Reg. No.										

MANIPAL INSTITUTE OF TECHNOLOGY
MANIPAL
(A constituent unit of MAHE, Manipal)

VI SEMESTER B.TECH. (CSE)
MAKEUP EXAMINATION-JUNE 2019
SUBJECT: PRINCIPLES OF CRYPTOGRAPHY [CSE 4015]
REVISED CREDIT SYSTEM
(18/06/2019)

Time: 3 Hours MAX. MARKS: 50

Instructions to Candidates:

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

1A. Explain the various security services. 3M

1B. What is cryptanalysis? Explain the different types of cryptanalytic attacks based on the amount of information known to a cryptanalyst. 3M

1C. Explain the working of transposition ciphers. Use an autokey system to decrypt the message "ZICVTWQNGKZEIIG" given the key as "deceptive". 4M

2A. Draw a neat diagram and explain the single round of DES algorithm. What are the security attacks possible on DES algorithm? 5M

2B. Draw neat diagrams and describe the counter mode of encryption and decryption of a block cipher. What is 3DES? 5M

3A. Find the following: 2M
i) $\varphi(512)$(Using Euler's Totient function)
ii) $7^{301} \bmod 11$(Using Fermat theorem)

3B. What are the applications of Fermat's little theorem? Find the multiplicative inverse of each nonzero element in Z_{11}? 3M

3C. Draw a neat diagram and explain AES encryption along with sub key generation. 5M

4A. Explain Linear Congruential Generator (LCG). Given a=1, c=1, X_0=1 and m=31, generate the sequence of random numbers using LCG. What is the drawback of LCG? How can it be overcome? 5M

4B.	Distinguish between conventional encryption and public key encryption. Draw a neat diagram and explain optimal asymmetric encryption padding. Why is it required?	5M
5A.	Explain the attacks possible on hash functions. Explain how a block cipher can be used as a hash function.	3M
5B.	Draw a neat diagram to illustrate message authentication and confidentiality in which authentication is tied to cipher text. Explain any two situations in which a message authentication code is used.	4M
5C.	What are the properties of a digital signature? Mention the different types of digital signature forgeries.	3M

****