Università degli Studi di Torino

Corso di Laurea in Informatica

Esame di Sicurezza – 19 settembre 2016

Nome Cognome

Numero documento

1. Descrivere un metodo per calcolare la radice primitiva a di un primo q, dimostrarne la correttezza

2a.: Una VPN (virtual private network)

A) separa una LAN in reti virtuali che si comportano come se fossero fisicamente distinte

B) separa una LAN in due o più LAN con indirizzamenti IP distinti

C) separa una LAN in due o piu' reti virtuali attraverso un proxy

D) è realizzata a livello 2 della pila ISO/OSI

E) è realizzata a livello 3 della pila ISO/OSI

2b. una funzione di hash resistente alle collisioni

A) rende impossibili le collisioni

B) rende improbabili le collisioni

C) rende computazionalmente difficile la generazione di collisioni

C) dato un input produce un codice (hash code) che autentica l'input stesso

D) dato un input produce un codice (hash code) che cifra l'input stesso

3. Descrivere il cifrario di Vigenère

4. Discutere il concetto di IT risk management (gestione del rischio informatico)

5. Descrivere il funzionamento del NAPT (network address and port translation) e le sue conseguenze per la sicurezza di una rete