No. of Printed Pages : 6

MMTE-006

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

Term-End Examination

June, 2020

MMTE-006 : CRYPTOGRAPHY

Time : 2 Hours *Maximum Marks : 50*

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

1. (a) Find out if the polynomial $x^3 - x^2 - 2x + 1$ in $\mathbf{Z}_7$ is reducible or not. 2

   (b) Draw the schematic circuit for the recurrence relation : 4

$$x_{m+7} = x_{m+3} + x_{m+1} + x_m$$

P. T. O.

(c) Let $f(x) = x^3 + x + 1 \in Z_2[x]$. Construct the multiplication table for the field $F = Z_2[x]/\langle f(x)\rangle$. Further, what is the order of F ? 4

2. (a) Decrypt the following cipher assuming that it has been generated using Affine map and that "Y" and "V" are actual encryption of plain alphabets "E" and "T" respectively. (Assuming that 11 and 19 are inverses w.r.t. multiplican in Z_{26}) : 5

QAOOYQQEVHEQV

(b) In each round of AES, which transformations are used for confusion and which are used for diffusion ? 3

(c) Construct the discrete logarithm table to the base 2 in Z_{11}. 2

3. (a) (i) Find the encryption and decryption keys for an RSA cryptosystem with $p = 5$ and $q = 7$. Further, which information should be made public and which should be kept secret ? 3

(ii) Encrypt the message "5" with the encryption key of the RSA system above. 3

(b) Compute 5^{11} (mod 37), using the repeated squaring algorithm. 4

4. (a) How does the Runs test work for testing the randomness of a sequence ?

Apply the test for checking whether the following sequence is random or not, with significance level $\alpha = 0.05$:

01110	10010	01010	10011	11011
10101	11001	10000	00111	01011
11101	00011	01101	01000	01111
01101	00101	11000	10100	11000
01011	01001	00111	10101	10110
10001	00011	10011	01101	10010
00011	10101			

You may find the following value useful : 5

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

$$\chi^2_{0.05,4} = 9.48773$$

$$x^2_{0.01,5} = 15.08627$$

(b) Generate a pseudorandom number sequence, of period 20, using a linear congruential generator. 5

5. (a) Suppose Alia sets up an El Gamal digital signature scheme with $p = 17$, 3 as the primitive root and $a = 5$. 7

(i) What are the public and private parameters for the system ?

(ii) Find the digital signature for the message "10" if $k = 7$.

(iii) If Alia sends the signed message above to Babu, how would he verify her signature ?

(b) Assume that you are using a block size of 64 bits and a character representation of 8 bits. What will the Merkle-Damgärd strengthening string of "Todayisagoodday" be ? 3

6. Which of the following statements are true ? Give reasons for your answers : 2 each

(i) If $m \in \mathbf{N}$ and $\mathbf{Z}_m^*$ is cyclic, then the number of generators is $\phi(\phi(m))$.

(ii) The Vigenère cipher is a transposition cipher.

(iii) hash functions are bijective.

(iv) Every block cipher can be used as a stream cipher.

(v) A hash function is used for the verification of digital signatures.

560