Reg. No.										

MANIPAL INSTITUTE OF TECHNOLOGY

MANIPAL

(A constituent unit of MAHE, Manipal)

SIXTH SEMESTER B.Tech. (E & C) DEGREE END SEMESTER EXAMINATION
APRIL 2018
SUBJECT: CIPHER SYSTEMS (ECE - 4019)

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

Instructions to candidates

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

1A. Determine a smallest nonnegative solution for a system of congruence's using Chinese Remainder Theorem. $5x \equiv 14 \bmod 17$; and *and* $3x \equiv 2 \bmod 13$

1B. Explain the key generation in DES.

1C. Determine the index of coincidence and length of the key if the relative frequencies for certain ciphertext corresponding to alphabets A to Z are {**6,0,1,4,3,8,3,9,7,2,4,9,2,3,1,3,4,4,8,2,3,5,5,7,2,0**}.

(5+3+2)

2A. Decrypt the intercepted message "RBW?XA" received by Bob that was encrypted using affine transformation on digraphs. Bob detects the enciphering key used is a=347, b=523. Alphabet is { **A=0, B=1, …Z, .(dot), ☺(blankspace, ?=28**}.

2B. Explain Whirlpool algorithm.

2C. Decrypt the ciphertext "**DOKWFMPGS**" using Vigenere cipher with key **LEMON**.

(5+3+2)

3A. Encrypt the plaintext 10100101 using the S-DES with key (0010010111). Use the given permutation and substitution table.

P4	2	4	3	1						
P8	6	3	7	4	8	5	10	9		
P10	3	5	2	7	4	10	1	9	8	6
IP	2	6	3	1	4	8	5	7		
EP	4	1	2	3	2	3	4	1		

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

3B. Construct GF(2^4) using $p(x) = x^4 + x + 1$. Find one primitive and non-primitive field elements. List the order of those elements.

3C. Find the number of affine transformation keys if n=60.

(5+3+2)

4A. Using AES key expansion algorithm compute the output of Mix column transformation for the input [D4, BF, 5D, 30]

4B. Merkle Hellman Knapsack cryptosystem uses the public key sequence is {57, 14, 3, 24, 8} and the private key is $b = 23$, $n = 61$. Find the superincreasing sequence.

4C. Determine two points and its image on the elliptic curve defined by $E_{11}(1,6)$

(5+3+2)

5A. Alice chooses private key $d_A = 67$. Find Alice's public key computed using El-Gamal algorithm & keys ($p_A = 107$, $\alpha_A = 2$). Bob chooses random integer $k = 45$ to encrypt plaintext "**B** (**ASCII code 66**)" and sends to Alice. Find the ciphertext received by Alice and decrypt it.

5B. Draw the block diagram of HMAC. Explain the computation of n-bit HMAC.

5C. Compute $99^{82} \bmod 991$ using repeated squaring method.

(5+3+2)