PG Even Semester Examination, May 2025

MATHEMATICS

4th Semester

Course No. : MAT - 653 (C)

(Cryptography)

Full Marks : 70

Pass Marks : 28

Time : 3 hours

The figures in the margin indicate full marks for the questions

(Answer one question from each unit)

Unit - I

1. (a) Let n be a positive integer written in base b. Show that the number of digits in n is given by $\left[\frac{ln\, n}{ln\, b}\right] + 1$ 3

(b) Divide $(HAPPY)_{26}$ by $(SAD)_{26}$ 6

(c) Find an upper bound for the number of bit operations required to compute n!. 5

2. (a) Divide $(40122)_7$ by $(126)_7$ and multiply $(YES)_{26}$ by $(NO)_{26}$. 4+3=7

(b) Estimate the time required to convert a K-bit integer to its representation in base 10. Is your algorithm a polynomial time Algorithm? Justify. 7

(Turn Over)

Unit - II

3. (a) State and prove Chinese remainder theorem. 5

(b) Show that $\sum_{d/n} \varphi(d) = n$ 4

(c) For every prime p and every $n \in \mathbb{N}$, show that there exists a field with p^n elements. 5

4. (a) Show that any finite subgroup of the multiplicative group of a field is cyclic. 6

(b) Find all monic irreducible polynomials of degree 2 and degree 3 over $\mathbb{Z}_2$. 5

(c) Construct a field with 16 elements. 3

Unit - III

5. (a) Suppose you intercept the aphertext "OFJDFOHFXOL", which was enciphered using an affine transformation of single-letter plain text units in the 27-letter alphabet (with blank=26), You know that the first word is " I " (I followed by blank). Determine the enciphering key and hence read the message. 6

(b) Find the inverse of the matrix $A := \begin{pmatrix} 2 & 3 \\ 7 & 8 \end{pmatrix}$ *over* $\mathbb{Z}/_{26\,\mathbb{Z}}$. Use it to solve the congruence.

$$2x + 3y \equiv 1 \text{ med } 26$$
$$7x + 8y \equiv 2 \text{ med } 26$$

Working in the 26-letter alphabet, use the matrix A above to encepher the message "NO".

2+3+2=8

6. (a) Use the matrix $A := \begin{pmatrix} 2 & 3 \\ 7 & 8 \end{pmatrix} \in M_2\left(\mathbb{Z}/_{26\,\mathbb{Z}}\right)$ is deceptor the uphertext "FWMDIQ" in the the 26-letter alphabet. 6

(b) Explain the RSA crypto system. 8

Unit - IV

7. (a) Explain the ElGamal cryptosystem based on descrete logarithm problem. 7

(b) Prove that a square free odd composite integer n is a carmichael number iff p-1 | n-1 for every prime p dividing n. 7

8. (a) Let n be an odd composite integer which is divisible by a perfect square greater than 1. Show that n can't be a carmichael number. 7

(b) Describe Miller-Rabin premality test. 7

Unit - V

9. (a) Describe the group structure on the set of points of an elliptic curves over the real numbers. Can this group law be extended over any field? 8

(b) Discuss briefly the elliptic curve crypto system. 6

10. (a) Let n be a positive integer. Let k be the set given by an equation $y^2 = x^3 + ax + b$ modulo n. Let m be any integer. Supose that there is a prime q dividing m which is greater than $\left(n^{1/4} + 1\right)^2$. If there exist a point p of E such that (i) mp = 0 and (ii) (m/q) p is defined and non-zero, then n must be prime. 8

(b) Factorise 540143 by using pollards 'p-1' method. 6

★★★