Cognome: Nome: Matricola:

Sicurezza su Reti

Docente: A. De Santis

Appello del 15/06/2017

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 AES.
    a. (15 punti) Descrivere ed analizzare l'algoritmo dell'AES.
    a. (10 punti) Si chiarisca l'importanza delle modalità operative ed i relativi vantaggi e svantaggi.

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

3. (25 punti) Password ed autenticazione.
    a. (5 punti) Si chiarisca che cosa è una password ed il suo utilizzo.
    b. (5 punti) Si chiarisca ed analizzi l'uso di funzioni di cifratura e funzioni hash per un sistema di password.
    c. (5 punti) Si descriva ed analizzi l'autenticazione a due fattori (two-factor authentication).
    d. (10 punti) Si analizzino le problematiche di sicurezza legate alla scelta ed all'uso delle password.

4. (25 punti) Certificati e PKI.
    a. (5 punti) Chiarire cos'è un certificato.
    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.