Sicurezza

30 Gennaio 2009

Esercizio 1

Si consideri la composizione di un cifrario a spostamento, con chiave $k = 2$, con un cifrario a sostituzione con chiave:

```
Testo in chiaro: A B C D E F G H I L M N O P Q R S T U V Z
Testo cifrato:   N O P M B S V Z U C T H G I L F E D Q A R
```

1. Mostrare la decifratura del testo cifrato `BPIV`;
2. A quale cifrario corrisponde la composizione dei due cifrari? Cosa accade se si inverte l'ordine di composizione dei cifrari? Si può dire che la composizione è commutativa?
3. Cosa accade se la chiave del cifrario a sostituzione viene scelta in modo equiprobabile per ogni lettera da cifrare? Discutere tramite la teoria di Shannon.

Esercizio 2

La sicurezza del cifrario RSA si basa sulla difficoltà nel fattorizzare n in p e q. Spiegare questa affermazione e discuterne le conseguenze, facendo particolare riferimento all'implementazione del cifrario.

Esercizio 3

Perché è utile firmare un hash di un messaggio invece che il messaggio stesso? Quali proprietà deve avere la funzione hash affinché il suo utilizzo nello schema di firma risulti sicuro? Motivare mostrando possibili attacchi.

Esercizio 4

Considerare il semplice protocollo di autenticazione di entità:

$$A \ \rightarrow \ B \ : \ A, Sign_A(B)$$

in cui A vuole identificarsi con B

1. Mostrare un attacco di *replica* (replay) in cui il nemico riesce a utilizzare una vecchia sessione per impersonare A con B;
2. Proporre almeno due differenti modifiche al protocollo che evitino l'attacco discusso al punto precedente, illustrandole approfonditamente.

Esercizio 5 (facoltativo)

Dimostrare che una funzione hash $h : Z \rightarrow W$ strong collision free è anche one-way, quando $|W| \leq |Z|/2$.