No. of Printed Pages : 4 **MMTE–006**

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

## Term-End Examination

## June, 2024

### MMTE-006 : CRYPTOGRAPHY

*Time : 2 Hours* *Maximum Marks : 50*

---

***Note :*** *(i) There are six questions in this paper. Do any **four** from Q. No. **1** to Q. No. **5**.*

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

*(iii) Use of calculator is not allowed.*

---

1. (a) Find a generator for the finite field :

$$\frac{\mathbf{F}_2[x]}{\left\langle x^3 + x + 1 \right\rangle}$$

Also, write all the elements of the finite fields in polynomial representation. 4

(b) Explain the Diffie-Hellman key exchange protocol. 3

(c) Explain how the keyed cryptographic hash function is better than the normal hash function. 3

2. (a) Define a pseudoprime to a base $b, b \in \mathbf{N}$. Show that, if $n$ is a pseudoprime to the bases $b_1$ and $b_2$, then $n$ is also a pseudoprime to the base $b_1 b_2$ and $b_1 b_2^{-1}$, where $b_2^{-1}$ is the inverse of $b_2$ modulo $n$. 4

(b) Solve the equation :

$$14^x \equiv 22 \pmod{97}$$

using baby step-giant step algorithm. 6

3. (a) Explain the main goals of cryptography. 4

(b) Check whether the following sequence passes poker test : 6

1001 1101 1101 1011 0011 1101

0111 0100 0010 1100 0010 0101

you may like to use the following values :

$\chi^2_{0.05,1} = 3.84146$, $\chi^2_{0.05,3} = 7.81473$.

4. (a) Representing :

$$\mathbf{F}_{2^8} = \frac{\mathbf{F}_2[x]}{< g(x) >},$$

where $g(x) = x^8 + x^4 + x^3 + x + 1,$ find inverse of the byte 10001100 in $\mathbf{F}_{2^8}$. 4

(b) For a RSA cryptosystem with parameter $n = 899$, encryption key $e = 11$ and $\phi(n) = 840$, find the decryption exponent $d$. Encrypt the message $\mu = 10$. Also, factorise $n$. 6

5. (a) Explain the difference between AKS algorithm and the Rabin Miller algorithm. 2

(b) Describe the Caesar cipher and Affine cipher. How are these two ciphers related ? 3

(c) Describe the key scheduling of RC4 and its pseudo random generation algorithm. Give *two* examples where RC4 encryption is being used. 5

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

(i) Hash functions provide confidentiality.

(ii) If $n = 391$ for an RSA cryptosystem $e = 11$ is a valid encryption exponent.

(iii) Vigenere cipher is a monoalphabetic cipher.

(iv) In digital signature schemes, the hash of the message is signed using the sender's public key.

(v) The digital signature standard algorithm uses two $p$ and $q$ such gcd $(p - 1, q) = 1$.