Reg. No.										

MANIPAL INSTITUTE OF TECHNOLOGY

MANIPAL

(A constituent unit of MAHE, Manipal)

SIXTH SEMESTER B.TECH. (E & C) DEGREE END SEMESTER EXAMINATION
JUNE 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. i. Construct GF(2^3) using $p(x) = x^3 + x^2 + 1$.

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

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

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

ii. Compute $99^{435} \bmod 991$

(5+5)

2A. Determine the output(O/P) of S-P Network shown in **Figure 2A** for the input (I/P) 111 001 110.

2B. Decipher the intercepted message "?QXOFKFB" if the plain text "BEST" have been enciphered as "?DRG" using affine cipher on digraphs of 28 letter alphabet numbered as {0 to 25 for A to Z respectively, blank space=26, ?=27}.

(5+5)

3A. Determine the AES SubByte transformation of 0x73. Show step by step computation & Verify using SubByte Transformation table.

3B Encrypt the message (11010110) using S-DES given key: (1111001010).

(5+5)

4A. Determine private key for RSA cryptosystem with public key {e, n} as {17, 77} respectively. Decrypt the message {16, 3, 0, 72}. The numbers 0 - 25 corresponds to A - Z respectively.

4B Decrypt 77 using Rabin cryptosystem with n=3569(prime factors as 43 & 83). Also decrypt the ciphered number.

(5+5)

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

5B. Define Message integrity, Message Authentication and Hash function. Explain each of them along with their properties.

(5+5)

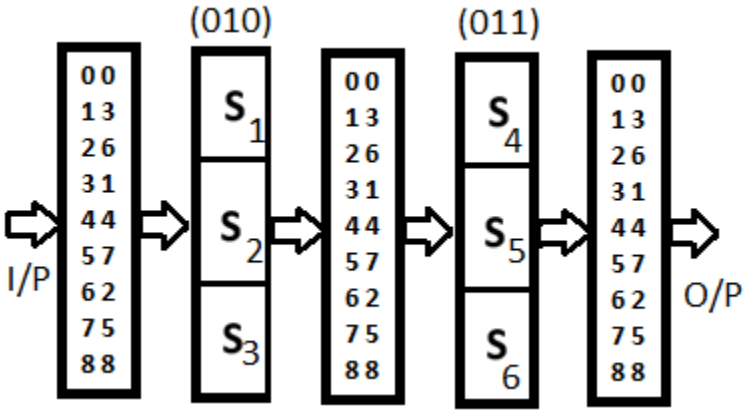

Figure 2A