Reg. No.										

MANIPAL INSTITUTE OF TECHNOLOGY
Manipal University

FIFTH SEMESTER B.TECH (E & C) DEGREE END SEMESTER EXAMINATION - NOV/DEC 2016
SUBJECT: CIPHER SYSTEM (ECE - 331)

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

Instructions to candidates

- Answer **ANY FIVE** full questions.
- Missing data may be suitably assumed.

1A. The public key used in a RSA public cryptosystem is (97, 2077), in which alphabets A→Z corresponds to 0 →25. Decrypt the ciphertext message **“BFTCIW”**. The plaintext message blocks are digraph and ciphertext blocks are trigraph.

1B. Solve the system of congruences : $5x \equiv 14 \; mod \; 17$ and $3x \equiv 2 \; mod \; 13$.

1C. Express GCD of 841 and 160 as a linear combination of two integers.

(5+3+2)

2A. The intercepted ciphertext message “**RBW?XAΦCXYCO**” was enciphered using an affine transformation on digraphs. It is known that a =347, b =523 and N = 29. If “**A-Z**” corresponds to 0 - 25, **.** = 26, **Φ** = 27, **?** = 28, decrypt the message.

2B. The relative frequencies for certain cipher text 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 and 0, corresponding to A-Z respectively. Calculate the period of the key.

2C. The ciphertext **DRZNUO** was produced by using a Vigenere cipher with keyword **BABY**. What is the plaintext?

(5+3+2)

3A. With neat diagram explain the RC5 encryption algorithm.

3B. If the input to the S-box is 0x6D, what is the output of S-box in AES encryption algorithm?

3C. Determine Φ(3528) = ………………

(5+3+2)

4A. The intercepted message {2496, 8099} was encrypted by Hellmen-Merkel algorithm with the public key {2106, 880, 1320, 974, 2388, 1617, 1568, 2523, 48, 897}. Given that A - Z corresponds to $(00000)_2$ – $(11001)_2$ respectively, If the private key is {a, m} = {1053, 2719}, decrypt the message.

4B. Describe the Subkey generation DES algorithm with neat block diagram.

4C. Find the number of genuine keys for an affine transformation of monographs with N = 40.

(5+3+2)

5A. With a neat block diagram explain the Blowfish encryption algorithm.

5B. Multiply the polynomials 0x57 and 0x13 with irreducible polynomial 0x11B.

5C. Find the first four points (excluding images) on the elliptic curve $E_{19}(4, -3)$.

(5+3+2)

6A. For the group G = < Z_7*, X >, find the followings:
Order of the group, order of each element in the group, number of primitive roots in the group, and primitive roots in the group.

6B. Describe the CMAC message authentication code in detail with necessary block diagram.

6C. Prove that “Superencipherment using two affine transformations results in another affine transformation”

(5+3+2)