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. You receive a message "**YMI?YW.C** " which was enciphered using an affine transformation on digraphs. It is known that a =347, b =412 and N = 29. If A-Z → 0 -25, Space (ϕ)→ 26, '**.**' → 27, '?' → 28, decrypt the message.

1B. Find the smallest positive integer which leaves a remainder of 12 when divided by 31, a remainder of 87 when divided by 127 and a remainder of 91 when divided by 255.

1C. The relative frequencies of alphabets in a cryptogram from A to Z are as follows: 16, 05, 12, 10, 18, 09, 06, 04, 06, 03, 04, 05, 12, 14, 10, 09, 14, 20, 04, 09, 15, 02, 02, 03, 06 and 05. Calculate the index of coincidence and length of key

(5+3+2)

2A. You intercept the message "**ZRIXXYVBMNPO**" which you know result from a linear enciphering transformation of digraph-vectors in a 27-letter alphabet, in which A-Z have numerical equivalents 0-25, and blank(ϕ)=26. You have found that the most frequently occurring ciphertext digraphs are "**PK**" and "**RZ**.' You guess that they correspond to the most frequently occurring plaintext digraphs in the 27-letter alphabet, namely, "**E**ϕ " (E followed by blank) and "**S**ϕ " (S followed by blank). Find the deciphering matrix, and read the message.

2B. Evaluate 357^{31} mod 2349 using repeated squaring method.

2C. Add two points P and Q on the elliptic curve defined by $E_{13}(1,1)$ given P=(4, 2) and Q=(10, 6).

(5+3+2)

3A. Using S-DES, encrypt the string (**11011110**) using the key (**1101001011**). Show intermediate results after each function (IP, Fk, SW, F_K, IP^{-1}). Use the data given in Figure Q3A.

3B. Explain the key generation algorithm in AES.

3C. Write short note on cipher feedback mode of DES.

(5+3+2)

4A. In an affine block cipher system with s = 3, the 2, 3, 4 and 6's transformations are 0, 7, 5 and 4 respectively. Determine the key A and t, also determine the rest of the transformations.

4B. Explain RC5 encryption with the help of neat diagrams.

4C. For the group **G=<Z_8*, x>**, find: a. Order of group b. Order of each element

(5+3+2)

5A. In Merkle - Hellman Public crypto system, the public key is {1628, 1571, 1737, 1058, 1779, 1142, 2631, 990} you receive a message {6147, 3689, 5317, 7609}. Your private key is {m = 2753, a = 337}. If $(41)_h \rightarrow (5A)_h$ corresponds to A → Z and each message block is a monograph, decrypt the message.

5B. Describe the steps involved in HMAC algorithm with a neat sketch.

5C. In RSA crypto system if the public key is {71, 9991} Find the private key.

(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						

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

Figure Q3A