1511781

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

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

Term-End Examination

June, 2019

MMTE-006 : CRYPTOGRAPHY

Time : 2 Hours *Maximum Marks : 50*

***Note :** Attempt any four questions from question nos. 1-5. Q. 6 is compulsory.*

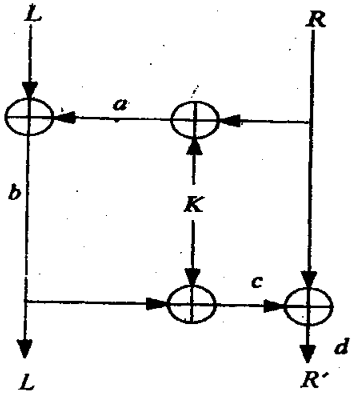
1. (a) Show that the composition of 2 simple substitution ciphers is again a simple substitution cipher. 2

(b) Give an example, with justification, to bring out the main difference between monoalphabetic and polyalphabetic substitution ciphers. 2

(c) Suppose the modulus for an RSA system is $\pi = 50429$ and $\phi(n) = 49980$. If $e = 92$, use the extended Euclidean algorithm to find the decryption exponent d. Further, factor n. 6

2. (a) Describe the Miller-Rabin primality test algorithm. Apply it to check whether 3729 is a prime with base 2. Show all the steps you have followed while doing so. 6

(b) Calculate the output of the Feistel-Network given in the following figure, given the input 01101011010111101010001111010101 and the key 0111010010101001. Assume that the left and right parts are 16 bits each. 4



3. (a) Consider a pseudorandom number sequence generated by a LFSR characterized by ($c_2 = 1$, $c_1 = 0$, $c_0 = 1$). 6

(i) What is the sequence generated from the initialization vector ($s_2 = 1$, $s_1 = 0$, $s_0 = 0$) ?

(ii) What is the sequence generated from the initialization vector ($s_2 = 0, s_1 = 1, s_0 = 1$) ?

(iii) How are the two sequence related ?

(b) Suppose Asha chooses $p = 79$, $g = 3$, $x = 5$ and publishes the public key $(p, g, y) = (79, 3, 6)$ for the El Ganal cryptosystem. Suppose Latha sends $(g^k, M\,y^k) = (54, 31)$ to Asha. Find M. 4

4. (a) Compute A(x) B(x) mod P(x) in GF(2^4) using the shift and multiply method, where $P(x) = x^4 + x + 1$, $A(x) = x^2 + 1$ and $B(x) = x^3 + x^2 + 1$. 4

(b) Give four requirements for designing hash functions. Prove that any hash function that is collision resistant is second primage resistant. 6

5. (a) Write down Golumb's randomness postulates. 3

(b) Check whether the following sequence passes the serial test with $\alpha = 0.05$: 3

10001000000001101000000110

[You may find the following values useful : $\chi^2_{0.05,3} = 7.81473$, $\chi^2_{0.05,2} = 5.99146$]

(c) Encrypt the plaintext '*Privacy is a fundamental right*' by keyed transposition cypher using the key '41523'. 4

6. Which of the following statements are true and which are false ? Give reasons for your answer : 2 each

(i) The key space for an affine cipher over the English alphabet has 25 elements.

(ii) The Discrete logarithm problem over any cyclic group is not computationally feasible.

(iii) Electronic Code Book (ECB) mode is a secure way to encrypting using a block cipher.

(iv) If a polynomial $F(x) \in K[x]$ is reducible, then it has a root in the field K.

(v) In the sign first and encrypt later method, the intended recipient cannot be determined.