Prova scritta del 20 febbraio 2008 (10 pt)

Si consideri il seguente protocollo di identificazione di tipo challenge-response basato sulla crittografia a chiave pubblica.

M1 $A \rightarrow B$: A

M2 $B \rightarrow A$: $E_A(r)$

M3 $A \rightarrow B$: r

Dove $E_A(r)$ denota la cifratura di r con la chiave pubblica di A e r una quantità generata per mezzo di un generatore sicuro di numeri random. Si assuma che B conosca la chiave pubblica di A.

Il candidato risponda ai seguenti quesiti motivando le risposte.

1) Al termine dell'esecuzione del protocollo quali prove ha B di essere in presenza di A?

2) Nel protocollo è possibile generare la quantità r per mezzo di un semplice contatore senza indebolire il protocollo?

3) Riprogettare il protocollo sotto le seguenti ipotesi:

a. A e B utilizzano solo un cifrario simmetrico E;
b. A e B condividono una chiave segreta k_{ab};
c. né A né B dispongono di un generatore random sicuro

Soluzione

Domanda 1. Il processo B è convinto che il messaggio M3 proviene da *A* perché solo *A* può aver decifrato il contenuto del messaggio M2. Inoltre, siccome B considera *r* fresco, allora ritiene che il messaggio M3 non sia una replica di un vecchio messaggio. Per cui alla fine del protocollo, B ritiene di essere in presenza di A.

Domanda 2. Il generatore sicuro di numeri random non può essere sostituito da un contatore. Il numero *r*, oltre alla proprietà di freschezza (mai utilizzato in precedenti esecuzioni) deve anche godere della proprietà di *imprevedibilità*. Altrimenti, un avversario potrebbe prevedere il prossimo valore di *r* e costruire il messaggio M3 senza aver decifrato il contenuto M2. Così facendo l'avversario potrebbe impersonare A.

Domanda 3.

M1 $A \rightarrow B$: A

M2 $B \rightarrow A$: r

M3 $A \rightarrow B$: $\mathsf{E}_{K_{ab}}(r)$