Sicurezza

15 Luglio 2008

Esercizio 1

Si consideri la composizione di un cifrario a spostamento, con chiave $k = 2$ (cifrario di Cesare), con un cifrario di Vigenère con chiave `SARA`.

1. Dare la definizione formale dei due cifrari e della loro composizione;
2. Mostrare la cifratura, tramite la composizione dei due cifrari, del testo in chiaro `CONTEGGI`. Mostrare che la stessa cifratura si ottiene con un solo cifrario di Vigenère; indicare la chiave e dimostrare l'equivalenza di questo cifrario con la composizione dei primi due;
3. Ipotizzare di scegliere la chiave k del cifrario a spostamento in modo equiprobabile (quindi diversa per ogni lettera da cifrare) mantenendo invece fissa la chiave di Vigenère. Che cifrario si ottiene? Qual è la distribuzione delle chiavi? Discutere tramite la teoria di Shannon.

Esercizio 2

Dare la definizione di funzioni *trap-door one-way* e spiegare la relazione tra tali funzioni e la crittografia a chiave pubblica.

Esercizio 3

Perchè è importante certificare le chiavi pubbliche tramite una o più *Certification Authority*? Illustare brevemente la struttura e il funzionamento dei certificati a chiave pubblica.

Esercizio 4

Si consideri il seguente protocollo di autenticazione unilaterale:

$$\begin{array}{lcl} B & \rightarrow & A \ : \ E_{K_{AB}}(N_B) \\ A & \rightarrow & B \ : \ N_B \end{array}$$

dove K_{AB} è una chiave simmetrica condivisa tra A e B, e N_B è un nonce generato da B. Illustrare almeno due debolezze di questo protocollo descivendo in dettaglio i relativi attacchi.

Esercizio 5 (facoltativo)

Spiegare come le "correspondence assertions", $begin(A, B)$ e $end(B, A)$, possano catturare gli attacchi ai protocolli di autenticazione illustrando, in particolare, un attacco di replica.