Cognome: Nome: Matricola:

Sicurezza su Reti

Docente: A. De Santis

Appello del 3/09/2015

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

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

1. (25 punti) Cifrari a sostituzione.
   a. (15 punti) Si descriva la tecnica di cifratura a sostituzione e le tecniche di crittoanalisi note e le relative contromisure.
   b. (10 punti) Si esprima, giustificando la risposta, il numero di chiavi possibili nel caso di:
      i. sostituzione generica;
      ii. sostituzione con alfabeto shiftato (cifrario con shift).

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) 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) 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.