Sicurezza nelle reti e nei sistemi informatici – esame del 13-9-2012. Tempo: 120 min.
NB: I quesiti prevedono più punti

1. Firme digitali e hashing

Una firma digitale è solitamente realizzata calcolando uno hashing di un messaggio e cifrando il risultato dello hashing attraverso la chiave private di colui che firma.

a. Cosa potrebbe accadere se si verificasse una collisione nella funzione di hashing usata per la firma?
b. Quale potrebbe essere il possibile impatto di una tale collisione sulla sicurezza del meccanismo di firma digitale?
c. Quali fattori condizioneranno l'impatto e quali azioni potrebbero essere intraprese per mitigare l'effetto di tali collisioni (si considerino, ad esempio, le soluzioni implementate in standard come PKCS e DSS)?

2. RSA

a. Si assuma un sistema di cifratura RSA con p=23 e q= 29. L'esponente di cifratura è scelto pari a e=3. Determinare l'esponente di decifratura d.
b. Mostrare che RSA è insicuro rispetto un attacco "chosen cyphertext", in cui un attaccante che osserva $c = m^e \bmod n$ può determinare m richiedendo la decifratura di $c' \neq c$.
   Suggerimento: sfruttare la proprietà omomorfica di RSA, secondo la quale
   $$(m1\ m2)^e \bmod n = (m1^e \bmod n)(m2^e \bmod n) \bmod n.$$

3. Autenticazione

a. Descrivere dettagliatamente cosa è il Lamport's Hash e come lavora. In quali casi risulta particolarmente utile?
b. Descrivere dettagliatamente l'uso dello standard X509 per l'autenticazione basata su chiave pubblica e discutere le caratteristiche principali del protocollo.

4. SSL e IPSEC

a. Descrivere sommariamente la fase di autenticazione di SSL
b. Spiegare le ragioni per cui SSL permette a un intruso di ottenere più informazioni per l'analisi del traffico rispetto a IPSec.
c. Cosa è una virtual private network (VPN)? Come può IPSec aiutare a costruirne una?

5. Controllo degli accessi

a. Illustrare sommariamente le principali caratteristiche del modello di Bell – La Padula per il controllo degli accessi (10 righe)
b. L'amministratore della rete di una società ha creato un gruppo denominato NewIdeas. L'obiettivo principale del gruppo è l'identificazione di nuovi mercati e lo sviluppo della strategia aziendale per la penetrazione dei mercati individuati. Il gruppo include i seguenti quattro membri:

Nome	Dipartimento
John	Marketing
Alice	Sales
William	Marketing
Elaine	Management

   L'amministratore di rete ha assegnato al gruppo i seguenti diritti di accesso ai file di una cartella usata dai membri del gruppo. La cartella contiene sia dati che applicazioni.
   Permessi del gruppo: esecuzione, visione del contenuto di cartelle, creazione file, creazione cartelle, cancellazione, lettura, presa possesso (proprietà).
   Quale modalità di controllo accessi è stata usata nell'assegnare i diritti di accesso?
   - b1. Mandatory Access Control
   - b2. Role-Based Access Control
   - b3. Discretionary Access Control
   - b4. Un controllo similare a quello del sistema operativo UNIX

c. Spiegare la risposta alla domanda 5b