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

DEPARTMENT OF SCIENCES,
Manipal Academy of Higher Education

IV Semester M. Sc., Online Examination June 2021

Applied Mathematics and Computing

Elective II: Cryptography - MAT-5007

Time: 10:00 AM -12:00 NOON **Date:12-06-2021** **MAX. MARKS: 40**

INSTRUCTION: ANSWER ANY **FOUR FULL** QUESTIONS.

1A. Solve $1776x + 1976y = 4152$.

1B. Prove that there are infinitely many prime numbers.

1C. Define Möbius function and write the values of it up to $n = 6$.

(4+4+2)

2A. If $a \equiv b(mod\ m)$ the prove that $f(a) \equiv f(b)(mod\ m)$ for every polynomial f with integer coefficients.

2B. For $n \geq 1$, prove that $\varphi(n) = n\prod_{p/n}\left(1 - \frac{1}{p}\right)$. Where the product is taken over all distinct prime divisors of n. Give an example.

2C. If p be a prime and a be any integer such that $p \nmid a$, then prove that the least residue of the integers $a, 2a, \ldots., (p-1)a$ modulo p are the permutation of the integers $1, 2, \ldots, (p-1)$. **(4+4+2)**

3A. Using the affine cipher $C \equiv 7P + 10\ (mod\ 26)$ encipher the message

ALL THAT GLITTERS IS NOT GOLD

3B. Using the deciphering key $\begin{pmatrix} 7 & 18 & 19 \\ 15 & 1 & 19 \\ 17 & 17 & 0 \end{pmatrix}$, decipher the cipher text

ZTH QLJ MOA NLG GPN EXA OCA QTY

3C. State Wilson's theorem and give an example. **(4+4+2)**

4A. Prove that distinct Fermat numbers are coprimes.

4B. If $(a, m) = 1$, then the linear congruence $ax \equiv b \ (mod\ m)$ has exactly one solution.

4C. Encrypt the message

ALL IS WELL THAT ENDS WELL

using the keyword COVID for a Vigenere cipher. **(4+4+2)**

5A. Solve the linear system

$x \equiv 3 \ (mod\ 5), x \equiv 5 \ (mod\ 7), x \equiv 8 \ (mod\ 12)$ by using Chinese remainder theorem.

5B. Using exponentiation modulus $p = 2333$ and $e = 13$ decipher the ciphertext

1560 1250 0522 0631 1505

5C. Solve the Knapsack problem with superincresing weights

$4x_1 + 5x_2 + 11x_3 + 23x_4 + 45x_5 = 60.$ **(4+4+2)**

6A. Using RSA enciphering modulus $n = 2773$ and the enciphering key $e = 21$ encrypt the message PRIDE AND PREJUDICE.

6B. Cryptanalyze the ciphertext created by the affine cipher:

IRCCH EKKEV CLLFK EIOKL

XKKLF ILIGM EKOIV EKKE **(5+5)**

*****