Reg. No.										

MANIPAL INSTITUTE OF TECHNOLOGY
Manipal University

FIFTH SEMESTER B.TECH (E & C) DEGREE END SEMESTER EXAMINATION
NOV/DEC 2015
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 intercepted coded message **"*VMZCUU*"** was encrypted using an affine transformation on diagraphs in the 31 letter alphabet, in which A-Z have numerical equivalents 0-25, **Φ (blank)** = 26, **?**=27, **!**=28, **#** =29 and **'**=30. A frequency analysis shows that the most common digraphs in earlier ciphertext are **"*UΦ*"** and **"*IH*"** in that order. Suppose that in the English language the most frequently occurring digraphs in 31-letter alphabet are **"*SΦ*"** and **"*ΦI*"** in that order. Find the deciphering key and decrypt the message.

1B. Solve the following congruence equations:

$$25x + 13y \equiv 29 \ mod\ 53$$
$$15x + 17y \equiv 15 \ mod\ 53$$

1C. $160^{-1} \bmod 851 =$ ……

(5+4+1)

2A. If the input is 111001110, find the output of the block cipher system shown in **Figure 2A**. The permutation and substitutions are as follows:
0→0, 1→3, 2→6, 3→1, 4→4, 5→7, 6→2, 7→5, 8→8 and

$$s_i(x) = \begin{cases} \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \end{pmatrix} x + \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} & if\ K_i = 0 \\ \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} x & if\ K_i = 1 \end{cases}$$

2B. Describe the key expansion algorithm in DES with block diagram.

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

(5+4+1)

3A. The ciphertext *"**GEZXDS**"* was enciphered by a monograph enciphering key using linear transformation. The plaintext is *"**SOLVED**"*. Find the encryption matrix and encrypt the message "***FOUR***"

3B. Describe the RC5 encryption algorithm with diagram.

3C. Find the number of primitive roots in **G = <Z_{23} *, ×>.**

(5+4+1)

4A. The received message "***AMX***" was enciphered using RSA public key cryptosystem with public key {13, 2747}. The length of the ciphertext is 3 and that of plaintext is 2. If 0-25 corresponds to A-Z, decrypt the message.

4B. If the input to the S-box is 0x79, what is the output of S-box in AES?

4C. The number of genuine keys in an affine transformation with *N=31* is ……

(5+4+1)

5A. In Merkle-Hellman public key crypto system the public key is {3655, 1010, 1289, 664, 2059, 3387, 474, 3141, 3397, 1465}. The received message was {2508, 2321, 567}. The private key is m=4107, a = 731. If $(00000)_2$ to $(11001)_2$ corresponds to A-Z and message block is digraph, decrypt the message.

5B. Multiply $(x^6 + x^5 + x^4 + x^2 + 1)$ by $(x^7 + x^4 + x^2 + x)$ in GF(2^8) with irreducible polynomial $(x^8 + x^4 + x^3 + 1)$ using left shift and Ex-OR algorithm.

5C. Number of rounds in AES-192 algorithm is ……..

(5+4+1)

6A. Determine the equation and find all the points on the elliptic curve $E_{11}(2, 1)$.

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

6C. …….. mode of operation is used to achieve minimum propagation error.

(5+4+1)

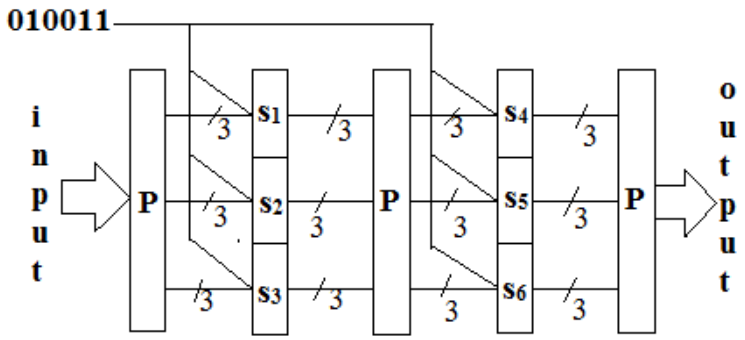

Figure 2A