

B.E. Eighth Semester (Computer Technology) (C.B.S.)  
**Cyber & Information Security**

P. Pages : 2

KNT/KW/16/7597

Time : Three Hours

\* 0 2 9 8 \*

- 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. Solve Question 11 OR Questions No. 12.
  8. Due credit will be given to neatness and adequate dimensions.
- 

1. a) Explain the model of Network security with access security model. 7
- b) What are the aspects of Information Security? Explain various active and passive attacks. 7

OR

2. a) Encrypt the following text as follows IMINEIGHTSEM 9
- i) Using ceasor technique.
- ii) Using transposition cipher (2-state)
- Key → CLASS
- iii) Using playfair cipher, Key → EIGHT
- b) Write a note on need of information security in legal aspect. 5
3. a) Explain DES algorithm in detail. 8
- b) Explain centralized Key Distribution Scenario. 5

OR

4. a) What are block cipher modes of operation of DES ? Explain any two in detail. 6
- b) Explain IDEA algorithm in brief. 7
5. a) Differentiate conventional cryptography and public key cryptography. 6

b) Describe Diffie-Hellman Key Exchange algorithm with "Man in the middle attack". 8  
OR

6. a) Describe RSA algorithm. If RSA has following parameters then calculate plaintext. 10  
C = 10  
{e, n} = {5, 35}

b) Write a short note on Elliptic curve cryptography. 4

7. a) Explain in detail about X.509 directory authentication service. 8

b) Differentiate Authentication and Digital Signature. 5

OR

8. a) Describe MDS in detail. 7

b) What is message authentication ? And what are the requirements of message authentications. 6

9. a) What is firewall ? What are its type? Explain in brief. 7

b) What is intruder ? Explain intrusion detection techniques. 6

OR

10. a) Differentiate Host based versus N/W based IDS. 6

b) What is firewall ? Characteristics of firewall and also write its goals. 7

11. a) Explain chip-card transaction and attacks. 8

b) Write a note on electronic cash. 5

OR

12. a) Write a brief note on SET (Secure Electronic Transaction) 10

b) Write a short note on cross-site scripting. 3

\*\*\*\*\*



