Sicurezza

3 Febbraio 2010

Esercizio 1

Si consideri un cifrario di Vigenère con lunghezza della chiave uguale a 5 e chiavi equiprobabili ($p_{\mathcal{K}}(k) = \frac{1}{|\mathcal{K}|}$). Considerare testi lunghi 5 e calcolare la probabilità che il testo in chiaro sia ACQUA, supponendo di osservare il testo cifrato ZZZZZ e sapendo che $p_{\mathcal{P}}(\text{ACQUA}) = 0.0043$. Motivare accuratamente la risposta.

Esercizio 2

Scrivere un protocollo che permetta ad un utente A di mandare una email E cifrata ed autenticata a un destinatario B. In particolare A vuole proteggere la segretezza di E e B vuole verificare che la email proviene da A e non è una replica di un vecchio messaggio. Assumere che A e B conoscano le rispettive chiavi pubbliche PK_A e PK_B e considerare la possibilità che la email E sia di grandi dimensioni e non possa quindi essere cifrata tramite crittografia a chiave pubblica.

Esercizio 3

Considerare la funzione hash $h(X_1 \dots X_n) = X_1 \oplus b_1 \oplus X_2 \oplus b_2 \oplus \dots \oplus X_n \oplus b_n$, dove $\oplus$ è l'operazione di xor bit a bit, $X_1, \dots X_n$ sono blocchi di 256 bit e b_i è la rappresentazione binaria, sempre in 256 bit, del numero i. La funzione $h(X)$ è adatta per essere utilizzata in un meccanismo di firma elettronica? Perché?

Esercizio 4

Per migliorare uno schema di autenticazione login-password viene suggerito il seguente protocollo:

$$A \quad \rightarrow \quad B \quad : \quad A, E_K(pwd)$$

in cui A è la login, pwd è la password e K è una chiave a lungo termine condivisa tra A e B.

1. Il protocollo purtroppo non migliora molto la sicurezza. Illustrare descrivendo una sequenza di attacco;
2. Rendere sicuro il protocollo utilizzando due diverse tecniche viste a lezione. Mostrare come l'attacco al punto precedente viene evitato/individuato.

Esercizio 5 (facoltativo)

I cifrari a chiave pubblica basano, generalmente, la loro sicurezza su problemi difficili da risolvere, da un punto di vista computazionale. Illustrare un esempio di tale risultato e discuterne le ricadute pratiche.