No. of Printed Pages : 03 **Roll No. .....**

II344

M. Sc. (5 Year Integrated) EXAMINATION, 2020

(Ninth Semester)

(B. Scheme) (Re-appear)

MATHEMATICS

MAT617H

Analytical Number Theory and Cryptography

B.Sc. (Hons.) M.Sc. Mathematics

Time : 3 *Hours*] [*Maximum Marks :* 75

Before answering the question-paper candidates should ensure that they have been supplied to correct and complete question-paper. No complaint, in this regard, will be entertained after the examination.

Note : Attempt *Five* questions in all, selecting at least *one* question from each Unit. All questions carry equal marks.

Unit I

1. (a) Prove that the primes of the form $4k+1$ are infinite.

(b) Define Format and Mersenne numbers and prove that the format number F_5 is divisible by 641.

2. (a) Prove that π is irrational.

(b) Prove that the constant $\sqrt{5}$ appearing Hurwitz Theorem is the best possible.

Unit II

3. (a) Prove that all the integral solutions of $x^2 + y^2 = z^2$, $x > 0$, $y > 0$, $z > 0$, $(x, y) = 1$, $2 / x$ are given by $x = 2ab$, $y = a^2 - b^2$, $z = a^2 + b^2$, where $a > b > 0$, $(a, b) = 1$ and a and b are of opposite parity.

(b) Define linear diophantine equation and find all solutions in positive integers of $5x + 3y = 52$.

4. (a) State and prove Lagrange's four square theorem.

(b) Define G(k) and prove that G(2) = 4.

Unit III

5. (a) Let p be an odd prime. Then prove that :

(i) $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$

(ii) $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$

(iii) If $(a, p) = 1$, then $\left(\frac{a^2 b}{p}\right) = \left(\frac{b}{p}\right)$

(iv) $\left(-\frac{1}{p}\right) = (-1)^{(p-1)/2}$.

(b) Define the group U_n and prove that if p is an odd prime, then U_{p^2} is cyclic.

6. (a) Prove that the group U_2e is not cyclic for $e \geq 3$ and $U_2 e = \left\{\pm 3^i \mid 0 \leq i < 2^{e-2}\right\}$ where $e \geq 3$.

(b) Prove that the set of quadratic residues modulo a prime forms a group under multiplication.

Unit IV

7. (a) What do you mean by monoalphabetic cipher and polyalphabetic cipher ? Explain by taking one example in each case.

(b) Explain RSA cryptosystem by taking a suitable example.

8. (a) The ciphertext message produced by the knapsack cryptosystem employing the super increasing sequence 1, 3, 5, 11, 35, modulus $m = 73$ and multiplier $a = 5$ is 55, 15, 124, 109, 25, 34. Obtain the plaintext message.

(b) Explain the ElGamal cryptosystem by taking an example.