Sicurezza

23 Giugno 2010

Esercizio 1

Dare la definizione formale di cifrario di Vigenère con chiavi lunghe d. Dimostrare, tramite un controesempio, che il cifrario non è perfetto se, come avviene normalmente, la chiave viene riutilizzata per cifrare i diversi blocchi lunghi d. Sotto quale condizione il cifrario diventa perfetto? Discutere e dare una dimostrazione formale.

Esercizio 2

Viene progettato un sistema di consegna di compiti d'esame in cui il lavoro C effettuato dallo studente viene inviato cifrato con la chiave pubblica PK_P del professore e firmato con la chiave segreta SK_S dello studente, nella forma $Sign_{SK_S}(E_{PK_P}(C))$. Una volta ricevuto il compito, il professore verifica che esso non coincida con altri compiti inviati da altri studenti. Mostrare un attacco in cui uno studente sia in grado di 'rubare' il compito ad un altro facendosi attribuire il voto, illustrando le diverse operazioni necessarie per effettuare l'attacco. Proporre una modifica al protocollo in modo da evitare tale attacco.

Esercizio 3

Cosa sono e a cosa servono i *Key Distribution Center* (KDC)? Mostrare un protocollo basato su KDC illustrandone in dettaglio il funzionamento e discutendo le proprietà di sicurezza che esso garantisce.

Esercizio 4

Considerare il seguente protocollo:

$$\begin{array}{lcll} A & \rightarrow & B & : M_A, N_A \\ B & \rightarrow & A & : M_B, MAC_k(B, M_B, M_A, N_A) \\ A & \rightarrow & B & : MAC_k(A, M_A, M_B) \end{array}$$

in cui N_A è un nonce generato da A e k è una chiave a lungo termine condivisa tra A e B.

1. Quali garanzie di sicurezza su M_A e M_B offre tale protocollo?
2. È possibile replicare una sessione impersonando A? Spiegare.
3. È possibile replicare una sessione impersonando B? Spiegare.

Esercizio 5 (facoltativo)

Illustrare la modalità Cipher Feedback (CFB) nella variante per cifrare stream di singoli byte. Illustrare lo schema di cifratura e decifratura e discutere la sicurezza di tale modalità.