Reg. No.										

MANIPAL INSTITUTE OF TECHNOLOGY

MANIPAL

(A constituent unit of MAHE, Manipal)

SECOND SEMESTER M.TECH. (DEC/ME) DEGREE END SEMESTER EXAMINATION
JUNE 2019
SUBJECT: CRYPTOGRAPHY AND NETWORK SECURITY (ECE - 5237)

TIME: 3 HOURS **MAX. MARKS: 50**

Instructions to candidates

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

1A. The plaintext '**BEST**' has been enciphered as '**!DRG**' using an affine cipher on the digraphs of the 28-letter alphabet {**A , B , . . . , Z , _ , !**}. Determine the deciphering key and hence decipher the message '**!QXOFKFB**'.

1B. The ciphertext *"**GEZXDS**"* was enciphered by a monograph enciphering matrix using linear transformation. The plaintext is *"**SOLVED**"*. Find the encryption matrix and encrypt the message "FOUR"

(5+5)

2A. Describe the following operations in the AES.

i. Mix column ii. Shift rows

2B. Describe the Simple DES encryption algorithm with neat block diagram.

(5+5)

3A. Find the smallest positive integer which leaves a remainder of 1 when it is divided by 11, a remainder of 2 when divided by 12, and a remainder of 3 when divided by 13 using Chinese Remainder Theorem.

3B. In an RSA system, the public key is {7, 143}. Find the private key. Decrypt the ciphertext 48.

(5+5)

4A. What do you mean by message digest? Describe CMAC protocol with relevant block diagram.

4B. Define a virus and describe in detail.

(5+5)

5A. Describe an application layer firewalls with their advantages and disadvantages.

5B. Describe the possible attacks on digital signature.

(5+5)