Corso di Sicurezza nelle reti di telecomunicazioni
a.a. 2008/2009

Esempio di quesiti sulla prima parte del corso

1) Si consideri un semplice cifrario a sostituzione con shift (tipo cifrario di Cesare), con un alfabeto di N caratteri (con N=21 o 26 a scelta), con chiave K=4. Si cripti la stringa "SEGRETO"

Plain text	***Cipher text***
SEGRETO	

2) Si costruisca una coppia di chiavi privata/pubblica per RSA, utilizzando come coppia di numeri primi *p* e *q* i seguenti valori: p=3, q=11. Con tale chiavi si cripti il messaggio m=2.

3) Si faccia un esempio di creazione di chiave condivisa tra A e B con Diffie-Hellman, utilizzando per il generatore g e il numero primo p i seguenti valori: g=2, p=11.

4) Si supponga di voler inviare in modo sicuro un messaggio *m* da A a B, garantendo SOLO la confidenzialità dei dati inviati. Per la cifratura del messaggio si utilizzi un algoritmo di crittografia simmetrica. Indicare schematicamente quale funzioni possono essere svolte in fase di invio/ricezione, supponendo che A e B condividano tra loro solo le rispettive chiavi RSA pubbliche KU_A e KU_B (si indichino con KR_A e KR_B le corrispondenti chiavi private).

Invio	Ricezione

5) Si supponga di voler inviare in modo sicuro un messaggio *m* da A a B, garantendo SOLO l'autenticità/integrità dei dati inviati. Indicare schematicamente quale funzioni possono essere svolte in fase di invio/ricezione, supponendo che A e B condividano una chiave segreta K_{AB}, e che dispongano solo di un algoritmo di hash H().

Invio	Ricezione

6) Dato un algoritmo $E_K(\cdot)$ di crittografia a blocchi di lunghezza q, si descriva lo schema di codifica di tipo CBC (Cipher Block Chaining) di un messaggio m di lunghezza L>q (si supponga per semplicità L=n q).

7) Indicare un possibile schema sicuro di autenticazione tra Alice (supplicant) e Bob (authenticator), nell'ipotesi che Alice e Bob condividano le rispettive chiavi RSA pubbliche KU_A e KU_B (si indichino con KR_A e KR_B le corrispondenti chiavi private).

8) Indicare un possibile schema sicuro di mutua autenticazione tra due utenti Alice e Bob, basato sull'uso di una funzione hash $H(\cdot)$ e su un segreto condiviso K_{AB}.