessaria affinché una funzione hash sia crittograficamente sicura?
    (a) L'iniettività.
    (b) La suriettività.
    (c) La resistenza agli attacchi di preimmagine e di collisione.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Tema 58

Lunedì 4 giugno 2018

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 13$ e sul generatore $g = 7$.

1.1) Supponendo che Alice scelga il valore segreto $a = 10$ e Bob il valore $b = 2$, descrivere lo scambio di informazioni che avviene fra i due interlocutori.

1.2) Calcolare la chiave condivisa K utilizzando la formula più conveniente fra quella usata da Alice e quella usata da Bob.

Esercizio 2

Il server web di Alice dispone di un sistema di login basato su username e password; per comodità, assumiamo che le password siano stringhe di bit.
Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile: si assuma che utilizzi una stringa casuale di 64 bit.
Il server applica alle password degli utenti una funzione hash crittografica H che genera un valore a 26 bit. In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 26 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.

Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H, ma che sappia che Bob utilizza una password di 64 bit. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login verso il server ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password, portandola a 128 bit casuali.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash in locale (nel computer di Charlie) richieda un miliardesimo di secondo.
Le risposte alle domande 2.1 e 2.2 cambiano?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Un certificato di firma digitale solitamente accompagna...
   (a) ...una chiave di sessione, e ne garantisce l'autenticità.
   (b) ...una chiave privata, e garantisce l'identità del possessore della corrispondente chiave pubblica.
   (c) ...una chiave pubblica, e garantisce l'identità del possessore della corrispondente chiave privata.
2. Quale proprietà caratterizza i cifrari a flusso?
   (a) Combinano i dati da cifrare con un flusso potenzialmente infinito di dati (pseudo-) casuali.
   (b) Non richiedono che gli interlocutori abbiano concordato e condiviso una chiave.
   (c) Sono necessariamente interattivi.
3. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave pubblica del richiedente.
   (b) La chiave privata del richiedente.
   (c) Il common name del richiedente.
4. Quale, tra i seguenti, è un possibile problema del protocollo Diffie-Hellman?
   (a) La possibilità di un attacco Man-in-the-Middle.
   (b) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (c) La lentezza in rapporto ai cifrari a chiave condivisa.
5. Quale delle seguenti proprietà **non** è posseduta da nessuna funzione hash crittografica?
   (a) La suriettività.
   (b) L'iniettività.
   (c) La resistenza agli attacchi di preimmagine e di collisione.
6. Quale delle seguenti proprietà è necessaria per una funzione di cifratura?
   (a) L'iniettività.
   (b) La suriettività.
   (c) La resistenza agli attacchi di preimmagine e di collisione.
7. Quale, tra i seguenti, è un possibile problema del cifrario RSA?
   (a) La possibilità di un attacco Man-in-the-Middle.
   (b) La lentezza in rapporto ai cifrari a chiave condivisa.
   (c) La difficoltà di trovare numeri primi di dimensioni sufficienti.
8. Quale delle seguenti proprietà è necessaria affinché una funzione hash sia crittograficamente sicura?
   (a) La suriettività.
   (b) L'iniettività.
   (c) La resistenza agli attacchi di preimmagine e di collisione.
9. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (b) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (c) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
10. Alice e Bob avviano una sessione Diffie-Hellman; per decifrare la chiave di sessione, Charlie (in ascolto sul canale ma non in grado di interferire) deve...
    (a) ...risolvere un problema di logaritmo discreto.
    (b) ...fattorizzare un grande prodotto di numeri primi.
    (c) ...trovare una collisione in un valore hash crittografico.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Tema 59

Lunedì 4 giugno 2018

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 13$ e sul generatore $g = 6$.

1.1) Supponendo che Alice scelga il valore segreto $a = 9$ e Bob il valore $b = 5$, descrivere lo scambio di informazioni che avviene fra i due interlocutori.

1.2) Calcolare la chiave condivisa K utilizzando la formula più conveniente fra quella usata da Alice e quella usata da Bob.

Esercizio 2

Il server web di Alice dispone di un sistema di login basato su username e password; per comodità, assumiamo che le password siano stringhe di bit.
Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile: si assuma che utilizzi una stringa casuale di 64 bit.
Il server applica alle password degli utenti una funzione hash crittografica H che genera un valore a 26 bit. In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 26 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.

Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H, ma che sappia che Bob utilizza una password di 64 bit. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login verso il server ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password, portandola a 128 bit casuali.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash in locale (nel computer di Charlie) richieda un miliardesimo di secondo.
Le risposte alle domande 2.1 e 2.2 cambiano?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Quale proprietà caratterizza i cifrari a flusso?
   (a) Non richiedono che gli interlocutori abbiano concordato e condiviso una chiave.
   (b) Sono necessariamente interattivi.
   (c) Combinano i dati da cifrare con un flusso potenzialmente infinito di dati (pseudo-) casuali.
2. Quale, tra i seguenti, è un possibile problema del protocollo Diffie-Hellman?
   (a) La lentezza in rapporto ai cifrari a chiave condivisa.
   (b) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (c) La possibilità di un attacco Man-in-the-Middle.
3. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (b) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (c) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
4. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave pubblica del richiedente.
   (b) Il common name del richiedente.
   (c) La chiave privata del richiedente.
5. Alice e Bob avviano una sessione Diffie-Hellman; per decifrare la chiave di sessione, Charlie (in ascolto sul canale ma non in grado di interferire) deve...
   (a) ...risolvere un problema di logaritmo discreto.
   (b) ...fattorizzare un grande prodotto di numeri primi.
   (c) ...trovare una collisione in un valore hash crittografico.
6. Quale delle seguenti proprietà è necessaria per una funzione di cifratura?
   (a) La suriettività.
   (b) L'iniettività.
   (c) La resistenza agli attacchi di preimmagine e di collisione.
7. Quale delle seguenti proprietà **non** è posseduta da nessuna funzione hash crittografica?
   (a) L'iniettività.
   (b) La suriettività.
   (c) La resistenza agli attacchi di preimmagine e di collisione.
8. Quale delle seguenti proprietà è necessaria affinché una funzione hash sia crittograficamente sicura?
   (a) L'iniettività.
   (b) La suriettività.
   (c) La resistenza agli attacchi di preimmagine e di collisione.
9. Quale, tra i seguenti, è un possibile problema del cifrario RSA?
   (a) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (b) La lentezza in rapporto ai cifrari a chiave condivisa.
   (c) La possibilità di un attacco Man-in-the-Middle.
10. Un certificato di firma digitale solitamente accompagna...
    (a) ...una chiave pubblica, e garantisce l'identità del possessore della corrispondente chiave privata.
    (b) ...una chiave privata, e garantisce l'identità del possessore della corrispondente chiave pubblica.
    (c) ...una chiave di sessione, e ne garantisce l'autenticità.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Tema 60

Lunedì 4 giugno 2018

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 11$ e sul generatore $g = 6$.

1.1) Supponendo che Alice scelga il valore segreto $a = 8$ e Bob il valore $b = 3$, descrivere lo scambio di informazioni che avviene fra i due interlocutori.

1.2) Calcolare la chiave condivisa K utilizzando la formula più conveniente fra quella usata da Alice e quella usata da Bob.

Esercizio 2

Il server web di Alice dispone di un sistema di login basato su username e password; per comodità, assumiamo che le password siano stringhe di bit.
Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile: si assuma che utilizzi una stringa casuale di 64 bit.
Il server applica alle password degli utenti una funzione hash crittografica H che genera un valore a 24 bit. In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 24 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.

Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H, ma che sappia che Bob utilizza una password di 64 bit. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login verso il server ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password, portandola a 128 bit casuali.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash in locale (nel computer di Charlie) richieda un miliardesimo di secondo.
Le risposte alle domande 2.1 e 2.2 cambiano?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Un certificato di firma digitale solitamente accompagna...
   (a) ...una chiave pubblica, e garantisce l'identità del possessore della corrispondente chiave privata.
   (b) ...una chiave privata, e garantisce l'identità del possessore della corrispondente chiave pubblica.
   (c) ...una chiave di sessione, e ne garantisce l'autenticità.
2. Quale delle seguenti proprietà **non** è posseduta da nessuna funzione hash crittografica?
   (a) La suriettività.
   (b) La resistenza agli attacchi di preimmagine e di collisione.
   (c) L'iniettività.
3. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave privata del richiedente.
   (b) Il common name del richiedente.
   (c) La chiave pubblica del richiedente.
4. Quale delle seguenti proprietà è necessaria affinché una funzione hash sia crittograficamente sicura?
   (a) La resistenza agli attacchi di preimmagine e di collisione.
   (b) L'iniettività.
   (c) La suriettività.
5. Quale proprietà caratterizza i cifrari a flusso?
   (a) Combinano i dati da cifrare con un flusso potenzialmente infinito di dati (pseudo-) casuali.
   (b) Sono necessariamente interattivi.
   (c) Non richiedono che gli interlocutori abbiano concordato e condiviso una chiave.
6. Quale, tra i seguenti, è un possibile problema del cifrario RSA?
   (a) La lentezza in rapporto ai cifrari a chiave condivisa.
   (b) La possibilità di un attacco Man-in-the-Middle.
   (c) La difficoltà di trovare numeri primi di dimensioni sufficienti.
7. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (b) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (c) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
8. Quale delle seguenti proprietà è necessaria per una funzione di cifratura?
   (a) L'iniettività.
   (b) La resistenza agli attacchi di preimmagine e di collisione.
   (c) La suriettività.
9. Quale, tra i seguenti, è un possibile problema del protocollo Diffie-Hellman?
   (a) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (b) La lentezza in rapporto ai cifrari a chiave condivisa.
   (c) La possibilità di un attacco Man-in-the-Middle.
10. Alice e Bob avviano una sessione Diffie-Hellman; per decifrare la chiave di sessione, Charlie (in ascolto sul canale ma non in grado di interferire) deve...
    (a) ...risolvere un problema di logaritmo discreto.
    (b) ...trovare una collisione in un valore hash crittografico.
    (c) ...fattorizzare un grande prodotto di numeri primi.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Tema 61

Lunedì 4 giugno 2018

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 11$ e sul generatore $g = 6$.

1.1) Supponendo che Alice scelga il valore segreto $a = 9$ e Bob il valore $b = 4$, descrivere lo scambio di informazioni che avviene fra i due interlocutori.

1.2) Calcolare la chiave condivisa K utilizzando la formula più conveniente fra quella usata da Alice e quella usata da Bob.

Esercizio 2

Il server web di Alice dispone di un sistema di login basato su username e password; per comodità, assumiamo che le password siano stringhe di bit.
Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile: si assuma che utilizzi una stringa casuale di 64 bit.
Il server applica alle password degli utenti una funzione hash crittografica H che genera un valore a 30 bit. In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 30 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.

Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H, ma che sappia che Bob utilizza una password di 64 bit. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login verso il server ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password, portandola a 128 bit casuali.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash in locale (nel computer di Charlie) richieda un miliardesimo di secondo.
Le risposte alle domande 2.1 e 2.2 cambiano?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (b) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (c) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
2. Quale delle seguenti proprietà **non** è posseduta da nessuna funzione hash crittografica?
   (a) La suriettività.
   (b) La resistenza agli attacchi di preimmagine e di collisione.
   (c) L'iniettività.
3. Un certificato di firma digitale solitamente accompagna...
   (a) ...una chiave pubblica, e garantisce l'identità del possessore della corrispondente chiave privata.
   (b) ...una chiave di sessione, e ne garantisce l'autenticità.
   (c) ...una chiave privata, e garantisce l'identità del possessore della corrispondente chiave pubblica.
4. Quale proprietà caratterizza i cifrari a flusso?
   (a) Combinano i dati da cifrare con un flusso potenzialmente infinito di dati (pseudo-) casuali.
   (b) Sono necessariamente interattivi.
   (c) Non richiedono che gli interlocutori abbiano concordato e condiviso una chiave.
5. Quale, tra i seguenti, è un possibile problema del protocollo Diffie-Hellman?
   (a) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (b) La possibilità di un attacco Man-in-the-Middle.
   (c) La lentezza in rapporto ai cifrari a chiave condivisa.
6. Quale delle seguenti proprietà è necessaria per una funzione di cifratura?
   (a) La suriettività.
   (b) La resistenza agli attacchi di preimmagine e di collisione.
   (c) L'iniettività.
7. Alice e Bob avviano una sessione Diffie-Hellman; per decifrare la chiave di sessione, Charlie (in ascolto sul canale ma non in grado di interferire) deve...
   (a) ...risolvere un problema di logaritmo discreto.
   (b) ...fattorizzare un grande prodotto di numeri primi.
   (c) ...trovare una collisione in un valore hash crittografico.
8. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave privata del richiedente.
   (b) Il common name del richiedente.
   (c) La chiave pubblica del richiedente.
9. Quale delle seguenti proprietà è necessaria affinché una funzione hash sia crittograficamente sicura?
   (a) La suriettività.
   (b) La resistenza agli attacchi di preimmagine e di collisione.
   (c) L'iniettività.
10. Quale, tra i seguenti, è un possibile problema del cifrario RSA?
    (a) La possibilità di un attacco Man-in-the-Middle.
    (b) La lentezza in rapporto ai cifrari a chiave condivisa.
    (c) La difficoltà di trovare numeri primi di dimensioni sufficienti.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Tema 62

Lunedì 4 giugno 2018

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 13$ e sul generatore $g = 7$.

1.1) Supponendo che Alice scelga il valore segreto $a = 10$ e Bob il valore $b = 4$, descrivere lo scambio di informazioni che avviene fra i due interlocutori.

1.2) Calcolare la chiave condivisa K utilizzando la formula più conveniente fra quella usata da Alice e quella usata da Bob.

Esercizio 2

Il server web di Alice dispone di un sistema di login basato su username e password; per comodità, assumiamo che le password siano stringhe di bit.
Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile: si assuma che utilizzi una stringa casuale di 64 bit.
Il server applica alle password degli utenti una funzione hash crittografica H che genera un valore a 26 bit. In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 26 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.

Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H, ma che sappia che Bob utilizza una password di 64 bit. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login verso il server ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password, portandola a 128 bit casuali.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash in locale (nel computer di Charlie) richieda un miliardesimo di secondo.
Le risposte alle domande 2.1 e 2.2 cambiano?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Quale, tra i seguenti, è un possibile problema del cifrario RSA?
   (a) La possibilità di un attacco Man-in-the-Middle.
   (b) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (c) La lentezza in rapporto ai cifrari a chiave condivisa.
2. Quale, tra i seguenti, è un possibile problema del protocollo Diffie-Hellman?
   (a) La possibilità di un attacco Man-in-the-Middle.
   (b) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (c) La lentezza in rapporto ai cifrari a chiave condivisa.
3. Alice e Bob avviano una sessione Diffie-Hellman; per decifrare la chiave di sessione, Charlie (in ascolto sul canale ma non in grado di interferire) deve...
   (a) ...risolvere un problema di logaritmo discreto.
   (b) ...fattorizzare un grande prodotto di numeri primi.
   (c) ...trovare una collisione in un valore hash crittografico.
4. Un certificato di firma digitale solitamente accompagna...
   (a) ...una chiave privata, e garantisce l'identità del possessore della corrispondente chiave pubblica.
   (b) ...una chiave di sessione, e ne garantisce l'autenticità.
   (c) ...una chiave pubblica, e garantisce l'identità del possessore della corrispondente chiave privata.
5. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave privata del richiedente.
   (b) Il common name del richiedente.
   (c) La chiave pubblica del richiedente.
6. Quale delle seguenti proprietà è necessaria per una funzione di cifratura?
   (a) La resistenza agli attacchi di preimmagine e di collisione.
   (b) La suriettività.
   (c) L'iniettività.
7. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (b) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (c) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
8. Quale delle seguenti proprietà è necessaria affinché una funzione hash sia crittograficamente sicura?
   (a) L'iniettività.
   (b) La suriettività.
   (c) La resistenza agli attacchi di preimmagine e di collisione.
9. Quale proprietà caratterizza i cifrari a flusso?
   (a) Sono necessariamente interattivi.
   (b) Combinano i dati da cifrare con un flusso potenzialmente infinito di dati (pseudo-) casuali.
   (c) Non richiedono che gli interlocutori abbiano concordato e condiviso una chiave.
10. Quale delle seguenti proprietà **non** è posseduta da nessuna funzione hash crittografica?
    (a) La suriettività.
    (b) La resistenza agli attacchi di preimmagine e di collisione.
    (c) L'iniettività.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Tema 63

Lunedì 4 giugno 2018

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 11$ e sul generatore $g = 6$.

1.1) Supponendo che Alice scelga il valore segreto $a = 9$ e Bob il valore $b = 3$, descrivere lo scambio di informazioni che avviene fra i due interlocutori.

1.2) Calcolare la chiave condivisa K utilizzando la formula più conveniente fra quella usata da Alice e quella usata da Bob.

Esercizio 2

Il server web di Alice dispone di un sistema di login basato su username e password; per comodità, assumiamo che le password siano stringhe di bit.
Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile: si assuma che utilizzi una stringa casuale di 64 bit.
Il server applica alle password degli utenti una funzione hash crittografica H che genera un valore a 28 bit. In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 28 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.

Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H, ma che sappia che Bob utilizza una password di 64 bit. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login verso il server ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password, portandola a 128 bit casuali.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash in locale (nel computer di Charlie) richieda un miliardesimo di secondo.
Le risposte alle domande 2.1 e 2.2 cambiano?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Quale, tra i seguenti, è un possibile problema del protocollo Diffie-Hellman?
   (a) La possibilità di un attacco Man-in-the-Middle.
   (b) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (c) La lentezza in rapporto ai cifrari a chiave condivisa.
2. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) Il common name del richiedente.
   (b) La chiave pubblica del richiedente.
   (c) La chiave privata del richiedente.
3. Quale, tra i seguenti, è un possibile problema del cifrario RSA?
   (a) La lentezza in rapporto ai cifrari a chiave condivisa.
   (b) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (c) La possibilità di un attacco Man-in-the-Middle.
4. Un certificato di firma digitale solitamente accompagna...
   (a) ...una chiave privata, e garantisce l'identità del possessore della corrispondente chiave pubblica.
   (b) ...una chiave pubblica, e garantisce l'identità del possessore della corrispondente chiave privata.
   (c) ...una chiave di sessione, e ne garantisce l'autenticità.
5. Quale delle seguenti proprietà è necessaria affinché una funzione hash sia crittograficamente sicura?
   (a) La resistenza agli attacchi di preimmagine e di collisione.
   (b) La suriettività.
   (c) L'iniettività.
6. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (b) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (c) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
7. Alice e Bob avviano una sessione Diffie-Hellman; per decifrare la chiave di sessione, Charlie (in ascolto sul canale ma non in grado di interferire) deve...
   (a) ...trovare una collisione in un valore hash crittografico.
   (b) ...fattorizzare un grande prodotto di numeri primi.
   (c) ...risolvere un problema di logaritmo discreto.
8. Quale proprietà caratterizza i cifrari a flusso?
   (a) Non richiedono che gli interlocutori abbiano concordato e condiviso una chiave.
   (b) Combinano i dati da cifrare con un flusso potenzialmente infinito di dati (pseudo-) casuali.
   (c) Sono necessariamente interattivi.
9. Quale delle seguenti proprietà **non** è posseduta da nessuna funzione hash crittografica?
   (a) La suriettività.
   (b) L'iniettività.
   (c) La resistenza agli attacchi di preimmagine e di collisione.
10. Quale delle seguenti proprietà è necessaria per una funzione di cifratura?
    (a) L'iniettività.
    (b) La suriettività.
    (c) La resistenza agli attacchi di preimmagine e di collisione.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Tema 64

Lunedì 4 giugno 2018

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 11$ e sul generatore $g = 8$.

1.1) Supponendo che Alice scelga il valore segreto $a = 8$ e Bob il valore $b = 4$, descrivere lo scambio di informazioni che avviene fra i due interlocutori.

1.2) Calcolare la chiave condivisa K utilizzando la formula più conveniente fra quella usata da Alice e quella usata da Bob.

Esercizio 2

Il server web di Alice dispone di un sistema di login basato su username e password; per comodità, assumiamo che le password siano stringhe di bit.
Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile: si assuma che utilizzi una stringa casuale di 64 bit.
Il server applica alle password degli utenti una funzione hash crittografica H che genera un valore a 26 bit. In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 26 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.

Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H, ma che sappia che Bob utilizza una password di 64 bit. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login verso il server ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password, portandola a 128 bit casuali.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash in locale (nel computer di Charlie) richieda un miliardesimo di secondo.
Le risposte alle domande 2.1 e 2.2 cambiano?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Quale, tra i seguenti, è un possibile problema del protocollo Diffie-Hellman?
   (a) La lentezza in rapporto ai cifrari a chiave condivisa.
   (b) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (c) La possibilità di un attacco Man-in-the-Middle.
2. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) Il common name del richiedente.
   (b) La chiave pubblica del richiedente.
   (c) La chiave privata del richiedente.
3. Quale delle seguenti proprietà è necessaria per una funzione di cifratura?
   (a) La suriettività.
   (b) L'iniettività.
   (c) La resistenza agli attacchi di preimmagine e di collisione.
4. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (b) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (c) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
5. Quale, tra i seguenti, è un possibile problema del cifrario RSA?
   (a) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (b) La lentezza in rapporto ai cifrari a chiave condivisa.
   (c) La possibilità di un attacco Man-in-the-Middle.
6. Alice e Bob avviano una sessione Diffie-Hellman; per decifrare la chiave di sessione, Charlie (in ascolto sul canale ma non in grado di interferire) deve...
   (a) ...trovare una collisione in un valore hash crittografico.
   (b) ...risolvere un problema di logaritmo discreto.
   (c) ...fattorizzare un grande prodotto di numeri primi.
7. Quale delle seguenti proprietà **non** è posseduta da nessuna funzione hash crittografica?
   (a) L'iniettività.
   (b) La suriettività.
   (c) La resistenza agli attacchi di preimmagine e di collisione.
8. Quale delle seguenti proprietà è necessaria affinché una funzione hash sia crittograficamente sicura?
   (a) L'iniettività.
   (b) La suriettività.
   (c) La resistenza agli attacchi di preimmagine e di collisione.
9. Quale proprietà caratterizza i cifrari a flusso?
   (a) Combinano i dati da cifrare con un flusso potenzialmente infinito di dati (pseudo-) casuali.
   (b) Sono necessariamente interattivi.
   (c) Non richiedono che gli interlocutori abbiano concordato e condiviso una chiave.
10. Un certificato di firma digitale solitamente accompagna...
    (a) ...una chiave pubblica, e garantisce l'identità del possessore della corrispondente chiave privata.
    (b) ...una chiave di sessione, e ne garantisce l'autenticità.
    (c) ...una chiave privata, e garantisce l'identità del possessore della corrispondente chiave pubblica.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Tema 65

Lunedì 4 giugno 2018

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 11$ e sul generatore $g = 7$.

1.1) Supponendo che Alice scelga il valore segreto $a = 8$ e Bob il valore $b = 4$, descrivere lo scambio di informazioni che avviene fra i due interlocutori.

1.2) Calcolare la chiave condivisa K utilizzando la formula più conveniente fra quella usata da Alice e quella usata da Bob.

Esercizio 2

Il server web di Alice dispone di un sistema di login basato su username e password; per comodità, assumiamo che le password siano stringhe di bit.
Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile: si assuma che utilizzi una stringa casuale di 64 bit.
Il server applica alle password degli utenti una funzione hash crittografica H che genera un valore a 30 bit. In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 30 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.

Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H, ma che sappia che Bob utilizza una password di 64 bit. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login verso il server ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password, portandola a 128 bit casuali.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash in locale (nel computer di Charlie) richieda un miliardesimo di secondo.
Le risposte alle domande 2.1 e 2.2 cambiano?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Un certificato di firma digitale solitamente accompagna...
   (a) ...una chiave di sessione, e ne garantisce l'autenticità.
   (b) ...una chiave privata, e garantisce l'identità del possessore della corrispondente chiave pubblica.
   (c) ...una chiave pubblica, e garantisce l'identità del possessore della corrispondente chiave privata.
2. Alice e Bob avviano una sessione Diffie-Hellman; per decifrare la chiave di sessione, Charlie (in ascolto sul canale ma non in grado di interferire) deve...
   (a) ...risolvere un problema di logaritmo discreto.
   (b) ...fattorizzare un grande prodotto di numeri primi.
   (c) ...trovare una collisione in un valore hash crittografico.
3. Quale, tra i seguenti, è un possibile problema del protocollo Diffie-Hellman?
   (a) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (b) La possibilità di un attacco Man-in-the-Middle.
   (c) La lentezza in rapporto ai cifrari a chiave condivisa.
4. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (b) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (c) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
5. Quale, tra i seguenti, è un possibile problema del cifrario RSA?
   (a) La possibilità di un attacco Man-in-the-Middle.
   (b) La lentezza in rapporto ai cifrari a chiave condivisa.
   (c) La difficoltà di trovare numeri primi di dimensioni sufficienti.
6. Quale delle seguenti proprietà **non** è posseduta da nessuna funzione hash crittografica?
   (a) La resistenza agli attacchi di preimmagine e di collisione.
   (b) La suriettività.
   (c) L'iniettività.
7. Quale delle seguenti proprietà è necessaria affinché una funzione hash sia crittograficamente sicura?
   (a) La resistenza agli attacchi di preimmagine e di collisione.
   (b) L'iniettività.
   (c) La suriettività.
8. Quale delle seguenti proprietà è necessaria per una funzione di cifratura?
   (a) La resistenza agli attacchi di preimmagine e di collisione.
   (b) La suriettività.
   (c) L'iniettività.
9. Quale proprietà caratterizza i cifrari a flusso?
   (a) Non richiedono che gli interlocutori abbiano concordato e condiviso una chiave.
   (b) Combinano i dati da cifrare con un flusso potenzialmente infinito di dati (pseudo-) casuali.
   (c) Sono necessariamente interattivi.
10. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
    (a) La chiave pubblica del richiedente.
    (b) La chiave privata del richiedente.
    (c) Il common name del richiedente.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Tema 66

Lunedì 4 giugno 2018

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 11$ e sul generatore $g = 6$.

1.1) Supponendo che Alice scelga il valore segreto $a = 8$ e Bob il valore $b = 4$, descrivere lo scambio di informazioni che avviene fra i due interlocutori.

1.2) Calcolare la chiave condivisa K utilizzando la formula più conveniente fra quella usata da Alice e quella usata da Bob.

Esercizio 2

Il server web di Alice dispone di un sistema di login basato su username e password; per comodità, assumiamo che le password siano stringhe di bit.
Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile: si assuma che utilizzi una stringa casuale di 64 bit.
Il server applica alle password degli utenti una funzione hash crittografica H che genera un valore a 30 bit. In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 30 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.

Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H, ma che sappia che Bob utilizza una password di 64 bit. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login verso il server ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password, portandola a 128 bit casuali.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash in locale (nel computer di Charlie) richieda un miliardesimo di secondo.
Le risposte alle domande 2.1 e 2.2 cambiano?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Quale delle seguenti proprietà è necessaria per una funzione di cifratura?
   (a) La suriettività.
   (b) L'iniettività.
   (c) La resistenza agli attacchi di preimmagine e di collisione.
2. Quale, tra i seguenti, è un possibile problema del cifrario RSA?
   (a) La possibilità di un attacco Man-in-the-Middle.
   (b) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (c) La lentezza in rapporto ai cifrari a chiave condivisa.
3. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) Il common name del richiedente.
   (b) La chiave pubblica del richiedente.
   (c) La chiave privata del richiedente.
4. Quale proprietà caratterizza i cifrari a flusso?
   (a) Sono necessariamente interattivi.
   (b) Non richiedono che gli interlocutori abbiano concordato e condiviso una chiave.
   (c) Combinano i dati da cifrare con un flusso potenzialmente infinito di dati (pseudo-) casuali.
5. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (b) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (c) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
6. Quale delle seguenti proprietà è necessaria affinché una funzione hash sia crittograficamente sicura?
   (a) La suriettività.
   (b) L'iniettività.
   (c) La resistenza agli attacchi di preimmagine e di collisione.
7. Quale delle seguenti proprietà **non** è posseduta da nessuna funzione hash crittografica?
   (a) La resistenza agli attacchi di preimmagine e di collisione.
   (b) La suriettività.
   (c) L'iniettività.
8. Un certificato di firma digitale solitamente accompagna…
   (a) …una chiave pubblica, e garantisce l'identità del possessore della corrispondente chiave privata.
   (b) …una chiave di sessione, e ne garantisce l'autenticità.
   (c) …una chiave privata, e garantisce l'identità del possessore della corrispondente chiave pubblica.
9. Alice e Bob avviano una sessione Diffie-Hellman; per decifrare la chiave di sessione, Charlie (in ascolto sul canale ma non in grado di interferire) deve…
   (a) …fattorizzare un grande prodotto di numeri primi.
   (b) …risolvere un problema di logaritmo discreto.
   (c) …trovare una collisione in un valore hash crittografico.
10. Quale, tra i seguenti, è un possibile problema del protocollo Diffie-Hellman?
    (a) La difficoltà di trovare numeri primi di dimensioni sufficienti.
    (b) La possibilità di un attacco Man-in-the-Middle.
    (c) La lentezza in rapporto ai cifrari a chiave condivisa.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Tema 67

Lunedì 4 giugno 2018

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 13$ e sul generatore $g = 6$.

1.1) Supponendo che Alice scelga il valore segreto $a = 10$ e Bob il valore $b = 5$, descrivere lo scambio di informazioni che avviene fra i due interlocutori.

1.2) Calcolare la chiave condivisa K utilizzando la formula più conveniente fra quella usata da Alice e quella usata da Bob.

Esercizio 2

Il server web di Alice dispone di un sistema di login basato su username e password; per comodità, assumiamo che le password siano stringhe di bit.
Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile: si assuma che utilizzi una stringa casuale di 64 bit.
Il server applica alle password degli utenti una funzione hash crittografica H che genera un valore a 32 bit. In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 32 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.

Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H, ma che sappia che Bob utilizza una password di 64 bit. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login verso il server ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password, portandola a 128 bit casuali.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash in locale (nel computer di Charlie) richieda un miliardesimo di secondo.
Le risposte alle domande 2.1 e 2.2 cambiano?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Quale delle seguenti proprietà è necessaria affinché una funzione hash sia crittograficamente sicura?
   (a) La resistenza agli attacchi di preimmagine e di collisione.
   (b) La suriettività.
   (c) L'iniettività.
2. Quale delle seguenti proprietà **non** è posseduta da nessuna funzione hash crittografica?
   (a) La suriettività.
   (b) La resistenza agli attacchi di preimmagine e di collisione.
   (c) L'iniettività.
3. Quale proprietà caratterizza i cifrari a flusso?
   (a) Combinano i dati da cifrare con un flusso potenzialmente infinito di dati (pseudo-) casuali.
   (b) Non richiedono che gli interlocutori abbiano concordato e condiviso una chiave.
   (c) Sono necessariamente interattivi.
4. Alice e Bob avviano una sessione Diffie-Hellman; per decifrare la chiave di sessione, Charlie (in ascolto sul canale ma non in grado di interferire) deve...
   (a) ...trovare una collisione in un valore hash crittografico.
   (b) ...fattorizzare un grande prodotto di numeri primi.
   (c) ...risolvere un problema di logaritmo discreto.
5. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave privata del richiedente.
   (b) La chiave pubblica del richiedente.
   (c) Il common name del richiedente.
6. Un certificato di firma digitale solitamente accompagna...
   (a) ...una chiave pubblica, e garantisce l'identità del possessore della corrispondente chiave privata.
   (b) ...una chiave privata, e garantisce l'identità del possessore della corrispondente chiave pubblica.
   (c) ...una chiave di sessione, e ne garantisce l'autenticità.
7. Quale, tra i seguenti, è un possibile problema del cifrario RSA?
   (a) La lentezza in rapporto ai cifrari a chiave condivisa.
   (b) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (c) La possibilità di un attacco Man-in-the-Middle.
8. Quale, tra i seguenti, è un possibile problema del protocollo Diffie-Hellman?
   (a) La possibilità di un attacco Man-in-the-Middle.
   (b) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (c) La lentezza in rapporto ai cifrari a chiave condivisa.
9. Quale delle seguenti proprietà è necessaria per una funzione di cifratura?
   (a) La resistenza agli attacchi di preimmagine e di collisione.
   (b) La suriettività.
   (c) L'iniettività.
10. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
    (a) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
    (b) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
    (c) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Tema 68

Lunedì 4 giugno 2018

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 13$ e sul generatore $g = 6$.

1.1) Supponendo che Alice scelga il valore segreto $a = 10$ e Bob il valore $b = 5$, descrivere lo scambio di informazioni che avviene fra i due interlocutori.

1.2) Calcolare la chiave condivisa K utilizzando la formula più conveniente fra quella usata da Alice e quella usata da Bob.

Esercizio 2

Il server web di Alice dispone di un sistema di login basato su username e password; per comodità, assumiamo che le password siano stringhe di bit.
Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile: si assuma che utilizzi una stringa casuale di 64 bit.
Il server applica alle password degli utenti una funzione hash crittografica H che genera un valore a 28 bit. In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 28 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.

Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H, ma che sappia che Bob utilizza una password di 64 bit. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login verso il server ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password, portandola a 128 bit casuali.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash in locale (nel computer di Charlie) richieda un miliardesimo di secondo.
Le risposte alle domande 2.1 e 2.2 cambiano?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Quale delle seguenti proprietà **non** è posseduta da nessuna funzione hash crittografica?
   (a) La resistenza agli attacchi di preimmagine e di collisione.
   (b) L'iniettività.
   (c) La suriettività.
2. Quale delle seguenti proprietà è necessaria affinché una funzione hash sia crittograficamente sicura?
   (a) L'iniettività.
   (b) La resistenza agli attacchi di preimmagine e di collisione.
   (c) La suriettività.
3. Quale, tra i seguenti, è un possibile problema del protocollo Diffie-Hellman?
   (a) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (b) La lentezza in rapporto ai cifrari a chiave condivisa.
   (c) La possibilità di un attacco Man-in-the-Middle.
4. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (b) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (c) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
5. Un certificato di firma digitale solitamente accompagna...
   (a) ...una chiave di sessione, e ne garantisce l'autenticità.
   (b) ...una chiave privata, e garantisce l'identità del possessore della corrispondente chiave pubblica.
   (c) ...una chiave pubblica, e garantisce l'identità del possessore della corrispondente chiave privata.
6. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave privata del richiedente.
   (b) Il common name del richiedente.
   (c) La chiave pubblica del richiedente.
7. Alice e Bob avviano una sessione Diffie-Hellman; per decifrare la chiave di sessione, Charlie (in ascolto sul canale ma non in grado di interferire) deve...
   (a) ...fattorizzare un grande prodotto di numeri primi.
   (b) ...risolvere un problema di logaritmo discreto.
   (c) ...trovare una collisione in un valore hash crittografico.
8. Quale proprietà caratterizza i cifrari a flusso?
   (a) Sono necessariamente interattivi.
   (b) Combinano i dati da cifrare con un flusso potenzialmente infinito di dati (pseudo-) casuali.
   (c) Non richiedono che gli interlocutori abbiano concordato e condiviso una chiave.
9. Quale, tra i seguenti, è un possibile problema del cifrario RSA?
   (a) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (b) La possibilità di un attacco Man-in-the-Middle.
   (c) La lentezza in rapporto ai cifrari a chiave condivisa.
10. Quale delle seguenti proprietà è necessaria per una funzione di cifratura?
    (a) L'iniettività.
    (b) La resistenza agli attacchi di preimmagine e di collisione.
    (c) La suriettività.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Tema 69

Lunedì 4 giugno 2018

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 11$ e sul generatore $g = 8$.

1.1) Supponendo che Alice scelga il valore segreto $a = 7$ e Bob il valore $b = 4$, descrivere lo scambio di informazioni che avviene fra i due interlocutori.

1.2) Calcolare la chiave condivisa K utilizzando la formula più conveniente fra quella usata da Alice e quella usata da Bob.

Esercizio 2

Il server web di Alice dispone di un sistema di login basato su username e password; per comodità, assumiamo che le password siano stringhe di bit.
Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile: si assuma che utilizzi una stringa casuale di 64 bit.
Il server applica alle password degli utenti una funzione hash crittografica H che genera un valore a 32 bit. In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 32 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.

Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H, ma che sappia che Bob utilizza una password di 64 bit. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login verso il server ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password, portandola a 128 bit casuali.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash in locale (nel computer di Charlie) richieda un miliardesimo di secondo.
Le risposte alle domande 2.1 e 2.2 cambiano?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Un certificato di firma digitale solitamente accompagna...
   (a) ...una chiave di sessione, e ne garantisce l'autenticità.
   (b) ...una chiave pubblica, e garantisce l'identità del possessore della corrispondente chiave privata.
   (c) ...una chiave privata, e garantisce l'identità del possessore della corrispondente chiave pubblica.
2. Quale delle seguenti proprietà è necessaria affinché una funzione hash sia crittograficamente sicura?
   (a) L'iniettività.
   (b) La suriettività.
   (c) La resistenza agli attacchi di preimmagine e di collisione.
3. Quale, tra i seguenti, è un possibile problema del cifrario RSA?
   (a) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (b) La lentezza in rapporto ai cifrari a chiave condivisa.
   (c) La possibilità di un attacco Man-in-the-Middle.
4. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (b) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (c) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
5. Quale, tra i seguenti, è un possibile problema del protocollo Diffie-Hellman?
   (a) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (b) La possibilità di un attacco Man-in-the-Middle.
   (c) La lentezza in rapporto ai cifrari a chiave condivisa.
6. Quale delle seguenti proprietà **non** è posseduta da nessuna funzione hash crittografica?
   (a) L'iniettività.
   (b) La resistenza agli attacchi di preimmagine e di collisione.
   (c) La suriettività.
7. Alice e Bob avviano una sessione Diffie-Hellman; per decifrare la chiave di sessione, Charlie (in ascolto sul canale ma non in grado di interferire) deve...
   (a) ...risolvere un problema di logaritmo discreto.
   (b) ...fattorizzare un grande prodotto di numeri primi.
   (c) ...trovare una collisione in un valore hash crittografico.
8. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave pubblica del richiedente.
   (b) La chiave privata del richiedente.
   (c) Il common name del richiedente.
9. Quale proprietà caratterizza i cifrari a flusso?
   (a) Sono necessariamente interattivi.
   (b) Combinano i dati da cifrare con un flusso potenzialmente infinito di dati (pseudo-) casuali.
   (c) Non richiedono che gli interlocutori abbiano concordato e condiviso una chiave.
10. Quale delle seguenti proprietà è necessaria per una funzione di cifratura?
    (a) L'iniettività.
    (b) La suriettività.
    (c) La resistenza agli attacchi di preimmagine e di collisione.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Tema 70

Lunedì 4 giugno 2018

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 13$ e sul generatore $g = 7$.

1.1) Supponendo che Alice scelga il valore segreto $a = 11$ e Bob il valore $b = 3$, descrivere lo scambio di informazioni che avviene fra i due interlocutori.

1.2) Calcolare la chiave condivisa K utilizzando la formula più conveniente fra quella usata da Alice e quella usata da Bob.

Esercizio 2

Il server web di Alice dispone di un sistema di login basato su username e password; per comodità, assumiamo che le password siano stringhe di bit.
Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile: si assuma che utilizzi una stringa casuale di 64 bit.
Il server applica alle password degli utenti una funzione hash crittografica H che genera un valore a 30 bit. In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 30 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.

Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H, ma che sappia che Bob utilizza una password di 64 bit. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login verso il server ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password, portandola a 128 bit casuali.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash in locale (nel computer di Charlie) richieda un miliardesimo di secondo.
Le risposte alle domande 2.1 e 2.2 cambiano?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) Il common name del richiedente.
   (b) La chiave pubblica del richiedente.
   (c) La chiave privata del richiedente.
2. Quale, tra i seguenti, è un possibile problema del cifrario RSA?
   (a) La possibilità di un attacco Man-in-the-Middle.
   (b) La lentezza in rapporto ai cifrari a chiave condivisa.
   (c) La difficoltà di trovare numeri primi di dimensioni sufficienti.
3. Quale delle seguenti proprietà è necessaria affinché una funzione hash sia crittograficamente sicura?
   (a) L'iniettività.
   (b) La suriettività.
   (c) La resistenza agli attacchi di preimmagine e di collisione.
4. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (b) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (c) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
5. Quale delle seguenti proprietà è necessaria per una funzione di cifratura?
   (a) La resistenza agli attacchi di preimmagine e di collisione.
   (b) L'iniettività.
   (c) La suriettività.
6. Quale proprietà caratterizza i cifrari a flusso?
   (a) Non richiedono che gli interlocutori abbiano concordato e condiviso una chiave.
   (b) Sono necessariamente interattivi.
   (c) Combinano i dati da cifrare con un flusso potenzialmente infinito di dati (pseudo-) casuali.
7. Quale delle seguenti proprietà **non** è posseduta da nessuna funzione hash crittografica?
   (a) La resistenza agli attacchi di preimmagine e di collisione.
   (b) La suriettività.
   (c) L'iniettività.
8. Alice e Bob avviano una sessione Diffie-Hellman; per decifrare la chiave di sessione, Charlie (in ascolto sul canale ma non in grado di interferire) deve...
   (a) ...risolvere un problema di logaritmo discreto.
   (b) ...fattorizzare un grande prodotto di numeri primi.
   (c) ...trovare una collisione in un valore hash crittografico.
9. Quale, tra i seguenti, è un possibile problema del protocollo Diffie-Hellman?
   (a) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (b) La possibilità di un attacco Man-in-the-Middle.
   (c) La lentezza in rapporto ai cifrari a chiave condivisa.
10. Un certificato di firma digitale solitamente accompagna...
    (a) ...una chiave di sessione, e ne garantisce l'autenticità.
    (b) ...una chiave pubblica, e garantisce l'identità del possessore della corrispondente chiave privata.
    (c) ...una chiave privata, e garantisce l'identità del possessore della corrispondente chiave pubblica.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Tema 71

Lunedì 4 giugno 2018

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 13$ e sul generatore $g = 6$.

1.1) Supponendo che Alice scelga il valore segreto $a = 10$ e Bob il valore $b = 3$, descrivere lo scambio di informazioni che avviene fra i due interlocutori.

1.2) Calcolare la chiave condivisa K utilizzando la formula più conveniente fra quella usata da Alice e quella usata da Bob.

Esercizio 2

Il server web di Alice dispone di un sistema di login basato su username e password; per comodità, assumiamo che le password siano stringhe di bit.
Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile: si assuma che utilizzi una stringa casuale di 64 bit.
Il server applica alle password degli utenti una funzione hash crittografica H che genera un valore a 26 bit. In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 26 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.

Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H, ma che sappia che Bob utilizza una password di 64 bit. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login verso il server ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password, portandola a 128 bit casuali.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash in locale (nel computer di Charlie) richieda un miliardesimo di secondo.
Le risposte alle domande 2.1 e 2.2 cambiano?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave pubblica del richiedente.
   (b) La chiave privata del richiedente.
   (c) Il common name del richiedente.
2. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (b) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (c) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
3. Quale, tra i seguenti, è un possibile problema del protocollo Diffie-Hellman?
   (a) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (b) La possibilità di un attacco Man-in-the-Middle.
   (c) La lentezza in rapporto ai cifrari a chiave condivisa.
4. Alice e Bob avviano una sessione Diffie-Hellman; per decifrare la chiave di sessione, Charlie (in ascolto sul canale ma non in grado di interferire) deve...
   (a) ...trovare una collisione in un valore hash crittografico.
   (b) ...risolvere un problema di logaritmo discreto.
   (c) ...fattorizzare un grande prodotto di numeri primi.
5. Un certificato di firma digitale solitamente accompagna...
   (a) ...una chiave privata, e garantisce l'identità del possessore della corrispondente chiave pubblica.
   (b) ...una chiave di sessione, e ne garantisce l'autenticità.
   (c) ...una chiave pubblica, e garantisce l'identità del possessore della corrispondente chiave privata.
6. Quale delle seguenti proprietà è necessaria per una funzione di cifratura?
   (a) L'iniettività.
   (b) La resistenza agli attacchi di preimmagine e di collisione.
   (c) La suriettività.
7. Quale delle seguenti proprietà è necessaria affinché una funzione hash sia crittograficamente sicura?
   (a) L'iniettività.
   (b) La resistenza agli attacchi di preimmagine e di collisione.
   (c) La suriettività.
8. Quale, tra i seguenti, è un possibile problema del cifrario RSA?
   (a) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (b) La lentezza in rapporto ai cifrari a chiave condivisa.
   (c) La possibilità di un attacco Man-in-the-Middle.
9. Quale delle seguenti proprietà **non** è posseduta da nessuna funzione hash crittografica?
   (a) L'iniettività.
   (b) La resistenza agli attacchi di preimmagine e di collisione.
   (c) La suriettività.
10. Quale proprietà caratterizza i cifrari a flusso?
    (a) Sono necessariamente interattivi.
    (b) Combinano i dati da cifrare con un flusso potenzialmente infinito di dati (pseudo-) casuali.
    (c) Non richiedono che gli interlocutori abbiano concordato e condiviso una chiave.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Tema 72

Lunedì 4 giugno 2018

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 13$ e sul generatore $g = 7$.

1.1) Supponendo che Alice scelga il valore segreto $a = 11$ e Bob il valore $b = 5$, descrivere lo scambio di informazioni che avviene fra i due interlocutori.

1.2) Calcolare la chiave condivisa K utilizzando la formula più conveniente fra quella usata da Alice e quella usata da Bob.

Esercizio 2

Il server web di Alice dispone di un sistema di login basato su username e password; per comodità, assumiamo che le password siano stringhe di bit.
Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile: si assuma che utilizzi una stringa casuale di 64 bit.
Il server applica alle password degli utenti una funzione hash crittografica H che genera un valore a 32 bit. In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 32 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.

Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H, ma che sappia che Bob utilizza una password di 64 bit. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login verso il server ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password, portandola a 128 bit casuali.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash in locale (nel computer di Charlie) richieda un miliardesimo di secondo.
Le risposte alle domande 2.1 e 2.2 cambiano?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Un certificato di firma digitale solitamente accompagna...
   (a) ...una chiave privata, e garantisce l'identità del possessore della corrispondente chiave pubblica.
   (b) ...una chiave pubblica, e garantisce l'identità del possessore della corrispondente chiave privata.
   (c) ...una chiave di sessione, e ne garantisce l'autenticità.
2. Quale delle seguenti proprietà è necessaria per una funzione di cifratura?
   (a) La resistenza agli attacchi di preimmagine e di collisione.
   (b) L'iniettività.
   (c) La suriettività.
3. Quale delle seguenti proprietà **non** è posseduta da nessuna funzione hash crittografica?
   (a) L'iniettività.
   (b) La suriettività.
   (c) La resistenza agli attacchi di preimmagine e di collisione.
4. Quale delle seguenti proprietà è necessaria affinché una funzione hash sia crittograficamente sicura?
   (a) La suriettività.
   (b) La resistenza agli attacchi di preimmagine e di collisione.
   (c) L'iniettività.
5. Alice e Bob avviano una sessione Diffie-Hellman; per decifrare la chiave di sessione, Charlie (in ascolto sul canale ma non in grado di interferire) deve...
   (a) ...trovare una collisione in un valore hash crittografico.
   (b) ...risolvere un problema di logaritmo discreto.
   (c) ...fattorizzare un grande prodotto di numeri primi.
6. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (b) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (c) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
7. Quale, tra i seguenti, è un possibile problema del protocollo Diffie-Hellman?
   (a) La lentezza in rapporto ai cifrari a chiave condivisa.
   (b) La possibilità di un attacco Man-in-the-Middle.
   (c) La difficoltà di trovare numeri primi di dimensioni sufficienti.
8. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave pubblica del richiedente.
   (b) La chiave privata del richiedente.
   (c) Il common name del richiedente.
9. Quale proprietà caratterizza i cifrari a flusso?
   (a) Non richiedono che gli interlocutori abbiano concordato e condiviso una chiave.
   (b) Sono necessariamente interattivi.
   (c) Combinano i dati da cifrare con un flusso potenzialmente infinito di dati (pseudo-) casuali.
10. Quale, tra i seguenti, è un possibile problema del cifrario RSA?
    (a) La lentezza in rapporto ai cifrari a chiave condivisa.
    (b) La difficoltà di trovare numeri primi di dimensioni sufficienti.
    (c) La possibilità di un attacco Man-in-the-Middle.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Tema 73

Lunedì 4 giugno 2018

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 13$ e sul generatore $g = 7$.

1.1) Supponendo che Alice scelga il valore segreto $a = 10$ e Bob il valore $b = 4$, descrivere lo scambio di informazioni che avviene fra i due interlocutori.

1.2) Calcolare la chiave condivisa K utilizzando la formula più conveniente fra quella usata da Alice e quella usata da Bob.

Esercizio 2

Il server web di Alice dispone di un sistema di login basato su username e password; per comodità, assumiamo che le password siano stringhe di bit.
Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile: si assuma che utilizzi una stringa casuale di 64 bit.
Il server applica alle password degli utenti una funzione hash crittografica H che genera un valore a 32 bit. In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 32 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.

Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H, ma che sappia che Bob utilizza una password di 64 bit. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login verso il server ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password, portandola a 128 bit casuali.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash in locale (nel computer di Charlie) richieda un miliardesimo di secondo.
Le risposte alle domande 2.1 e 2.2 cambiano?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave pubblica del richiedente.
   (b) La chiave privata del richiedente.
   (c) Il common name del richiedente.
2. Alice e Bob avviano una sessione Diffie-Hellman; per decifrare la chiave di sessione, Charlie (in ascolto sul canale ma non in grado di interferire) deve...
   (a) ...risolvere un problema di logaritmo discreto.
   (b) ...fattorizzare un grande prodotto di numeri primi.
   (c) ...trovare una collisione in un valore hash crittografico.
3. Un certificato di firma digitale solitamente accompagna...
   (a) ...una chiave di sessione, e ne garantisce l'autenticità.
   (b) ...una chiave pubblica, e garantisce l'identità del possessore della corrispondente chiave privata.
   (c) ...una chiave privata, e garantisce l'identità del possessore della corrispondente chiave pubblica.
4. Quale, tra i seguenti, è un possibile problema del protocollo Diffie-Hellman?
   (a) La lentezza in rapporto ai cifrari a chiave condivisa.
   (b) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (c) La possibilità di un attacco Man-in-the-Middle.
5. Quale delle seguenti proprietà **non** è posseduta da nessuna funzione hash crittografica?
   (a) La suriettività.
   (b) L'iniettività.
   (c) La resistenza agli attacchi di preimmagine e di collisione.
6. Quale delle seguenti proprietà è necessaria affinché una funzione hash sia crittograficamente sicura?
   (a) L'iniettività.
   (b) La suriettività.
   (c) La resistenza agli attacchi di preimmagine e di collisione.
7. Quale, tra i seguenti, è un possibile problema del cifrario RSA?
   (a) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (b) La lentezza in rapporto ai cifrari a chiave condivisa.
   (c) La possibilità di un attacco Man-in-the-Middle.
8. Quale delle seguenti proprietà è necessaria per una funzione di cifratura?
   (a) La suriettività.
   (b) L'iniettività.
   (c) La resistenza agli attacchi di preimmagine e di collisione.
9. Quale proprietà caratterizza i cifrari a flusso?
   (a) Non richiedono che gli interlocutori abbiano concordato e condiviso una chiave.
   (b) Combinano i dati da cifrare con un flusso potenzialmente infinito di dati (pseudo-) casuali.
   (c) Sono necessariamente interattivi.
10. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
    (a) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
    (b) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
    (c) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Tema 74

Lunedì 4 giugno 2018

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 13$ e sul generatore $g = 6$.

1.1) Supponendo che Alice scelga il valore segreto $a = 10$ e Bob il valore $b = 2$, descrivere lo scambio di informazioni che avviene fra i due interlocutori.

1.2) Calcolare la chiave condivisa K utilizzando la formula più conveniente fra quella usata da Alice e quella usata da Bob.

Esercizio 2

Il server web di Alice dispone di un sistema di login basato su username e password; per comodità, assumiamo che le password siano stringhe di bit.
Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile: si assuma che utilizzi una stringa casuale di 64 bit.
Il server applica alle password degli utenti una funzione hash crittografica H che genera un valore a 28 bit. In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 28 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.

Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H, ma che sappia che Bob utilizza una password di 64 bit. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login verso il server ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password, portandola a 128 bit casuali.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash in locale (nel computer di Charlie) richieda un miliardesimo di secondo.
Le risposte alle domande 2.1 e 2.2 cambiano?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Quale, tra i seguenti, è un possibile problema del cifrario RSA?
   (a) La lentezza in rapporto ai cifrari a chiave condivisa.
   (b) La possibilità di un attacco Man-in-the-Middle.
   (c) La difficoltà di trovare numeri primi di dimensioni sufficienti.
2. Alice e Bob avviano una sessione Diffie-Hellman; per decifrare la chiave di sessione, Charlie (in ascolto sul canale ma non in grado di interferire) deve...
   (a) ...fattorizzare un grande prodotto di numeri primi.
   (b) ...risolvere un problema di logaritmo discreto.
   (c) ...trovare una collisione in un valore hash crittografico.
3. Quale delle seguenti proprietà **non** è posseduta da nessuna funzione hash crittografica?
   (a) L'iniettività.
   (b) La suriettività.
   (c) La resistenza agli attacchi di preimmagine e di collisione.
4. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (b) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (c) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
5. Quale delle seguenti proprietà è necessaria per una funzione di cifratura?
   (a) La suriettività.
   (b) L'iniettività.
   (c) La resistenza agli attacchi di preimmagine e di collisione.
6. Quale proprietà caratterizza i cifrari a flusso?
   (a) Combinano i dati da cifrare con un flusso potenzialmente infinito di dati (pseudo-) casuali.
   (b) Non richiedono che gli interlocutori abbiano concordato e condiviso una chiave.
   (c) Sono necessariamente interattivi.
7. Un certificato di firma digitale solitamente accompagna...
   (a) ...una chiave privata, e garantisce l'identità del possessore della corrispondente chiave pubblica.
   (b) ...una chiave di sessione, e ne garantisce l'autenticità.
   (c) ...una chiave pubblica, e garantisce l'identità del possessore della corrispondente chiave privata.
8. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave pubblica del richiedente.
   (b) La chiave privata del richiedente.
   (c) Il common name del richiedente.
9. Quale delle seguenti proprietà è necessaria affinché una funzione hash sia crittograficamente sicura?
   (a) L'iniettività.
   (b) La suriettività.
   (c) La resistenza agli attacchi di preimmagine e di collisione.
10. Quale, tra i seguenti, è un possibile problema del protocollo Diffie-Hellman?
    (a) La possibilità di un attacco Man-in-the-Middle.
    (b) La lentezza in rapporto ai cifrari a chiave condivisa.
    (c) La difficoltà di trovare numeri primi di dimensioni sufficienti.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Tema 75

Lunedì 4 giugno 2018

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 11$ e sul generatore $g = 8$.

1.1) Supponendo che Alice scelga il valore segreto $a = 7$ e Bob il valore $b = 4$, descrivere lo scambio di informazioni che avviene fra i due interlocutori.

1.2) Calcolare la chiave condivisa K utilizzando la formula più conveniente fra quella usata da Alice e quella usata da Bob.

Esercizio 2

Il server web di Alice dispone di un sistema di login basato su username e password; per comodità, assumiamo che le password siano stringhe di bit.
Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile: si assuma che utilizzi una stringa casuale di 64 bit.
Il server applica alle password degli utenti una funzione hash crittografica H che genera un valore a 28 bit. In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 28 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.

Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H, ma che sappia che Bob utilizza una password di 64 bit. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login verso il server ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password, portandola a 128 bit casuali.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash in locale (nel computer di Charlie) richieda un miliardesimo di secondo.
Le risposte alle domande 2.1 e 2.2 cambiano?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Alice e Bob avviano una sessione Diffie-Hellman; per decifrare la chiave di sessione, Charlie (in ascolto sul canale ma non in grado di interferire) deve...
   (a) ...fattorizzare un grande prodotto di numeri primi.
   (b) ...trovare una collisione in un valore hash crittografico.
   (c) ...risolvere un problema di logaritmo discreto.
2. Quale delle seguenti proprietà **non** è posseduta da nessuna funzione hash crittografica?
   (a) L'iniettività.
   (b) La suriettività.
   (c) La resistenza agli attacchi di preimmagine e di collisione.
3. Quale delle seguenti proprietà è necessaria per una funzione di cifratura?
   (a) La suriettività.
   (b) La resistenza agli attacchi di preimmagine e di collisione.
   (c) L'iniettività.
4. Un certificato di firma digitale solitamente accompagna...
   (a) ...una chiave pubblica, e garantisce l'identità del possessore della corrispondente chiave privata.
   (b) ...una chiave privata, e garantisce l'identità del possessore della corrispondente chiave pubblica.
   (c) ...una chiave di sessione, e ne garantisce l'autenticità.
5. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (b) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (c) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
6. Quale delle seguenti proprietà è necessaria affinché una funzione hash sia crittograficamente sicura?
   (a) L'iniettività.
   (b) La resistenza agli attacchi di preimmagine e di collisione.
   (c) La suriettività.
7. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave pubblica del richiedente.
   (b) Il common name del richiedente.
   (c) La chiave privata del richiedente.
8. Quale proprietà caratterizza i cifrari a flusso?
   (a) Non richiedono che gli interlocutori abbiano concordato e condiviso una chiave.
   (b) Sono necessariamente interattivi.
   (c) Combinano i dati da cifrare con un flusso potenzialmente infinito di dati (pseudo-) casuali.
9. Quale, tra i seguenti, è un possibile problema del protocollo Diffie-Hellman?
   (a) La possibilità di un attacco Man-in-the-Middle.
   (b) La lentezza in rapporto ai cifrari a chiave condivisa.
   (c) La difficoltà di trovare numeri primi di dimensioni sufficienti.
10. Quale, tra i seguenti, è un possibile problema del cifrario RSA?
    (a) La lentezza in rapporto ai cifrari a chiave condivisa.
    (b) La difficoltà di trovare numeri primi di dimensioni sufficienti.
    (c) La possibilità di un attacco Man-in-the-Middle.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Tema 76

Lunedì 4 giugno 2018

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 11$ e sul generatore $g = 7$.

1.1) Supponendo che Alice scelga il valore segreto $a = 9$ e Bob il valore $b = 3$, descrivere lo scambio di informazioni che avviene fra i due interlocutori.

1.2) Calcolare la chiave condivisa K utilizzando la formula più conveniente fra quella usata da Alice e quella usata da Bob.

Esercizio 2

Il server web di Alice dispone di un sistema di login basato su username e password; per comodità, assumiamo che le password siano stringhe di bit.
Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile: si assuma che utilizzi una stringa casuale di 64 bit.
Il server applica alle password degli utenti una funzione hash crittografica H che genera un valore a 30 bit. In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 30 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.

Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H, ma che sappia che Bob utilizza una password di 64 bit. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login verso il server ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password, portandola a 128 bit casuali.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash in locale (nel computer di Charlie) richieda un miliardesimo di secondo.
Le risposte alle domande 2.1 e 2.2 cambiano?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) Il common name del richiedente.
   (b) La chiave pubblica del richiedente.
   (c) La chiave privata del richiedente.
2. Quale, tra i seguenti, è un possibile problema del protocollo Diffie-Hellman?
   (a) La lentezza in rapporto ai cifrari a chiave condivisa.
   (b) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (c) La possibilità di un attacco Man-in-the-Middle.
3. Alice e Bob avviano una sessione Diffie-Hellman; per decifrare la chiave di sessione, Charlie (in ascolto sul canale ma non in grado di interferire) deve...
   (a) ...trovare una collisione in un valore hash crittografico.
   (b) ...risolvere un problema di logaritmo discreto.
   (c) ...fattorizzare un grande prodotto di numeri primi.
4. Un certificato di firma digitale solitamente accompagna...
   (a) ...una chiave di sessione, e ne garantisce l'autenticità.
   (b) ...una chiave privata, e garantisce l'identità del possessore della corrispondente chiave pubblica.
   (c) ...una chiave pubblica, e garantisce l'identità del possessore della corrispondente chiave privata.
5. Quale delle seguenti proprietà è necessaria affinché una funzione hash sia crittograficamente sicura?
   (a) La resistenza agli attacchi di preimmagine e di collisione.
   (b) L'iniettività.
   (c) La suriettività.
6. Quale delle seguenti proprietà è necessaria per una funzione di cifratura?
   (a) La suriettività.
   (b) La resistenza agli attacchi di preimmagine e di collisione.
   (c) L'iniettività.
7. Quale delle seguenti proprietà **non** è posseduta da nessuna funzione hash crittografica?
   (a) La suriettività.
   (b) L'iniettività.
   (c) La resistenza agli attacchi di preimmagine e di collisione.
8. Quale, tra i seguenti, è un possibile problema del cifrario RSA?
   (a) La possibilità di un attacco Man-in-the-Middle.
   (b) La lentezza in rapporto ai cifrari a chiave condivisa.
   (c) La difficoltà di trovare numeri primi di dimensioni sufficienti.
9. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (b) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (c) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
10. Quale proprietà caratterizza i cifrari a flusso?
    (a) Sono necessariamente interattivi.
    (b) Combinano i dati da cifrare con un flusso potenzialmente infinito di dati (pseudo-) casuali.
    (c) Non richiedono che gli interlocutori abbiano concordato e condiviso una chiave.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Tema 77

Lunedì 4 giugno 2018

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 11$ e sul generatore $g = 6$.

1.1) Supponendo che Alice scelga il valore segreto $a = 7$ e Bob il valore $b = 2$, descrivere lo scambio di informazioni che avviene fra i due interlocutori.

1.2) Calcolare la chiave condivisa K utilizzando la formula più conveniente fra quella usata da Alice e quella usata da Bob.

Esercizio 2

Il server web di Alice dispone di un sistema di login basato su username e password; per comodità, assumiamo che le password siano stringhe di bit.
Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile: si assuma che utilizzi una stringa casuale di 64 bit.
Il server applica alle password degli utenti una funzione hash crittografica H che genera un valore a 32 bit. In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 32 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.

Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H, ma che sappia che Bob utilizza una password di 64 bit. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login verso il server ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password, portandola a 128 bit casuali.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash in locale (nel computer di Charlie) richieda un miliardesimo di secondo.
Le risposte alle domande 2.1 e 2.2 cambiano?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) Il common name del richiedente.
   (b) La chiave privata del richiedente.
   (c) La chiave pubblica del richiedente.
2. Quale delle seguenti proprietà **non** è posseduta da nessuna funzione hash crittografica?
   (a) La resistenza agli attacchi di preimmagine e di collisione.
   (b) L'iniettività.
   (c) La suriettività.
3. Alice e Bob avviano una sessione Diffie-Hellman; per decifrare la chiave di sessione, Charlie (in ascolto sul canale ma non in grado di interferire) deve...
   (a) ...trovare una collisione in un valore hash crittografico.
   (b) ...risolvere un problema di logaritmo discreto.
   (c) ...fattorizzare un grande prodotto di numeri primi.
4. Un certificato di firma digitale solitamente accompagna...
   (a) ...una chiave di sessione, e ne garantisce l'autenticità.
   (b) ...una chiave pubblica, e garantisce l'identità del possessore della corrispondente chiave privata.
   (c) ...una chiave privata, e garantisce l'identità del possessore della corrispondente chiave pubblica.
5. Quale, tra i seguenti, è un possibile problema del protocollo Diffie-Hellman?
   (a) La possibilità di un attacco Man-in-the-Middle.
   (b) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (c) La lentezza in rapporto ai cifrari a chiave condivisa.
6. Quale delle seguenti proprietà è necessaria per una funzione di cifratura?
   (a) L'iniettività.
   (b) La suriettività.
   (c) La resistenza agli attacchi di preimmagine e di collisione.
7. Quale, tra i seguenti, è un possibile problema del cifrario RSA?
   (a) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (b) La lentezza in rapporto ai cifrari a chiave condivisa.
   (c) La possibilità di un attacco Man-in-the-Middle.
8. Quale delle seguenti proprietà è necessaria affinché una funzione hash sia crittograficamente sicura?
   (a) L'iniettività.
   (b) La suriettività.
   (c) La resistenza agli attacchi di preimmagine e di collisione.
9. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (b) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (c) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
10. Quale proprietà caratterizza i cifrari a flusso?
    (a) Combinano i dati da cifrare con un flusso potenzialmente infinito di dati (pseudo-) casuali.
    (b) Sono necessariamente interattivi.
    (c) Non richiedono che gli interlocutori abbiano concordato e condiviso una chiave.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Tema 78

Lunedì 4 giugno 2018

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 13$ e sul generatore $g = 7$.

1.1) Supponendo che Alice scelga il valore segreto $a = 10$ e Bob il valore $b = 4$, descrivere lo scambio di informazioni che avviene fra i due interlocutori.

1.2) Calcolare la chiave condivisa K utilizzando la formula più conveniente fra quella usata da Alice e quella usata da Bob.

Esercizio 2

Il server web di Alice dispone di un sistema di login basato su username e password; per comodità, assumiamo che le password siano stringhe di bit.
Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile: si assuma che utilizzi una stringa casuale di 64 bit.
Il server applica alle password degli utenti una funzione hash crittografica H che genera un valore a 28 bit. In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 28 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.

Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H, ma che sappia che Bob utilizza una password di 64 bit. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login verso il server ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password, portandola a 128 bit casuali.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash in locale (nel computer di Charlie) richieda un miliardesimo di secondo.
Le risposte alle domande 2.1 e 2.2 cambiano?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Quale, tra i seguenti, è un possibile problema del cifrario RSA?
   (a) La possibilità di un attacco Man-in-the-Middle.
   (b) La lentezza in rapporto ai cifrari a chiave condivisa.
   (c) La difficoltà di trovare numeri primi di dimensioni sufficienti.
2. Quale proprietà caratterizza i cifrari a flusso?
   (a) Non richiedono che gli interlocutori abbiano concordato e condiviso una chiave.
   (b) Sono necessariamente interattivi.
   (c) Combinano i dati da cifrare con un flusso potenzialmente infinito di dati (pseudo-) casuali.
3. Quale, tra i seguenti, è un possibile problema del protocollo Diffie-Hellman?
   (a) La lentezza in rapporto ai cifrari a chiave condivisa.
   (b) La possibilità di un attacco Man-in-the-Middle.
   (c) La difficoltà di trovare numeri primi di dimensioni sufficienti.
4. Quale delle seguenti proprietà è necessaria per una funzione di cifratura?
   (a) La resistenza agli attacchi di preimmagine e di collisione.
   (b) L'iniettività.
   (c) La suriettività.
5. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (b) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (c) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
6. Quale delle seguenti proprietà **non** è posseduta da nessuna funzione hash crittografica?
   (a) L'iniettività.
   (b) La suriettività.
   (c) La resistenza agli attacchi di preimmagine e di collisione.
7. Quale delle seguenti proprietà è necessaria affinché una funzione hash sia crittograficamente sicura?
   (a) La suriettività.
   (b) La resistenza agli attacchi di preimmagine e di collisione.
   (c) L'iniettività.
8. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) Il common name del richiedente.
   (b) La chiave privata del richiedente.
   (c) La chiave pubblica del richiedente.
9. Alice e Bob avviano una sessione Diffie-Hellman; per decifrare la chiave di sessione, Charlie (in ascolto sul canale ma non in grado di interferire) deve...
   (a) ...risolvere un problema di logaritmo discreto.
   (b) ...fattorizzare un grande prodotto di numeri primi.
   (c) ...trovare una collisione in un valore hash crittografico.
10. Un certificato di firma digitale solitamente accompagna...
    (a) ...una chiave privata, e garantisce l'identità del possessore della corrispondente chiave pubblica.
    (b) ...una chiave pubblica, e garantisce l'identità del possessore della corrispondente chiave privata.
    (c) ...una chiave di sessione, e ne garantisce l'autenticità.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Tema 79

Lunedì 4 giugno 2018

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 11$ e sul generatore $g = 6$.

1.1) Supponendo che Alice scelga il valore segreto $a = 8$ e Bob il valore $b = 3$, descrivere lo scambio di informazioni che avviene fra i due interlocutori.

1.2) Calcolare la chiave condivisa K utilizzando la formula più conveniente fra quella usata da Alice e quella usata da Bob.

Esercizio 2

Il server web di Alice dispone di un sistema di login basato su username e password; per comodità, assumiamo che le password siano stringhe di bit.
Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile: si assuma che utilizzi una stringa casuale di 64 bit.
Il server applica alle password degli utenti una funzione hash crittografica H che genera un valore a 24 bit. In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 24 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.

Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H, ma che sappia che Bob utilizza una password di 64 bit. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login verso il server ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password, portandola a 128 bit casuali.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash in locale (nel computer di Charlie) richieda un miliardesimo di secondo.
Le risposte alle domande 2.1 e 2.2 cambiano?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Quale delle seguenti proprietà è necessaria per una funzione di cifratura?
   (a) L'iniettività.
   (b) La suriettività.
   (c) La resistenza agli attacchi di preimmagine e di collisione.
2. Alice e Bob avviano una sessione Diffie-Hellman; per decifrare la chiave di sessione, Charlie (in ascolto sul canale ma non in grado di interferire) deve...
   (a) ...risolvere un problema di logaritmo discreto.
   (b) ...fattorizzare un grande prodotto di numeri primi.
   (c) ...trovare una collisione in un valore hash crittografico.
3. Quale proprietà caratterizza i cifrari a flusso?
   (a) Non richiedono che gli interlocutori abbiano concordato e condiviso una chiave.
   (b) Sono necessariamente interattivi.
   (c) Combinano i dati da cifrare con un flusso potenzialmente infinito di dati (pseudo-) casuali.
4. Quale, tra i seguenti, è un possibile problema del cifrario RSA?
   (a) La possibilità di un attacco Man-in-the-Middle.
   (b) La lentezza in rapporto ai cifrari a chiave condivisa.
   (c) La difficoltà di trovare numeri primi di dimensioni sufficienti.
5. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) Il common name del richiedente.
   (b) La chiave pubblica del richiedente.
   (c) La chiave privata del richiedente.
6. Quale delle seguenti proprietà è necessaria affinché una funzione hash sia crittograficamente sicura?
   (a) L'iniettività.
   (b) La resistenza agli attacchi di preimmagine e di collisione.
   (c) La suriettività.
7. Un certificato di firma digitale solitamente accompagna...
   (a) ...una chiave di sessione, e ne garantisce l'autenticità.
   (b) ...una chiave pubblica, e garantisce l'identità del possessore della corrispondente chiave privata.
   (c) ...una chiave privata, e garantisce l'identità del possessore della corrispondente chiave pubblica.
8. Quale, tra i seguenti, è un possibile problema del protocollo Diffie-Hellman?
   (a) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (b) La lentezza in rapporto ai cifrari a chiave condivisa.
   (c) La possibilità di un attacco Man-in-the-Middle.
9. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (b) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (c) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
10. Quale delle seguenti proprietà **non** è posseduta da nessuna funzione hash crittografica?
    (a) La suriettività.
    (b) La resistenza agli attacchi di preimmagine e di collisione.
    (c) L'iniettività.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Tema 80

Lunedì 4 giugno 2018

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 13$ e sul generatore $g = 6$.

1.1) Supponendo che Alice scelga il valore segreto $a = 10$ e Bob il valore $b = 5$, descrivere lo scambio di informazioni che avviene fra i due interlocutori.

1.2) Calcolare la chiave condivisa K utilizzando la formula più conveniente fra quella usata da Alice e quella usata da Bob.

Esercizio 2

Il server web di Alice dispone di un sistema di login basato su username e password; per comodità, assumiamo che le password siano stringhe di bit.
Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile: si assuma che utilizzi una stringa casuale di 64 bit.
Il server applica alle password degli utenti una funzione hash crittografica H che genera un valore a 26 bit. In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 26 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.

Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H, ma che sappia che Bob utilizza una password di 64 bit. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login verso il server ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password, portandola a 128 bit casuali.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash in locale (nel computer di Charlie) richieda un miliardesimo di secondo.
Le risposte alle domande 2.1 e 2.2 cambiano?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (b) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (c) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
2. Un certificato di firma digitale solitamente accompagna...
   (a) ...una chiave privata, e garantisce l'identità del possessore della corrispondente chiave pubblica.
   (b) ...una chiave pubblica, e garantisce l'identità del possessore della corrispondente chiave privata.
   (c) ...una chiave di sessione, e ne garantisce l'autenticità.
3. Quale delle seguenti proprietà **non** è posseduta da nessuna funzione hash crittografica?
   (a) L'iniettività.
   (b) La resistenza agli attacchi di preimmagine e di collisione.
   (c) La suriettività.
4. Quale proprietà caratterizza i cifrari a flusso?
   (a) Sono necessariamente interattivi.
   (b) Non richiedono che gli interlocutori abbiano concordato e condiviso una chiave.
   (c) Combinano i dati da cifrare con un flusso potenzialmente infinito di dati (pseudo-) casuali.
5. Quale, tra i seguenti, è un possibile problema del protocollo Diffie-Hellman?
   (a) La lentezza in rapporto ai cifrari a chiave condivisa.
   (b) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (c) La possibilità di un attacco Man-in-the-Middle.
6. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave pubblica del richiedente.
   (b) La chiave privata del richiedente.
   (c) Il common name del richiedente.
7. Quale delle seguenti proprietà è necessaria per una funzione di cifratura?
   (a) La resistenza agli attacchi di preimmagine e di collisione.
   (b) L'iniettività.
   (c) La suriettività.
8. Quale delle seguenti proprietà è necessaria affinché una funzione hash sia crittograficamente sicura?
   (a) La suriettività.
   (b) L'iniettività.
   (c) La resistenza agli attacchi di preimmagine e di collisione.
9. Quale, tra i seguenti, è un possibile problema del cifrario RSA?
   (a) La possibilità di un attacco Man-in-the-Middle.
   (b) La lentezza in rapporto ai cifrari a chiave condivisa.
   (c) La difficoltà di trovare numeri primi di dimensioni sufficienti.
10. Alice e Bob avviano una sessione Diffie-Hellman; per decifrare la chiave di sessione, Charlie (in ascolto sul canale ma non in grado di interferire) deve...
    (a) ...fattorizzare un grande prodotto di numeri primi.
    (b) ...risolvere un problema di logaritmo discreto.
    (c) ...trovare una collisione in un valore hash crittografico.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Tema 81

Lunedì 4 giugno 2018

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 11$ e sul generatore $g = 6$.

1.1) Supponendo che Alice scelga il valore segreto $a = 8$ e Bob il valore $b = 2$, descrivere lo scambio di informazioni che avviene fra i due interlocutori.

1.2) Calcolare la chiave condivisa K utilizzando la formula più conveniente fra quella usata da Alice e quella usata da Bob.

Esercizio 2

Il server web di Alice dispone di un sistema di login basato su username e password; per comodità, assumiamo che le password siano stringhe di bit.
Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile: si assuma che utilizzi una stringa casuale di 64 bit.
Il server applica alle password degli utenti una funzione hash crittografica H che genera un valore a 30 bit. In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 30 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.

Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H, ma che sappia che Bob utilizza una password di 64 bit. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login verso il server ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password, portandola a 128 bit casuali.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash in locale (nel computer di Charlie) richieda un miliardesimo di secondo.
Le risposte alle domande 2.1 e 2.2 cambiano?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave pubblica del richiedente.
   (b) La chiave privata del richiedente.
   (c) Il common name del richiedente.
2. Quale proprietà caratterizza i cifrari a flusso?
   (a) Sono necessariamente interattivi.
   (b) Combinano i dati da cifrare con un flusso potenzialmente infinito di dati (pseudo-) casuali.
   (c) Non richiedono che gli interlocutori abbiano concordato e condiviso una chiave.
3. Quale, tra i seguenti, è un possibile problema del cifrario RSA?
   (a) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (b) La possibilità di un attacco Man-in-the-Middle.
   (c) La lentezza in rapporto ai cifrari a chiave condivisa.
4. Un certificato di firma digitale solitamente accompagna...
   (a) ...una chiave privata, e garantisce l'identità del possessore della corrispondente chiave pubblica.
   (b) ...una chiave di sessione, e ne garantisce l'autenticità.
   (c) ...una chiave pubblica, e garantisce l'identità del possessore della corrispondente chiave privata.
5. Quale, tra i seguenti, è un possibile problema del protocollo Diffie-Hellman?
   (a) La lentezza in rapporto ai cifrari a chiave condivisa.
   (b) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (c) La possibilità di un attacco Man-in-the-Middle.
6. Quale delle seguenti proprietà **non** è posseduta da nessuna funzione hash crittografica?
   (a) La resistenza agli attacchi di preimmagine e di collisione.
   (b) L'iniettività.
   (c) La suriettività.
7. Quale delle seguenti proprietà è necessaria affinché una funzione hash sia crittograficamente sicura?
   (a) La resistenza agli attacchi di preimmagine e di collisione.
   (b) La suriettività.
   (c) L'iniettività.
8. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (b) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (c) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
9. Alice e Bob avviano una sessione Diffie-Hellman; per decifrare la chiave di sessione, Charlie (in ascolto sul canale ma non in grado di interferire) deve...
   (a) ...trovare una collisione in un valore hash crittografico.
   (b) ...fattorizzare un grande prodotto di numeri primi.
   (c) ...risolvere un problema di logaritmo discreto.
10. Quale delle seguenti proprietà è necessaria per una funzione di cifratura?
    (a) L'iniettività.
    (b) La suriettività.
    (c) La resistenza agli attacchi di preimmagine e di collisione.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Tema 82

Lunedì 4 giugno 2018

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 11$ e sul generatore $g = 6$.

1.1) Supponendo che Alice scelga il valore segreto $a = 9$ e Bob il valore $b = 3$, descrivere lo scambio di informazioni che avviene fra i due interlocutori.

1.2) Calcolare la chiave condivisa K utilizzando la formula più conveniente fra quella usata da Alice e quella usata da Bob.

Esercizio 2

Il server web di Alice dispone di un sistema di login basato su username e password; per comodità, assumiamo che le password siano stringhe di bit.
Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile: si assuma che utilizzi una stringa casuale di 64 bit.
Il server applica alle password degli utenti una funzione hash crittografica H che genera un valore a 24 bit. In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 24 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.

Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H, ma che sappia che Bob utilizza una password di 64 bit. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login verso il server ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password, portandola a 128 bit casuali.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash in locale (nel computer di Charlie) richieda un miliardesimo di secondo.
Le risposte alle domande 2.1 e 2.2 cambiano?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Quale delle seguenti proprietà **non** è posseduta da nessuna funzione hash crittografica?
   (a) La suriettività.
   (b) La resistenza agli attacchi di preimmagine e di collisione.
   (c) L'iniettività.
2. Un certificato di firma digitale solitamente accompagna...
   (a) ...una chiave privata, e garantisce l'identità del possessore della corrispondente chiave pubblica.
   (b) ...una chiave di sessione, e ne garantisce l'autenticità.
   (c) ...una chiave pubblica, e garantisce l'identità del possessore della corrispondente chiave privata.
3. Quale delle seguenti proprietà è necessaria per una funzione di cifratura?
   (a) L'iniettività.
   (b) La resistenza agli attacchi di preimmagine e di collisione.
   (c) La suriettività.
4. Quale proprietà caratterizza i cifrari a flusso?
   (a) Combinano i dati da cifrare con un flusso potenzialmente infinito di dati (pseudo-) casuali.
   (b) Sono necessariamente interattivi.
   (c) Non richiedono che gli interlocutori abbiano concordato e condiviso una chiave.
5. Quale, tra i seguenti, è un possibile problema del cifrario RSA?
   (a) La possibilità di un attacco Man-in-the-Middle.
   (b) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (c) La lentezza in rapporto ai cifrari a chiave condivisa.
6. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (b) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (c) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
7. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) Il common name del richiedente.
   (b) La chiave pubblica del richiedente.
   (c) La chiave privata del richiedente.
8. Alice e Bob avviano una sessione Diffie-Hellman; per decifrare la chiave di sessione, Charlie (in ascolto sul canale ma non in grado di interferire) deve...
   (a) ...fattorizzare un grande prodotto di numeri primi.
   (b) ...risolvere un problema di logaritmo discreto.
   (c) ...trovare una collisione in un valore hash crittografico.
9. Quale delle seguenti proprietà è necessaria affinché una funzione hash sia crittograficamente sicura?
   (a) La resistenza agli attacchi di preimmagine e di collisione.
   (b) L'iniettività.
   (c) La suriettività.
10. Quale, tra i seguenti, è un possibile problema del protocollo Diffie-Hellman?
    (a) La difficoltà di trovare numeri primi di dimensioni sufficienti.
    (b) La lentezza in rapporto ai cifrari a chiave condivisa.
    (c) La possibilità di un attacco Man-in-the-Middle.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Tema 83

Lunedì 4 giugno 2018

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 13$ e sul generatore $g = 7$.

1.1) Supponendo che Alice scelga il valore segreto $a = 10$ e Bob il valore $b = 2$, descrivere lo scambio di informazioni che avviene fra i due interlocutori.

1.2) Calcolare la chiave condivisa K utilizzando la formula più conveniente fra quella usata da Alice e quella usata da Bob.

Esercizio 2

Il server web di Alice dispone di un sistema di login basato su username e password; per comodità, assumiamo che le password siano stringhe di bit.
Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile: si assuma che utilizzi una stringa casuale di 64 bit.
Il server applica alle password degli utenti una funzione hash crittografica H che genera un valore a 26 bit. In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 26 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.

Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H, ma che sappia che Bob utilizza una password di 64 bit. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login verso il server ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password, portandola a 128 bit casuali.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash in locale (nel computer di Charlie) richieda un miliardesimo di secondo.
Le risposte alle domande 2.1 e 2.2 cambiano?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Quale proprietà caratterizza i cifrari a flusso?
   (a) Non richiedono che gli interlocutori abbiano concordato e condiviso una chiave.
   (b) Sono necessariamente interattivi.
   (c) Combinano i dati da cifrare con un flusso potenzialmente infinito di dati (pseudo-) casuali.
2. Quale delle seguenti proprietà **non** è posseduta da nessuna funzione hash crittografica?
   (a) L'iniettività.
   (b) La resistenza agli attacchi di preimmagine e di collisione.
   (c) La suriettività.
3. Quale, tra i seguenti, è un possibile problema del cifrario RSA?
   (a) La possibilità di un attacco Man-in-the-Middle.
   (b) La lentezza in rapporto ai cifrari a chiave condivisa.
   (c) La difficoltà di trovare numeri primi di dimensioni sufficienti.
4. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (b) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (c) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
5. Quale delle seguenti proprietà è necessaria per una funzione di cifratura?
   (a) La resistenza agli attacchi di preimmagine e di collisione.
   (b) L'iniettività.
   (c) La suriettività.
6. Alice e Bob avviano una sessione Diffie-Hellman; per decifrare la chiave di sessione, Charlie (in ascolto sul canale ma non in grado di interferire) deve...
   (a) ...risolvere un problema di logaritmo discreto.
   (b) ...trovare una collisione in un valore hash crittografico.
   (c) ...fattorizzare un grande prodotto di numeri primi.
7. Un certificato di firma digitale solitamente accompagna...
   (a) ...una chiave di sessione, e ne garantisce l'autenticità.
   (b) ...una chiave privata, e garantisce l'identità del possessore della corrispondente chiave pubblica.
   (c) ...una chiave pubblica, e garantisce l'identità del possessore della corrispondente chiave privata.
8. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave privata del richiedente.
   (b) Il common name del richiedente.
   (c) La chiave pubblica del richiedente.
9. Quale delle seguenti proprietà è necessaria affinché una funzione hash sia crittograficamente sicura?
   (a) L'iniettività.
   (b) La suriettività.
   (c) La resistenza agli attacchi di preimmagine e di collisione.
10. Quale, tra i seguenti, è un possibile problema del protocollo Diffie-Hellman?
    (a) La possibilità di un attacco Man-in-the-Middle.
    (b) La difficoltà di trovare numeri primi di dimensioni sufficienti.
    (c) La lentezza in rapporto ai cifrari a chiave condivisa.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Tema 84

Lunedì 4 giugno 2018

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 11$ e sul generatore $g = 8$.

1.1) Supponendo che Alice scelga il valore segreto $a = 7$ e Bob il valore $b = 5$, descrivere lo scambio di informazioni che avviene fra i due interlocutori.

1.2) Calcolare la chiave condivisa K utilizzando la formula più conveniente fra quella usata da Alice e quella usata da Bob.

Esercizio 2

Il server web di Alice dispone di un sistema di login basato su username e password; per comodità, assumiamo che le password siano stringhe di bit.
Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile: si assuma che utilizzi una stringa casuale di 64 bit.
Il server applica alle password degli utenti una funzione hash crittografica H che genera un valore a 24 bit. In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 24 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.

Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H, ma che sappia che Bob utilizza una password di 64 bit. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login verso il server ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password, portandola a 128 bit casuali.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash in locale (nel computer di Charlie) richieda un miliardesimo di secondo.
Le risposte alle domande 2.1 e 2.2 cambiano?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Quale delle seguenti proprietà **non** è posseduta da nessuna funzione hash crittografica?
   (a) L'iniettività.
   (b) La resistenza agli attacchi di preimmagine e di collisione.
   (c) La suriettività.
2. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (b) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (c) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
3. Quale delle seguenti proprietà è necessaria per una funzione di cifratura?
   (a) La suriettività.
   (b) La resistenza agli attacchi di preimmagine e di collisione.
   (c) L'iniettività.
4. Quale proprietà caratterizza i cifrari a flusso?
   (a) Sono necessariamente interattivi.
   (b) Combinano i dati da cifrare con un flusso potenzialmente infinito di dati (pseudo-) casuali.
   (c) Non richiedono che gli interlocutori abbiano concordato e condiviso una chiave.
5. Quale delle seguenti proprietà è necessaria affinché una funzione hash sia crittograficamente sicura?
   (a) L'iniettività.
   (b) La resistenza agli attacchi di preimmagine e di collisione.
   (c) La suriettività.
6. Quale, tra i seguenti, è un possibile problema del cifrario RSA?
   (a) La possibilità di un attacco Man-in-the-Middle.
   (b) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (c) La lentezza in rapporto ai cifrari a chiave condivisa.
7. Quale, tra i seguenti, è un possibile problema del protocollo Diffie-Hellman?
   (a) La possibilità di un attacco Man-in-the-Middle.
   (b) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (c) La lentezza in rapporto ai cifrari a chiave condivisa.
8. Alice e Bob avviano una sessione Diffie-Hellman; per decifrare la chiave di sessione, Charlie (in ascolto sul canale ma non in grado di interferire) deve...
   (a) ...trovare una collisione in un valore hash crittografico.
   (b) ...risolvere un problema di logaritmo discreto.
   (c) ...fattorizzare un grande prodotto di numeri primi.
9. Un certificato di firma digitale solitamente accompagna...
   (a) ...una chiave privata, e garantisce l'identità del possessore della corrispondente chiave pubblica.
   (b) ...una chiave pubblica, e garantisce l'identità del possessore della corrispondente chiave privata.
   (c) ...una chiave di sessione, e ne garantisce l'autenticità.
10. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
    (a) La chiave privata del richiedente.
    (b) Il common name del richiedente.
    (c) La chiave pubblica del richiedente.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Tema 85

Lunedì 4 giugno 2018

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 11$ e sul generatore $g = 7$.

1.1) Supponendo che Alice scelga il valore segreto $a = 8$ e Bob il valore $b = 4$, descrivere lo scambio di informazioni che avviene fra i due interlocutori.

1.2) Calcolare la chiave condivisa K utilizzando la formula più conveniente fra quella usata da Alice e quella usata da Bob.

Esercizio 2

Il server web di Alice dispone di un sistema di login basato su username e password; per comodità, assumiamo che le password siano stringhe di bit.
Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile: si assuma che utilizzi una stringa casuale di 64 bit.
Il server applica alle password degli utenti una funzione hash crittografica H che genera un valore a 32 bit. In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 32 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.

Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H, ma che sappia che Bob utilizza una password di 64 bit. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login verso il server ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password, portandola a 128 bit casuali.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash in locale (nel computer di Charlie) richieda un miliardesimo di secondo.
Le risposte alle domande 2.1 e 2.2 cambiano?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Quale proprietà caratterizza i cifrari a flusso?
   (a) Sono necessariamente interattivi.
   (b) Non richiedono che gli interlocutori abbiano concordato e condiviso una chiave.
   (c) Combinano i dati da cifrare con un flusso potenzialmente infinito di dati (pseudo-) casuali.
2. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (b) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (c) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
3. Quale delle seguenti proprietà **non** è posseduta da nessuna funzione hash crittografica?
   (a) La suriettività.
   (b) L'iniettività.
   (c) La resistenza agli attacchi di preimmagine e di collisione.
4. Quale, tra i seguenti, è un possibile problema del cifrario RSA?
   (a) La lentezza in rapporto ai cifrari a chiave condivisa.
   (b) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (c) La possibilità di un attacco Man-in-the-Middle.
5. Quale, tra i seguenti, è un possibile problema del protocollo Diffie-Hellman?
   (a) La lentezza in rapporto ai cifrari a chiave condivisa.
   (b) La possibilità di un attacco Man-in-the-Middle.
   (c) La difficoltà di trovare numeri primi di dimensioni sufficienti.
6. Alice e Bob avviano una sessione Diffie-Hellman; per decifrare la chiave di sessione, Charlie (in ascolto sul canale ma non in grado di interferire) deve...
   (a) ...fattorizzare un grande prodotto di numeri primi.
   (b) ...trovare una collisione in un valore hash crittografico.
   (c) ...risolvere un problema di logaritmo discreto.
7. Quale delle seguenti proprietà è necessaria affinché una funzione hash sia crittograficamente sicura?
   (a) La suriettività.
   (b) L'iniettività.
   (c) La resistenza agli attacchi di preimmagine e di collisione.
8. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave privata del richiedente.
   (b) Il common name del richiedente.
   (c) La chiave pubblica del richiedente.
9. Un certificato di firma digitale solitamente accompagna...
   (a) ...una chiave privata, e garantisce l'identità del possessore della corrispondente chiave pubblica.
   (b) ...una chiave pubblica, e garantisce l'identità del possessore della corrispondente chiave privata.
   (c) ...una chiave di sessione, e ne garantisce l'autenticità.
10. Quale delle seguenti proprietà è necessaria per una funzione di cifratura?
    (a) La suriettività.
    (b) La resistenza agli attacchi di preimmagine e di collisione.
    (c) L'iniettività.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Tema 86

Lunedì 4 giugno 2018

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 13$ e sul generatore $g = 6$.

1.1) Supponendo che Alice scelga il valore segreto $a = 11$ e Bob il valore $b = 5$, descrivere lo scambio di informazioni che avviene fra i due interlocutori.

1.2) Calcolare la chiave condivisa K utilizzando la formula più conveniente fra quella usata da Alice e quella usata da Bob.

Esercizio 2

Il server web di Alice dispone di un sistema di login basato su username e password; per comodità, assumiamo che le password siano stringhe di bit.
Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile: si assuma che utilizzi una stringa casuale di 64 bit.
Il server applica alle password degli utenti una funzione hash crittografica H che genera un valore a 32 bit. In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 32 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.

Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H, ma che sappia che Bob utilizza una password di 64 bit. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login verso il server ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password, portandola a 128 bit casuali.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash in locale (nel computer di Charlie) richieda un miliardesimo di secondo.
Le risposte alle domande 2.1 e 2.2 cambiano?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Quale, tra i seguenti, è un possibile problema del protocollo Diffie-Hellman?
   (a) La possibilità di un attacco Man-in-the-Middle.
   (b) La lentezza in rapporto ai cifrari a chiave condivisa.
   (c) La difficoltà di trovare numeri primi di dimensioni sufficienti.
2. Quale proprietà caratterizza i cifrari a flusso?
   (a) Combinano i dati da cifrare con un flusso potenzialmente infinito di dati (pseudo-) casuali.
   (b) Sono necessariamente interattivi.
   (c) Non richiedono che gli interlocutori abbiano concordato e condiviso una chiave.
3. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (b) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (c) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
4. Quale delle seguenti proprietà è necessaria per una funzione di cifratura?
   (a) La resistenza agli attacchi di preimmagine e di collisione.
   (b) L'iniettività.
   (c) La suriettività.
5. Quale delle seguenti proprietà è necessaria affinché una funzione hash sia crittograficamente sicura?
   (a) La resistenza agli attacchi di preimmagine e di collisione.
   (b) La suriettività.
   (c) L'iniettività.
6. Alice e Bob avviano una sessione Diffie-Hellman; per decifrare la chiave di sessione, Charlie (in ascolto sul canale ma non in grado di interferire) deve...
   (a) ...risolvere un problema di logaritmo discreto.
   (b) ...trovare una collisione in un valore hash crittografico.
   (c) ...fattorizzare un grande prodotto di numeri primi.
7. Un certificato di firma digitale solitamente accompagna...
   (a) ...una chiave privata, e garantisce l'identità del possessore della corrispondente chiave pubblica.
   (b) ...una chiave di sessione, e ne garantisce l'autenticità.
   (c) ...una chiave pubblica, e garantisce l'identità del possessore della corrispondente chiave privata.
8. Quale delle seguenti proprietà **non** è posseduta da nessuna funzione hash crittografica?
   (a) La resistenza agli attacchi di preimmagine e di collisione.
   (b) L'iniettività.
   (c) La suriettività.
9. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave privata del richiedente.
   (b) Il common name del richiedente.
   (c) La chiave pubblica del richiedente.
10. Quale, tra i seguenti, è un possibile problema del cifrario RSA?
    (a) La possibilità di un attacco Man-in-the-Middle.
    (b) La lentezza in rapporto ai cifrari a chiave condivisa.
    (c) La difficoltà di trovare numeri primi di dimensioni sufficienti.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Tema 87

Lunedì 4 giugno 2018

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 13$ e sul generatore $g = 6$.

1.1) Supponendo che Alice scelga il valore segreto $a = 11$ e Bob il valore $b = 5$, descrivere lo scambio di informazioni che avviene fra i due interlocutori.

1.2) Calcolare la chiave condivisa K utilizzando la formula più conveniente fra quella usata da Alice e quella usata da Bob.

Esercizio 2

Il server web di Alice dispone di un sistema di login basato su username e password; per comodità, assumiamo che le password siano stringhe di bit.
Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile: si assuma che utilizzi una stringa casuale di 64 bit.
Il server applica alle password degli utenti una funzione hash crittografica H che genera un valore a 32 bit. In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 32 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.

Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H, ma che sappia che Bob utilizza una password di 64 bit. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login verso il server ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password, portandola a 128 bit casuali.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash in locale (nel computer di Charlie) richieda un miliardesimo di secondo.
Le risposte alle domande 2.1 e 2.2 cambiano?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Quale proprietà caratterizza i cifrari a flusso?
   (a) Sono necessariamente interattivi.
   (b) Combinano i dati da cifrare con un flusso potenzialmente infinito di dati (pseudo-) casuali.
   (c) Non richiedono che gli interlocutori abbiano concordato e condiviso una chiave.
2. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) Il common name del richiedente.
   (b) La chiave pubblica del richiedente.
   (c) La chiave privata del richiedente.
3. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (b) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (c) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
4. Quale delle seguenti proprietà è necessaria affinché una funzione hash sia crittograficamente sicura?
   (a) La suriettività.
   (b) L'iniettività.
   (c) La resistenza agli attacchi di preimmagine e di collisione.
5. Un certificato di firma digitale solitamente accompagna...
   (a) ...una chiave privata, e garantisce l'identità del possessore della corrispondente chiave pubblica.
   (b) ...una chiave pubblica, e garantisce l'identità del possessore della corrispondente chiave privata.
   (c) ...una chiave di sessione, e ne garantisce l'autenticità.
6. Quale, tra i seguenti, è un possibile problema del protocollo Diffie-Hellman?
   (a) La possibilità di un attacco Man-in-the-Middle.
   (b) La lentezza in rapporto ai cifrari a chiave condivisa.
   (c) La difficoltà di trovare numeri primi di dimensioni sufficienti.
7. Quale, tra i seguenti, è un possibile problema del cifrario RSA?
   (a) La possibilità di un attacco Man-in-the-Middle.
   (b) La lentezza in rapporto ai cifrari a chiave condivisa.
   (c) La difficoltà di trovare numeri primi di dimensioni sufficienti.
8. Quale delle seguenti proprietà è necessaria per una funzione di cifratura?
   (a) La resistenza agli attacchi di preimmagine e di collisione.
   (b) L'iniettività.
   (c) La suriettività.
9. Alice e Bob avviano una sessione Diffie-Hellman; per decifrare la chiave di sessione, Charlie (in ascolto sul canale ma non in grado di interferire) deve...
   (a) ...trovare una collisione in un valore hash crittografico.
   (b) ...fattorizzare un grande prodotto di numeri primi.
   (c) ...risolvere un problema di logaritmo discreto.
10. Quale delle seguenti proprietà **non** è posseduta da nessuna funzione hash crittografica?
    (a) La resistenza agli attacchi di preimmagine e di collisione.
    (b) La suriettività.
    (c) L'iniettività.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Tema 88

Lunedì 4 giugno 2018

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 13$ e sul generatore $g = 6$.

1.1) Supponendo che Alice scelga il valore segreto $a = 10$ e Bob il valore $b = 2$, descrivere lo scambio di informazioni che avviene fra i due interlocutori.

1.2) Calcolare la chiave condivisa K utilizzando la formula più conveniente fra quella usata da Alice e quella usata da Bob.

Esercizio 2

Il server web di Alice dispone di un sistema di login basato su username e password; per comodità, assumiamo che le password siano stringhe di bit.
Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile: si assuma che utilizzi una stringa casuale di 64 bit.
Il server applica alle password degli utenti una funzione hash crittografica H che genera un valore a 32 bit. In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 32 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.

Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H, ma che sappia che Bob utilizza una password di 64 bit. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login verso il server ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password, portandola a 128 bit casuali.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash in locale (nel computer di Charlie) richieda un miliardesimo di secondo.
Le risposte alle domande 2.1 e 2.2 cambiano?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Alice e Bob avviano una sessione Diffie-Hellman; per decifrare la chiave di sessione, Charlie (in ascolto sul canale ma non in grado di interferire) deve...
   (a) ...risolvere un problema di logaritmo discreto.
   (b) ...trovare una collisione in un valore hash crittografico.
   (c) ...fattorizzare un grande prodotto di numeri primi.
2. Quale delle seguenti proprietà è necessaria per una funzione di cifratura?
   (a) L'iniettività.
   (b) La resistenza agli attacchi di preimmagine e di collisione.
   (c) La suriettività.
3. Quale delle seguenti proprietà **non** è posseduta da nessuna funzione hash crittografica?
   (a) L'iniettività.
   (b) La resistenza agli attacchi di preimmagine e di collisione.
   (c) La suriettività.
4. Quale delle seguenti proprietà è necessaria affinché una funzione hash sia crittograficamente sicura?
   (a) L'iniettività.
   (b) La suriettività.
   (c) La resistenza agli attacchi di preimmagine e di collisione.
5. Un certificato di firma digitale solitamente accompagna...
   (a) ...una chiave di sessione, e ne garantisce l'autenticità.
   (b) ...una chiave pubblica, e garantisce l'identità del possessore della corrispondente chiave privata.
   (c) ...una chiave privata, e garantisce l'identità del possessore della corrispondente chiave pubblica.
6. Quale, tra i seguenti, è un possibile problema del cifrario RSA?
   (a) La possibilità di un attacco Man-in-the-Middle.
   (b) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (c) La lentezza in rapporto ai cifrari a chiave condivisa.
7. Quale, tra i seguenti, è un possibile problema del protocollo Diffie-Hellman?
   (a) La lentezza in rapporto ai cifrari a chiave condivisa.
   (b) La possibilità di un attacco Man-in-the-Middle.
   (c) La difficoltà di trovare numeri primi di dimensioni sufficienti.
8. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave privata del richiedente.
   (b) La chiave pubblica del richiedente.
   (c) Il common name del richiedente.
9. Quale proprietà caratterizza i cifrari a flusso?
   (a) Combinano i dati da cifrare con un flusso potenzialmente infinito di dati (pseudo-) casuali.
   (b) Sono necessariamente interattivi.
   (c) Non richiedono che gli interlocutori abbiano concordato e condiviso una chiave.
10. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
    (a) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
    (b) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
    (c) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Tema 89

Lunedì 4 giugno 2018

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 11$ e sul generatore $g = 6$.

1.1) Supponendo che Alice scelga il valore segreto $a = 9$ e Bob il valore $b = 3$, descrivere lo scambio di informazioni che avviene fra i due interlocutori.

1.2) Calcolare la chiave condivisa K utilizzando la formula più conveniente fra quella usata da Alice e quella usata da Bob.

Esercizio 2

Il server web di Alice dispone di un sistema di login basato su username e password; per comodità, assumiamo che le password siano stringhe di bit.
Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile: si assuma che utilizzi una stringa casuale di 64 bit.
Il server applica alle password degli utenti una funzione hash crittografica H che genera un valore a 28 bit. In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 28 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.

Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H, ma che sappia che Bob utilizza una password di 64 bit. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login verso il server ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password, portandola a 128 bit casuali.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash in locale (nel computer di Charlie) richieda un miliardesimo di secondo.
Le risposte alle domande 2.1 e 2.2 cambiano?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Un certificato di firma digitale solitamente accompagna...
   (a) ...una chiave pubblica, e garantisce l'identità del possessore della corrispondente chiave privata.
   (b) ...una chiave di sessione, e ne garantisce l'autenticità.
   (c) ...una chiave privata, e garantisce l'identità del possessore della corrispondente chiave pubblica.
2. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (b) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (c) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
3. Quale delle seguenti proprietà è necessaria per una funzione di cifratura?
   (a) La resistenza agli attacchi di preimmagine e di collisione.
   (b) La suriettività.
   (c) L'iniettività.
4. Quale delle seguenti proprietà è necessaria affinché una funzione hash sia crittograficamente sicura?
   (a) La resistenza agli attacchi di preimmagine e di collisione.
   (b) La suriettività.
   (c) L'iniettività.
5. Quale, tra i seguenti, è un possibile problema del protocollo Diffie-Hellman?
   (a) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (b) La possibilità di un attacco Man-in-the-Middle.
   (c) La lentezza in rapporto ai cifrari a chiave condivisa.
6. Quale delle seguenti proprietà **non** è posseduta da nessuna funzione hash crittografica?
   (a) La resistenza agli attacchi di preimmagine e di collisione.
   (b) L'iniettività.
   (c) La suriettività.
7. Alice e Bob avviano una sessione Diffie-Hellman; per decifrare la chiave di sessione, Charlie (in ascolto sul canale ma non in grado di interferire) deve...
   (a) ...fattorizzare un grande prodotto di numeri primi.
   (b) ...risolvere un problema di logaritmo discreto.
   (c) ...trovare una collisione in un valore hash crittografico.
8. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) Il common name del richiedente.
   (b) La chiave pubblica del richiedente.
   (c) La chiave privata del richiedente.
9. Quale proprietà caratterizza i cifrari a flusso?
   (a) Sono necessariamente interattivi.
   (b) Combinano i dati da cifrare con un flusso potenzialmente infinito di dati (pseudo-) casuali.
   (c) Non richiedono che gli interlocutori abbiano concordato e condiviso una chiave.
10. Quale, tra i seguenti, è un possibile problema del cifrario RSA?
    (a) La possibilità di un attacco Man-in-the-Middle.
    (b) La lentezza in rapporto ai cifrari a chiave condivisa.
    (c) La difficoltà di trovare numeri primi di dimensioni sufficienti.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Tema 90

Lunedì 4 giugno 2018

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 13$ e sul generatore $g = 7$.

1.1) Supponendo che Alice scelga il valore segreto $a = 10$ e Bob il valore $b = 4$, descrivere lo scambio di informazioni che avviene fra i due interlocutori.

1.2) Calcolare la chiave condivisa K utilizzando la formula più conveniente fra quella usata da Alice e quella usata da Bob.

Esercizio 2

Il server web di Alice dispone di un sistema di login basato su username e password; per comodità, assumiamo che le password siano stringhe di bit.
Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile: si assuma che utilizzi una stringa casuale di 64 bit.
Il server applica alle password degli utenti una funzione hash crittografica H che genera un valore a 30 bit. In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 30 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.

Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H, ma che sappia che Bob utilizza una password di 64 bit. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login verso il server ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password, portandola a 128 bit casuali.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash in locale (nel computer di Charlie) richieda un miliardesimo di secondo.
Le risposte alle domande 2.1 e 2.2 cambiano?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Quale, tra i seguenti, è un possibile problema del cifrario RSA?
   (a) La possibilità di un attacco Man-in-the-Middle.
   (b) La lentezza in rapporto ai cifrari a chiave condivisa.
   (c) La difficoltà di trovare numeri primi di dimensioni sufficienti.
2. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (b) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (c) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
3. Un certificato di firma digitale solitamente accompagna...
   (a) ...una chiave di sessione, e ne garantisce l'autenticità.
   (b) ...una chiave pubblica, e garantisce l'identità del possessore della corrispondente chiave privata.
   (c) ...una chiave privata, e garantisce l'identità del possessore della corrispondente chiave pubblica.
4. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) Il common name del richiedente.
   (b) La chiave pubblica del richiedente.
   (c) La chiave privata del richiedente.
5. Quale delle seguenti proprietà **non** è posseduta da nessuna funzione hash crittografica?
   (a) L'iniettività.
   (b) La suriettività.
   (c) La resistenza agli attacchi di preimmagine e di collisione.
6. Quale proprietà caratterizza i cifrari a flusso?
   (a) Combinano i dati da cifrare con un flusso potenzialmente infinito di dati (pseudo-) casuali.
   (b) Non richiedono che gli interlocutori abbiano concordato e condiviso una chiave.
   (c) Sono necessariamente interattivi.
7. Quale delle seguenti proprietà è necessaria affinché una funzione hash sia crittograficamente sicura?
   (a) L'iniettività.
   (b) La suriettività.
   (c) La resistenza agli attacchi di preimmagine e di collisione.
8. Quale delle seguenti proprietà è necessaria per una funzione di cifratura?
   (a) L'iniettività.
   (b) La resistenza agli attacchi di preimmagine e di collisione.
   (c) La suriettività.
9. Quale, tra i seguenti, è un possibile problema del protocollo Diffie-Hellman?
   (a) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (b) La lentezza in rapporto ai cifrari a chiave condivisa.
   (c) La possibilità di un attacco Man-in-the-Middle.
10. Alice e Bob avviano una sessione Diffie-Hellman; per decifrare la chiave di sessione, Charlie (in ascolto sul canale ma non in grado di interferire) deve...
    (a) ...trovare una collisione in un valore hash crittografico.
    (b) ...fattorizzare un grande prodotto di numeri primi.
    (c) ...risolvere un problema di logaritmo discreto.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Tema 91

Lunedì 4 giugno 2018

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 11$ e sul generatore $g = 8$.

1.1) Supponendo che Alice scelga il valore segreto $a = 7$ e Bob il valore $b = 5$, descrivere lo scambio di informazioni che avviene fra i due interlocutori.

1.2) Calcolare la chiave condivisa K utilizzando la formula più conveniente fra quella usata da Alice e quella usata da Bob.

Esercizio 2

Il server web di Alice dispone di un sistema di login basato su username e password; per comodità, assumiamo che le password siano stringhe di bit.
Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile: si assuma che utilizzi una stringa casuale di 64 bit.
Il server applica alle password degli utenti una funzione hash crittografica H che genera un valore a 24 bit. In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 24 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.

Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H, ma che sappia che Bob utilizza una password di 64 bit. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login verso il server ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password, portandola a 128 bit casuali.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash in locale (nel computer di Charlie) richieda un miliardesimo di secondo.
Le risposte alle domande 2.1 e 2.2 cambiano?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Quale, tra i seguenti, è un possibile problema del cifrario RSA?
   (a) La possibilità di un attacco Man-in-the-Middle.
   (b) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (c) La lentezza in rapporto ai cifrari a chiave condivisa.
2. Un certificato di firma digitale solitamente accompagna...
   (a) ...una chiave privata, e garantisce l'identità del possessore della corrispondente chiave pubblica.
   (b) ...una chiave di sessione, e ne garantisce l'autenticità.
   (c) ...una chiave pubblica, e garantisce l'identità del possessore della corrispondente chiave privata.
3. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (b) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (c) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
4. Quale delle seguenti proprietà **non** è posseduta da nessuna funzione hash crittografica?
   (a) La suriettività.
   (b) L'iniettività.
   (c) La resistenza agli attacchi di preimmagine e di collisione.
5. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave privata del richiedente.
   (b) Il common name del richiedente.
   (c) La chiave pubblica del richiedente.
6. Quale delle seguenti proprietà è necessaria affinché una funzione hash sia crittograficamente sicura?
   (a) La resistenza agli attacchi di preimmagine e di collisione.
   (b) La suriettività.
   (c) L'iniettività.
7. Quale, tra i seguenti, è un possibile problema del protocollo Diffie-Hellman?
   (a) La lentezza in rapporto ai cifrari a chiave condivisa.
   (b) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (c) La possibilità di un attacco Man-in-the-Middle.
8. Alice e Bob avviano una sessione Diffie-Hellman; per decifrare la chiave di sessione, Charlie (in ascolto sul canale ma non in grado di interferire) deve...
   (a) ...fattorizzare un grande prodotto di numeri primi.
   (b) ...trovare una collisione in un valore hash crittografico.
   (c) ...risolvere un problema di logaritmo discreto.
9. Quale delle seguenti proprietà è necessaria per una funzione di cifratura?
   (a) L'iniettività.
   (b) La resistenza agli attacchi di preimmagine e di collisione.
   (c) La suriettività.
10. Quale proprietà caratterizza i cifrari a flusso?
    (a) Combinano i dati da cifrare con un flusso potenzialmente infinito di dati (pseudo-) casuali.
    (b) Sono necessariamente interattivi.
    (c) Non richiedono che gli interlocutori abbiano concordato e condiviso una chiave.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Tema 92

Lunedì 4 giugno 2018

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 13$ e sul generatore $g = 6$.

1.1) Supponendo che Alice scelga il valore segreto $a = 10$ e Bob il valore $b = 2$, descrivere lo scambio di informazioni che avviene fra i due interlocutori.

1.2) Calcolare la chiave condivisa K utilizzando la formula più conveniente fra quella usata da Alice e quella usata da Bob.

Esercizio 2

Il server web di Alice dispone di un sistema di login basato su username e password; per comodità, assumiamo che le password siano stringhe di bit.
Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile: si assuma che utilizzi una stringa casuale di 64 bit.
Il server applica alle password degli utenti una funzione hash crittografica H che genera un valore a 28 bit. In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 28 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.

Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H, ma che sappia che Bob utilizza una password di 64 bit. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login verso il server ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password, portandola a 128 bit casuali.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash in locale (nel computer di Charlie) richieda un miliardesimo di secondo.
Le risposte alle domande 2.1 e 2.2 cambiano?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Quale delle seguenti proprietà è necessaria affinché una funzione hash sia crittograficamente sicura?
   (a) L'iniettività.
   (b) La suriettività.
   (c) La resistenza agli attacchi di preimmagine e di collisione.
2. Alice e Bob avviano una sessione Diffie-Hellman; per decifrare la chiave di sessione, Charlie (in ascolto sul canale ma non in grado di interferire) deve...
   (a) ...risolvere un problema di logaritmo discreto.
   (b) ...fattorizzare un grande prodotto di numeri primi.
   (c) ...trovare una collisione in un valore hash crittografico.
3. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave pubblica del richiedente.
   (b) La chiave privata del richiedente.
   (c) Il common name del richiedente.
4. Quale, tra i seguenti, è un possibile problema del cifrario RSA?
   (a) La lentezza in rapporto ai cifrari a chiave condivisa.
   (b) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (c) La possibilità di un attacco Man-in-the-Middle.
5. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (b) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (c) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
6. Quale, tra i seguenti, è un possibile problema del protocollo Diffie-Hellman?
   (a) La lentezza in rapporto ai cifrari a chiave condivisa.
   (b) La possibilità di un attacco Man-in-the-Middle.
   (c) La difficoltà di trovare numeri primi di dimensioni sufficienti.
7. Quale delle seguenti proprietà è necessaria per una funzione di cifratura?
   (a) L'iniettività.
   (b) La resistenza agli attacchi di preimmagine e di collisione.
   (c) La suriettività.
8. Un certificato di firma digitale solitamente accompagna...
   (a) ...una chiave privata, e garantisce l'identità del possessore della corrispondente chiave pubblica.
   (b) ...una chiave pubblica, e garantisce l'identità del possessore della corrispondente chiave privata.
   (c) ...una chiave di sessione, e ne garantisce l'autenticità.
9. Quale delle seguenti proprietà **non** è posseduta da nessuna funzione hash crittografica?
   (a) La resistenza agli attacchi di preimmagine e di collisione.
   (b) L'iniettività.
   (c) La suriettività.
10. Quale proprietà caratterizza i cifrari a flusso?
    (a) Non richiedono che gli interlocutori abbiano concordato e condiviso una chiave.
    (b) Sono necessariamente interattivi.
    (c) Combinano i dati da cifrare con un flusso potenzialmente infinito di dati (pseudo-) casuali.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Tema 93

Lunedì 4 giugno 2018

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 11$ e sul generatore $g = 8$.

1.1) Supponendo che Alice scelga il valore segreto $a = 8$ e Bob il valore $b = 4$, descrivere lo scambio di informazioni che avviene fra i due interlocutori.

1.2) Calcolare la chiave condivisa K utilizzando la formula più conveniente fra quella usata da Alice e quella usata da Bob.

Esercizio 2

Il server web di Alice dispone di un sistema di login basato su username e password; per comodità, assumiamo che le password siano stringhe di bit.
Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile: si assuma che utilizzi una stringa casuale di 64 bit.
Il server applica alle password degli utenti una funzione hash crittografica H che genera un valore a 26 bit. In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 26 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.

Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H, ma che sappia che Bob utilizza una password di 64 bit. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login verso il server ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password, portandola a 128 bit casuali.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash in locale (nel computer di Charlie) richieda un miliardesimo di secondo.
Le risposte alle domande 2.1 e 2.2 cambiano?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Quale delle seguenti proprietà **non** è posseduta da nessuna funzione hash crittografica?
   (a) L'iniettività.
   (b) La suriettività.
   (c) La resistenza agli attacchi di preimmagine e di collisione.
2. Un certificato di firma digitale solitamente accompagna...
   (a) ...una chiave pubblica, e garantisce l'identità del possessore della corrispondente chiave privata.
   (b) ...una chiave privata, e garantisce l'identità del possessore della corrispondente chiave pubblica.
   (c) ...una chiave di sessione, e ne garantisce l'autenticità.
3. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) Il common name del richiedente.
   (b) La chiave privata del richiedente.
   (c) La chiave pubblica del richiedente.
4. Quale, tra i seguenti, è un possibile problema del cifrario RSA?
   (a) La possibilità di un attacco Man-in-the-Middle.
   (b) La lentezza in rapporto ai cifrari a chiave condivisa.
   (c) La difficoltà di trovare numeri primi di dimensioni sufficienti.
5. Quale proprietà caratterizza i cifrari a flusso?
   (a) Sono necessariamente interattivi.
   (b) Non richiedono che gli interlocutori abbiano concordato e condiviso una chiave.
   (c) Combinano i dati da cifrare con un flusso potenzialmente infinito di dati (pseudo-) casuali.
6. Quale, tra i seguenti, è un possibile problema del protocollo Diffie-Hellman?
   (a) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (b) La possibilità di un attacco Man-in-the-Middle.
   (c) La lentezza in rapporto ai cifrari a chiave condivisa.
7. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (b) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (c) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
8. Alice e Bob avviano una sessione Diffie-Hellman; per decifrare la chiave di sessione, Charlie (in ascolto sul canale ma non in grado di interferire) deve...
   (a) ...risolvere un problema di logaritmo discreto.
   (b) ...fattorizzare un grande prodotto di numeri primi.
   (c) ...trovare una collisione in un valore hash crittografico.
9. Quale delle seguenti proprietà è necessaria affinché una funzione hash sia crittograficamente sicura?
   (a) La suriettività.
   (b) L'iniettività.
   (c) La resistenza agli attacchi di preimmagine e di collisione.
10. Quale delle seguenti proprietà è necessaria per una funzione di cifratura?
    (a) La resistenza agli attacchi di preimmagine e di collisione.
    (b) La suriettività.
    (c) L'iniettività.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Tema 94

Lunedì 4 giugno 2018

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 11$ e sul generatore $g = 8$.

1.1) Supponendo che Alice scelga il valore segreto $a = 8$ e Bob il valore $b = 4$, descrivere lo scambio di informazioni che avviene fra i due interlocutori.

1.2) Calcolare la chiave condivisa K utilizzando la formula più conveniente fra quella usata da Alice e quella usata da Bob.

Esercizio 2

Il server web di Alice dispone di un sistema di login basato su username e password; per comodità, assumiamo che le password siano stringhe di bit.
Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile: si assuma che utilizzi una stringa casuale di 64 bit.
Il server applica alle password degli utenti una funzione hash crittografica H che genera un valore a 24 bit. In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 24 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.

Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H, ma che sappia che Bob utilizza una password di 64 bit. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login verso il server ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password, portandola a 128 bit casuali.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash in locale (nel computer di Charlie) richieda un miliardesimo di secondo.
Le risposte alle domande 2.1 e 2.2 cambiano?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Quale delle seguenti proprietà è necessaria affinché una funzione hash sia crittograficamente sicura?
   (a) L'iniettività.
   (b) La resistenza agli attacchi di preimmagine e di collisione.
   (c) La suriettività.
2. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave privata del richiedente.
   (b) Il common name del richiedente.
   (c) La chiave pubblica del richiedente.
3. Quale delle seguenti proprietà è necessaria per una funzione di cifratura?
   (a) La resistenza agli attacchi di preimmagine e di collisione.
   (b) L'iniettività.
   (c) La suriettività.
4. Alice e Bob avviano una sessione Diffie-Hellman; per decifrare la chiave di sessione, Charlie (in ascolto sul canale ma non in grado di interferire) deve...
   (a) ...risolvere un problema di logaritmo discreto.
   (b) ...trovare una collisione in un valore hash crittografico.
   (c) ...fattorizzare un grande prodotto di numeri primi.
5. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (b) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (c) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
6. Quale, tra i seguenti, è un possibile problema del protocollo Diffie-Hellman?
   (a) La possibilità di un attacco Man-in-the-Middle.
   (b) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (c) La lentezza in rapporto ai cifrari a chiave condivisa.
7. Quale delle seguenti proprietà **non** è posseduta da nessuna funzione hash crittografica?
   (a) La resistenza agli attacchi di preimmagine e di collisione.
   (b) L'iniettività.
   (c) La suriettività.
8. Un certificato di firma digitale solitamente accompagna...
   (a) ...una chiave privata, e garantisce l'identità del possessore della corrispondente chiave pubblica.
   (b) ...una chiave di sessione, e ne garantisce l'autenticità.
   (c) ...una chiave pubblica, e garantisce l'identità del possessore della corrispondente chiave privata.
9. Quale proprietà caratterizza i cifrari a flusso?
   (a) Combinano i dati da cifrare con un flusso potenzialmente infinito di dati (pseudo-) casuali.
   (b) Non richiedono che gli interlocutori abbiano concordato e condiviso una chiave.
   (c) Sono necessariamente interattivi.
10. Quale, tra i seguenti, è un possibile problema del cifrario RSA?
    (a) La possibilità di un attacco Man-in-the-Middle.
    (b) La lentezza in rapporto ai cifrari a chiave condivisa.
    (c) La difficoltà di trovare numeri primi di dimensioni sufficienti.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Tema 95

Lunedì 4 giugno 2018

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 11$ e sul generatore $g = 8$.

1.1) Supponendo che Alice scelga il valore segreto $a = 9$ e Bob il valore $b = 4$, descrivere lo scambio di informazioni che avviene fra i due interlocutori.

1.2) Calcolare la chiave condivisa K utilizzando la formula più conveniente fra quella usata da Alice e quella usata da Bob.

Esercizio 2

Il server web di Alice dispone di un sistema di login basato su username e password; per comodità, assumiamo che le password siano stringhe di bit.
Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile: si assuma che utilizzi una stringa casuale di 64 bit.
Il server applica alle password degli utenti una funzione hash crittografica H che genera un valore a 26 bit. In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 26 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.

Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H, ma che sappia che Bob utilizza una password di 64 bit. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login verso il server ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password, portandola a 128 bit casuali.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash in locale (nel computer di Charlie) richieda un miliardesimo di secondo.
Le risposte alle domande 2.1 e 2.2 cambiano?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (b) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (c) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
2. Un certificato di firma digitale solitamente accompagna...
   (a) ...una chiave privata, e garantisce l'identità del possessore della corrispondente chiave pubblica.
   (b) ...una chiave di sessione, e ne garantisce l'autenticità.
   (c) ...una chiave pubblica, e garantisce l'identità del possessore della corrispondente chiave privata.
3. Quale, tra i seguenti, è un possibile problema del protocollo Diffie-Hellman?
   (a) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (b) La lentezza in rapporto ai cifrari a chiave condivisa.
   (c) La possibilità di un attacco Man-in-the-Middle.
4. Quale, tra i seguenti, è un possibile problema del cifrario RSA?
   (a) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (b) La possibilità di un attacco Man-in-the-Middle.
   (c) La lentezza in rapporto ai cifrari a chiave condivisa.
5. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) Il common name del richiedente.
   (b) La chiave pubblica del richiedente.
   (c) La chiave privata del richiedente.
6. Quale delle seguenti proprietà è necessaria affinché una funzione hash sia crittograficamente sicura?
   (a) L'iniettività.
   (b) La suriettività.
   (c) La resistenza agli attacchi di preimmagine e di collisione.
7. Quale proprietà caratterizza i cifrari a flusso?
   (a) Non richiedono che gli interlocutori abbiano concordato e condiviso una chiave.
   (b) Combinano i dati da cifrare con un flusso potenzialmente infinito di dati (pseudo-) casuali.
   (c) Sono necessariamente interattivi.
8. Quale delle seguenti proprietà è necessaria per una funzione di cifratura?
   (a) La resistenza agli attacchi di preimmagine e di collisione.
   (b) La suriettività.
   (c) L'iniettività.
9. Quale delle seguenti proprietà **non** è posseduta da nessuna funzione hash crittografica?
   (a) La resistenza agli attacchi di preimmagine e di collisione.
   (b) La suriettività.
   (c) L'iniettività.
10. Alice e Bob avviano una sessione Diffie-Hellman; per decifrare la chiave di sessione, Charlie (in ascolto sul canale ma non in grado di interferire) deve...
    (a) ...fattorizzare un grande prodotto di numeri primi.
    (b) ...trovare una collisione in un valore hash crittografico.
    (c) ...risolvere un problema di logaritmo discreto.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Tema 96

Lunedì 4 giugno 2018

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 11$ e sul generatore $g = 6$.

1.1) Supponendo che Alice scelga il valore segreto $a = 8$ e Bob il valore $b = 2$, descrivere lo scambio di informazioni che avviene fra i due interlocutori.

1.2) Calcolare la chiave condivisa K utilizzando la formula più conveniente fra quella usata da Alice e quella usata da Bob.

Esercizio 2

Il server web di Alice dispone di un sistema di login basato su username e password; per comodità, assumiamo che le password siano stringhe di bit.
Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile: si assuma che utilizzi una stringa casuale di 64 bit.
Il server applica alle password degli utenti una funzione hash crittografica H che genera un valore a 24 bit. In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 24 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.

Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H, ma che sappia che Bob utilizza una password di 64 bit. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login verso il server ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password, portandola a 128 bit casuali.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash in locale (nel computer di Charlie) richieda un miliardesimo di secondo.
Le risposte alle domande 2.1 e 2.2 cambiano?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Quale, tra i seguenti, è un possibile problema del cifrario RSA?
   (a) La lentezza in rapporto ai cifrari a chiave condivisa.
   (b) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (c) La possibilità di un attacco Man-in-the-Middle.
2. Quale delle seguenti proprietà **non** è posseduta da nessuna funzione hash crittografica?
   (a) La resistenza agli attacchi di preimmagine e di collisione.
   (b) L'iniettività.
   (c) La suriettività.
3. Un certificato di firma digitale solitamente accompagna...
   (a) ...una chiave di sessione, e ne garantisce l'autenticità.
   (b) ...una chiave pubblica, e garantisce l'identità del possessore della corrispondente chiave privata.
   (c) ...una chiave privata, e garantisce l'identità del possessore della corrispondente chiave pubblica.
4. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave pubblica del richiedente.
   (b) Il common name del richiedente.
   (c) La chiave privata del richiedente.
5. Quale delle seguenti proprietà è necessaria affinché una funzione hash sia crittograficamente sicura?
   (a) La suriettività.
   (b) L'iniettività.
   (c) La resistenza agli attacchi di preimmagine e di collisione.
6. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
   (b) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (c) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
7. Quale proprietà caratterizza i cifrari a flusso?
   (a) Non richiedono che gli interlocutori abbiano concordato e condiviso una chiave.
   (b) Combinano i dati da cifrare con un flusso potenzialmente infinito di dati (pseudo-) casuali.
   (c) Sono necessariamente interattivi.
8. Quale delle seguenti proprietà è necessaria per una funzione di cifratura?
   (a) La suriettività.
   (b) L'iniettività.
   (c) La resistenza agli attacchi di preimmagine e di collisione.
9. Alice e Bob avviano una sessione Diffie-Hellman; per decifrare la chiave di sessione, Charlie (in ascolto sul canale ma non in grado di interferire) deve...
   (a) ...risolvere un problema di logaritmo discreto.
   (b) ...trovare una collisione in un valore hash crittografico.
   (c) ...fattorizzare un grande prodotto di numeri primi.
10. Quale, tra i seguenti, è un possibile problema del protocollo Diffie-Hellman?
    (a) La possibilità di un attacco Man-in-the-Middle.
    (b) La difficoltà di trovare numeri primi di dimensioni sufficienti.
    (c) La lentezza in rapporto ai cifrari a chiave condivisa.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Tema 97

Lunedì 4 giugno 2018

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 13$ e sul generatore $g = 7$.

1.1) Supponendo che Alice scelga il valore segreto $a = 10$ e Bob il valore $b = 3$, descrivere lo scambio di informazioni che avviene fra i due interlocutori.

1.2) Calcolare la chiave condivisa K utilizzando la formula più conveniente fra quella usata da Alice e quella usata da Bob.

Esercizio 2

Il server web di Alice dispone di un sistema di login basato su username e password; per comodità, assumiamo che le password siano stringhe di bit.
Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile: si assuma che utilizzi una stringa casuale di 64 bit.
Il server applica alle password degli utenti una funzione hash crittografica H che genera un valore a 24 bit. In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 24 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.

Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H, ma che sappia che Bob utilizza una password di 64 bit. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login verso il server ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password, portandola a 128 bit casuali.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash in locale (nel computer di Charlie) richieda un miliardesimo di secondo.
Le risposte alle domande 2.1 e 2.2 cambiano?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Quale, tra i seguenti, è un possibile problema del protocollo Diffie-Hellman?
   (a) La possibilità di un attacco Man-in-the-Middle.
   (b) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (c) La lentezza in rapporto ai cifrari a chiave condivisa.
2. Quale delle seguenti proprietà **non** è posseduta da nessuna funzione hash crittografica?
   (a) La suriettività.
   (b) L'iniettività.
   (c) La resistenza agli attacchi di preimmagine e di collisione.
3. Un certificato di firma digitale solitamente accompagna...
   (a) ...una chiave privata, e garantisce l'identità del possessore della corrispondente chiave pubblica.
   (b) ...una chiave di sessione, e ne garantisce l'autenticità.
   (c) ...una chiave pubblica, e garantisce l'identità del possessore della corrispondente chiave privata.
4. Quale delle seguenti proprietà è necessaria per una funzione di cifratura?
   (a) L'iniettività.
   (b) La suriettività.
   (c) La resistenza agli attacchi di preimmagine e di collisione.
5. Quale proprietà caratterizza i cifrari a flusso?
   (a) Sono necessariamente interattivi.
   (b) Combinano i dati da cifrare con un flusso potenzialmente infinito di dati (pseudo-) casuali.
   (c) Non richiedono che gli interlocutori abbiano concordato e condiviso una chiave.
6. Quale delle seguenti proprietà è necessaria affinché una funzione hash sia crittograficamente sicura?
   (a) La resistenza agli attacchi di preimmagine e di collisione.
   (b) La suriettività.
   (c) L'iniettività.
7. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) Il common name del richiedente.
   (b) La chiave pubblica del richiedente.
   (c) La chiave privata del richiedente.
8. Alice e Bob avviano una sessione Diffie-Hellman; per decifrare la chiave di sessione, Charlie (in ascolto sul canale ma non in grado di interferire) deve...
   (a) ...fattorizzare un grande prodotto di numeri primi.
   (b) ...trovare una collisione in un valore hash crittografico.
   (c) ...risolvere un problema di logaritmo discreto.
9. Quale, tra i seguenti, è un possibile problema del cifrario RSA?
   (a) La possibilità di un attacco Man-in-the-Middle.
   (b) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (c) La lentezza in rapporto ai cifrari a chiave condivisa.
10. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
    (a) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
    (b) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
    (c) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Tema 98

Lunedì 4 giugno 2018

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 13$ e sul generatore $g = 6$.

1.1) Supponendo che Alice scelga il valore segreto $a = 10$ e Bob il valore $b = 5$, descrivere lo scambio di informazioni che avviene fra i due interlocutori.

1.2) Calcolare la chiave condivisa K utilizzando la formula più conveniente fra quella usata da Alice e quella usata da Bob.

Esercizio 2

Il server web di Alice dispone di un sistema di login basato su username e password; per comodità, assumiamo che le password siano stringhe di bit.
Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile: si assuma che utilizzi una stringa casuale di 64 bit.
Il server applica alle password degli utenti una funzione hash crittografica H che genera un valore a 28 bit. In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 28 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.

Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H, ma che sappia che Bob utilizza una password di 64 bit. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login verso il server ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password, portandola a 128 bit casuali.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash in locale (nel computer di Charlie) richieda un miliardesimo di secondo.
Le risposte alle domande 2.1 e 2.2 cambiano?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave privata del richiedente.
   (b) La chiave pubblica del richiedente.
   (c) Il common name del richiedente.
2. Quale proprietà caratterizza i cifrari a flusso?
   (a) Non richiedono che gli interlocutori abbiano concordato e condiviso una chiave.
   (b) Sono necessariamente interattivi.
   (c) Combinano i dati da cifrare con un flusso potenzialmente infinito di dati (pseudo-) casuali.
3. Quale delle seguenti proprietà è necessaria per una funzione di cifratura?
   (a) La resistenza agli attacchi di preimmagine e di collisione.
   (b) La suriettività.
   (c) L'iniettività.
4. Quale delle seguenti proprietà **non** è posseduta da nessuna funzione hash crittografica?
   (a) L'iniettività.
   (b) La resistenza agli attacchi di preimmagine e di collisione.
   (c) La suriettività.
5. Un certificato di firma digitale solitamente accompagna...
   (a) ...una chiave privata, e garantisce l'identità del possessore della corrispondente chiave pubblica.
   (b) ...una chiave di sessione, e ne garantisce l'autenticità.
   (c) ...una chiave pubblica, e garantisce l'identità del possessore della corrispondente chiave privata.
6. Alice e Bob avviano una sessione Diffie-Hellman; per decifrare la chiave di sessione, Charlie (in ascolto sul canale ma non in grado di interferire) deve...
   (a) ...fattorizzare un grande prodotto di numeri primi.
   (b) ...risolvere un problema di logaritmo discreto.
   (c) ...trovare una collisione in un valore hash crittografico.
7. Quale, tra i seguenti, è un possibile problema del protocollo Diffie-Hellman?
   (a) La possibilità di un attacco Man-in-the-Middle.
   (b) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (c) La lentezza in rapporto ai cifrari a chiave condivisa.
8. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (b) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (c) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
9. Quale delle seguenti proprietà è necessaria affinché una funzione hash sia crittograficamente sicura?
   (a) La suriettività.
   (b) La resistenza agli attacchi di preimmagine e di collisione.
   (c) L'iniettività.
10. Quale, tra i seguenti, è un possibile problema del cifrario RSA?
    (a) La difficoltà di trovare numeri primi di dimensioni sufficienti.
    (b) La lentezza in rapporto ai cifrari a chiave condivisa.
    (c) La possibilità di un attacco Man-in-the-Middle.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Tema 99

Lunedì 4 giugno 2018

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 11$ e sul generatore $g = 6$.

1.1) Supponendo che Alice scelga il valore segreto $a = 9$ e Bob il valore $b = 4$, descrivere lo scambio di informazioni che avviene fra i due interlocutori.

1.2) Calcolare la chiave condivisa K utilizzando la formula più conveniente fra quella usata da Alice e quella usata da Bob.

Esercizio 2

Il server web di Alice dispone di un sistema di login basato su username e password; per comodità, assumiamo che le password siano stringhe di bit.
Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile: si assuma che utilizzi una stringa casuale di 64 bit.
Il server applica alle password degli utenti una funzione hash crittografica H che genera un valore a 24 bit. In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 24 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.

Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H, ma che sappia che Bob utilizza una password di 64 bit. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login verso il server ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password, portandola a 128 bit casuali.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash in locale (nel computer di Charlie) richieda un miliardesimo di secondo.
Le risposte alle domande 2.1 e 2.2 cambiano?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Un certificato di firma digitale solitamente accompagna...
   (a) ...una chiave di sessione, e ne garantisce l'autenticità.
   (b) ...una chiave pubblica, e garantisce l'identità del possessore della corrispondente chiave privata.
   (c) ...una chiave privata, e garantisce l'identità del possessore della corrispondente chiave pubblica.
2. Alice e Bob avviano una sessione Diffie-Hellman; per decifrare la chiave di sessione, Charlie (in ascolto sul canale ma non in grado di interferire) deve...
   (a) ...fattorizzare un grande prodotto di numeri primi.
   (b) ...risolvere un problema di logaritmo discreto.
   (c) ...trovare una collisione in un valore hash crittografico.
3. Quale delle seguenti proprietà è necessaria affinché una funzione hash sia crittograficamente sicura?
   (a) L'iniettività.
   (b) La suriettività.
   (c) La resistenza agli attacchi di preimmagine e di collisione.
4. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) La chiave pubblica del richiedente.
   (b) La chiave privata del richiedente.
   (c) Il common name del richiedente.
5. Quale delle seguenti proprietà è necessaria per una funzione di cifratura?
   (a) L'iniettività.
   (b) La resistenza agli attacchi di preimmagine e di collisione.
   (c) La suriettività.
6. Quale delle seguenti proprietà **non** è posseduta da nessuna funzione hash crittografica?
   (a) L'iniettività.
   (b) La resistenza agli attacchi di preimmagine e di collisione.
   (c) La suriettività.
7. Quale, tra i seguenti, è un possibile problema del protocollo Diffie-Hellman?
   (a) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (b) La lentezza in rapporto ai cifrari a chiave condivisa.
   (c) La possibilità di un attacco Man-in-the-Middle.
8. Quale, tra i seguenti, è un possibile problema del cifrario RSA?
   (a) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (b) La lentezza in rapporto ai cifrari a chiave condivisa.
   (c) La possibilità di un attacco Man-in-the-Middle.
9. Quale proprietà caratterizza i cifrari a flusso?
   (a) Combinano i dati da cifrare con un flusso potenzialmente infinito di dati (pseudo-) casuali.
   (b) Sono necessariamente interattivi.
   (c) Non richiedono che gli interlocutori abbiano concordato e condiviso una chiave.
10. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
    (a) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
    (b) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
    (c) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Seconda prova parziale

Tema 100

Lunedì 4 giugno 2018

Esercizio 1

Alice e Bob devono condividere una chiave simmetrica K e decidono di affidarsi al protocollo Diffie-Hellman. Concordano sull'uso del numero primo $p = 11$ e sul generatore $g = 7$.

1.1) Supponendo che Alice scelga il valore segreto $a = 9$ e Bob il valore $b = 4$, descrivere lo scambio di informazioni che avviene fra i due interlocutori.

1.2) Calcolare la chiave condivisa K utilizzando la formula più conveniente fra quella usata da Alice e quella usata da Bob.

Esercizio 2

Il server web di Alice dispone di un sistema di login basato su username e password; per comodità, assumiamo che le password siano stringhe di bit.
Bob possiede un account sul server web di Alice, e il suo nome utente è noto a tutti; è però abbastanza furbo da non utilizzare una password prevedibile: si assuma che utilizzi una stringa casuale di 64 bit.
Il server applica alle password degli utenti una funzione hash crittografica H che genera un valore a 32 bit. In altri termini, quando Bob si è registrato e ha creato la propria password P_{Bob}, il server ha calcolato il valore a 32 bit $h_{\text{Bob}} = H(P_{\text{Bob}})$ e l'ha memorizzato nella tabella degli utenti del database in corrispondenza del nome utente di Bob.

Quando Bob effettua il login usando una password P, il server verifica se $H(P)$ è uguale al valore h_{Bob} memorizzato nella tabella utenti.
Charlie vuole impersonare Bob, quindi costruisce un bot che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

2.1) Supponiamo che Charlie non conosca la funzione di hash H, ma che sappia che Bob utilizza una password di 64 bit. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?
Se Charlie riesce ad iniziare una sessione di login verso il server ogni millisecondo, quanto tempo può aspettarsi di impiegare?

2.2) Supponiamo che Bob raddoppi la lunghezza della propria password, portandola a 128 bit casuali.
La risposta alla domanda 2.1 cambia?

2.3) Supponiamo che Charlie conosca la funzione di hash H, e che il calcolo di un singolo hash in locale (nel computer di Charlie) richieda un miliardesimo di secondo.
Le risposte alle domande 2.1 e 2.2 cambiano?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare selvaggiamente le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 3

Per ciascuna delle seguenti domande, riportare nel foglio protocollo il numero della domanda e la lettera della risposta ritenuta corretta. Si prega di non segnare in alcun modo le domande e le risposte su questo foglio.
In caso di incertezza è consentito motivare una risposta con una riga di testo.

1. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?
   (a) Il common name del richiedente.
   (b) La chiave pubblica del richiedente.
   (c) La chiave privata del richiedente.
2. Alice e Bob avviano una sessione Diffie-Hellman; per decifrare la chiave di sessione, Charlie (in ascolto sul canale ma non in grado di interferire) deve...
   (a) ... fattorizzare un grande prodotto di numeri primi.
   (b) ... risolvere un problema di logaritmo discreto.
   (c) ... trovare una collisione in un valore hash crittografico.
3. Quale delle seguenti proprietà è necessaria per una funzione di cifratura?
   (a) La resistenza agli attacchi di preimmagine e di collisione.
   (b) La suriettività.
   (c) L'iniettività.
4. Quale delle seguenti proprietà **non** è posseduta da nessuna funzione hash crittografica?
   (a) La suriettività.
   (b) L'iniettività.
   (c) La resistenza agli attacchi di preimmagine e di collisione.
5. Quale proprietà caratterizza i cifrari a flusso?
   (a) Sono necessariamente interattivi.
   (b) Non richiedono che gli interlocutori abbiano concordato e condiviso una chiave.
   (c) Combinano i dati da cifrare con un flusso potenzialmente infinito di dati (pseudo-) casuali.
6. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?
   (a) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.
   (b) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.
   (c) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.
7. Un certificato di firma digitale solitamente accompagna...
   (a) ... una chiave di sessione, e ne garantisce l'autenticità.
   (b) ... una chiave privata, e garantisce l'identità del possessore della corrispondente chiave pubblica.
   (c) ... una chiave pubblica, e garantisce l'identità del possessore della corrispondente chiave privata.
8. Quale, tra i seguenti, è un possibile problema del protocollo Diffie-Hellman?
   (a) La possibilità di un attacco Man-in-the-Middle.
   (b) La difficoltà di trovare numeri primi di dimensioni sufficienti.
   (c) La lentezza in rapporto ai cifrari a chiave condivisa.
9. Quale delle seguenti proprietà è necessaria affinché una funzione hash sia crittograficamente sicura?
   (a) La resistenza agli attacchi di preimmagine e di collisione.
   (b) La suriettività.
   (c) L'iniettività.
10. Quale, tra i seguenti, è un possibile problema del cifrario RSA?
    (a) La possibilità di un attacco Man-in-the-Middle.
    (b) La difficoltà di trovare numeri primi di dimensioni sufficienti.
    (c) La lentezza in rapporto ai cifrari a chiave condivisa.

Traccia della soluzione all'esercizio 1 (tema 1)

1.1 — Calcolo dei valori pubblici di Alice e Bob

In aritmetica modulo 13:

$$7^1 = 7, 7^2 = 10, 7^3 = 5, 7^4 = 9, 7^5 = 11, 7^6 = 12, 7^7 = 6, 7^8 = 3, 7^9 = 8, 7^{10} = 4, 7^{11} = 2, 7^{12} = 1.$$

Applichiamo le formule, basandoci sulle potenze che abbiamo calcolato al punto 1:

$$A = g^a = 7^{10} \equiv 4 \pmod{13};$$

$$B = g^b = 7^5 \equiv 11 \pmod{13}.$$

1.2 — Chiave condivisa

Possiamo calcolare K in due modi:

$$K \equiv A^b \equiv B^a \pmod{13}$$

Ad esempio,

$$K = A^b = 4^5 \equiv 10 \pmod{13}.$$

Osservazioni

Anche la chiave K va calcolata modulo p.

Traccia della soluzione all'esercizio 2 (tema 1)

2.1 — Tempo per un attacco brute force

Charlie non ne sa nulla della funzione H, ovviamente non conosce h_{Bob}, e possiamo assumere che non conosca nemmeno la dimensione dell'hash generato. Tutto quello che può fare è generare password in sequenza e spedirle al server, sperando che una delle password P sia in collisione con quella di Bob:

$$H(P) = h_{\text{Bob}}.$$

Dato che i valori hash possibili sono 2^{30}, la probabilità di una collisione ad ogni tentativo è 2^{-30}, quindi saranno necessari mediamente 2^{30} tentativi. Si noti che Charlie può generare password sempre diverse, ma non può sperare che gli hash generati siano tutti diversi.

Potendo controllare 10^3 password al secondo, il tempo medio per arrivare a una collisione è

$$2^{30} \cdot 10^{-3} \approx 10^9 \cdot 10^{-3} = 10^6\text{s}.$$

Siccome in un giorno ci sono $86400 \approx 10^5$ secondi, Charlie impiegherà circa 10 giorni a trovare una collisione che gli permetta di assumere l'identità di Bob.

2.2 — Dipendenza dalla lunghezza della password

La risposta precedente non dipende dalla lunghezza della password di Bob, ma solo dal numero di bit dell'hash e dalla velocità con cui possono essere provati. Infatti, Charlie non ha bisogno di trovare la password di Bob, ma un valore che generi lo stesso hash.

2.3 — Conoscenza della funzione di hash

Anche se Charlie è ora in grado di calcolare 10^9 hash al secondo, non conoscendo h_{Bob} non può farsene molto. Il collo di bottiglia rimane sempre il tempo di avvio della sessione di login, quindi Charlie è vincolato a provare 1000 password al secondo.

In realtà, Charlie può utilizzare la propria capacità di calcolare a priori gli hash delle password prima di inviarle al server, escludendo quelle che collidono con password già provate. In questo modo, i 2^{30} hash possibili sono tentati senza ripetizione, e il numero medio di tentativi necessari si dimezza.

Osservazioni

Gil errori dovuti ad approssimazioni numeriche sono ovviamente stati perdonati, così pure eventuali dimezzamenti nella stima dei tempi dovuti a errate interpretazioni della probabilità.

Esercizio 3 — domande a risposta multipla

Nel seguito, la prima risposta è sempre quella corretta.

1. Quale, tra i seguenti, è un possibile problema del protocollo Diffie-Hellman?

   (a) La possibilità di un attacco Man-in-the-Middle.

   (b) La difficoltà di trovare numeri primi di dimensioni sufficienti.

   (c) La lentezza in rapporto ai cifrari a chiave condivisa.

   Visto a lezione. D-H non si basa su numeri primi e la lentezza non è un problema, perché viene applicato solo una tantum.

2. Alice e Bob avviano una sessione Diffie-Hellman; per decifrare la chiave di sessione, Charlie (in ascolto sul canale ma non in grado di interferire) deve…

   (a) …risolvere un problema di logaritmo discreto.

   (b) …fattorizzare un grande prodotto di numeri primi.

   (c) …trovare una collisione in un valore hash crittografico.

3. Quale, tra i seguenti, è un possibile problema del cifrario RSA?

   (a) La lentezza in rapporto ai cifrari a chiave condivisa.

   (b) La possibilità di un attacco Man-in-the-Middle.

   (c) La difficoltà di trovare numeri primi di dimensioni sufficienti.

   RSA non risente, di per sé, degli attacchi MitM (se non nella distribuzione delle chiavi, ma questa è una debolezza di tutti i cifrari), e i numeri primi, per quanto pochi, sono abbastanza abbondanti da rendere il cifrario praticabile.

4. Quale proprietà caratterizza i cifrari a flusso?

   (a) Combinano i dati da cifrare con un flusso potenzialmente infinito di dati (pseudo-) casuali.

   (b) Sono necessariamente interattivi.

   (c) Non richiedono che gli interlocutori abbiano concordato e condiviso una chiave.

5. Quale delle seguenti proprietà **non** è posseduta da nessuna funzione hash crittografica?

   (a) La suriettività.

   (b) La resistenza agli attacchi di preimmagine e di collisione.

   (c) L'iniettività.

   Le funzioni hash sono fatte per generare riassunti dei dati (mappano dai arbitrari in stringhe di dimensione prefissata), quindi non possono essere suriettive.

6. Quale delle seguenti proprietà è necessaria per una funzione di cifratura?

   (a) L'iniettività.

   (b) La suriettività.

   (c) La resistenza agli attacchi di preimmagine e di collisione.

   Una funzione di cifratura dev'essere innanzitutto invertibile, quindi iniettiva. La suriettività non è necessaria (non tutti i codici sono necessariamente validi), mentre gli attacchi di preimmagine e di collisione non sono applicabili (per via dell'iniettività, le collisioni non sono possibili).

7. Nell'applicazione di un cifrario a blocchi, a cosa si riferiscono i termini "Electronic Codebook" (ECB) e "Chained Block Cipher" (CBC)?

   (a) Alla modalità di cifratura dei blocchi successivi di uno stesso messaggio.

   (b) Alla decisione se applicare un cifrario monouso (one-time pad) o con chiave riutilizzabile.

(c) Alla determinazione del padding per aggiustare la dimensione dell'ultimo blocco di un messaggio da cifrare.

8. Quale delle seguenti informazioni **non** è contenuta in una Certificate Signing Request (CSR)?

   (a) La chiave privata del richiedente.

   (b) Il common name del richiedente.

   (c) La chiave pubblica del richiedente.

9. Un certificato di firma digitale solitamente accompagna...

   (a) ...una chiave pubblica, e garantisce l'identità del possessore della corrispondente chiave privata.

   (b) ...una chiave di sessione, e ne garantisce l'autenticità.

   (c) ...una chiave privata, e garantisce l'identità del possessore della corrispondente chiave pubblica.

   Una chiave privata non viaggia mai in rete, e le chiavi di sessione non vengono certificate, ma create all'occorrenza.

10. Quale delle seguenti proprietà è necessaria affinché una funzione hash sia crittograficamente sicura?

    (a) La resistenza agli attacchi di preimmagine e di collisione.

    (b) L'iniettività.

    (c) La suriettività.

    Come detto prima, una funzione hash non è mai iniettiva; la suriettività è una buona proprietà, ma non è strettamente necessaria.

Griglie di soluzione

Sono elencati, per ogni tema:

- i valori pubblici A e B e la chiave K ottenuti con l'esercizio 1;
- il numero di tentativi N e il tempo richiesto T per l'esercizio 2;
- l'elenco delle risposte corrette alle domande dell'ultimo esercizio.

```
1
 p = 13; g = 7; a = 10; b = 5; A = 4; B = 11; K = 10
 bit = 30; N = 1073741824; T = 1073741.824
 1.a 2.a 3.b 4.b 5.c 6.b 7.b 8.c 9.c 10.a
2
 p = 11; g = 7; a = 8; b = 4; A = 9; B = 3; K = 5
 bit = 28; N = 268435456; T = 268435.456
 1.a 2.c 3.b 4.c 5.b 6.c 7.b 8.c 9.a 10.c
3
 p = 11; g = 7; a = 9; b = 4; A = 8; B = 3; K = 4
 bit = 30; N = 1073741824; T = 1073741.824
 1.a 2.c 3.a 4.c 5.b 6.a 7.a 8.b 9.b 10.a
4
 p = 13; g = 7; a = 10; b = 2; A = 4; B = 10; K = 3
 bit = 32; N = 4294967296; T = 4294967.296
 1.b 2.c 3.b 4.c 5.c 6.a 7.a 8.b 9.b 10.c
5
 p = 11; g = 8; a = 7; b = 2; A = 2; B = 9; K = 4
 bit = 30; N = 1073741824; T = 1073741.824
 1.c 2.a 3.a 4.b 5.c 6.c 7.c 8.a 9.b 10.c
6
 p = 11; g = 7; a = 7; b = 3; A = 6; B = 2; K = 7
 bit = 32; N = 4294967296; T = 4294967.296
 1.c 2.a 3.a 4.c 5.a 6.a 7.a 8.a 9.b 10.c
7
 p = 13; g = 7; a = 10; b = 2; A = 4; B = 10; K = 3
 bit = 30; N = 1073741824; T = 1073741.824
 1.b 2.b 3.c 4.a 5.c 6.b 7.c 8.c 9.c 10.a
8
 p = 13; g = 6; a = 10; b = 2; A = 4; B = 10; K = 3
 bit = 30; N = 1073741824; T = 1073741.824
 1.b 2.c 3.b 4.c 5.a 6.b 7.b 8.c 9.b 10.b
9
 p = 11; g = 6; a = 9; b = 5; A = 2; B = 10; K = 10
 bit = 30; N = 1073741824; T = 1073741.824
 1.b 2.a 3.b 4.b 5.c 6.b 7.b 8.c 9.a 10.c
10
 p = 11; g = 8; a = 9; b = 4; A = 7; B = 4; K = 3
 bit = 24; N = 16777216; T = 16777.216
 1.a 2.b 3.a 4.b 5.c 6.c 7.b 8.c 9.a 10.b
11
 p = 13; g = 6; a = 9; b = 5; A = 5; B = 2; K = 5
 bit = 30; N = 1073741824; T = 1073741.824
 1.a 2.a 3.c 4.c 5.b 6.c 7.b 8.a 9.b 10.a
12
 p = 11; g = 6; a = 9; b = 2; A = 2; B = 3; K = 4
 bit = 24; N = 16777216; T = 16777.216
 1.b 2.c 3.b 4.a 5.a 6.c 7.c 8.b 9.b 10.b
13
 p = 11; g = 7; a = 9; b = 3; A = 8; B = 2; K = 6
```

```
 bit = 32; N = 4294967296; T = 4294967.296
 1.b 2.a 3.b 4.b 5.b 6.a 7.c 8.c 9.b 10.b
14
 p = 13; g = 6; a = 10; b = 5; A = 4; B = 2; K = 10
 bit = 30; N = 1073741824; T = 1073741.824
 1.b 2.a 3.a 4.c 5.c 6.c 7.a 8.c 9.c 10.a
15
 p = 11; g = 6; a = 8; b = 4; A = 4; B = 9; K = 3
 bit = 32; N = 4294967296; T = 4294967.296
 1.c 2.a 3.a 4.b 5.a 6.b 7.a 8.a 9.a 10.a
16
 p = 11; g = 7; a = 9; b = 4; A = 8; B = 3; K = 4
 bit = 30; N = 1073741824; T = 1073741.824
 1.a 2.a 3.a 4.b 5.b 6.a 7.a 8.c 9.b 10.b
17
 p = 13; g = 6; a = 10; b = 2; A = 4; B = 10; K = 3
 bit = 28; N = 268435456; T = 268435.456
 1.b 2.c 3.b 4.c 5.a 6.b 7.a 8.a 9.b 10.b
18
 p = 11; g = 8; a = 7; b = 3; A = 2; B = 6; K = 8
 bit = 30; N = 1073741824; T = 1073741.824
 1.b 2.b 3.a 4.c 5.b 6.b 7.a 8.a 9.c 10.b
19
 p = 11; g = 6; a = 8; b = 2; A = 4; B = 3; K = 5
 bit = 32; N = 4294967296; T = 4294967.296
 1.b 2.c 3.a 4.b 5.c 6.c 7.a 8.b 9.c 10.c
20
 p = 11; g = 6; a = 7; b = 2; A = 8; B = 3; K = 9
 bit = 32; N = 4294967296; T = 4294967.296
 1.b 2.b 3.c 4.b 5.c 6.a 7.a 8.c 9.c 10.b
21
 p = 13; g = 7; a = 10; b = 3; A = 4; B = 5; K = 12
 bit = 24; N = 16777216; T = 16777.216
 1.c 2.c 3.c 4.c 5.c 6.b 7.b 8.c 9.c 10.a
22
 p = 13; g = 7; a = 10; b = 4; A = 4; B = 9; K = 9
 bit = 30; N = 1073741824; T = 1073741.824
 1.b 2.a 3.b 4.b 5.c 6.c 7.c 8.a 9.c 10.a
23
 p = 11; g = 7; a = 8; b = 4; A = 9; B = 3; K = 5
 bit = 32; N = 4294967296; T = 4294967.296
 1.a 2.b 3.c 4.a 5.c 6.c 7.b 8.a 9.c 10.a
24
 p = 11; g = 6; a = 8; b = 4; A = 4; B = 9; K = 3
 bit = 30; N = 1073741824; T = 1073741.824
 1.b 2.c 3.b 4.a 5.a 6.b 7.b 8.b 9.c 10.c
25
 p = 11; g = 6; a = 9; b = 4; A = 2; B = 9; K = 5
 bit = 26; N = 67108864; T = 67108.864
 1.c 2.c 3.b 4.b 5.b 6.a 7.a 8.b 9.c 10.c
26
 p = 11; g = 6; a = 8; b = 4; A = 4; B = 9; K = 3
 bit = 30; N = 1073741824; T = 1073741.824
 1.b 2.b 3.a 4.a 5.a 6.a 7.a 8.b 9.a 10.c
27
 p = 11; g = 6; a = 9; b = 5; A = 2; B = 10; K = 10
 bit = 30; N = 1073741824; T = 1073741.824
 1.c 2.b 3.a 4.b 5.c 6.a 7.c 8.a 9.a 10.c
28
```

p = 13; g = 6; a = 11; b = 5; A = 11; B = 2; K = 7
bit = 26; N = 67108864; T = 67108.864
1.c 2.b 3.a 4.b 5.b 6.b 7.b 8.a 9.b 10.c
29
p = 11; g = 7; a = 8; b = 3; A = 9; B = 2; K = 3
bit = 24; N = 16777216; T = 16777.216
1.b 2.a 3.b 4.c 5.b 6.b 7.a 8.b 9.a 10.b
30
p = 11; g = 6; a = 9; b = 2; A = 2; B = 3; K = 4
bit = 30; N = 1073741824; T = 1073741.824
1.c 2.b 3.c 4.c 5.b 6.b 7.c 8.a 9.b 10.c
31
p = 11; g = 8; a = 9; b = 4; A = 7; B = 4; K = 3
bit = 30; N = 1073741824; T = 1073741.824
1.b 2.b 3.a 4.a 5.c 6.c 7.b 8.b 9.c 10.b
32
p = 11; g = 8; a = 9; b = 4; A = 7; B = 4; K = 3
bit = 24; N = 16777216; T = 16777.216
1.c 2.b 3.a 4.b 5.c 6.b 7.b 8.b 9.b 10.a
33
p = 13; g = 7; a = 10; b = 4; A = 4; B = 9; K = 9
bit = 28; N = 268435456; T = 268435.456
1.b 2.c 3.b 4.b 5.b 6.a 7.b 8.b 9.b 10.c
34
p = 13; g = 7; a = 10; b = 3; A = 4; B = 5; K = 12
bit = 32; N = 4294967296; T = 4294967.296
1.a 2.b 3.a 4.c 5.a 6.a 7.c 8.b 9.b 10.c
35
p = 13; g = 6; a = 10; b = 2; A = 4; B = 10; K = 3
bit = 26; N = 67108864; T = 67108.864
1.a 2.b 3.a 4.b 5.a 6.a 7.c 8.c 9.b 10.a
36
p = 11; g = 8; a = 9; b = 4; A = 7; B = 4; K = 3
bit = 30; N = 1073741824; T = 1073741.824
1.b 2.b 3.b 4.a 5.b 6.b 7.b 8.b 9.b 10.a
37
p = 11; g = 6; a = 9; b = 4; A = 2; B = 9; K = 5
bit = 26; N = 67108864; T = 67108.864
1.a 2.b 3.b 4.c 5.b 6.a 7.c 8.a 9.a 10.a
38
p = 11; g = 6; a = 7; b = 2; A = 8; B = 3; K = 9
bit = 26; N = 67108864; T = 67108.864
1.c 2.c 3.a 4.c 5.c 6.c 7.b 8.c 9.a 10.c
39
p = 11; g = 6; a = 8; b = 4; A = 4; B = 9; K = 3
bit = 28; N = 268435456; T = 268435.456
1.a 2.c 3.b 4.b 5.a 6.c 7.b 8.c 9.c 10.a
40
p = 11; g = 8; a = 8; b = 4; A = 5; B = 4; K = 9
bit = 32; N = 4294967296; T = 4294967.296
1.b 2.c 3.b 4.b 5.c 6.b 7.a 8.b 9.b 10.b
41
p = 13; g = 6; a = 10; b = 3; A = 4; B = 8; K = 12
bit = 28; N = 268435456; T = 268435.456
1.b 2.a 3.b 4.b 5.b 6.b 7.b 8.c 9.b 10.b
42
p = 11; g = 8; a = 7; b = 3; A = 2; B = 6; K = 8
bit = 28; N = 268435456; T = 268435.456
1.a 2.b 3.c 4.c 5.b 6.a 7.a 8.a 9.c 10.b

43
p = 11; g = 7; a = 9; b = 4; A = 8; B = 3; K = 4
bit = 28; N = 268435456; T = 268435.456
1.a 2.a 3.a 4.b 5.c 6.c 7.c 8.a 9.a 10.b
44
p = 11; g = 7; a = 9; b = 3; A = 8; B = 2; K = 6
bit = 24; N = 16777216; T = 16777.216
1.c 2.b 3.a 4.a 5.b 6.c 7.a 8.b 9.b 10.c
45
p = 11; g = 8; a = 7; b = 4; A = 2; B = 4; K = 5
bit = 32; N = 4294967296; T = 4294967.296
1.c 2.a 3.b 4.a 5.a 6.b 7.a 8.c 9.a 10.b
46
p = 11; g = 8; a = 7; b = 2; A = 2; B = 9; K = 4
bit = 32; N = 4294967296; T = 4294967.296
1.b 2.c 3.a 4.c 5.a 6.c 7.b 8.b 9.b 10.c
47
p = 11; g = 8; a = 9; b = 4; A = 7; B = 4; K = 3
bit = 30; N = 1073741824; T = 1073741.824
1.c 2.b 3.a 4.c 5.b 6.a 7.c 8.a 9.a 10.a
48
p = 11; g = 6; a = 9; b = 2; A = 2; B = 3; K = 4
bit = 32; N = 4294967296; T = 4294967.296
1.a 2.a 3.c 4.a 5.b 6.a 7.c 8.c 9.c 10.a
49
p = 13; g = 6; a = 10; b = 5; A = 4; B = 2; K = 10
bit = 32; N = 4294967296; T = 4294967.296
1.c 2.b 3.b 4.c 5.a 6.c 7.c 8.c 9.b 10.c
50
p = 13; g = 7; a = 11; b = 2; A = 2; B = 10; K = 4
bit = 28; N = 268435456; T = 268435.456
1.a 2.a 3.a 4.c 5.c 6.a 7.c 8.c 9.b 10.c
51
p = 13; g = 6; a = 10; b = 3; A = 4; B = 8; K = 12
bit = 30; N = 1073741824; T = 1073741.824
1.a 2.b 3.c 4.b 5.c 6.c 7.a 8.b 9.a 10.a
52
p = 13; g = 7; a = 11; b = 5; A = 2; B = 11; K = 6
bit = 24; N = 16777216; T = 16777.216
1.a 2.a 3.a 4.c 5.a 6.c 7.c 8.b 9.a 10.c
53
p = 11; g = 8; a = 7; b = 2; A = 2; B = 9; K = 4
bit = 28; N = 268435456; T = 268435.456
1.c 2.c 3.c 4.b 5.b 6.c 7.b 8.a 9.a 10.c
54
p = 13; g = 7; a = 10; b = 4; A = 4; B = 9; K = 9
bit = 30; N = 1073741824; T = 1073741.824
1.c 2.a 3.c 4.a 5.c 6.a 7.c 8.c 9.c 10.a
55
p = 11; g = 8; a = 7; b = 4; A = 2; B = 4; K = 5
bit = 28; N = 268435456; T = 268435.456
1.a 2.b 3.a 4.c 5.c 6.c 7.a 8.c 9.a 10.a
56
p = 13; g = 6; a = 9; b = 5; A = 5; B = 2; K = 5
bit = 30; N = 1073741824; T = 1073741.824
1.c 2.b 3.a 4.c 5.c 6.c 7.c 8.c 9.b 10.a
57
p = 13; g = 7; a = 10; b = 4; A = 4; B = 9; K = 9
bit = 30; N = 1073741824; T = 1073741.824

1.b 2.c 3.a 4.c 5.a 6.a 7.c 8.b 9.b 10.c
58
p = 13; g = 7; a = 10; b = 2; A = 4; B = 10; K = 3
bit = 26; N = 67108864; T = 67108.864
1.c 2.a 3.b 4.a 5.b 6.a 7.b 8.c 9.c 10.a
59
p = 13; g = 6; a = 9; b = 5; A = 5; B = 2; K = 5
bit = 26; N = 67108864; T = 67108.864
1.c 2.c 3.a 4.c 5.a 6.b 7.a 8.c 9.b 10.a
60
p = 11; g = 6; a = 8; b = 3; A = 4; B = 7; K = 9
bit = 24; N = 16777216; T = 16777.216
1.a 2.c 3.a 4.a 5.a 6.a 7.c 8.a 9.c 10.a
61
p = 11; g = 6; a = 9; b = 4; A = 2; B = 9; K = 5
bit = 30; N = 1073741824; T = 1073741.824
1.c 2.c 3.a 4.a 5.b 6.c 7.a 8.a 9.b 10.b
62
p = 13; g = 7; a = 10; b = 4; A = 4; B = 9; K = 9
bit = 26; N = 67108864; T = 67108.864
1.c 2.a 3.a 4.c 5.a 6.c 7.c 8.c 9.b 10.c
63
p = 11; g = 6; a = 9; b = 3; A = 2; B = 7; K = 8
bit = 28; N = 268435456; T = 268435.456
1.a 2.c 3.a 4.b 5.a 6.c 7.c 8.b 9.b 10.a
64
p = 11; g = 8; a = 8; b = 4; A = 5; B = 4; K = 9
bit = 26; N = 67108864; T = 67108.864
1.c 2.c 3.b 4.c 5.b 6.b 7.a 8.c 9.a 10.a
65
p = 11; g = 7; a = 8; b = 4; A = 9; B = 3; K = 5
bit = 30; N = 1073741824; T = 1073741.824
1.c 2.a 3.b 4.a 5.b 6.c 7.a 8.c 9.b 10.b
66
p = 11; g = 6; a = 8; b = 4; A = 4; B = 9; K = 3
bit = 30; N = 1073741824; T = 1073741.824
1.b 2.c 3.c 4.c 5.b 6.c 7.c 8.a 9.b 10.b
67
p = 13; g = 6; a = 10; b = 5; A = 4; B = 2; K = 10
bit = 32; N = 4294967296; T = 4294967.296
1.a 2.c 3.a 4.c 5.a 6.a 7.a 8.a 9.c 10.b
68
p = 13; g = 6; a = 10; b = 5; A = 4; B = 2; K = 10
bit = 28; N = 268435456; T = 268435.456
1.b 2.b 3.c 4.c 5.c 6.a 7.b 8.b 9.c 10.a
69
p = 11; g = 8; a = 7; b = 4; A = 2; B = 4; K = 5
bit = 32; N = 4294967296; T = 4294967.296
1.b 2.c 3.b 4.b 5.b 6.a 7.a 8.b 9.b 10.a
70
p = 13; g = 7; a = 11; b = 3; A = 2; B = 5; K = 8
bit = 30; N = 1073741824; T = 1073741.824
1.c 2.b 3.c 4.a 5.b 6.c 7.c 8.a 9.b 10.b
71
p = 13; g = 6; a = 10; b = 3; A = 4; B = 8; K = 12
bit = 26; N = 67108864; T = 67108.864
1.b 2.b 3.b 4.b 5.c 6.a 7.b 8.b 9.a 10.b
72
p = 13; g = 7; a = 11; b = 5; A = 2; B = 11; K = 6

```
 bit = 32; N = 4294967296; T = 4294967.296
 1.b 2.b 3.a 4.b 5.b 6.c 7.b 8.b 9.c 10.a
73
 p = 13; g = 7; a = 10; b = 4; A = 4; B = 9; K = 9
 bit = 32; N = 4294967296; T = 4294967.296
 1.b 2.a 3.b 4.c 5.b 6.c 7.b 8.b 9.b 10.a
74
 p = 13; g = 6; a = 10; b = 2; A = 4; B = 10; K = 3
 bit = 28; N = 268435456; T = 268435.456
 1.a 2.b 3.a 4.b 5.b 6.a 7.c 8.b 9.c 10.a
75
 p = 11; g = 8; a = 7; b = 4; A = 2; B = 4; K = 5
 bit = 28; N = 268435456; T = 268435.456
 1.c 2.a 3.c 4.a 5.c 6.b 7.c 8.c 9.a 10.a
76
 p = 11; g = 7; a = 9; b = 3; A = 8; B = 2; K = 6
 bit = 30; N = 1073741824; T = 1073741.824
 1.c 2.c 3.b 4.c 5.a 6.c 7.b 8.b 9.a 10.b
77
 p = 11; g = 6; a = 7; b = 2; A = 8; B = 3; K = 9
 bit = 32; N = 4294967296; T = 4294967.296
 1.b 2.b 3.b 4.b 5.a 6.a 7.b 8.c 9.a 10.a
78
 p = 13; g = 7; a = 10; b = 4; A = 4; B = 9; K = 9
 bit = 28; N = 268435456; T = 268435.456
 1.b 2.c 3.b 4.b 5.b 6.a 7.b 8.b 9.a 10.b
79
 p = 11; g = 6; a = 8; b = 3; A = 4; B = 7; K = 9
 bit = 24; N = 16777216; T = 16777.216
 1.a 2.a 3.c 4.b 5.c 6.b 7.b 8.c 9.b 10.c
80
 p = 13; g = 6; a = 10; b = 5; A = 4; B = 2; K = 10
 bit = 26; N = 67108864; T = 67108.864
 1.c 2.b 3.a 4.c 5.c 6.b 7.b 8.c 9.b 10.b
81
 p = 11; g = 6; a = 8; b = 2; A = 4; B = 3; K = 5
 bit = 30; N = 1073741824; T = 1073741.824
 1.b 2.b 3.c 4.c 5.c 6.b 7.a 8.a 9.c 10.a
82
 p = 11; g = 6; a = 9; b = 3; A = 2; B = 7; K = 8
 bit = 24; N = 16777216; T = 16777.216
 1.c 2.c 3.a 4.a 5.c 6.c 7.c 8.b 9.a 10.c
83
 p = 13; g = 7; a = 10; b = 2; A = 4; B = 10; K = 3
 bit = 26; N = 67108864; T = 67108.864
 1.c 2.a 3.b 4.c 5.b 6.a 7.c 8.a 9.c 10.a
84
 p = 11; g = 8; a = 7; b = 5; A = 2; B = 10; K = 10
 bit = 24; N = 16777216; T = 16777.216
 1.a 2.a 3.c 4.b 5.b 6.c 7.a 8.b 9.b 10.a
85
 p = 11; g = 7; a = 8; b = 4; A = 9; B = 3; K = 5
 bit = 32; N = 4294967296; T = 4294967.296
 1.c 2.c 3.b 4.a 5.b 6.c 7.c 8.a 9.b 10.c
86
 p = 13; g = 6; a = 11; b = 5; A = 11; B = 2; K = 7
 bit = 32; N = 4294967296; T = 4294967.296
 1.a 2.a 3.c 4.b 5.a 6.a 7.c 8.b 9.a 10.b
87
```

p = 13; g = 6; a = 11; b = 5; A = 11; B = 2; K = 7
bit = 32; N = 4294967296; T = 4294967.296
1.b 2.c 3.b 4.c 5.b 6.a 7.b 8.b 9.c 10.c
88
p = 13; g = 6; a = 10; b = 2; A = 4; B = 10; K = 3
bit = 32; N = 4294967296; T = 4294967.296
1.a 2.a 3.a 4.c 5.b 6.c 7.b 8.a 9.a 10.c
89
p = 11; g = 6; a = 9; b = 3; A = 2; B = 7; K = 8
bit = 28; N = 268435456; T = 268435.456
1.a 2.b 3.c 4.a 5.b 6.b 7.b 8.c 9.b 10.b
90
p = 13; g = 7; a = 10; b = 4; A = 4; B = 9; K = 9
bit = 30; N = 1073741824; T = 1073741.824
1.b 2.c 3.b 4.c 5.a 6.a 7.c 8.a 9.c 10.c
91
p = 11; g = 8; a = 7; b = 5; A = 2; B = 10; K = 10
bit = 24; N = 16777216; T = 16777.216
1.c 2.c 3.a 4.b 5.a 6.a 7.c 8.c 9.a 10.a
92
p = 13; g = 6; a = 10; b = 2; A = 4; B = 10; K = 3
bit = 28; N = 268435456; T = 268435.456
1.c 2.a 3.b 4.a 5.a 6.b 7.a 8.b 9.b 10.c
93
p = 11; g = 8; a = 8; b = 4; A = 5; B = 4; K = 9
bit = 26; N = 67108864; T = 67108.864
1.a 2.a 3.b 4.b 5.c 6.b 7.b 8.a 9.c 10.c
94
p = 11; g = 8; a = 8; b = 4; A = 5; B = 4; K = 9
bit = 24; N = 16777216; T = 16777.216
1.b 2.a 3.b 4.a 5.c 6.a 7.b 8.c 9.a 10.b
95
p = 11; g = 8; a = 9; b = 4; A = 7; B = 4; K = 3
bit = 26; N = 67108864; T = 67108.864
1.a 2.c 3.c 4.c 5.c 6.c 7.b 8.c 9.c 10.c
96
p = 11; g = 6; a = 8; b = 2; A = 4; B = 3; K = 5
bit = 24; N = 16777216; T = 16777.216
1.a 2.b 3.b 4.c 5.c 6.a 7.b 8.b 9.a 10.a
97
p = 13; g = 7; a = 10; b = 3; A = 4; B = 5; K = 12
bit = 24; N = 16777216; T = 16777.216
1.a 2.b 3.c 4.a 5.b 6.a 7.c 8.c 9.c 10.a
98
p = 13; g = 6; a = 10; b = 5; A = 4; B = 2; K = 10
bit = 28; N = 268435456; T = 268435.456
1.a 2.c 3.c 4.a 5.c 6.b 7.a 8.c 9.b 10.b
99
p = 11; g = 6; a = 9; b = 4; A = 2; B = 9; K = 5
bit = 24; N = 16777216; T = 16777.216
1.b 2.b 3.c 4.b 5.a 6.a 7.c 8.b 9.a 10.b
100
p = 11; g = 7; a = 9; b = 4; A = 8; B = 3; K = 4
bit = 32; N = 4294967296; T = 4294967.296
1.c 2.b 3.c 4.b 5.c 6.c 7.c 8.a 9.a 10.c