# CORSO DI SICUREZZA INFORMATICA 1 (A.A. 2008/2009)

# Prof. A. Armando

(25 Giugno 2009)

Si risponda alle domande utilizzando lo spazio apposito **giustificando le risposte date**.
Non è consentito l'utilizzo di libri, appunti, nè dispositivi elettronici di alcun tipo.

Nome e Cognome: _____

Matricola: _____

---

1. ***Crittografia Simmetrica e Funzioni di Hash***

   *Si consideri la seguente definizione di una funzione di hash basata su un algoritmo crittografico. Sia $K$ una chiave crittografica data e sia $M = M_1 M_2 \cdots M_n$ (con $n \geq 1$) un messaggio dove gli $M_i$ (per $1 \leq i \leq n$) sono blocchi di bit di ugual lunghezza:*

$$\begin{aligned} H(M_1) &= E(K, M_1) \\ H(M_1 \cdots M_i M_{i+1}) &= E(K, H(M_1 \cdots M_i) \oplus M_{i+1}) \quad \text{per } i = 1, \ldots, n-1 \end{aligned}$$

   *Si dimostri che lo schema non è sicuro mostrando che dato un messaggio $A_1 A_2$ ed un blocco arbitrario $B_1$ è possibile determinare un blocco $B_2$ tale che $H(B_1 B_2) = H(A_1 A_2)$, ovvero che $H$ non è* weak collision resistant.

**Soluzione.**

$$H(A_1 A_2) = E(K, E(K, A_1) \oplus A_2)$$

mentre

$$H(B_1 B_2) = E(K, E(K, B_1) \oplus B_2)$$

Quindi è sufficiente trovare un blocco $B_2$ tale che

$$E(K, B_1) \oplus B_2 = E(K, A_1) \oplus A_2.$$

Mettendo in $\oplus$ ambo i lati con $E(K, B_1)$ e semplificando, otteniamo:

$$B_2 = E(K, B_1) \oplus E(K, A_1) \oplus A_2.$$

Quindi se $B_2 = E(K, B_1) \oplus E(K, A_1) \oplus A_2$, allora $H(B_1 B_2) = H(A_1 A_2)$ per qualunque valore di $A_1$, $A2$ e $B_1$. Quindi $H$ non è *weak collision resistant*.

2. ***Crittografia***

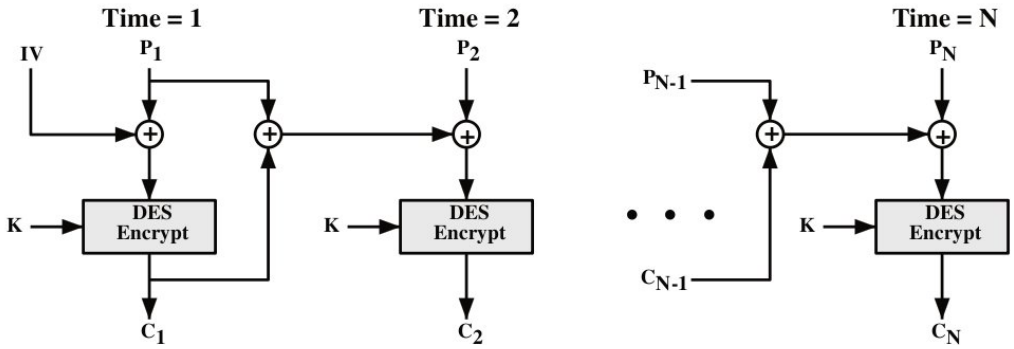
*Si consideri il seguente algoritmo crittografico basato sull'idea di sostituire ogni lettera dell'alfabeto* $m$ *con* $(am + b) \bmod 26$ *dove la chiave è data da* $k = \langle a, b \rangle$ *con* $a$ *e* $b$ *interi positivi nell'intervallo* $[0, 25]$.

*Si dimostri, mediante un esempio, che se* $a$ *e* $26$ *non sono relativamente primi allora lo schema non è utilizzabile.*

**Soluzione.** Si consideri la chiave $k = \langle 2, 0 \rangle$. (2 non è relativamente primo con 26.) Il ciphertext corrispondente a $m_1 = 0$ coincide con il ciphertext corrispondente a $m_2 = 13$. Ciò significa che la funzione di cifratura non è invertibile e quindi che non è sempre possibile risalire univocamente al plaintext corrispondente ad un dato ciphertext. Ciò rende lo schema proposto inutilizzabile.

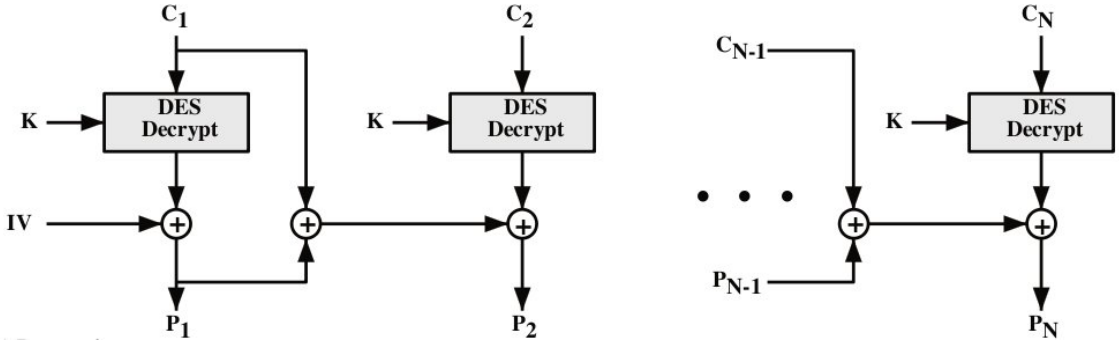
3. ***Crittografia***

*Il seguente schema crittografico per* block encription *è utilizzato in Kerberos v.4.*




*Si disegni il corrispondente schema crittografico da usarsi in fase di decifratura.*

**Soluzione.**



4. ***Protocolli di Sicurezza***

*Si consideri il protocollo di autenticazione a chiave pubblica di Needham Schroeder:*

$$\begin{array}{ll} 1. & A \to B: \ \{A, N_A\}_{K_B} \\ 2. & B \to A: \ \{N_A, N_B\}_{K_A} \\ 3. & A \to B: \ \{N_B\}_{K_B} \end{array}$$

*Come visto a lezione tale protocollo è vulnerabile ad un* man-in-the-middle attack*.*

*Dire quali delle seguenti varianti del protocollo impediscono tale attacco e quali invece continuano a soffrirne. Si giustificano le risposte date.*

*(a)*

$$\begin{array}{ll} 1. & A \to B: \ \{A, B, N_A\}_{K_B} \\ 2. & B \to A: \ \{N_A, N_B\}_{K_A} \\ 3. & A \to B: \ \{N_B\}_{K_B} \end{array}$$

**Soluzione.** L'attacco è ancora possibile

*(b)*

$$\begin{array}{ll} 1. & A \to B: \ \{A, B, N_A\}_{K_B} \\ 2. & B \to A: \ \{N_A, N_B, B\}_{K_A} \\ 3. & A \to B: \ \{N_B\}_{K_B} \end{array}$$

**Soluzione.** L'attacco non è più possibile.

*(c)*

$$\begin{array}{ll} 1. & A \to B: \ \{A, B, N_A\}_{K_B} \\ 2. & B \to A: \ \{N_A, N_B\}_{K_A} \\ 3. & A \to B: \ \{A, B, N_B\}_{K_B} \end{array}$$

**Soluzione.** L'attacco è ancora possibile.

5. ***Crittografia a Chiave Pubblica***

*Rispondere alle seguenti domande, giutificando le risposte date:*

*(a) È vero che la chiave privata è generata dalla Certification Authority e viene consegnata assieme al certificato digitale relativo alla corrispondente chiave pubblica?*

**Soluzione.**

(b) *È vero che una smartcard usata per la firma digitale contiene la chiave privata del possessore?*

**Soluzione.**

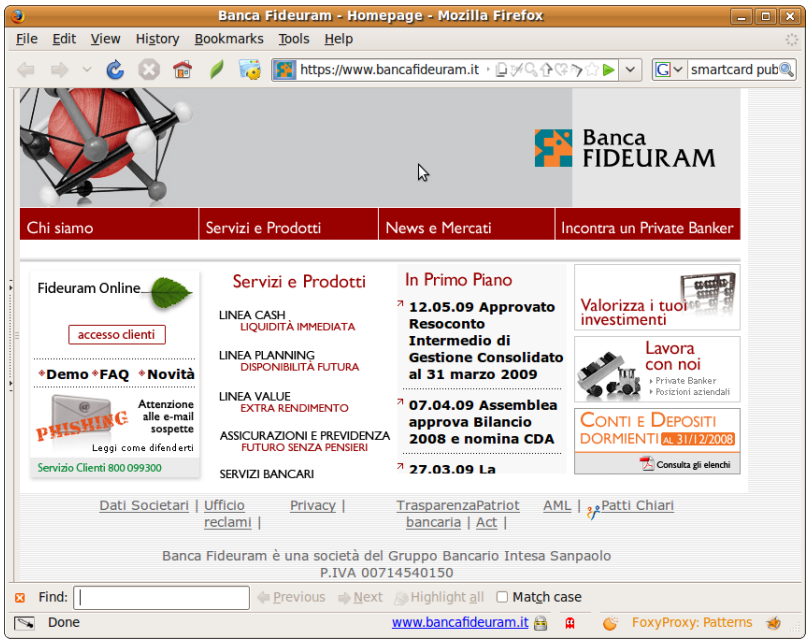
(c) *È vero che per verificare l'autenticità di una firma digitale è necessario possedere una smartcard?*

**Soluzione.**

(d) *È vero che esistono dei certificati digitali la cui autenticità non può essere controllata verificandone la firma?*

**Soluzione.**

(e) *Supponete di essere un correntista di Banca Fideuram e che vi troviate davanti ad un browser che vi mostra la seguente schermata. Indicare le situazioni in cui* ***non*** *ritenete sicuro effettuare il login con le vostre credenziali e quali invece ritenete che ciò possa essere fatto con ragionevole sicurezza.*




**Soluzione.**

6. ***Controllo degli Accessi*** *Si consideri un sistema con tre utenti: Alice, Bob e Charlie. Alice possiede il file* `alice.bat`*, Bob può solo leggerlo e scriverlo, mentre Charlie può solo eseguirlo. Charlie può solo leggere il file* `bob.bat`*, che è posseduto da Bob, mentre Alice lo può solo leggere e scrivere. Charlie possiede il file* `charlie.bat`*; Alice lo può solo scrivere e Bob può solo eseguirlo. Ogni file può essere letto, scritto ed eseguito dagli utenti che lo posseggono.*

   (a) *Si scriva la matrice di controllo degli accessi corrispondente a tale situazione.*

**Soluzione.**

| | `alice.bat` | `bob.bat` | `charlie.bat` |
|---|---|---|---|
| *Alice* | $rwx$ | $rw$ | $w$ |
| *Bob* | $rw$ | $rwx$ | $x$ |
| *Charlie* | $x$ | $r$ | $rwx$ |

   (b) *Si scriva la matrice di controllo degli accessi che si ottiene se Charlie dà ad Alice il permesso di leggere* `charlie.bat` *e Alice revoca a Bob il permesso di scrivere* `alice.bat`*.*

**Soluzione.**

| | `alice.bat` | `bob.bat` | `charlie.bat` |
|---|---|---|---|
| *Alice* | $rwx$ | $rw$ | $wr$ |
| *Bob* | $r$ | $rwx$ | $x$ |
| *Charlie* | $x$ | $r$ | $rwx$ |