PROVA SCRITTA DEL 30 GENNAIO 2009
10 PUNTI

TESTO

Sia *S* un server e sia Π la sua chiave pubblica. Sia *C* un client che condivide con *S* un PIN *P* di 4 cifre decimali. Si assuma che *C* conosca la chiave pubblica Π del server. Si assuma inoltre che il client ed il server dispongano solo di un cifrario a chiave simmetrica e di uno a chiave pubblica.

Quesito 1. Il candidato progetti un protocollo che permetta al server di identificare il cliente, ovvero alla fine del protocollo il server deve avere prova di essere in presenza del cliente. Il protocollo deve essere sicuro rispetto ad un brute-force attack sullo spazio dei messaggi.

Quesito 2. Il candidato progetti un protocollo di distribuzione delle chiavi tra *S* e *C* che soddisfi i seguenti requisiti:

1. alla fine del protocollo C ed S dispongono della chiave di sessione *K*;
2. alla fine del protocollo, *C* ha la certezza che *S* dispone della chiave *K* e viceversa.

SOLUZIONE

Quesito 1.

M1 S $\rightarrow$C: n

M2 C $\rightarrow$S: $E_{\Pi_S}(C, S, P, n, \rho)$

Dopo la ricezione del messaggio M2, *S* pensa che il messaggio provenga da *C* perché contiene *P*; S ritiene tale messaggio fresco perché contiene *n*.

Il sale ρ è necessario per evitare un attacco esaustivo sullo spazio dei messaggi. Infatti, a parte ρ tutte le quantità, inclusa la chiave pubblica, sono note eccetto il PIN. Perciò se ρ non ci fosse, siccome i pin sono solo 10 mila, l'avversario potrebbe eseguire un attacco esaustivo cercando quel valore di *x* per cui M2 = $E_{\Pi_S}(C, S, x, n)$.

Quesito 2.

M1 S $\rightarrow$C: n

M2 C $\rightarrow$S: $E_{\Pi_S}(C, S, P, n, K)$

M3 S $\rightarrow$C: $E_K(C, S)$

Dopo la ricezione del messaggio M2, *S* pensa che la chiave *K* proviene da *C* perché combinata con *P* e che è fresca perché combinata con *n*.

Dopo la ricezione di M3, *C* ha la garanzia che *S* dispone della chiave di sessione *K* perché solo *S* può aver decifrato *K*.