M.E. First Semester (Electronics & Tele.) (Full Time) (C.G.S. - New)

13338 : Elective-I : Cryptography & Network Security : 1 ENTC 5

AX - 3633

P. Pages : 2

Time : Three Hours

* 0 8 8 4 *

Max. Marks : 80

Notes : 1. Assume suitable data wherever necessary.
2. Illustrate your answer necessary with the help of neat sketches.
3. Use of pen Blue/Black ink/refill only for writing the answer book.

SECTION – A

1. a) Discuss the modes of operation of block ciphers. 6

b) Using Caser cipher with (P+4) mod 26 pattern decrypt the following code to plain text. 7
XALKOEPEAWJZDWLLU

OR

2. a) Explain Traffic confidentiality. 6

b) Explain the salient features of AES. 7

3. a) Explain, how elliptical curve architecture is important in key management. 6

b) Explain End to End encryption method. 8

OR

4. For prime numbers, p = 5 and q = 13 calculate using RSA. 14
a) η and ϕ
b) public key
c) private key

5. a) Discuss the properties of Hash algorithm. 6

b) Explain MD_5 algorithm. 7

OR

6. a) Explain HMAC algorithm. 6

b) Compare Hash function and message authentication. 7

SECTION – B

7. a) With neat block diagram, explain password authentication in real system. 6

b) Discuss kerberos in detail. 7

OR

8. a) What do you mean by pretty good privacy with reference to email. **6**

b) Explain how IP ensures the web security. **7**

9. a) Enlist the types of viruses which affect network security. **6**

b) Explain the issues related to firewall design principles. **7**

OR

10. a) List the features of Trusted system. **6**

b) How viruses can be eliminated, explain in detail. **7**

11. a) Describe header format used in network security. **6**

b) How malicious softwares can be encountered. **8**

OR

12. a) Enlist various web security considerations. **6**

b) Compare virus, intruders and malicious softwares. **8**

****