Reg. No.										

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

SECOND SEMESTER M.TECH. (DEC & ME) DEGREE END SEMESTER EXAMINATION

APRIL/MAY 2019

SUBJECT: CRYPTOGRAPHY & NETWORK SECURITY (ECE - 5237)

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

Instructions to candidates

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

1A. Briefly explain the categories of security attacks.

1B. The intercepted message was enciphered by affine matrix cipher on digraph vectors of 26 letter alphabet. The alphabets A-Z have numerical equivalents 0-25. The most frequently occurring digraphs in the ciphertext are **'VM'**, **'QS'**, **'TH'**, which corresponds to plaintext digraphs **'TH'**, **'HE'** and **'IN'** in that order. Find the deciphering key and decrypt the message **"WDBTAF".**

(5+5)

2A. Find the ciphertext using S-DES encryption algorithm for the input plaintext and key 10100101 and 0010010111 respectively. Tabulate the results after IP, SW, output of 2nd round and IP^{-1}. Use the following permutation and substitution:

P10	3	5	2	7	4	10	1	9	8	6
IP	2	6	3	1	4	8	5	7		
E/P	4	1	2	3	2	3	4	1		

P8	6	3	7	4	8	5	10	9
P4	2	4	3	1				

$$s0 = \begin{bmatrix} 1 & 0 & 3 & 2 \\ 3 & 2 & 1 & 0 \\ 0 & 2 & 1 & 3 \\ 3 & 1 & 3 & 2 \end{bmatrix} \qquad s1 = \begin{bmatrix} 0 & 1 & 2 & 3 \\ 2 & 0 & 1 & 3 \\ 3 & 0 & 1 & 0 \\ 2 & 1 & 0 & 3 \end{bmatrix}$$

2B. In an RSA system, the public key is {17, 77}. Find the private key and decrypt the message "16, 3, 0, 72" and write the equivalent plain text. The alphabets A-Z have numerical equivalents from 0-25.

(5+5)

3A. What is the output of AES S-box if the input is 0xAB?

3B. Write the notation and equation for the elliptic curve if P=11, a=1 and b=6. Also find all points on the given elliptic curve.

(5+5)

4A. Discuss the Secure Hash Algorithm with relevant block diagram.

4B. What is meant by Transport mode and tunnel mode? How is authentication header implemented in these two modes?

(5+5)

5A. Discuss the techniques used for Statistical anomaly detection.

5B. Describe the following types of firewalls:
a. Packet Filtering Firewall b. Stateful Inspection Firewalls

(5+5)