No. of Printed Pages : 3

MMTE-006

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

M.Sc. (MACS)

00505 **Term-End Examination**

June, 2018

MMTE-006 : CRYPTOGRAPHY

Time : 2 hours *Maximum Marks : 50*

Note : *Answer any **four** questions out of questions no. 1 to 5. Question no. **6** is **compulsory**. Calculators are **not** allowed.*

1. (a) Construct a field consisting of 9 elements. Find the inverses of all its non-zero elements. 5

(b) What is a Mersenne Prime ? Give an example, with justification. 2

(c) Describe the Linear Congruential Generator for generating random numbers. Under what conditions do we get the maximal period ? 3

2. (a) Determine the orders of all the elements in $\mathbf{Z}_{30}^{*}$. Hence, determine whether this group is cyclic or not. 5

(b) Draw the LFSR circuit for the following recurrence relation :

$$x_{n+3} = x_{n+2} + x_n \pmod 2$$

Also write down the characteristic polynomial and check whether it is primitive or not. *5*

3. (a) Suppose Bano chooses p = 73, g = 5, x = 59, and publishes the public key (73, 5, 59) for the ElGamal crypto system. Rama wants to send the message M = 15 to Bano. She chooses the secret value k = 3. What will Bano receive from Rama ? Decrypt the encrypted message received by Bano. *8*

(b) Explain collision resistance and second pre-image resistance properties of the hash function. *2*

4. (a) Define the following ciphers with an example of each :

(i) Simple Substitution Ciphers;

(ii) Polyalphabetic Substitution Ciphers. *4*

(b) Representing

$$\mathbf{F}_2 8 = \mathbf{F}_2[x] / \langle g(x) \rangle,$$

where $g(x) = x^8 + x^4 + x^3 + x + 1$,

show that the following bytes

10001100 and 11110111

are inverses of each other in $\mathbf{F}_2 8$. *4*

(c) Check whether $(x^3 + 1)$ is irreducible or not over $\mathbf{F}_5$. 2

5. (a) Bano has published the public parameters (119, 11) for her signature using the RSA digital signature algorithm. Calculate her signature for the message M = 10. 7

(b) Decrypt the ciphertext

O G H N Q X D B G G D B B R R

encrypted with Vigenère cipher using the key WARS. 3

6. Which of the following statements are *True*, and which are *False* ? Justify your answers. 10

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

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

(c) Vigenère cipher is a transposition cipher.

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

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