No. of Printed Pages : 4

MMTE-006

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

Term-End Examination

June, 2022

MMTE-006 : CRYPTOGRAPHY

Time : 2 hours *Maximum Marks : 50*

Note :

(i) For computing your answer, write all the steps clearly.

(ii) Answer any ***four*** *questions from questions no. 1 to 5.*

(iii) Question no. ***6*** *is* ***compulsory****.*

1. (a) Check that $f(x) = x^2 + x - 1 \in \mathbb{F}_3 [x]$ is a primitive polynomial. *5*

(b) For the initial segment of bits 01100100 of a sequence of period 15, find the recurrence that generates it. *5*

2. (a) Explain the runs test for random sequences.

Apply the test for the following sequence : *5*

11101 00011 10110 01001 01101 00010

00000 10101 00110 01001 10001 10011

11101 10111 11110 10110 11010 11100

10011 11001 10001 11000 10100 10010

11010 10011 10100 10110 10011 10100

11011 00010

You may use the following values :

$\chi^2_{0\cdot05,\,3} = 7\cdot81473$, $\chi^2_{0\cdot05,\,4} = 9\cdot48773$,

$\chi^2_{0\cdot05,\,5} = 11\cdot0705$

(b) If $f(x) = x^3 - 2x^2 - 14x - 5$ and $g(x) = x^3 - x^2 - 17x - 15$ are polynomials in $\mathbf{Q}[x]$, use the extended Euclidean algorithm to find $Q(x)$ and $R(x)$ in $Q[x]$ such that $Q(x)\,f(x) + R(x)\,g(x) = h(x)$, where $h(x)$ is the gcd of $f(x)$ and $g(x)$. The values at the end of the first iteration are :

$T_1(x) = x^3 - x^2 - 17x - 15$, $Q_1(x) = 0$,

$R_1(x) = 1$, $T_2(x) = -x^2 + 3x + 10$, $Q_2(x) = 1$,

$R_2(x) = -1$. *5*

3. (a) Explain the RC4 pseudo random generator algorithm with pseudocode. *6*

(b) Decrypt the following cipher text which was encrypted using the Vigenère cipher with the key word 'ORDERS' :

GLVKVLCDRVICK

Is the Vigenère cipher a transposition cipher or a substitution cipher ? Justify your answer. *4*

4. (a) Explain the CRC and CFB modes of operation of a block cipher. *4*

(b) Find 17^6 (mod 61) using repeated squaring algorithm. *3*

(c) For a RSA cryptosystem, $n = 391 = 17 \times 23$ and the encryption exponent is 17. Find the decryption exponent. *3*

5. (a) Suppose Bano chooses $p = 19$, $g = 2$, $x = 5$ and publishes the public key (19, 2, 13). Rama wants to send the message $M = 10$ 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 the collision resistance and second pre-image resistance properties of the hash function. *2*

6. Which of the following statements are *True* and which are *False* ? Justify your answer with a short proof or a counter example. *5×2=10*

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

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

(c) Affine cipher is a transposition cipher.

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

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