

B.E. Eighth Semester (Computer Science & Engineering) (C.B.S.)

Information & Cyber Security

P. Pages : 2

Time : Three Hours

**KNT/KW/16/7609**

Max. Marks : 80

- 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.
 9. Assume suitable data whenever necessary.
 10. Diagrams should be given whenever necessary.
 11. Illustrate your answers whenever necessary with the help of neat sketches.
 12. Use of non programmable calculator is permitted.

1. a) Explain network security and access security model in brief. 8
- b) Explain security services in brief. 5

OR

2. a) Explain principles of security in detail. 8
- b) Explain any one transposition cipher. 5
3. a) What is AES? Explain the algorithm in detail. 9
- b) Describe key generation of AES algorithm. 5

OR

4. a) What is block cipher? Explain DES algorithm in detail. 10
- b) Differentiate between confusion & Diffusion terms in cryptography. 4
5. a) Describe Diffie-Hellman key exchange Algorithm with suitable example. What are the weakness of the Algorithm Explain. 8
- b) What do you mean by man in middle Attack? Explain using Diffie-Hellman. Algorithm. 5

OR

6. a) Encrypt "Hello World" using RSA Algorithm for the following data 8
 $p = 3; q = 11; e = 7; m = 5$
- b) Write note on ECC. 5

7. a) Explain MD5 message Digest Algorithm in detail. 7
b) Explain Hash Function. 7

OR

8. Explain Kerberos in detail. Also elaborate various steps of Kerberos version 4 in detail. 14
9. a) Explain IP Sec protocol in detail. Also write applications & advantages of IP Sec. 7
b) What are the services provided by SSL record protocol? 6

OR

10. a) What do you mean by "Trusted Systems", "Intrusion Detection System" & "Intrusion Prevention System". 9
b) Explain design principles of firewall. 4
11. a) What do you mean by E-mail security? Explain pretty Good privacy. 7
b) What do you mean by E-Transaction Attacks explain in detail. 6

OR

12. a) Explain "Payment over Internet-issues & concerns" & "Secure electronic Transaction". 7
b) What is software Vulnerabilities? Explain cross-site scripting in detail. 6
