

Printed Pages – 3

Roll No. :

322734(22)

**B. E. (Seventh Semester) Examination,
April-May 2021**

(New Scheme)

(CSE, IT Engg. Branch)

CRYPTOGRAPHY and NETWORK SECURITY

Time Allowed : Three hours

Maximum Marks : 80

Minimum Pass Marks : 28

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

1. (a) What is Rotor machine? 2
- (b) Explain play fair cipher with example. 7

[2]

- (c) Explain the classic techniques of cryptography. 7
- (d) What is DES? Also explained DES strength? 7
- 2. (a) What is modular arithmetic? 2
- (b) What is RC4? Explain it with a suitable example. 7
- (c) What is AES? How it is better than DES give reasons? 7
- (d) Explain groups, rings and fields. 7
- 3. (a) Explain Fermat's theorem. 2
- (b) How RSA works? Explain with example. 7
- (c) What is the concept of Diffie Hellmen Key Exchange? Explain. 7
- (d) What do you mean by Eliptic Curve Cryptography? 7
- 4. (a) What is Hash function? 2
- (b) What is the full form of SHA? Explain its security concept. 7
- (c) How Digital Signature work? Explain. 7
- (d) Explain CMAC. 7

[3]

- 5. (a) What do you mean by Web Security? 2
- (b) Explain Kerberos in detail. 7
- (c) What are SSL and TLS? Which one is best and why? 7
- (d) What is fire wall? Explain the types of fire wall. 7