Sicurezza

12 Febbraio 2007

Esercizio 1

Si consideri il seguente crittogramma in lingua italiana, ottenuto tramite una variante polialfabetica del cifrario a spostamento in cui la prima lettera viene cifrata con la chiave K (scelta con distribuzione uniforme), la seconda con $K + 1 \bmod 21$, la terza con $K + 2 \bmod 21$, e così via:

`VOHDBOILN`

1. Crittoanalizzare tale testo, illustrando il metodo adottato.
2. Sia X il testo in chiaro ottenuto al punto precedente. Quanto valgono, intuitivamente, le probabilità $p_{\mathcal{P}}(X|\texttt{VOHDBOILN})$ e $p_{\mathcal{P}}(X'|\texttt{VOHDBOILN})$ con $X' \neq X$? Discutere.
3. Considerare un'ulteriore variante del cifrario in cui le lettere successive alla prima sono cifrate con chiave $K + R \bmod 21$, con R scelto, per ogni singola lettera, con distribuzione uniforme. Calcolare, tramite la teoria di Shannon, $p_{\mathcal{P}}(X|\texttt{VOHDBOILN})$ e $p_{\mathcal{P}}(X'|\texttt{VOHDBOILN})$ con $X' \neq X$. Confrontare la sicurezza di questo cifrario rispetto al precedente.

Esercizio 2

Dare la definizione di firma digitale. Discutere quali possibili vantaggi e svantaggi si hanno nel firmare un "riassunto" (hash) del messaggio invece che il messaggio vero e proprio. Dare la definizione di almeno una proprietà che dovrebbe avere una funzione hash per poter essere utilizzata per la firma digitale, discutendo possibili attacchi.

Esercizio 3

Considerare una variante della modalità CBC in cui il feedback viene "prelevato" subito prima della cifratura E_K. Sia $X_1, \ldots, X_n$ il testo in chiaro opportunamente diviso in blocchi e $Y_1, \ldots, Y_n$ il corrispettivo testo cifrato; tale variante del CBC può essere definita dalle seguenti espressioni:

$$\begin{aligned} z_1 &= X_1 \oplus IV \\ z_j &= X_j \oplus z_{j-1} \text{ per } 1 < j \leq n \\ Y_i &= E_K(z_i) \text{ per } 1 \leq i \leq n \end{aligned}$$

Disegnare gli schemi di cifratura e decifratura di questa variante del CBC. Considerare, infine, il MAC definito come $MAC_K(X_1, \ldots, X_n) = Y_n$ e valutarne la sicurezza rispetto al medesimo MAC basato sul CBC classico.

Esercizio 4

Si consideri il seguente protocollo

$$\begin{aligned} B &\rightarrow A : E_{PK_A}(B, N_B, M_B) \\ A &\rightarrow B : M_A, N_B \end{aligned}$$

dove M_A e M_B sono messaggi di A e B, N_B è un nonce generato da B e PK_A è la chiave pubblica di A.

1. Elencare le proprietà (autenticazione di entità e messaggi, segretezza) garantite dal protocollo evidenziando le componenti dei messaggi necessarie al raggiungimento di tali proprietà e le relative verifiche svolte da A o B.
2. Cosa accade se B, nel primo messaggio, viene inviato in chiaro?
3. Cosa accade se si elimina il nonce dal protocollo?

Esercizio 5 (facoltativo)

Dimostrare che, nel cifrario RSA, $D_{SK}(E_{PK}(X)) = X$ (considerare solo il caso in cui X è primo con il modulo n del cifrario).