Sicurezza

8 Febbraio 2008

Esercizio 1

Si consideri un cifrario a sostituzione con chiave π

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

e si supponga di osservare il testo cifrato `FSZGT`.

1. Qual è la probabilità che il testo in chiaro sia, rispettivamente, PIPPO e PLUTO? Commentare.
2. Dimostrare che il cifrario non è perfetto. Questo risultato è coerente con il fatto che il cifrario è crittoanalizzabile. Discutere.
3. Si consideri una variante del cifrario precedente in cui ogni singolo carattere in chiaro, prima di essere cifrato con la chiave π, viene spostato (shifted) di k posizioni, con k scelto a caso tra 0 e 20. Scrivere la nuova funzione di cifratura, e ricavare la probabilità che il testo in chiaro sia PIPPO e PLUTO (sempre osservando il testo cifrato `FSZGT` e ipotizzando di conoscere la probabilità $p_{\mathcal{P}}$(PIPPO) e $p_{\mathcal{P}}$(PLUTO)). Commentare.

Esercizio 2

Illustrare gli schemi del double e triple DES (senza mostrare lo schema interno del DES).

1. per quale ragione sono stati introdotti tali schemi?
2. di quanto migliorano la sicurezza del DES? Discutere eventuali attacchi, indicandone la complessità.
3. cosa accade se applichiamo tali schemi ad un cifrario idempotente? Illustrare tramite un esempio.

Esercizio 3

Perchè, in crittografia, sono utili le funzioni hash? Dare la definizione di funzione hash collision-free e mostrare un esempio in cui risulta necessaria tale proprietà. Illustrare in dettaglio un attacco basato sull'assenza di tale proprietà.

Esercizio 4

Considerare il protocollo

$$\begin{array}{lcll} B & \rightarrow & A & : E_{K_{AB}}(M_B, N_B, B) \\ A & \rightarrow & B & : M_A, N_B, A \end{array}$$

dove K_{AB} è una chiave simmetrica condivisa tra A e B, N_B è un nonce generato da B, M_A e M_B sono due messaggi generati rispettivamente da A e B.

1. Quali garanzie di sicurezza (identificazione di A e B, autenticazione del mittente/destinatario di M_A e M_B, segretezza di M_A e M_B) hanno A e B al termine del protocollo?
2. cosa cambia se il protocollo viene modificato come segue (N_A è un nonce generato da A)

$$\begin{array}{lcll} A & \rightarrow & B & : N_A \\ B & \rightarrow & A & : E_{K_{AB}}(M_B, N_A, N_B, B) \\ A & \rightarrow & B & : M_A, N_B, A \end{array}$$

Esercizio 5 (facoltativo)

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