Sicurezza

6 Settembre 2007

Esercizio 1

Si consideri la seguente matrice M

1	2	3
3	2	1
2	3	1

Tale matrice viene utilizzata per definire il seguente cifrario: $\mathcal{P} = \mathcal{C} = \mathcal{K} = \{1, 2, 3\}$; per cifrare il testo i con la chiave k si prende l'i-esimo elemento della riga k, cioè $E_k(i) = M[k, i]$.

1. Qual è la cifratura dei testi $1, 2, 3$ con la chiave 2?
2. Mostrare che E_k è iniettiva per ogni chiave k e spiegare perchè questa properietà è di fondamentale importanza.
3. Considerare il caso in cui la chiave è scelta in modo equiprobabile, $p_{\mathcal{K}}(k) = 1/3$. Il cifrario è perfetto? Spiegare. (Assumere che i testi in chiaro siano tutti "possibili": $p_{\mathcal{P}}(x) > 0$ per ogni $x \in \mathcal{P}$.)

Esercizio 2

Si vuole cifrare una trasmissione televisiva satellitare tramite DES.

1. Quale modalità del DES risulta essere la più appropriata e perchè?
2. Disegnare gli schemi per la cifratura e decifratura di tale modalità;
3. descrivere brevemente un'altra modalità del DES e spiegare perchè, per questa specifica applicazione, risulta essere meno adatta rispetto a quella proposta.

Esercizio 3

L'implementazione di cifrari come RSA è problematica e deve essere effettuata con algoritmi particolari. Discutere e mostrare un algoritmo a scelta tra quelli utilizzati per implementare RSA.

Esercizio 4

Considerare il semplice protocollo di autenticazione unilaterale:

$$A \quad \rightarrow \quad B \quad : \; Sign_A(\text{“sono proprio A”})$$

in cui $Sign_A$ è implementato tramite RSA.

1. Mostrare un attacco *replay* (replica) in cui il nemico riesce a sfruttare una vecchia sessione di A per impersonare A;
2. Modificare il protocollo aggiungendo una sfida basata su nonce, e mostrando che l'attacco non è più possibile.
3. La variante con nonce potrebbe indebolire il sistema di cifratura. Discutere e proporre una nuova soluzione che non crei problemi di crittoanalisi.

Esercizio 5 (facoltativo)

RSA è basato su un numero $n = pq$ con p e q primi, sufficientemente grandi.

1. Perchè è importante che p e q restino segreti?
2. Dimostrare che se un crittoanalista riesce a calcolare $\phi(n)$ allora riesce facilmente a fattorizzare n. Discutere l'importanza di questo risultato.