Prova scritta del 24 giugno 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 $B \rightarrow A$: $E(e_A, r)$

M3 $A \rightarrow B$: r

Dove $E(e, x)$ denota la cifratura di x con la chiave pubblica e (quindi E è *asimmetrico*) ed r è una quantità generata per mezzo di un generatore sicuro di numeri random. Si assuma che B conosca e_A, la chiave pubblica di A.

1. Al termine dell'esecuzione del protocollo quali garanzie, B può concludere di essere in presenza di A? Motivare la risposta.
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: 1) A e B utilizzano adesso un cifrario simmetrico E_s; 2) A e B condividono una chiave segreta k_{AB}; 3) 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 star effettivamente parlando con 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 $A \rightarrow B$: r

M3 $A \rightarrow B$: $E_s(k_{AB}, r)$