



Name :

Roll No. :

Invigilator's Signature :

CS/M.TECH (CSE)/SEM-2/MCSE-205/2012

2012

CRYPTOGRAPHY AND NETWORK SECURITY

Time Allotted : 3 Hours

Full Marks : 70

The figures in the margin indicate full marks.

*Candidates are required to give their answers in their own words
as far as practicable.*

GROUP – A

(Multiple Choice Type Questions)

Answer the following.

5 × 2 = 10

1. DES consists

- a) S-box
- b) P-box
- c) both S-box and P-box
- d) None of these.

2. Total no of primary classes in threat is

- a) 1
- b) 3
- c) 4
- d) above 5.



3. Full form of MAC is
- a) Message Authentication Code
 - b) Message Authorized Code
 - c) Mail Automation Code
 - d) Message Authentication Cipher
4. Packet filtering firewall maintains
- a) Filtering Table
 - b) Record Table
 - c) ARP table
 - d) Routing Table.
5. SSL defines
- a) Secure Socket Layer
 - b) Security Selection Layer
 - c) Symmetric Secure Layer
 - d) Selection Socket Layer.

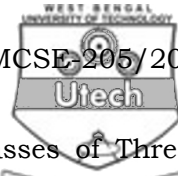
GROUP – B

(Long Answer Type Questions)

Answer any *four* of the following.

6. Explain RSA Algorithm. Explain Diffie-Hellman Key Exchange Algorithm. 7 + 8
7. What is Cryptography ? What is Encryption and Decryption technique ? What are different vulnerabilities in Network Security ? Explain the need of Network security.

2 + 3 + 6 + 4



8. What is Threat ? Explain Four Primary classes of Threats along with proper diagram. Explain Public Key Cryptography technique. 2 + (4 × 2) + 5
9. What is Firewall ? What are the two types of Firewall ? Explain Packet filter Firewall and Proxy Firewall with suitable diagram. What is VPN ? 2 + 1 + (5 + 5) + 2
10. What is DES ? Explain DES technique with P-Box and S-Box mechanism along with suitable diagram. What is Triple DES ? 2 + 10 + 3
11. Explain the term a) Integrity, b) Authentication, c) Non-Repudiation in Network Security. What is digital signature ? What is digital Certificate ? (3 × 3) + 3 + 3
12. What is Kerberos ? Explain SET (Secure Electronic Transaction). Describe AES. 2 + 6 + 7
13. Write short notes any *three* of the following : 3 × 5 = 15
 - a) Needham Schroeder Protocol
 - b) DoS Attack
 - c) Zero Knowledge Protocol
 - d) Hash Function
 - e) Biometric Authentication
 - f) Virtual private Network.
