Laurea Specialistica in Ingegneria Informatica
SICUREZZA NELLE RETI
Appello del 19 febbraio 2010

Nome e Cognome_____ Matricola _____

ESERCIZIO 1 **PUNTI:6**

Con proprietà di linguaggio e precisione matematica, il candidato

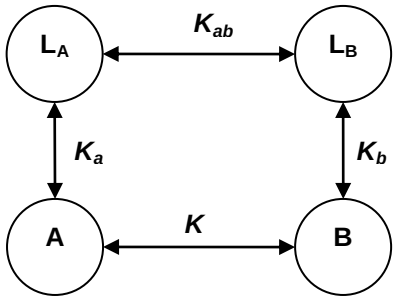
a) enunci le proprietà di *preimage resistance*, 2*nd-preimage resistance* e *collision resistance* di una funzione hash sicura;

b) ne discuta la rilevanza rispetto alla firma digitale; ed

c) indichi il limite superiore della sicurezza (in termini di complessità) di una funzione hash con *m* bit di output.

ESERCIZIO 2 **punti: 14**

Due soggetti *A* e *B* stabiliscono una chiave di sessione *K* utilizzando il protocollo Diffie-Hellmann con parametri pubblici *p* e *g*. Al fine di evitare il MIM-attack, essi usano un sistema di certificazione online riportato in figura. Ogni soggetto fa riferimento ad una autorità di certificazione locale (ad esempio L_A) ed ha con essa una relazione di fiducia che si concretizza nella condivisione di una chiave segreta (ad esempio K_a). L'autorità di certificazione ne certifica il parametro pubblico (Ad esempio L_A certifica il parametro pubblico X_A di *A*). Tra le autorità di certificazione locali esiste una cross-certificazione che si concretizza nella condivisione di una chiave segreta (ad esempio K_{ab}).



Usando la logica BAN, il candidato progetti e verifichi il protocollo completo di autenticazione e definizione di una chiave di sessione tra i soggetti A e B sia nel caso in cui i clock non sono sincronizzati sia in quello in cui lo sono. Nel secondo caso, si assuma che il certificato abbia una validità di D unità di tempo.

ESERCIZIO 3 **punti:8**

Con proprietà di linguaggio il candidato descriva il meccanismo a finestra anti-replay di IpSec.

Laurea Specialistica in Ingegneria Informatica
SICUREZZA NELLE RETI
Appello del 19 febbraio 2009

Soluzione

ESERCIZIO 1

Vedi appunti.

ESERCIZIO 2

Senza clock sincronizzati

M1. A -> B: Na

M2. B->LB: {Na, XB}Kb

M3. LB->LA: {Na, XB}Kab

M4. LA->A: {Na, XB}Ka

Parallelamente a questi msg ci sono quelli M1'-M4' per la certificazione di A rispetto a B. Il protocollo si ottiene sostituendo A con B.

Con i clock sincronizzati

M1. A->LA: {tA, XA}Ka

M2. LA->LB: {tA, XA}Ka

M3. LB->B: {tA, XA}Kb

Parallelamente a questi msg ci sono quelli M1'-M3' per la certificazione di A rispetto a B. Il protocollo si ottiene sostituendo A con B.

ESERCIZIO 3

Vedi appunti.