Laurea Specialistica in Ingegneria Informatica

RETI DI CALCOLATORI

Appello del 17 luglio 2007

ESERCIZIO DI SECURITY — PUNTI: 6

Il candidato definisca un protocollo di distribuzione delle chiavi che, al termine della sua esecuzione, soddisfi i seguenti requisiti:

1. Alice e Bob condividono una chiave segreta di sessione *K*;
2. Alice ha la prova che Bob dispone della chiave K e viceversa;
3. il protocollo è resistente ad attacchi di replay.

Tali requisiti devo essere soddisfatti assumendo i seguenti vincoli

A. Alice e Bob dispongano *solo* di un cifrario asimmetrico (no firma digitale);

B. Alice (Bob) conosce e_b (e_a) la chiave pubblica di Bob (Alice);

C. la chiave di sessione viene definita da Alice.

Si indichi con: (i) $E_e(X)$ la cifratura della quantità *Y* con la *chiave pubblica e*; (ii) (*X*, *Y*) la concatenazione di *X* ed *Y*.

Il candidato dimostri brevemente, ma con precisione e proprietà di linguaggio, che il protocollo proposto soddisfa i requisiti specificando sotto quali ipotesi ciò avviene.

SICUREZZA NELLE RETI

Appello del 1 Febbraio 2007

Soluzione

Messaggio M1 A→B: $\{A,B,K\}_{e_b}$

Messaggio M2 B→A: $\{\{A,B\}_K, A,B,n_b\}_{e_a}$

Messaggio M3 A→B: $\{A,B,n_b\}_K$

Dopo la ricezione di M1, B non può dire niente.

Dopo la ricezione di M2, A può concludere che il messaggio viene da B e quindi che B detiene la chiave K perché la parte interna è cifrata con K. Inoltre conclude che il messaggio non è un replay perché la chiave K è fresca.

Dopo M3, B può concludere che il messaggio proviene da A perché solo A può aver decifrato M2 e inserito n_b in M3 che, a tutti gli effetti, è un segreto condiviso. La cifratura con K prova a B che A detiene tale chiave.