Registration No.: | | | | | | | | | | |

Total Number of Pages: 02 **Course: M.Sc.I**

Sub_Code: FMCE1002

10th Semester Regular Examination: 2024-25

SUBJECT: Cryptography

BRANCH(S): M.Sc.I(MC)

Time: 3 Hours

Max Marks: 70

Q.Code: S102

Answer Question No.1 (Part-I) which is compulsory, any five from rest (Part-II)

The figures in the right hand margin indicate marks.

Part-I

Q1 **Answer the following questions :** **(2 x 10)**

a) Distinguish between passive and active security attacks.

b) Differentiate between symmetric and asymmetric cryptosystems with an example of each.

c) Explain the working of the Affine Cipher with an example.

d) What is cryptanalysis? Name two common cryptanalysis techniques.

e) State the mathematical foundation of the RSA cryptosystem.

f) What is the significance of the Diffie-Hellman key exchange in modern cryptography?

g) Why is the ElGamal encryption scheme considered probabilistic?

h) What is a birthday attack in the context of hash functions?

i) Define the Discrete Logarithm Problem (DLP) and its significance in cryptography.

j) Name two digital signature schemes based on public-key cryptography.

Part-II

Long Answer Type Questions (Answer Any five)

Q2 **a)** Describe the encryption and decryption procedure in vigenere cipher. Show the encryption and decryption of the message “”Meet me after the class” using the key “Teacher”. **(5)**

b) Alice often needs to encipher plaintext made of both letters (a to z) and digits (0 to 9). Consider the upper case and lowercase alphabets are same. **(1+2+2)**

i) If she uses an additive cipher, what is the key domain? What is the modulus?

ii) If she uses a multiplication cipher, what is the key domain? What is the modulus?

iii) If she uses an affine cipher, what is the key domain? What is the modulus?

Q3 **a)** Use a Hill cipher to encipher the message “we live in an insecure world”. Use the key $K = \begin{bmatrix} 03 & 02 \\ 05 & 07 \end{bmatrix}$. **(5)**

b) Explain the concept of multiple encryption in block ciphers. How does Triple-DES improve security over DES? **(5)**

Q4	**a)**	Explain the RSA algorithm with an example. Discuss its security assumptions.	**(5)**
	b)	Describe the working of the Diffie-Hellman key exchange protocol. What is the man-in-the-middle vulnerability?	**(5)**
Q5	**a)**	Perform encryption and decryption using the ElGamal cryptosystem with suitable parameters.	**(5)**
	b)	Discuss the efficiency of the Quadratic Sieve algorithm in factoring large integers.	**(5)**
Q6	**a)**	Explain the Pollard's ρ-Algorithm for solving the Discrete Logarithm Problem.	**(5)**
	b)	Discuss the construction of hash functions from block ciphers. Provide an example.	**(5)**
Q7	**a)**	Compare RSA signatures and ElGamal signatures in terms of security and efficiency.	**(5)**
	b)	Explain the concept of blind signatures and their applications in e-voting.	**(5)**
Q8	**a)**	Describe the Index Calculus Algorithm for solving DLP in multiplicative groups.	**(5)**
	b)	What are secure cryptosystems? Discuss Kerckhoffs's principle in this context.	**(5)**