Sicurezza

19 Gennaio 2011

Esercizio 1

One-time pad è un celebre cifrario perfetto utilizzato, in passato, per il telegrafo. Considerare una variante di tale cifrario, denominata *two-time pad*, in cui la chiave viene riutilizzata per cifrare un secondo testo in chiaro della stessa lunghezza del primo.

1. Dare la definizione formale di two-time pad, indicando $\mathcal{P}, \mathcal{C}, \mathcal{K}, E, D$
2. Dare un esempio di cifratura di due testi in chiaro, riutilizzando la stessa chiave
3. Dimostrare che two-time pad non è perfetto (suggerimento: può essere conveniente formalizzare il cifrario considerando direttamente testi lunghi $2d$, corrispondenti alla concatenazione dei due testi lunghi d cifrati con la stessa chiave)

Esercizio 2

Viene proposta una modalità di cifratura concatenata denominata CKC (cipher key chaining) e definita nel modo seguente: dato un testo $X = x_1, \ldots x_n$ si calcola $Y = y_1, \ldots, y_n$ come segue:

$$\begin{aligned} y_1 &= E_K(x_1) \\ y_i &= E_{y_{i-1}}(x_i) \text{ per } 1 < i \leq n \end{aligned}$$

Disegnare lo schema di cifratura e decifratura di CKC e discuterne la (in)sicurezza.

Esercizio 3

Considerare un'istanza del cifrario RSA con modulo $n = 51$ e chiave pubblica $PK = 11$. Trovare la decifratura del testo cifrato $Y = 4$, illustrando in dettaglio l'attacco. Dove sarebbe fallito l'attacco se n fosse stato un numero molto grande?

Esercizio 4

Si consideri una carta di credito prepagata in cui sia possibile caricare denaro tramite il protocollo seguente:

$$A \rightarrow B : A, 10€, MAC_{K_A}(A, 10€)$$

dove K_A è una chiave condivisa tra l'utente A e la banca B.
Se la carta viene smarrita, rubata o clonata il potenziale danno dovrebbe essere limitato alla cifra attualmente sulla carta. Discutere mostrando eventuali attacchi e proponendo possibili rimedi.

Esercizio 5 (facoltativo)

Illustrare *l'attacco del compleanno* discutendone le implicazioni sulla sicurezza delle funzioni hash crittografiche.