Reg. No.										

MANIPAL INSTITUTE OF TECHNOLOGY
Manipal University

FIFTH SEMESTER B.TECH (E & C) DEGREE END SEMESTER EXAMINATION
NOV/DEC 2015
SUBJECT: CIPHER SYSTEM [ECE 331]

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

Instructions to candidates

- Answer **ANY FIVE** full questions.
- Missing data may be suitably assumed.

1A. The intercepted message was enciphered by affine matrix cipher on digraphs 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***".

1B. Find a least non-negative integer which leaves remainder of 12, 87 and 91 when divided by 31, 127 and 255 respectively.

1C. $\varphi(4200) =$……

(5+4+1)

2A. Using S-DES, encrypt the string (11011110) using the key (1101001011). Tabulate the results after each function (IP, F_k, SW, FK, IP^{-1}). Refer the permutation and substitution boxes given in the ***Table 2A.***

2B. The ***P(3, 10)*** is the one of the point on the elliptic curve $E_{23}(1, 1)$. Compute 5P.

2C. Prove that "Superencipherment using two affine transformations results in another affine transformation"

(5+4+1)

3A. In an RSA system, the public key is {59, 3233}. Find the private key. Encrypt the plaintext "***NONE***". The plaintext blocks are represented by diagraphs and ciphertext are by trigraphs. The alphabets A-Z have numerical equivalents 0-25.

3B. Describe the RC5 encryption algorithm in detail.

3C. If the index of coincidence is 0.0477 and n = 250, what is the length of the key?

(5+4+1)

4A. The intercepted message {2496, 8099} was encrypted by Hellman-Merkel algorithm with the public key {2106, 880, 1320, 974, 2388, 1617, 1568, 2523, 48, 897}. Given that A - Z corresponds to $(00000)_2$ – $(11001)_2$ respectively, If the private key is {a, m} = {1053, 2719}, decrypt the message.

4B. For the group **G=<Z_7*, X>**, find the followings:
Order of the group, order of each element in the group, number of primitive roots in the group, and primitive roots in the group.

4C. Solution to the congrences is $x^2 \equiv 12 \ mod \ 13$ is ……..

(5+4+1)

5A. Describe the key expansion algorithm in AES with block diagram.

5B. Find the multiplicative inverse of 0x55 mod 0x11B.

5C. Product of 0x25 and 0x21 mod 0x11B =……

(5+4+1)

6A. It is known that the received ciphertext C = 23 was encrypted using Rabin cryptosystem with n = 517. Determine the plaintext.

6B. Describe the CMAC message authentication code in detail with necessary block diagram.

6C. 21^{-1} mod 57=……

(5+4+1)

Table 2A

Key generation	**P10**	3	5	2	7	4	10	1	9	8	6
Encryption function:	**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				

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