Cognome: Nome: Matricola:

Sicurezza su Reti

Docente: A. De Santis

Appello del 18/07/2017

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

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

1. (25 punti) Cifrari di Feistel.
   a. (10 punti) Descrivere i cifrari di Feistel, mettendo in evidenza le relative caratteristiche ed i principi su cui essi si basano.
   b. (5 punti) Descrivere la struttura di un round all'interno di un cifrario di Feistel.
   c. (10 punti) Descrivere ed analizzare come avviene la cifratura e la decifratura nei cifrari di Feistel.

2. (25 punti) Funzioni hash.
    a. (5 punti) Chiarire cos'è una funzione hash e descrivere i suoi principali scenari di utilizzo.
    b. (5 punti) Descrivere i principali attacchi e le nozioni di sicurezza per una funzione hash.
    c. (10 punti) Chiarire cos'è il paradosso del compleanno e le sue implicazioni per le funzioni hash.
    d. (5 punti) Chiarire cos'è un digital timestamp (marca temporale) e descrivere un relativo protocollo.

3. (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 generazione delle chiavi e della cifratura RSA.

4. (25 punti) One-time Password ed autenticazione.
    a. (15 punti) Si descrivano ed analizzino le one-time password.
    b. (10 punti) Si descriva ed analizzi l'autenticazione a due fattori (two-factor authentication), descrivendo anche esempi di utilizzo.