Reg. No.										

MANIPAL INSTITUTE OF TECHNOLOGY
Manipal University

SIXTH SEMESTER B.Tech. (E & C) DEGREE END SEMESTER EXAMINATION - April/May 2017

SUBJECT: CIPHER SYSTEMS (ECE – 4019)

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

Instructions to candidates

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

1A.	The intercepted ciphertext message "**OVZGVRCOBPRQEPUM**" was enciphered using a linear transformation on digraphs. It is known that a=253 and N=26. If "A-Z" corresponds to 0 – 25, decrypt the message.
1B.	Using Chinese Reaminder Theorem solve the following system of congruence: X=6 mod 11 X=13 mod 16 X=9 mod 21
1C.	Decrypt the following message which was enciphered by using Vigenere cryptography with the key "**GALILIO**" . The message is {"**GDZXEBVKPLKPWTTAECCM**"}
	(5+3+2)
2A.	Using S-DES, encrypt the string (**01110011**) using the key (**0111001101**). Show intermediate results after each function (IP, Fk, SW, F_K, IP^{-1}). Use the data given in Fig. Q2A.
2B.	Find (x, y) for the following simultaneous equations. 480 x + 971 y = 416 mod 1111 297 x + 398 y = 319 mod 1111
2C.	Write short note on Output Feedback mode of DES.
	(5+3+2)
3A.	Suppose that the plaintext "frid" is encrypted using a 2x2 Hill cipher to yield the ciphertext "**PQCF**". The alphabets A-Z corresponds to 0 – 25. Find the key matrix and decrypt the message "**CQLWMGOKTZOF**".
3B.	Explain AES key generation with neat diagrams.
3C.	Multiply the polynomial 0x6C and 0x3F in GF(2^8) using the modulo polynomial 0x11B using shift left and XOR method
	(5+3+2)
4A.	With a neat block diagram explain the Blowfish algorithm.
4B.	Find the inverse of 0x55 using the irreducible polynomial 0x11B.
4C.	Explain the Diffie-Hellman key exchange algorithm
	(5+3+2)
5A.	In RSA, given n=12091 and e=13. Encrypt the message "THIS" using the 00 to 25 encoding scheme. Here plaintext are digraph and ciphertext are trigraph

5B.	Explain the CMAC algorithm.
5C.	Find all QR's and QNR's in Z_7*.
	(5+3+2)

Key generation	**P10**	3	5	2	7	4	10	1	9	8	6
	P8	6	3	7	4	8	5	10	9		
Encryption	**IP**	2	6	3	1	4	8	5	7		
	E/P	4	1	2	3	2	3	4	1		
	P4	2	4	3	1						

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

Figure Q3A

$$S_0 = \begin{bmatrix} 1 & 0 & 3 & 2 \\ 3 & 2 & 1 & 0 \\ 0 & 2 & 1 & 3 \\ 3 & 1 & 3 & 2 \end{bmatrix} \qquad S_1 = \begin{bmatrix} 0 & 1 & 2 & 3 \\ 2 & 0 & 1 & 3 \\ 3 & 0 & 1 & 0 \\ 2 & 1 & 0 & 3 \end{bmatrix}$$