CORSO DI SICUREZZA INFORMATICA 1 (A.A. 2007/2008)

Prof. A. Armando

(12 Giugno 2008)

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

Nome e Cognome: _____

Matricola: _____

---

1. ***Crittografia simmetrica***

   Si consideri il seguente algoritmo di cifratura. Il plaintext P è suddiviso in due parti P_l e P_r. Anche la chiave K è suddivisa in due part K_l e K_r. Ovvero,

   $$P = P_l|P_r \qquad\qquad K = K_l|K_r$$

   Il testo cifrato C è dato dalla concatenazione di C_l e C_r, definite nel seguente modo:

   $$C_r = P_r \oplus H(P_l|K_l) \quad (1)$$
   $$C_l = P_l \oplus H(C_r|K_r) \quad (2)$$

   dove H è una funzione di hash.

   (a) *Quale relazione deve sussistere tra funzione di hash e le dimensioni della chiave e del plaintext affinchè lo schema sia applicabile?*

   Soluzione. È necessario che P_l ed P_r abbiano un numero di bit pari alla lunghezza del hash tornato da H.

   (b) *Si definisca l'algoritmo che deve essere applicato per decrifrare il testo cifrato C generato con tale algoritmo assumendo che siano note la chiave K e la funzione di hash H.*

Soluzione.

$$P_l = C_l \oplus H(C_r|K_r) \quad (3)$$
$$P_r = C_r \oplus H(P_l|K_l) \quad (4)$$

(3) si ottiene da (1) moltiplicandone ambo i lati per $H(P_l|K_l)$ e semplificando con le seguenti proprietà dello $\oplus$:

$$\begin{aligned} X \oplus X &= \mathbf{0} \\ X \oplus \mathbf{0} &= X \\ (X \oplus Y) \oplus Z &= X \oplus (Y \oplus Z) \end{aligned}$$

(4) si ottiene in modo analogo da (2).

(c) Mostrare che l'algoritmo è insicuro se si dispone di ciphertexts corrispondenti a plaintexts che hanno la prima parte (P_l) in comune e uno dei due plaintext è noto.

Soluzione.
I due plaintext sono della forma:

$$P = P_l|P_r$$
$$P' = P_l|P'_r$$

e dunque i ciphertexts sono ottenuti nel seguente modo:

$$C_r = P_r \oplus H(P_l|K_l) \qquad C_l = P_l \oplus H(C_r|K_r)$$
$$C'_r = P'_r \oplus H(P_l|K_l) \qquad C'_l = P_l \oplus H(C'_r|K_r)$$

P'_r può essere derivato a partire da C_r e C'_r nel seguente modo: $P'_r = (C_r \oplus C'_r) \oplus P_r$. Infatti:

$$\begin{aligned} & (C_r \oplus C'_r) \oplus P_r \\ =& ((P_r \oplus H(P_l|K_l)) \oplus (P'_r \oplus H(P_l|K_l))) \oplus P_r \\ =& ((P_r \oplus P'_r) \oplus (H(P_l|K_l) \oplus H(P_l|K_l))) \oplus P_r \\ =& ((P_r \oplus P'_r) \oplus \mathbf{0}) \oplus P_r \\ =& (P_r \oplus P'_r) \oplus P_r \\ =& P'_r \oplus (P_r \oplus P_r) \\ =& P'_r \oplus \mathbf{0} \\ =& P'_r \end{aligned}$$

2. *Crittografia a Chiave Multipla*

Un sistema crittografico a chiave multipla *è caratterizzato da un insieme di* n *chiavi* $\mathcal{K} = \{K_1, \ldots, K_n\}$ *tali che se se* $C_0 = P$ *è un generico plaintext e* $C_{i+1} = E(C_i, K_i)$ *per* $i = 0, \ldots, n-1$*, allora* $C_n = P$*. Ovvero cifrando* P *con tutte le chiavi* $K_1, \ldots, K_n$ *(in qualunque ordine) si ottiene il plaintext di partenza.*

(a) *Un sistema crittografico a chiave multipla con* $n = 2$ *corrisponde ad uno dei sistemi crittografici visti a lezione. Quale? Si giustifichi la risposta data.*

Soluzione. Uno schema crittografico a chiave a chiave pubblica (ad esempio RSA), dove $\mathcal{K}$ è dato dalla chiave pubblica e dalla chiave privata.

(b) *Si discutano i possibili utilizzi di un sistema crittografico a chiave multipla con* $n > 2$*.*

Soluzione. Un primo possibile utilizzo è per la firma digitale congiunta tra due o più agenti. Ad esempio se $\mathcal{K} = \{K_1, \ldots, K_n\}$ e K_i è privata per l'agente A_i (per $i = 1, \ldots, n-1$) e K_n è pubblica, allora A_1 può firmare digitalmente un documento M cifrandone un hash con K_1 e mandando il risultato ad A_2, A_2 cifra quanto ricevuto da A_1 con la propria chiave privata K_2 e invia il risultato ad A_3, e così via fino a A_{n-1} che produce

$$E(K_{n-1}, E(K_{n-2}, \ldots E(K_2, E(K_1, H(M))) \ldots)) \tag{5}$$

La firma può essere verificata cifrando (5) con K_n. Si osservi che la sottoscrizione di un singolo agente è verificabile solo quando è verificabile la sottoscrizione dei co-signatari. Dualmente, sotto le stesse ipotesi sulla distribuzione delle chiavi, cifrando con K_n si ottiene confidenzialità nei confronti $A_1, \ldots A_{n-1}$.

3. ***Protocolli di Sicurezza***

Si consideri il seguente protocollo P_1 per l'autenticazione tra due agenti A e B:

$$
\begin{array}{l}
1.\ A \to B : N_a \\
2.\ B \to A : \{N_a\}_{K_{ab}}, N_b \\
3.\ A \to B : \{N_b\}_{K_{ab}}
\end{array}
$$

dove N_a e N_b sono nonces e K_{ab} è una chiave condivisa tra A e B.

(a) Si mostri che il protocollo non garantisce la mutua autenticazione.

Soluzione. Il protocollo non garantisce la proprietà di autenticazione mutua. Infatti il protocollo è vulnerabile al seguente *reflection attack*:

$$
\begin{array}{lll}
(s1) & 1. & a \to i \ : n_a \\
(s2) & 1. & a \leftarrow i \ : n_a \\
(s2) & 2. & a \to i \ : \{n_a\}_{k_{ab}}, n_b \\
(s1) & 2. & a \leftarrow i \ : \{n_a\}_{k_{ab}}, n_b \\
(s1) & 3. & a \to i \ : \{n_b\}_{k_{ab}}
\end{array}
$$

dove $s1$ e $s2$ indicano due esecuzioni/sessioni concorrenti del protocollo. A questo punto a è convinto di aver interagito con b, ma ciò non è avvenuto.

(b) Una delle regole di prudent engineering *per la progettazione di protocolli di sicurezza presentate a lezione suggerisce di includere nei messaggi l'identità del mittente e del destinatario. Si mostri come l'applicazione di questo principio può prevenire l'attacco trovato al punto precedente.*

Soluzione. Applicando tale principio di *prundent engineering* si ottiene

$$
\begin{array}{l}
1.\ A \to B : A, B, N_a \\
2.\ B \to A : \{A, B, N_a\}_{K_{ab}}, N_b \\
3.\ A \to B : \{A, B, N_b\}_{K_{ab}}
\end{array}
$$

È facile verificare che l'attacco precedente non è più riproducibile.

(c) Un ulteriore metodo per cercare di rendere sicuro il protocollo è quello di modicarlo nel seguente modo:

$$
\begin{array}{l}
1.\ A \to B : N_a \\
2.\ B \to A : \{N_a - 1\}_{K_{ab}}, N_b \\
3.\ A \to B : \{N_b - 1\}_{K_{ab}}
\end{array}
$$

Si discuta se questo protocollo garantisce o meno la proprietà di mutua autenticazione.

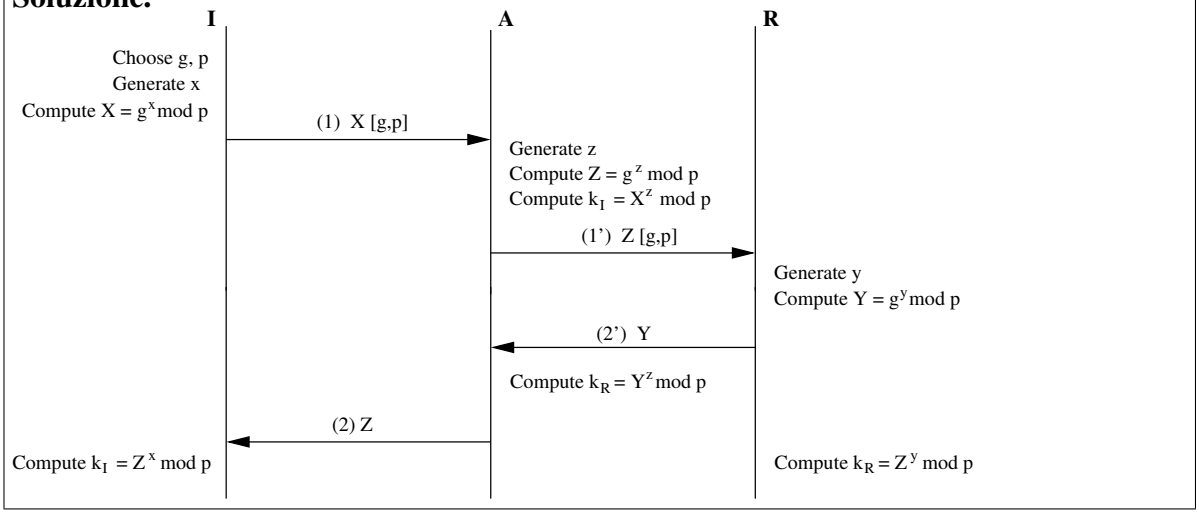
Soluzione. Non la garantisce. Infatti il protocollo continua ad essere vulnerabile allo stesso *reflection attack*:

$$
\begin{array}{llll}
(s1) & 1. & a \rightarrow i & : n_a \\
(s2) & 1. & a \leftarrow i & : n_a \\
(s2) & 2. & a \rightarrow i & : \{n_a - 1\}_{k_{ab}} \\
(s1) & 2. & a \leftarrow i & : \{n_a - 1\}_{k_{ab}}, n_b \\
(s1) & 3. & a \rightarrow i & : \{n_b - 1\}_{k_{ab}}
\end{array}
$$

4. ***Protocolli di Sicurezza***

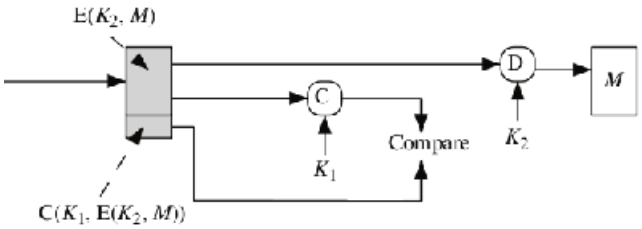
Si dimostri che il protocollo per scambio di chiavi di Diffie-Hellman non garantisce l'autenticazione.

Soluzione.



5. ***Crittografia II***

Si completi il seguente schema crittografico disegnandone il trasmettitore.



Soluzione.