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

CC-585

M. Tech. EXAMINATION, Dec. 2017

(Third Semester)

(Main & Re-appear)

(CSE)

CSE-657-B

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.

http://www.dcrustonline.com

Unit I

1. (a) What is a block cipher ? Explain the various modes of the operation of block cipher. **10**

   (b) Write a short note on triple DES. **5**

2. Explain the working of AES in detail. Also explain its evaluation criteria. **15**

Unit II

3. (a) Describe the RSA algorithm in detail. **8**

   (b) Write and explain the Diffie-Hellman key exchange algorithm. **7**

4. Discuss the concept of Elliptic curve cryptography in detail. **15**

Unit III

5. (a) What do you mean by authentication ? Write the MD5 algorithm in detail. **8**

   (b) What do you mean by digital signature standards ? Explain. **7**

6. Explain the concept of HMAC in detail. **15**

Unit IV

7. (a) Write the Firewall design principles. **7**

   (b) What is the concept of PGP ? Explain. **8**

8. Write short notes on the following : **15**

   (a) Kerberos

   (b) IP Security.

http://www.dcrustonline.com