Laurea Specialistica in Ingegneria Informatica

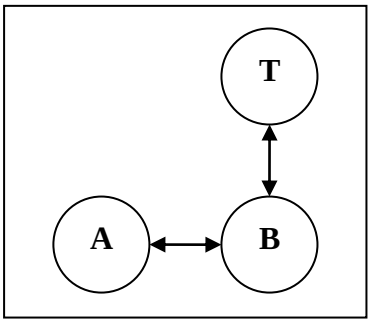
SICUREZZA NELLE RETI

Appello del 14 Gennaio 2010

Esercizio 1 — punti: 10

Con proprietà di linguaggio e precisione matematica il candidato (a) definisca il cifrario perfetto secondo Shannon e (b) dimostri che in tale cifrario il numero delle chiavi non può essere inferiore al numero dei messaggi.

Esercizio 2 — punti: 12



Con riferimento al sistema di comunicazione in figura, usando la logica BAN, definire un protocollo di distribuzione delle chiavi che soddisfi i seguenti requisiti:

1. *A* e *B* sono convinti che K_{ab} è la chiave di sessione;
2. *A* è convinto che *B* disponga di K_{ab} e viceversa;
3. il protocollo non è soggetto a *replay attack*;

sotto i seguenti vincoli

A. *A* e *B* condividono una chiave segreta, rispettivamente con K_a e K_b, con *T*;
B. *A* e *B* considerano *T* competente nella generazione delle chiavi;
C. i clock non sono sincronizzati.

Esercizio 3 — punti: 8

Il candidato (a) descriva il problema del Denial of Service nel protocollo Diffie-Hellman e (b) discuta la soluzione proposta nel protocollo di Oakley.

Soluzione

Esercizio 2

$M\ 1 \quad A \rightarrow B: \quad A, B, n_a$

$M\ 2 \quad B \rightarrow T: \quad A, B, n_a, n_b$

$M\ 3 \quad T \rightarrow B: \quad A, B, n_b, k_{ab}, \quad A, B, n_a, k_{ab}{}_{k_a}{}_{k_b}$

$M\ 4 \quad B \rightarrow A: \quad A, B, n_a, k_{ab}{}_{k_a}, \quad A, B{}_{k_{ab}}$

$M\ 5 \quad A \rightarrow B: \quad B, A{}_{k_{ab}}$