No. of Printed Pages : **3**

MMTE-006

00880

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

Term-End Examination

December, 2012

MMTE-006 : CRYPTOGRAPHY

Time : 2 hours | *Maximum Marks : 50*

Note : *Attempt any* ***five*** *questions.*
Use of Calculator is ***not*** *allowed.*

1. (a) Check whether the polynomial $g(x) = x^4+x^2+1 \in \mathbb{Z}_2[x]$ is irreducible with the help of the algorithm that checks the irreducibility of polynomials over finite fields. 4

(b) Given the initial sequence 101010000100101, find the recurrence that generates it. 6

2. (a) Define a strong pseudo prime. Explain the Rabin-Miller test for testing whether a large odd positive integer N is prime or composite. Also test whether 7937 is prime or composite using this test. 6

(b) Explain the principles of confusion and diffusion. Explain how it is achieved in DES ? 4

3. (a) Explain Kerchoff's principle. How is a known - plain-text attack different from chosen - plain - text attack ? Which design criteria resists exhaustive key search for cryptanalysis by an attacker ? 4

(b) Explain birthday paradox. Derive the expression for probability of two persons from a group on n persons having the same date of birth. 6

(i) Given an ideal hash function H with n bit output, find the probability of finding x and y such that $H(x)=H(y)$.

(ii) Given x_0, find the probability of finding a z such that $H(z)=H(x_0)$.

4. (a) Let $p=5$ and $q=11$ be two prime numbers used in RSA. Calculate two valid sets of public private key pairs, where $e < d$. 5

(b) Carry out one round of encryption of text 100111010110 using the toy block cipher with the key 110110111. The S-boxes are : 5

$$S_1 = \begin{bmatrix} 101 & 010 & 001 & 110 & 011 & 100 & 111 & 000 \\ 001 & 100 & 110 & 010 & 000 & 111 & 101 & 011 \end{bmatrix}$$

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

5. (a) Calculate by repeated squaring 2^{38} mod 29 showing all the steps. 3

(b) Find GCD [a(x), b(x)] for 4

$a(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \epsilon F_2[x]$

and $b(x) = x^4 + x^2 + x + 1 \epsilon F_2[x]$

(c) Explain with the help of a diagram Miyaguchi-Preneel method for constructing Hash function. 3

6. (a) Use simple columnar transformation cipher of width 5 to encrypt the plain text : 4

SEND FOOD ARMS AND MONEY TODAY

Use the key 21534 to permute columns of the ciphertext. Compare the security of the two ciphers, namely, simple columnar transformation and simple columnar transformation followed by permutation of columns.

(b) Use Pohlig Hellman algorithm to solve for x : 6

$7^x \equiv 12 (\text{mod } 41)$