MANIPAL ACADEMY of HIGHER EDUCATION
(Deemed to be University under Section 3 of the UGC Act, 1956)

Reg. No.										

DEPARTMENT OF SCIENCES, IV SEMESTER M.Sc,. (Applied Mathematics) END SEMESTER EXAMINATIONS, APRIL/MAY 2019

CRYPTOGRAPHY [MAT5007]

(REVISED CREDIT SYSTEM-2017)

Time: 3 Hours Date: 26 April 2019 MAX. MARKS: 50

Note: (i) Answer **ALL** questions

(ii) Draw diagrams and write equations wherever necessary and assume the standard notations.

1A. If $n \geq 1$ prove that $\varphi(n) = \sum_{d|n} \mu(d) \frac{n}{d}$.

1B. For a given modulus m, prove that the residue classes $[1], [2], \ldots, [m]$ are disjoint and their union is the set of all integers.

1C. Using the affine cipher $C \equiv 3P + 7 \ (mod\ 26)$, encipher the message

"THERE IS NO ROYAL ROAD TO GEOMETRY"

(3+3+4)

2A. Let n be a positive integer the prove that

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & if \quad n = 1 \\ 0 & otherwise \end{cases}.$$

Also give an example.

2B. Using the keyword 'MATH' and a Vigenere cipher, encrypt the message

"MATHEMATICS IS THE DOOR AND THE KEY TO THE SCIENCES"

2C. The largest integer the scientific calculator CASIO fx330A can handle is the eight digit number 99,999,999. Compute the exact value of 2^{31} Chinese remainder theorem. **(3+3+4)**

3A. If $(a, m) = d$ then prove that the linear congruence $ax \equiv b(mod\ m)$ has solution if and only if $d|b$.

3B. State and prove Mobius inversion formula.

3C. Using the matrix $A = \begin{bmatrix} 1 & 25 & 25 \\ 25 & 1 & 24 \\ 2 & 9 & 5 \end{bmatrix}$ encipher the plaintext

"THE PEN IS MIGHTIER THAN THE SWORD". (3+3+4)

4A. If $c_k = \frac{p_k}{q_k}$ be the k^{th} convergent of the simple continued fraction $[a_0; a_1, a_2, \dots, a_n\ ]$ where $1 \leq k \leq n$ then prove that

$$p_k q_{k-1} - q_k p_{k-1} = (-1)^{k-1}.$$

4B. Decrypt the ciphertext message 0592 2131 2584 2188 that was created using the RSA enciphering key $(e, n) = (17, 2867)$.

4C. State and prove Gauss lemma. **(3+3+4)**

5A. Solve $76x + 176y = 276$.

5B. Prove that there are infinitely many prime numbrs.

5C. Decipher the knapsack ciphertext message 54 47 47 57 97 81 97 57 50 31 created with modulus 65 multiplier 12 and the enciphering sequence is 7, 31, 50 and 47. **(3+3+4)**

*****