Reg. No.										

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

VI SEMESTER B.TECH. (CSE)
END SEMESTER EXAMINATION-MAY 2019
SUBJECT: PRINCIPLES OF CRYPTOGRAPHY [CSE 4015]
REVISED CREDIT SYSTEM
(03/05/2019)

Time: 3 Hours MAX. MARKS: 50

Instructions to Candidates:

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

1A. Give the taxonomy of security attacks with relation to security goals and explain all the attacks. 4M

1B. What is a computationally secure encryption algorithm? Differentiate between Vigenere and Vernam ciphers. Give a suitable example for each. 3M

1C. Construct the Playfair matrix using the key “accepted” and encrypt the message “computer engineer”. State the assumptions made if any. Comment on the security strength of Playfair cipher. 3M

2A. Distinguish between confusion and diffusion. Draw neat diagrams and explain Fiestel cipher structure for encryption and decryption. 5M

2B. Explain Double DES. What is meet in the middle attack? Explain. Why do some block cipher modes of operation use only encryption while others use both encryption and decryption? 5M

3A. Define Euler’s Totient function. Prove that $\varphi(n)=(p-1)(q-1)$ where $n=pXq$, p and q are prime numbers with $p \neq q$. Find $\varphi(143)$. 3M

3B. Mention one application of Chinese Remainder Theorem. Use Chinese Remainder Theorem to find z, given $z=x+5$ and $x \equiv 1 \bmod 2$, $x \equiv 0 \bmod 3$, $x \equiv 4 \bmod 5$ 3M

3C. What is a state array in AES? Explain the construction of S-box and Inverse S-box in AES algorithm. 4M

4A. Draw neat diagrams and explain pseudo random number generation using block ciphers and triple DES. 5M

4B.	Draw a neat diagram and explain how a public key cryptosystem can be used to provide both authentication and secrecy. In a public key system using RSA, you intercepted the cipher text C=8 sent to a user whose public key is e=13, n=33, what is the plaintext M?	5M
5A.	Write the Diffie Hellman Key exchange algorithm. What is a birthday attack?	3M
5B.	Draw a neat diagram and explain internal error control. What is a MAC? Explain the various attacks that can be countered using a MAC.	4M
5C.	What is a direct digital signature? Mention the attacks possible on digital signatures.	3M

****