Sicurezza

9 Giugno 2010

Esercizio 1

Si consideri un cifrario 'autokey' a flusso definito su testi lunghi d, ovvero $\mathcal{P} = \mathcal{C} = \mathbb{Z}_{21}^d$, e chiavi $\mathcal{K} = \mathbb{Z}_{21}$. Data la chiave iniziale $k \in \mathcal{K}$ e un testo in chiaro $x_1, \ldots, x_d$, il flusso di chiavi è definito come segue: $z_1 = k$, $z_i = x_{i-1}$ per $i \in [2, d]$. La funzione di cifratura è quindi definita come $E_k(x_i) = x_i + z_i \bmod 21$, per $i \in [1, d]$.
Definire la funzione di decifratura $D_k(y_i)$ e decifrare il testo TAPND cifrato con chiave k =B. Mostrare, tramite un controesempio, che il cifrario non è perfetto, indipendentemente da come la chiave k viene scelta.

Esercizio 2

Viene progettato un sistema di votazione elettronica in cui i voti degli elettori vengono inviati al server con una semplice cifratura $E_k(v)$, dove v è l'identificativo del candidato votato. Ipotizzando che un attaccante possa intercettare i messaggi in transito verso il server, mostrare un semplice scenario di attacco, di tipo *codebook*, in cui la segretezza dei voti viene violata senza necessariamente 'rompere' la chiave k o crittoanalizzare il cifrario E. Proporre una semplice tecnica per migliorare la sicurezza del protocollo.

Esercizio 3

Perchè i protocolli *sfida-risposta* offrono maggiori garanzie di sicurezza rispetto ai protocolli basati su password? Dare un esempio di protocollo sfida-risposta discutendone la sicurezza rispetto agli attacchi di *replica*.

Esercizio 4

Considerare il seguente protocollo:

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

in cui 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. Ipotizzando che M_A sia un'operazione bancaria che A chiede di eseguire alla banca B, e M_B un booleano che indica il successo dell'operazione M_A, mostrare uno scenario di attacco e proporre possibili modifiche al protocollo che lo rendano sicuro in questo contesto.

Esercizio 5 (facoltativo)

Un cifraro è perfetto, secondo la teoria di Shannon, se i testi in chiaro e i testi cifrati sono *indipendenti*. Discutere questa affermazione, prima intuitivamente, e poi dando una definizione formale di cifrario perfetto. Esibire, infine, un cifrario che soddisfa tale proprietà, dimostrandola formalmente.