Laurea Specialistica in Ingegneria Informatica

SICUREZZA NELLE RETI

Appello del 18 settembre 2009

Esercizio 1 — punti: 12

Con proprietà di linguaggio e precisione matematica si definiscano le proprietà one-way, weak collision resistance e strong collision resistance di una funzione hash sicura e se discuta la loro rilevanza nell'ambito della firma digitale.

Esercizio 2 — punti: 12

In un sistema cliente-servitore, sia Π la *chiave pubblica* del server *S* e sia PIN un *segreto condiviso* tra il server S ed il cliente C. Si assuma inoltre che la chiave Π sia nota al cliente C.

QUESITO 1. Si progetti un protocollo di distribuzione delle chiavi che, al termine della sua esecuzione, soddisfi i seguenti requisiti:

1. il cliente ed il server condividono una *chiave segreta di sessione K*;
2. il cliente ha identificato il server ed ha la prova che il server possiede la chiave *K*;
3. il server ha identificato il cliente ed ha la prova che il cliente possiede la chiave *K*;
4. il protocollo è resistente ad attacchi di *replay*.

Tali requisiti devo essere soddisfatti assumendo che: a) gli orologi del cliente e del server non siano sicronizzati e b) per quanto riguarda la crittografia a chiave pubblica, il server ed il cliente dispongono solo di un cifrario ma non della firma digitale.

Il candidato argomenti brevemente ma con precisione matematica e proprietà di linguaggio che il protocollo proposto soddisfa i requisiti posti.

Quesito 2. Modificare il protocollo assumendo che gli orologi del cliente e del server siano sincronizzati.

QUESITO 3. Siccome il PIN è un segreto condiviso tra il server ed il client, tale quantità potrebbe essere utilizzata come chiave simmetrica, ovvero per derivarne una, al fine di garantire i requisiti di confidenzialità ed autenticità della chiave di sessione. Il candidato argomenti brevemente ma con precisione matematica e proprietà di linguaggio se questa è un'opzione sicura.

Esercizio 3 — punti: 6

Si descrivano le informazioni minime che devono essere contenute in un certificato digitale ed i principali obblighi che un'autorità di certificazione deve assolvere per il rilascio di tale certificato.