Unit IV

7. (a) Define the following terms using suitable examples :

(i) Enciphering

(ii) Deciphering

(iii) Monoalphabetic cipher

(iv) Polyalphabetic cipher. **8**

(b) Encipher the message HAPPY DAYS ARE HERE using the autokey cipher with seed Q. **7**

8. Explain ElGamal cryptosystem in detail. The message REPLY TODAY is to be encrypted in the ElGamal cryptosystem and forwarded to a user with public key (47, 5, 10) and private key K = 19. If the random integer chosen for encryption is j = 3, determine the ciphertext. Indicate how the ciphertext can be decrypted using the recipient's private key.

II-344

M. Sc. EXAMINATION, May 2017

(Ninth Semester)

(5 Years Integrated)

(Main & Re-appear)

ANALYTICAL NUMBER THEORY AND CRYPTOGRAPHY

MAT-617-H

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.

Unit I

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

(b) Prove that $\gcd(F_m, F_n) = 1$, where $m > n \geq 0$ and F_m, F_n are format numbers.

(c) If p and $q = 2p + 1$ are primes, then prove that q/M_p or $q/M_p + 2$, but not both.

2. (a) If $\frac{a}{b}$ and $\frac{c}{d}$ are consecutive fractions in a Farey sequence, then prove that among all rational fractions, with value between these two $\frac{a+c}{b+d}$ is the unique fraction with smallest denomination.

(b) State and prove Hurwitz theorem.

Unit II

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

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

4. (a) State and prove Lagrange's Four Square theorem.

(b) Find the least positive integer x such that $x \equiv 5 \pmod 7$, $x \equiv 7 \pmod{11}$ and $x \equiv 3 \pmod{13}$.

Unit III

5. (a) Define Legendre symbol. State and prove Gauss lemma on Legendre symbols.

(b) If P and Q are odd and positive and if (P, Q) = 1, then prove that :

$$\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = (-1)^{\{(P-1)/2\}\{(Q-1)/2\}}$$

6. (a) Prove that the group U_2e is cyclic if and only if $e = 1$ or $e = 2$.

(b) Define Primitive Root. If p is an odd prime and g is a primitive root modulo p. Then prove that either g or $g + p$ is a primitive root modulo p^2.