No. of Printed Pages : 4 **MMTE–006**

MASTER IN MATHEMATICS WITH APPLICATIONS IN COMPUTER SCIENCE [M. SC. (MACS)]

Term-End Examination

December, 2023

MMTE-006 : CRYPTOGRAPHY

Time : 2 Hours *Maximum Marks : 50*

Note : *(i) Answer any **four** questions from question nos. **1** to **5**.*

*(ii) Question **No. 6** is compulsory.*

1. (a) Let $\mathbf{F}_{2^4} = \mathbf{F}_2 \dfrac{[x]}{\left\langle x^4 + x + 1 \right\rangle}$. Then $r = x + \left\langle x^4 + x + 1 \right\rangle$ is a primitive element of $\mathbf{F}_{2^4}$. Write all the elements of $\mathbf{F}_{2^4}$ as polynomials in r. Also write the vector representation of the elements. 5

(b) List all the various modes of operation of block ciphers. Why is ECB mode weak for encryption ? 3

(c) What is the difference between true random numbers and Pseudo random numbers ? 2

2. (a) Let G be group $\mathbf{Z}_n^*$. For which of the following values of n is G cyclic ? 5

17, 20, 38, 50

Find the number of primitive roots of $\mathbf{Z}_{17}^*$.

(b) List *five* tests for testing randomness of sequences. Describe the frequency test and the serial test. 5

3. (a) Encrypt the text ATTACK POSTPONED UNTIL TWO AM XYZ twice by applying the transposition cipher with the permutation : 5

1	2	3	4	5	6	7
2	5	1	3	6	7	4

(b) Let $n = 77$ be the modulus for a RSA cryptosystem. Check whether 10 is a proper exponent for encryption. Find the decryption exponent if the encryption exponent is 7. 5

4. (a) Alice and Bob decide to use Elgamal cryptosystem. Bob chooses p = 31, g = 3 and 29 as the public key and keeps x = 9 as secret key. Alice wants to send the message M = 7 to Bob. She chooses k = 5 as the secret parameter. What is the cipher text ? Explain how Bob will decrypt the cypher text. 5

(b) What is birthday paradox ? Explain how this is used to attack hash functions. 5

5. (a) Alice wants to use the digital signature standard (DSS) algorithm for signing messages. She chooses p = 23, q = 11, g = 5 and the secret value a = 3 and publishes the value $(p, q, \alpha, \beta) = (23, 11, 2, 8)$. She wants to sign the message M = 10. For signing she chooses the value k = 5. Find the digital signature. How will Bob check the signature ? 5

(b) Given the initial sequence 10101100, find the recurrence that generates it. 5

6. Which of the following statements are true and which are false ? Justify your answers : 10

(a) $7^{1228} \equiv 1 \pmod{1229}$

(b) $\mathbf{Z}_{15}^{*}$ is a cyclic group

(c) Digital signature algorithms provide confidentiality

(d) Any block can be used as a stream cipher

(e) A hash function h is collision resistant, if given M and h(M) it is difficult to find M' such that $h(M) = h(M')$.