Sicurezza nelle reti e nei sistemi informatici – 22/2/2011
Tempo: 100 minuti. N.B.: le domande potrebbero avere pesi differenti!

1. Autenticazione

a. Illustrare il protocollo di Diffie-Hellman per la definizione di una chiave di sessione e discuterne la robustezza rispetto a un avversario attivo.
b. Illustrare il protocollo EKE, discutendo come esso permetta la definizione di una chiave di sessione sicura anche in presenza di un avversario attivo.

2. Chiavi di sessione

a. Spiegare il termine *chiave di sessione*, con particolare riferimento agli scopi e ai requisiti di sicurezza (confidenzialità, integrità ed autenticità). Illustrare uno scenario ammissibile in cui sia opportuno che due (o più) partner di comunicazione concordino una chiave di sessione.
b. Alice, Bob e Charlie debbono stabilire una chiave di sessione condivisa (nota ai tre). KAB è una chiave condivisa fra Alice e Bob, mentre KAC è una chiave condivisa da Alice e Charlie.
Si consideri il seguente protocollo:

C -> A: (C, KAC(C, rC)) [rC è un nonce generato da C]
A -> B: (A, KAB(A, rC||rA)) [|| è la concatenazione, rA nonce generato da A]
B -> A: (B, KAB(B, rC||rA||rB))
A -> C: (A, KAC(A, rC||rA||rB)) [la chiave di sessione è rC||rA||rB]

b1. Spiegare perché il protocollo permette di definire una chiave comune ad A, B e C, sicura rispetto a un avversario passivo.
b2. Spiegare perché il protocollo è robusto anche rispetto a un attacco di tipo replay.

3. Generazione di numeri random

a. Spiegare cosa sono i numeri random e perché sono importanti nella crittografia. Illustrare il significato di generatore di numeri random, generatore di numeri pseudo-random e di generatore di numeri pseudo-random crittograficamente sicuro.
b. Si considerino i seguenti algoritmi per la generazione di numeri pseudo-random, ove s è un seed iniziale, H una funzione hash e ^ l'operatore XOR bit a bit.

```
Algoritmo A
 x = s;
 while(true)
   x = H(x);
   output(x);
```

```
Algoritmo B
 x = s;
 while(true)
   x = H(x^s);
   output(x);
```

```
Algoritmo C
 y = 0;
 x = s;
 while(true)
   z = H(x^y);
   y = x;
   x = z;
   output(z);
```

Discutere la qualità dei due generatori e la loro resistenza agli attacchi.

4. Cifrari a flusso e codifica a blocchi

a. Spiegare cosa è un cifrario perfetto; illustrare un cifrario a flusso perfetto e discutere le sue modalità di impiego.
b. Disegnare almeno due schemi di cifratura/decifratura (diversi da Electronic Code Book, ECB) di messaggi di lunghezza arbitraria, basati su un cifrario a blocchi, e confrontarli rispetto alla resistenza agli attacchi, propagazione degli errori e velocità di cifratura/decifratura.

5. Domande brevi (al più 8 linee e una figura per risposta)

a. Spiegare cosa è un firewall e quali tipi di firewall esistono.
b. Descrivere un attacco “chosen cyphertext.”