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.
- Use AES and DES tables (chart).

1A. Determine a smallest nonnegative solution for a system of congruence's using Chinese Remainder Theorem. $10x \equiv 511 \bmod 841$; and *and* $19x \equiv 103 \bmod 900$

1B. Construct GF(2^3) using $p(x) = x^3 + x + 1$. Find one primitive and one non primitive field element

1C. Compute gcd(4107, 731)

(5+3+2)

2A. The 64 bit plaintext (0123456789ABCDEF) is encrypted using DES. The subkey for round 1 obtained is (0 B 0 2 6 7 9 B 4 9 A 5). Determine the output of round 1 of DES.

2B. Decrypt the ciphertext is "IHEINEQK" that was encrypted using Linear cipher with encryption key 15 in a 26 letter alphabet numbered 0 to 25 for A to Z respectively.

2C. The relative frequencies for certain ciphertext corresponding to alphabets A to Z are {1, 1, 6, 8, 3, 4, 9, 3, 7, 2, 2, 4, 9, 3, 1, 3, 3, 8, 4, 4, 1, 2, 5, 5, 7, 2}. Specify the type of cipher used and compute the length of the key.

(5+3+2)

3A. The input state array to a mix column transformation block of AES is given below. Find the first two words of the output state array.

87	F2	4D	97
6E	4C	90	EC
46	E7	4A	C3
A6	8C	D8	95

3B. Show the computation of the entry in AES subbyte table corresponding to 0x95.

3C. Alice and Bob get public numbers (23,9). Compute shared public keys. Show that secret keys used by both Alice and Bob to encrypt and decrypt are same.

(5+3+2)

4A. Alice and Bob use RSA system for communication. Alice encrypts the **plaintext** as **digraph** using public key of Bob (97, 2077). Bob decrypts **ciphertext** as **trigraph**. The alphabets are A to Z numbered from 0 to 25 respectively. Bob receives "BFTCIW". Find the plain text received by Bob from Alice.

4B. Decrypt the ciphertext “SLHZY” that was encrypted using HILL cipher with key “CBDE”

4C. Compute $99^{435} \bmod 991$ using repeated squaring method

(5+3+2)

5A. Determine points $(x_1, y_1) = (4, \_\_)$ and $(x_2, y_2) = (5, \_\_)$ on the elliptic curve $E_{19}(4,-3)$. Find 2Q and 3Q points on the curve for point Q(5,3)

5B. Explain the overall processing of a message to produce a digest using Whirlpool secure hash function

5C. Explain CBC, and CFC modes of operations. Highlight advantages and limitations of each.

(5+3+2)