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

Prima prova scritta

Martedì 19 giugno 2018

Esercizio 1

Si consideri la seguente codifica a cinque bit:

A	00000	I	01000	Q	10000	Y	11000
B	00001	J	01001	R	10001	Z	11001
C	00010	K	01010	S	10010	.	11010
D	00011	L	01011	T	10011	,	11011
E	00100	M	01100	U	10100	;	11100
F	00101	N	01101	V	10101	:	11101
G	00110	O	01110	W	10110	?	11110
H	00111	P	01111	X	10111	!	11111

Data una chiave k a 5 bit, utilizziamo la funzione di cifratura a blocchi $f_k(m) = m \oplus k$, dove $\oplus$ è l'operazione di OR esclusivo (XOR). Ad esempio, se $k = 01100$ e $m = 10101$, allora $f_k(m) = 01100 \oplus 10101 = 11001$.

1.1) Dato il messaggio in chiaro "CIAO", cifrarlo a blocchi con la chiave $k = 11010$ in modalità Electronic Codebook (ECB).

1.2) Cifrare lo stesso messaggio con la stessa chiave in modalità Cipher Block Chaining (CBC).

1.3) Dato il codice cifrato "KFDM", decifrarlo a blocchi con la chiave $k = 01011$ in modalità CBC.

Esercizio 2

Descrivere a grandi linee l'handshake iniziale del protocollo TLS nel caso in cui il server si autentica tramite certificato, mentre non è richiesta l'autenticazione del client.

Esercizio 3

Per stabilire una chiave di sessione tramite protocollo Diffie-Hellman, due terminali concordano innanzitutto di lavorare in aritmetica modulo $p = 11$. Come base delle potenze possono scegliere $g = 3, 5, 7$; qual è la più sicura, e perché?

Esercizio 4

Una rete locale è composta da tre intranet:

- la prima contiene un server HTTP (porta TCP 80), un server DNS (porta UDP 53) e un proxy web (porta TCP 3128).
  - i tre server devono essere accessibili da tutte le macchine della rete locale;
  - il server HTTP dev'essere accessibile anche dall'esterno, ma non può iniziare comunicazioni verso l'esterno;
  - Il server DNS seve poter ricevere ed effettuare richieste DNS anche all'esterno;
  - il proxy web deve avere i permessi minimi necessari per servire le due intranet descritte qui sotto;
- due intranet separate da 200 host l'una;
  - le due intranet possono comunicare tra loro a livello rete;
  - le due intranet possono accedere ai server HTTP e DNS;
  - le due intranet possono accedere all'esterno solo attraverso il proxy web;

La rete ha a disposizione il solo indirizzo IP `195.221.23.45` con netmask `255.255.255.248`; il default gateway messo a disposizione dall'ISP ha l'indirizzo più basso utilizzabile della stessa sottorete.
Si ha a disposizione un router con due interfacce (una seriale verso l'ISP e una Ethernet verso le reti locali), capace di NAT e di incapsulamento 802.1Q, e di tutti gli switch gestiti di cui si ha bisogno.
Descrivere l'architettura fisica e logica della rete, attribuire indirizzi e sottoreti IP ale varie parti; descrivere la configurazione dei tre server (HTTP, DNS, proxy) e del router (porte fisiche e virtuali, tabelle di instradamento, tabelle di port forwarding, ACL).