Cognome: Nome: Matricola:

Sicurezza su Reti

Docente: A. De Santis

Appello del 27/07/2016

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

2. (25 punti) Descrivere ed analizzare il crittosistema RSA.
    a. (10 punti) Descrivere ed analizzare la fase di generazione delle chiavi e le fasi di cifratura e decifratura. Inoltre, dimostrare che le operazioni di cifratura e decifratura sono una l'inversa dell'altra.
    b. (15 punti) Analizzare la sicurezza della cifratura RSA e della scelta della lunghezza della chiave.

3. (25 punti) Autenticazione.
    a. (5 punti) Si chiarisca ed analizzi l'uso di funzioni di cifratura e funzioni hash per un sistema di password.
    b. (5 punti) Si descriva ed analizzi l'autenticazione a due fattori (two-factor authentication)
    c. (5 punti) Si analizzino le problematiche di sicurezza legate alla scelta ed all'uso delle password.
    a. (10 punti) Si illustri l'autenticazione basata su tecniche biometriche chiarendone la relativa sicurezza.

4. (25 punti) Funzioni hash.
   Chiarire quali sono le lunghezze dei valori hash delle funzioni hash in uso.
   Analizzare l'importanza della lunghezza del valore hash relativamente alla sicurezza, chiarendo anche cos'è il paradosso del compleanno e le sue implicazioni.