No. of Printed Pages : 3

MMTE-006

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

M.Sc. (MACS)

Term-End Examination

00951

December, 2017

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 of order 8. Find inverses of all the non-zero elements of this field. 5

(b) Carry out one round of encryption of the text 1100 1001 0110 using the toy block cipher with the key 101001110. The S-boxes are given below : 3

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

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

(c) Explain how confusion and diffusion are achieved in DES. 2

2. (a) Apply the extended euclidean algorithm to express GCD (141, 99) as a linear combination of 141 and 99. *5*

(b) You are given that n = 36977, $\phi(n) = 36516$. Factorise n. *5*

3. (a) Define a Pseudoprime. Further, prove that if n is an odd composite number which is not pseudoprime to some base $b \in (\mathbf{Z}/n\mathbf{Z})^*$, then n is not a pseudoprime to $\frac{\phi(n)}{2}$ bases in $(\mathbf{Z}/n\mathbf{Z})^*$. *5*

(b) Find the plain text of the ciphertext 71 which is obtained by RSA with the parameters n = 91, e = 29. *5*

4. (a) Compute $5^{17} \pmod{71}$ using the repeated square method. *5*

(b) Write the recurrence relation with characteristic polynomial $x^3 + x + 1 \in \mathbf{F}_2[x]$. Draw the LFSR for the recurrence relation. Is the polynomial primitive ? *5*

5. (a) Check whether 3 is a primitive root of $\mathbf{F}_{113}^*$. *5*

(b) Check whether the sequence 10100011100100100011011110 passes the frequency test and the serial test with $\alpha = 0{\cdot}05$. You may use the values $\chi^2_{0{\cdot}05,\,2} = 5{\cdot}99146$, $\chi^2_{0{\cdot}05,\,1} = 3{\cdot}84146$. *5*

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

(a) There is a finite field with 10 elements.

(b) A hash function is second pre-image resistant if it is computationally infeasible to find two inputs μ_1 and μ_2, $\mu_1 \neq \mu_2$ with $h(\mu_1) = h(\mu_2)$.

(c) The RSA system is secure for all choices of modulus of encryption.

(d) The actual key length of DES is 56.

(e) Any symmetric key cryptosystem cannot be used without secure key exchange.