Università degli Studi di Torino

Corso di Laurea in Informatica

Esame di Sicurezza – 18 settembre 2013

Nome Cognome

1a. Un MAC (message authentication code)

A) Autentica un utente

B) Autentica un messaggio con una chiave simmetrica

C) Autentica un messaggio con una chiave asimmetrica

D) Autentica un messaggio mediante un protocollo di challenge-response

E) Rende un messaggio non disconoscibile

1b. il cosiddetto ARP poisoning:

A) distribuisce un virus su rete locale

B) distribuisce un virus su rete geografica

C) provoca una errata associazione tra indirizzi DNS e indirizzi IP

D) provoca una errata associazione tra indirizzi MAC e indirizzi IP

E) provoca una errata associazione tra URL http e indirizzi IP

2. Definizione di radice primitiva di un numero q e metodo per generarne una

3. Dimostrare che ab mod M = (a mod M)(b mod M) mod M

4. Disegnare una topologia di rete locale con firewall in HA (high availability)

5. Differenza tra modalità tunnel e transport in una VPN