No. of Printed Pages : 3 **MMTE-006**

M. SC. (MATHEMATICS WITH COMPUTER SCIENCE)
[M. SC. (MACS)]
Term-End Examination
December, 2022

MMTE-006 : CRYPTOGRAPHY

Time : 2 Hours *Maximum Marks : 50*

Note : (*i*) *Question No.* ***6*** *is compulsory.*

(*ii*) *Answer any* ***four*** *questions from Question Nos.* ***1*** *to* ***5.***

---

1. (a) Define the characteristic of a field. What is the characteristic of $\mathbf{F}_{27}$? 2

   (b) Define the Euler ϕ-function. Find $\phi(72)$. 2

   (c) Describe 'known-plaintext attack'. How is it different from chosen-plaintext attack ? 3

   (d) What is the length of the key in DES ? How long is the actual key ? What are the extra bits used for ? 3

2. (a) Define a pseudo-random bit generator. When do we say that a pseudo-random bit generator passes all polynomial time statistical tests ? 3

(b) Define a cryptographic hash function, stating its properties. 3

(c) What is the discrete logarithm of a non-zero element in a finite field with respect a primitive element ? Taking 2 as the primitive element, find the discrete logarithm of 5 with respecto to 2. 2

(d) How does use of OAEP strengthen the RSA cryptosystem ? 2

3. (a) Factorise $x^2 - 9$ into irreducible factors in $\mathbf{F}_{11}[x]$. 5

(b) Explain the RC4 algorithm with pseudocode. 5

4. (a) Suppose Bob sets up the parameters for the Elhamal cryptosystem as follows :

He chooses the prime $p = 29$ and primitive root 2. He chooses $x = 7$ and publishes the values (29, 2, 12). He receives the message (12, 15) from Alice. Decrypt the message. 5

(b) Let $f(x) = x^4 + x^3 + x^2 + 1 \in \mathbf{F}_2[x]$ and $g(x) = x^3 + 1 \in \mathbf{F}_2[x]$. Find $\text{g.c.d.}(f, g)$ using the extended Euclidean algorithm and express the g.c.d. in the form $u(x)f(x) + v(x)g(x)$. 5

5. (a) Use Fermat factorization method to factorise 71273. 5

(b) Use the simple columnar transposition cipher with column width 4 to encrypt the text 'ATTACK FROM THE PAVILION END'. 2

(c) Explain the Davis-Meyer method for constructing a one-way compression function from a block cipher. 3

6. Which of the following statements are true and which are false ? Justify your answer with a short proof or a counter example : 5×2=10

(a) $35^6 \equiv 1 \pmod{37}$.

(b) $\mathbf{F}_{11}^{*}$ is a cyclic group.

(c) Vigenere cipher is a transposition cipher.

(d) The powers 2 modulo p are strictly increasing for any p.

(e) In an RSA system with modulus n, finding the factors of n is equivalent to finding $\phi(n)$.