No. of Printed Pages : 03 **Roll No. .....**

CC585

M.Tech. EXAMINATION, May 2019

(Third Semester)

(B. Scheme) (Re-appear)

(CSE)

CSE657B

CRYPTOGRAPHY AND NETWORK SECURITY

Time : 3 *Hours*] [*Maximum Marks :* 75

Before answering the question-paper candidates should ensure that they have been supplied to correct and complete question-paper. No complaint, in this regard, will be entertained after the examination.

Note : Attempt *Five* questions in all, selecting at least *one* question from each Unit. All questions carry equal marks.

Unit I

1. Write short notes on the following :

(a) Stream Cipher

(b) Block Cipher

(c) Confusion method in Cryptography.

2. Explain DES and its variants.

Unit II

3. Explain Elliptic Curve Cryptography.

4. Describe the following ciphers :

(a) Finite Fields of the Form GF(p)

(b) Chinese Remainder Theorem

(c) Modular Arithmetic.

Unit III

5. What is Message Digest ? Explain MD5 in detail.

6. Explain features of Digital Signature. Describe DSA.

Unit IV

7. Explain PGP and MIME.

8. Explain Firewall design principles.