Sicurezza

7 Settembre 2011

Esercizio 1

Si consideri un cifrario con: $\mathcal{P} = \mathcal{C} = \mathbb{Z}_{21}$, $\mathcal{K} = \{(\rho_1, \rho_2) \mid \rho_1, \rho_2 : \mathbb{Z}_{21} \to \mathbb{Z}_{21} \text{ biiettive}\}$, e la funzione di cifratura definita come segue:

$$E_{(\rho_1,\rho_2)}(x) = \rho_1(\rho_2(\rho_1(x)))$$

1. Scrivere la funzione di decifratura e dimostrarne la correttezza. Cosa accade se $\rho_2 = \rho_1^{-1}$?
2. Data la chiave (ρ_1, ρ_2) con ρ_1 definita come

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

   e ρ_2 definita come

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

   mostrare la decifratura del testo cifrato OGEG.
3. La cifratura con chiave (ρ_1, ρ_2) precedente può essere ottenuta con un semplice cifrario a sostituzione con una particolare chiave ρ. Esibire la chiave ρ e spiegare il procedimento seguito per ottenerla.
4. Dimostrare che, se viene riutilizzata la stessa chiave per cifrare le diverse lettere di un testo in chiaro, il cifrario definito sopra non è perfetto.

Esercizio 2

Un metodo per aumentare la sicurezza di un cifrario consiste nell'iterarlo più volte.

1. Quale proprietà deve avere il cifrario affinchè l'iterazione ne migliori effettivamente la sicurezza? Dare un esempio di cifrario che NON aumenta la propria sicurezza quando viene iterato.
2. Iterare un qualsiasi cifrario due volte tipicamente non porta a significativi miglioramenti della sicurezza. Perchè?

Esercizio 3

Per proteggere la segretezza di PIN di accesso (5 cifre decimali) a siti di home-banking, anche nel caso di intrusioni e sottrazioni di informazioni dal sistema, viene proposto di salvarli in un file sotto forma di hash crittografici MD5. Discutere la validità di questa soluzione illustrando eventuali attacchi.

Esercizio 4

Considerare il semplice protocollo di autenticazione (identificazione):

$$\begin{array}{lcll} A & \to & B & : E_{K_{AB}}(N_A) \\ B & \to & A & : N_A \end{array}$$

dove K_{AB} è una chiave a lungo termine condivisa tra A e B e N_A è un nonce generato da A. Illustrare un attacco di tipo 'reflection' e proporre una modifica al protocollo che eviti tale attacco.

Esercizio 5 (facoltativo)

Enunciare e dimostrare il teorema di Shannon sulla caratterizzazione dei cifrari perfetti nel caso in cui $|\mathcal{P}| = |\mathcal{C}| = |\mathcal{K}|$.