No. of Printed Pages : 4 **MMTE-006**

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

Term-End Examination

June, 2023

MMTE-006 : CRYPTOGRAPHY

Time : 2 Hours *Maximum Marks : 50*

Note : *(i) Answer any* ***four*** *questions from question nos.* ***1*** *to* ***5****.*

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

1. (a) Define a primitive element in a finite field $\mathbf{F}_q$. Give a primitive in $\mathbf{F}_7$ with justification. 2

(b) Let n and b be natural numbers such that $(n_i b) = 1$. When do we say that n is a pseudoprime of the base b ? Check whether 91 is a pseudoprime to the base 3. 2

(c) Decrypt the following clipher text which was encrypted using Vigenere Cipher with the key word “SECRET”, KYTXIMGQQIVHO. 3

(d) Explain the Cipher Block chaining and Cipher Feedback modes of operations of block cipher. 3

2. (a) Explain the Blum-Blum-Shub pseduo-random bit generator. Calculate the first five terms generated by Blum-Blum-Shub pseudo-random generator if $p = 11$, $q = 19$ and $x_0 = 7$. 3

(b) Explain the Miyaguchi-Prencel method for creating hash function with a diagram. 3

(c) Suppose Alice and Bob want to exchange a secret key using Diffie-Hellman key exchange algorithm. They choose the prime 31 with primitive root 3. Bob chooses the secret value 5 and Alice chooses 7. Find the common secret key explaining all the steps. 2

(d) Let $n = 21$, $e = 5$ is a RSA cryptosystem. If the plain text is 10, find the cipher text. 2

3. (a) Determine the number of keys in an Affine cipher over $\mathbf{Z}_m$ where $m = 1225$. 3

(b) Given the initial sequence 110010111001, find the recurrence relation that generates it. 5

(c) Check whether $x^3 + 4x^2 + 4$ is irreducible over $\mathbf{Z}_5$. 2

4. (a) Given the values $a = 161$ and $b = 28$, find $\gcd(a, b)$ by using the Extended Euclidean algorithm and also find s and t such that $sa + tb = \gcd(a, b)$. 5

(b) Suppose Alice wants to sign messages using Elhamal signature scheme and she chooses $p = 29$ and 3 as the primitive root. She chooses the secret parameter $a = 9$. She makes public the values (29, 3, 21). If she wants to send the message 25 to Bob, find the signature if she chooses $k = 5$. Explain in detail how Bob will verify the signature. 5

5. (a) Solve the discrete logarithm $2^x \equiv 19 \pmod{29}$ using Baly-step, Giant step method. 5

(b) Decrypt the text 001011011001 that was encrypted twice with the by block cipher using the key 010100110. The S-boxes are given below : 5

$$S_1 \begin{bmatrix} 101 & 010 & 001 & 110 & 011 & 100 & 111 & 000 \\ 001 & 100 & 110 & 010 & 000 & 111 & 101 & 011 \end{bmatrix}$$

$$S_2 \begin{bmatrix} 100 & 000 & 110 & 101 & 111 & 001 & 011 & 000 \\ 101 & 011 & 000 & 111 & 110 & 010 & 001 & 100 \end{bmatrix}$$

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

   (a) There is a finite field with 12 elements.

   (b) Harsh function is used for ensuring confidentiality of information.

   (c) S boxes provide confusion

   (d) If n is a product of two primes and use know the value of $\varphi(n)$, we can factorize n.

   (e) Vigenere cipher is a monoalphabetic, substitution cipher.