Roll No. | | | | | | | | | | | | | **Total No. of Pages : 02**

Total No. of Questions : 07

M.Sc. (Mathematics) (2018 Batch) (Sem.-3)

NUMBER THEORY AND CRYPTOGRAPHY

Subject Code : MSM-302-18

M.Code : 76673

Date of Examination : 14-12-22

Time : 3 Hrs. **Max. Marks : 70**

INSTRUCTIONS TO CANDIDATES :

1. **SECTION-A is COMPULSORY consisting of FIVE questions carrying TWO marks each.**
2. **SECTION - B & C. have THREE questions each.**
3. **Attempt any FOUR questions from SECTION B & C carrying FIFTEEN marks each.**
4. **Select atleast TWO questions from SECTION - B & C each.**

SECTION-A

1. Write short notes on :

   a) Define Euler function $\phi(n)$ and divisor function $d(n)$.

   b) Prove that $\sum_{d|n} \mu(d) = 0, \forall n > 1$.

   c) Determine whether N = 12365327 is divisible by 13 using special divisibility test.

   d) Check whether 2 is a primitive root modulo 7 or not.

   e) State the need of a Cryptosystem.

SECTION-B

2. a) State and prove Eulers Theorem.

   b) If p and q are primes, where, $q = 2p + 1$, then prove that either $q \mid M_p$ *or* $q \mid M_p + 2$, but not both. Here M_p is Mersene prime.

3. a) Find the least positive solution of the following system of congruences:

$x \equiv 2 \pmod 3$

$x \equiv 3 \pmod 5$

$x \equiv 2 \pmod 7$

b) Show that the Binomial coefficient ${}^{n}C_{r}$ is an integer if $1 \leq r \leq n$ with the help of greatest integer function.

4. a) Prove that $gcd\ (a, b, c) = ((a, b), c) = (a, (b, c))$.

b) Prove that any prime divisor p of the Fermat's number F_n, where $n \geq 2$ is of the form $k.\ 2^{n+2} + 1$.

SECTION-C

5. a) What is public key cryptography. What are the various cryptosystems used for public key cryptography. Write some of the advantages and disadvantages of public key cryptography.

b) State and Prove Gauss Lemma.

6. A Book store is using RSA encryption to receive secret messages from all the online customers. They have published their public decoding exponent $d = 7$ and their public modulus $M = pq = 39$. Find their secret encoding exponent e.

7. a) What is cryptography? What are the needs of cryptosystems? How RSA Croptosystem helps to safeguard the data from piracy/hacking?

b) Represent the integer 459 as sum of four squares.

NOTE : Disclosure of Identity by writing Mobile No. or Making of passing request on any page of Answer Sheet will lead to UMC against the Student.