Cognome: Nome: Matricola:

Sicurezza su Reti

Docente: A. De Santis

Appello del 3/2/2016

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.
   a. (13 punti) Descrivere l'algoritmo del DES.
   b. (6 punti) Descrivere come funziona la decifratura e ne si analizzi la correttezza.
   c. (6 punti) Si analizzi la sicurezza del DES chiarendo perché è stato sostituito come standard.

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

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.
    d. (10 punti) Si illustri l'autenticazione basata su tecniche biometriche chiarendo la relativa sicurezza.

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.