Reg. No.										

Manipal Institute of Technology, Manipal

(A Constituent Institute of Manipal University)

VI SEMESTER B.TECH (COMPUTER SCIENCE AND ENGINEERING)

MAKE UP EXAMINATIONS, JULY 2016

SUBJECT: CRYPTOGRAPHY AND NETWORK SECURITY [CSE 324]

REVISED CREDIT SYSTEM

Time: 3 Hours 04-07-2016 MAX. MARKS: 50

Instructions to Candidates:

- Answer **ANY FIVE FULL** questions.
- Missing data, if any, may be suitably assumed.

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

1B. Distinguish between specific security mechanisms and pervasive security mechanisms. 4M

1C. Explain the different types of transposition techniques. Give a suitable example for each to illustrate both encryption as well as decryption. 3M

2A. What is avalanche effect? Show that a known plaintext attack will succeed against double DES. 3M

2B. Draw neat diagrams and explain output feedback mode of block cipher encryption and decryption. What are its merits and demerits? 4M

2C. What is a computationally secure algorithm? Write the pseudo algorithm for AES key expansion. 3M

3A. Explain the following with reference to a random sequence of numbers:

i. Independence

ii. Scalability.

iii. Backward unpredictability (1+1+1)M

3B. Generate a sequence of random numbers using Linear Congruential Generator (LCG) in which a=1, c=1, X_0=1, m=31. Is this design generating a full period? What is the weakness of LCG? 3M

3C. Draw a neat diagram and explain pseudorandom number generation using triple DES. Explain the cryptographic strength of this method. 4M

4A. Find the following.

i. 5^{301} mod 11

ii. ø(256), dlog $_{3,19}$(3) (1+1)M

4B. Explain the different approaches that may be used to attack RSA algorithm. 5M

4C. Consider a Diffie-Hellman scheme with a common prime q=13, and a primitive root α=7.

i. If Alice has a public key Y_A=5, what is his private key X_A?

ii. If Bob has a public key Y_B=12, what is his private key X_B?

iii. What is the shared secret key? (1+1+1)M

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

5B. Along with necessary diagram explain efficient implementation of HMAC. 3M

5C. Explain the working of SSL record protocol. 2M

6A. What are the services provided by PGP protocol? 2M

6B. Write the top level format of an ESP packet and explain the various fields. 3M

6C. Explain the following:

i. Intruder behavior patterns.

ii. Limitations of Firewall. (3+2)M

****