Cognome: Nome: Matricola:

Sicurezza su Reti

Docente: A. De Santis

Appello del 23/07/2015

Non è ammesso alcun materiale per la consultazione. Buon lavoro!

1	2	3	4	totale
/25	/25	/25	/25	/100

1. (25 punti) DES e DES triplo.
   a. (10 punti) Analizzare l'algoritmo del DES.
   b. (15 punti) Descrivere ed analizzare il DES triplo.

2. (25 punti) Schema di firme RSA.
   a. (10 punti) Descrivere le fasi di generazione delle chiavi, firma e verifica, chiarendo quali sono i parametri scelti a caso e quali le loro caratteristiche.
   b. (10 punti) Analizzare la sicurezza dello schema di firme RSA.
   c. (5 punti) Chiarire come e perché vengono utilizzate le funzioni hash nella firma.

3. (25 punti) Certificati e PKI.
    a. (5 punti) Chiarire cos'è un certificato e descrivere il formato X.509.
    b. (5 punti) Chiarire l'importanza e l'utilizzo dei certificati.
    c. (15 punti) Chiarire le motivazioni che portano alla revoca di un certificato e come viene realizzata la revoca.

4. (25 punti) Cifrari a blocchi.
   Si consideri la seguente proposta di cifrario a blocchi per testi in chiaro m di 160 bit, costruita a partire da una funzione hash SHA-1,

$$C_k(m) = \text{SHA-1}(k) \text{ xor } m.$$

   Cioè, il testo cifrato si ottiene facendo lo xor tra il testo in chiaro m e l'hash SHA-1 della chiave k.
   Analizzare la sicurezza della proposta, giustificando le risposte.