Cognome: Nome: Matricola:

Sicurezza su Reti

Docente: A. De Santis

Appello del 8/07/2015

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

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

1. (25 punti) Descrivere ed analizzare il crittosistema DES.
   a. (15 punti) Descrivere l'algoritmo del DES.
   b. (5 punti) Descrivere come funziona la decifratura e ne si analizzi la correttezza.
   c. (5 punti) Si analizzi la sicurezza del DES chiarendo perché è stato sostituito come standard.

2. 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 casa e quali le loro caratteristiche.
    b. (10 punti) Analizzare la sicurezza dello schema di firme RSA.
    c. (5 punti) Fornire un semplice esempio numerico.

3. (25 punti) Descrivere ed analizzare lo schema di Merkle per l'accordo su chiavi tra due partecipanti.
    a. Descrivere le computazioni effettuate da Alice e analizzarne la complessità.
    b. Descrivere le computazioni effettuate da Bob e analizzarne la complessità.
    c. Descrivere le computazioni che un attaccante passivo deve effettuare per rompere lo schema e analizzarne la complessità.

4. (25 punti) Schema di Diffie-Hellman per l'accordo su chiavi tra due partecipanti.
    a. (20 punti) Descrivere ed analizzare gli algoritmi per la generazione dei parametri pubblici e per l'accordo sulla chiave. Inoltre, analizzare la sicurezza dello schema.
    b. (5 punti) E' possibile utilizzare p=17, g=2 come parametri pubblici? Giustificare la risposta.