

No. of Printed Pages : 6

MMTE-006

**M. Sc. (MATHEMATICS WITH
APPLICATIONS IN COMPUTER
SCIENCE) M. Sc. (MACS)**

Term-End Examination

December, 2021

MMTE-006 : CRYPTOGRAPHY

Time : 2 Hours

Maximum Marks : 50

*Note : Answer any **four** questions out of
Question Nos. 1 to 5. Question No. 6 is
compulsory.*

1. (i) Define the characteristic of a finite field.
What is the characteristic of the field \mathbf{F}_{27} ?
Justify your answer. 2

(ii) What is a Monte-Carlo algorithm ? How is
it different from a Las Vegas algorithm ? 2

(iii) Explain the Kirchhoff's law. 2

(iv) Explain the terms confusion and diffusion
in the context of cryptography. 2

(v) Define a strong prime. 2

2. (a) Explain the need for digital signature. 3

(b) State the Coloumb postulates for a pseudo-
random sequence of bits. 3

(c) Compute $2^{21} \bmod 37$ using the square and
multiply algorithm. 4

3. (a) Find the inverse of 01001100 represented
as an element of : 6

$$\mathbf{F}_2[x] / \langle x^8 + x^4 + x^3 + x + 1 \rangle$$

P. T. O.

[3]

MMTE-006

- (b) Set up an RSA cryptosystem for $p = 11, q = 13$ by choosing your own encryption and decryption other than $e = 1, d = 1$. Encrypt the message $M = 8$ using your system. 4
4. (a) Complete the padding block for the input message : 4
"Ashoka statement admits lapses."
(Consider 'space' is also a character) to SHA-256.
- (b) Compute the decryption function for the following affine encryption function defined over \mathbf{Z}_{400} : 4
$$\bar{y} = 33\bar{x} + 122 \pmod{400}$$
- (c) To exchange keys under Diffie-Heuman scheme Bob and Alice use the prime 17 and

[4]

MMTE-006

- 3 as the primitive root 3. If Alice chooses the secret value 2 and Bob chooses the secret value 2, what is the final key ? 2
5. (a) Apply the runs test to the sequence for testing randomness : 6
1001101000010000101111011
0111010010110110010011010
0110011100001100100111000
1100001101010111101001110
0010001111000001101010010
1000110100000110100101101
1110001001
- You may find the following values useful :
- $$\chi_{0.05,3}^2 = 7.81473,$$
- $$\chi_{0.05,4}^2 = 9.48773$$
- $$\chi_{0.05,5}^2 = 11.0705$$

P. T. O.

[5]

MMTE-006

- (b) Alice wants to use Elgamal digital signature scheme with public parameters $p = 47, \alpha = 2$ and secret values $\alpha = 7$ and $\beta = 34$. She wants to sign the message $M = 20$ and send it to Bob. She chooses $k = 5$ as the secret value. Explain the procedure that Alice will use for computing the signature. What information will she send Bob ?

4

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

10

- (i) There is a finite field with 10 elements.
- (ii) A Hash function is second pre-image resistant if it is computationally infeasible to find inputs μ_1 and $\mu_2, \mu_1 \neq \mu_2$ with $h(\mu_1) = h(\mu_2)$.

[6]

MMTE-006

- (iii) The RSA system is secure for all choices of modulus of encryption.
- (iv) The actual key length of DES is 56.
- (v) No symmetric key cryptosystem can be used without secure key exchange.

MMTE-006

P. T. O.