Cognome: Nome: Matricola:

Sicurezza su Reti

Docente: A. De Santis

Appello del 05/09/2017

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

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

1. (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. (5 punti) Analizzare la sicurezza dello schema di firme RSA.
   c. (10 punti) Chiarire come e perché vengono utilizzate le funzioni hash nella firma.

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) Message Authentication Code.
    a. (10 punti) Descrivere cosa è un MAC, enunciarne le caratteristiche di sicurezza ed illustrarne l'uso.
    b. (5 punti) Descrivere ed analizzare l'HMAC.
    c. (5 punti) Chiarire se il MAC garantisce il non ripudio e motivare la risposta.
    d. (5 punti) Descrivere che primitive possono essere utilizzate e come per ottenere confidenzialità ed autenticità/integrità.

4. (25 punti) Certificati e PKI.
    a. (5 punti) Chiarire cos'è un certificato e descrivere il formato X.509.
    b. (10 punti) Chiarire l'importanza e l'utilizzo dei certificati.
    c. (10 punti) Chiarire le motivazioni che portano alla revoca di un certificato e come viene realizzata la revoca.