Laurea Specialistica in Ingegneria Informatica

SICUREZZA NELLE RETI

APPELLO DEL 01 FEBBRAIO 2010

Esercizio 1 — punti: 10

La modalità CBC: schema, propagazione dell'errore e vantaggi rispetto alla modalità ECB.

Esercizio 2 — punti: 12

I processi *A* e *B* dispongono solo di un cifrario a chiave pubblica e di un cifrario a chiave simmetrica. Si assuma che *A* conosca la chiave pubblica Π_b di *B* e viceversa. Progettare per mezzo della logica BAN un protocollo di distribuzione delle chiavi che soddisfi i seguenti requisiti

1. *A* ha la prova che *B* dispone della chiave di sessione K_{ab} e viceversa;
2. i clock non sono sincronizzati;
3. il protocollo è resistente ad attacchi di replay;
4. la chiave di sessione è generata da uno dei due processi.

Modificare il protocollo assumendo che entrambi i processi contribuiscano alla generazione della chiave di sessione.

Esercizio 3 — punti: 8

Il problema della delega in Kerberos e le relative solutioni.

Soluzione

Esercizio 2

$M1 \quad A \rightarrow B: \quad K_a \; \Pi_b$

$M2 \quad B \rightarrow A: \quad K_a, K_b \; \Pi_a$

$M3 \quad A \rightarrow B: \quad A, B_{K_{ab}}$

$M1 \quad A \rightarrow B: \quad K_a \; \Pi_b$

$M2 \quad B \rightarrow A: \quad K_a, K_b \; \Pi_a$

$M3 \quad A \rightarrow B: \quad K_b, K_a \; \Pi_b$

$M4 \quad B \rightarrow A: \quad A, B_{K_{ab}}$

$M5 \quad A \rightarrow B: \quad B, A_{K_{ab}}$