Reg. No.										

MANIPAL INSTITUTE OF TECHNOLOGY

MANIPAL

(A constituent unit of MAHE, Manipal)

SIXTH SEMESTER B.TECH. (E & C) DEGREE END SEMESTER EXAMINATION
APRIL/MAY 2019
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. $10x \equiv 396 \bmod 841$; and *and* $19x \equiv 844 \bmod 900$

1B. i. Construct GF(2^3) using $p(x) = x^3 + x + 1$.

ii. Solve for x & y: $\alpha^4 x + \alpha^3 y = \alpha^5$; $\alpha^2 x + \alpha^5 y = 1 + \alpha^2$

iii. Implement a circuit to compute multiplication of any element with α^2 over GF(2^3). (5+5)

2A. Decrypt the text "GTDVSS" that was ciphered using Hill cipher key $A = \begin{bmatrix} 2 & 1 \\ 3 & 4 \end{bmatrix}$. Use A-Z corresponding to numbers 0-25.

2B. Decrypt the intercepted message "FQK FTV?AE " that was encrypted using affine cipher with keys (a=347, b=523) on digraphs. A 29 letter alphabet numbered as {numerical values from 0 to 25 corresponds to A to Z respectively, **.** = 26, blank space = 27, **?** = 28}. (5+5)

3A. Compute the AES first word of 9th round sub key given 8th round sub key as 0x(EE61ACDE EAFE1F4B 2F62A6E6 D8E39D92)

3B. Encrypt the message (11011110) using S–DES given key: (1101001011). (5+5)

4A. Decrypt the intercepted message {8601, 710, 0, 7023} using - Merkle Hellman knapsack cryptosystem wit public key {868, 4656, 710, 2367, 867} and private key is (947, 5761). Use A-Z corresponds to 0 to 25.

4B. (i) Encrypt 94 using Rabin cryptosystem with prime numbers as 23 & 7. Also decrypt the ciphered number.

(ii) Alice and Bob get public numbers (n, g) is (23, 9). Private key of Alice is 5 and that of Bob is 3. Compute shared public keys. Show that secret keys used by both Alice and Bob to encrypt and decrypt are same. (4+6)

5A. Determine the point $P(x_1, y_1) = (\alpha^2, \_)$ and its inverse on the elliptic curve $E\ (\alpha^3, 1)$ over $GF\ (2^3); g(x) = x^3 + x + 1$ as primitive polynomial. Find 2P on the curve.

5B. List the process in computation of message digest using Whirlpool cipher. Compare whirlpool cipher computations with that of AES. (5+5)