Printed Pages – 3 Roll No. : .....

322755(22)

B. E. (Seventh Semester) Examination, Nov.-Dec. 2021

(New Scheme)

(CSE Engg. Branch)

CRYPTOGRAPHY & NETWORK SECURITY

Time Allowed : Three hours

Maximum Marks : 80

Minimum Pass Marks : 28

Note : *Attempt all questions. Part (a) is compulsory and carries 2 marks. Attempt any two parts from (b), (c) and (d) and carries 7 marks each.*

Unit-I

1. (a) Define cryptanalaysis.

(b) Explain briefly DES.

(c) Write a brief note on model for Network Security.

(d) Encrypt the message "She is listening" with the key "PASCAL" using vigenere Cipher.

Unit-II

2. (a) Define symmetric ciphers.

(b) Explain briefly one round of AES.

(c) Explain key distribution scheme in symmetric key encryption.

(d) Write a brief note on RC4.

Unit-III

3. (a) Define asymmetric Cipher.

(b) Write a brief note on HMAC.

(c) Write a brief note on MD5.

(d) Explain the working of digital signature.

Unit-IV

4. (a) Define Euler's theorem.

(b) Write a brief note on working of Diffie-Hellman key exchange algorithm.

(c) Explain RSA algorithm with an example.

(d) Explain ANSI×9.17 pseudorandom number generator.

Unit-V

5. (a) Define virus.

(b) Write a brief note on Kerberos authentication system.

(c) Write a brief note on :

(i) SSL/TLS

(ii) Firewalls

(d) Write a brief note on Secure Electronic Transaction.