205

20

B.Tech. (Computer Science & Engineering / Computer Technology / Computer Engineering)
Seventh Semester (C.B.C.S.)

Cryptography & Network Security

P. Pages : 2
Time : Three Hours

* 2 3 1 5 *

PSM/KW/23/2876/2887/2909
Max. Marks : 70

Notes :
1. All questions carry marks as indicated.
2. Solve Question 1 OR Questions No. 2.
3. Solve Question 3 OR Questions No. 4.
4. Solve Question 5 OR Questions No. 6.
5. Solve Question 7 OR Questions No. 8.
6. Solve Question 9 OR Questions No. 10.
7. Due credit will be given to neatness and adequate dimensions.
8. Assume suitable data whenever necessary.
9. Use of non programmable calculator is permitted.

1. a) What is cryptography? Explain Encryption and Decryption with the help of diagram. 7

b) Explain the model of Symmetric encryption. 7

OR

2. a) Distinguish between monoalphabetic and polyalphabetic ciphers. 7

b) Define the following cryptosystem terms: 7

a) Confidentiality

b) Authentication

c) Integrity

3. a) Explain Block Cipher Modes of Operation. 7

b) Explain Key Distribution Scenario in detail. 7

OR

4. a) Differentiate between Block & stream ciphers in detail. 7

b) Describe key generation of AES Algorithm. 7

5. a) In a public key cryptosystem using RSA. Cipher text C = 10 sent to user whose public key is e = 5, n = 35 what is the plaintext? Also write steps of RSA. 7

b) Explain Diffie Hellman key exchange algorithm. Clearly mention the weaknesses of this algorithm. 7

OR

6. a) Explain Elliptic Curve Cryptography. 7

b) Explain the digital signature requirements and direct digital signature in detail. 7

7. a) Explain Kerberos version 4 in detail. 7

b) What is Hash function? Explain MD-5 algorithm. 7

OR

8. a) Authentication Requirement. 7

b) Explain X-509 digital certificate (directory) format. 7

9. a) Draw SSL stack and explain Handshake protocol in brief. 7

b) Explain pretty good privacy in detail. 7

OR

10. Write a note on **any two.** **14**

1) Fire wall

2) Intrusion Detection

3) VPN

****