Cognome: Nome: Matricola:

Sicurezza su Reti

Docente: A. De Santis

Appello del 04/07/2017

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

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

1. (25 punti) Autenticazione.
   a. (10 punti) Si illustri l'autenticazione basata su password, chiarendo le tecniche e la sicurezza.
   b. (5 punti) Si illustri l'autenticazione basata su tecniche *challenge-response*.
   c. (10 punti) Si illustri l'autenticazione basata su tecniche biometriche, chiarendo la relativa sicurezza.

2. (25 punti) Accordo su chiavi.
    a. (10 punti) Descrivere ed analizzare lo schema Diffie-Hellman per l'accordo su chiavi tra due partecipanti.
    b. (15 punti) Illustrare ed analizzare la generazione dei parametri per l'accordo di chiavi Diffie-Hellman.

3. (25 punti) Cifrari a blocchi.
    a. (10 punti) Descrivere l'algoritmo del DES ed analizzare la relativa sicurezza.
    b. (15 punti) Descrivere l'algoritmo del triplo DES ed analizzare la relativa sicurezza.

4. (25 punti) Firma digitale.
    a. (10 punti) Descrivere cosa è una firma digitale, indicando quali sono i requisiti che essa deve soddisfare e cosa si intende per sicurezza di uno schema di firme digitali.
    b. (15 punti) Descrivere ed analizzare la firma remota.