No. of Printed Pages : 6

MMTE–006

M. SC. (MATHEMATICS WITH APPLICATION IN COMPUTER SCIENCE)

[M. SC. (MACS)]

Term-End Examination

June, 2026

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.

---

1. (a) Define an irreducible polynomial. Check whether $x^3 + x + 1$ is irreducible over $\mathbf{F}_2$. 3

   (b) Define a primitive polynomial. Also, define the order of a primitive polynomial. 2

   (c) Alice is using the RSA cryptosystem with $n = 60$, $e = 19$. If M = 11 is the plaintext, find the ciphertext. Check your encryption by decrypting the ciphertext using the secret key $d = 19$. 5

2. (a) Define order of $a \in \mathbb{Z}_n^*$. Find the order of $\overline{3}$ in $\mathbb{Z}_x$. 2

   (b) Find $5^{31} \pmod{71}$ using the repeated square algorithm. 4

(c) Given the initial sequence 110010111001, find the recurrence that generates this sequence. 4

3. (a) Define the terms cryptography and cryptanalysis. 2

(b) Name functions or primitives used in symmetric key cryptography to introduce 'confusion and diffusion'. 2

(c) Define a cryptographic hash function. State any *three* essential properties of a cryptographic hash function. 4

(d) Given that $n = 391$ and $\phi(n) = 352$, factorise n. 2

4. (a) Sonu wants to use the digital signature algorithm. She chooses $p = 23$, $q = 11$, $g = 2$ and $a = 3$.

(i) What information does Sonu need to make public ?

(ii) She chooses the secret value $k = 5$. Calculate the digital signature of the message M = 13, showing all the steps used in the process. 5

(b) Explain the Runs test for random sequences. Apply the test for the following sequence :

10111	00001	10111	01001	01101	10110	10100	10101
00110	01001	10001	10011	11101	10111	11110	10110
11010	11000	10011	11001	10001	11000	10100	10010
11010	10100	10110	10111	10110	11011	01001	11010

You may like to use the following values : $\chi^2_{0.05,3} \equiv 7.8147$, $\chi^2_{0.05,4} = 9.48773$, $\chi^2_{0.05,5} = 11.0705$. 5

5. (a) Draw the LFSR circuit for the recurrence relation $\chi_{n+4} = \chi_n + \chi_{n+3} \pmod{\alpha}$. Generate ten terms of the sequence with (1, 1, 0, 1) as the initial sequence. 3

   (b) Bob and Alice use Diffie-Hellman key exchange with $p = 23$, $\alpha = 5$ as the primitive root. Bob chooses $x = 3$ and Alice chooses $y = 5$. What will be the common key shared by Bob and Alice at the end of key exchange ? 3

   (c) State any *four* types of cryptanalysis attack scenario. 4

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

   (a) AES and DES are stream ciphers. 2

   (b) $(\mathbb{Z}_{16}, +, .)$ is a field. 2

(c) RSA scheme can only be used for confidentiality of data. 2

(d) Symmetric key cryptosystem uses two different types of keys for encryption and decryption, respectively. 2

(e) Caesar's cipher is a transposition cipher. 2

× × × × ×