

No. of Printed Pages : 6

MMTE-006

**M. Sc. (MATHEMATICS WITH
COMPUTER SCIENCE)**

[M. SC. (MACS)]

Term-End Examination

June, 2025

MMTE-006 : CRYPTOGRAPHY

Time : 2 Hours

Maximum Marks : 50

- Note :** (i) *There are six questions in this paper.*
(ii) *The **sixth** question is compulsory.*
(iii) *Do any **four** questions from question nos. 1 to 5.*
(iv) *Use of calculator is not allowed.*
(v) *Show all the relevant steps. Do the rough work at the bottom or at the side of the page only.*
-
-

1. (a) Define a primitive element of a finite field. Check whether $\bar{2}$ is a primitive root for $\mathbf{Z}_7$. 2
- (b) Explain the properties of collision resistance and second pre-image resistance of a hash function. 2
- (c) Factorise 357 using Fermat factorisation method. 2
- (d) Explain the computational Diffie-Hellman problem. 2
- (e) Define a pseudoprime to a base b . Check that 15 is a pseudoprime to the base 4. 2
2. (a) Let $f(x) = x^4 + x + 1 \in \mathbf{F}_2[x]$. We represent the field $\mathbf{F}_{2^4}$ by $\mathbf{F}_2[x]/(f(x))$.

Let us write $\gamma = x + (f(x))$. The table of values is given below :

i	γ^i	Vector
0	1	(0, 0, 0, 1)
1	γ	(0, 0, 1, 0)
2	γ^2	(0, 1, 0, 0)
3	γ^3	(1, 0, 0, 0)
4	$\gamma + 1$	(0, 0, 1, 1)
5	$\gamma^2 + \gamma$	(0, 1, 1, 0)
6	$\gamma^3 + \gamma^2$	(1, 1, 0, 0)
7	$\gamma^3 + \gamma + 1$	(1, 0, 1, 1)
8	$\gamma^2 + 1$	(0, 1, 0, 1)
9	$\gamma^3 + \gamma$	(1, 0, 1, 0)
10	$\gamma^2 + \gamma + 1$	(0, 1, 1, 1)
11	$\gamma^3 + \gamma^2 + \gamma$	(1, 1, 1, 0)
12	$\gamma^3 + \gamma^2 + \gamma + 1$	(1, 1, 1, 1)
13	$\gamma^3 + \gamma^2 + 1$	(1, 1, 0, 1)
14	$\gamma^3 + 1$	(1, 0, 0, 1)

- (i) Prepare the logarithm tables 4
- (ii) Compute $\frac{(\gamma^2 + 1) + (\gamma^3 + \gamma + 1)}{(1 + \gamma^2)(\gamma + \gamma^2)}$ using the logarithm and anti-logarithm tables. 3
- (b) Describe the Linear Congruential Generator for generating random numbers. How will you construct a random number sequence of length 20 ? 3
3. (a) Explain the encryption process when you use the Cipher Feedback mode. 3
- (b) Decrypt each of the following cipher text
 “MHHBXMBOHGBBWJSGSZIBOIHN”
 which was encrypted with an affine cipher with key (9, 12). 3
- (c) Let $f(x) = x^3 + x^2 + x + 1 \in \mathbf{Z}_5[x]$ and $g(x) = x^4 + 3x^2 + 2 \in \mathbf{Z}_5[x]$. Using the extended Euclidean algorithm, find $Q(x), R(x) \in \mathbf{Z}_5[x]$ such that $P(x) f(x) + Q(x) g(x) = h(x)$, where $h(x)$ is the g.c.d. of $f(x)$ and $g(x)$. 4

4. (a) Check whether the sequence 1010001110010010011011110 passes the frequency test and the serial test with $\alpha = 0.05$. You may use the values $\chi^2_{0.05,2} = 5.99146$, $\chi^2_{0.05,1} = 3.84146$. 5
- (b) Solve the equation $5^x \equiv 18 \pmod{43}$ using Baby-step, Giant-step algorithm. 5
5. (a) Suppose Bob wants to receive messages using ElGamal public cryptosystem. He chooses a prime $p = 23$, a primitive root $g = 5$ and chooses $x = 5$. 6
- (i) What information will Bob make public and what will he keep as a secret ?
- (ii) If Alice wants to send the message $M = 21$ and chooses $k = 3$, what will she send to Bob ?
- (iii) How will Bob decrypt the message ?

- (b) Use the Toy block cipher to encrypt the text 110000110101 once using the key 101001011. Show all the steps. 4

6. Which of the following statements are true and which are false ? Justify your answer with a short proof or a counter-example as appropriate : 10

- (a) $35^{36} \equiv 1 \pmod{37}$.
- (b) S-box in a block cipher is used for diffusion.
- (c) Vigenère cipher is a transposition cipher.
- (d) The powers of 2 modulo p is strictly increasing for any prime p .
- (e) In an RSA system, finding the factors of n is equivalent to finding $\phi(n)$.

× × × × ×