Reg. No.										

MANIPAL INSTITUTE OF TECHNOLOGY
MANIPAL
A Constituent Institution of Manipal University

VI SEMESTER B.TECH. (COMPUTER SCIENCE & ENGINEERING) DEGREE
END SEMESTER EXAMINATION-APRIL/MAY 2017
SUBJECT: PRINCIPLES OF CRYPTOGRAPHY (CSE 4015)
REVISED CREDIT SYSTEM
(29/04/2017)

Time: 3 Hours MAX. MARKS: 50

Instructions to Candidates:

- Answer **ALL** the questions.
- Missing data may be suitably assumed.

1A. Explain the different types of security mechanisms. 3M

1B. It is required to encrypt the message "cryptographyLesson". Use the key as "MIGHTY". Design the Playfair cipher and give the encrypted message. Now pass this cipher text through a rail fence cipher of depth 3 for decryption. What is the output? State the assumptions made, if any. 5M

1C. Explain the following with regard to DES algorithm: 2M
i. Confusion ii. Diffusion
iii. Avalanche Effect iv. Timing Attack.

2A. What are the different operations that occur in the function F in a single round of DES algorithm? 3M

2B. What is double DES? Show that it is vulnerable to meet-in-the-middle attack. 3M

2C. Write the Miller-Rabin algorithm. Check whether 29 is a prime number or not by using Miller-Rabin algorithm. 4M

3A. Draw a neat diagram and explain all the stages of AES encryption. 5M

3B. Describe Linear Congruential Generator. Give a suitable example. Explain its drawback. How can it be strengthened? 5M

4A. Explain the different approaches for attacking RSA algorithm. 5M

4B. Differentiate between conventional encryption and public key encryption. Given q=19, α=10, X_A=5, k=6, and M=17 perform encryption and decryption using Elgamal cryptosystems. 5M

5A. Briefly explain any three different situations in which a message authentication code is used. 3M

5B. Draw a neat diagram and explain the working of SHA-512 algorithm. 5M

5C. What is direct digital signature? Explain. 2M

****