No. of Printed Pages : 3 **MMTE-006**

00953

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

## Term-End Examination

## June, 2011

## MMTE-006 : CRYPTOGRAPHY

*Time : 2 hours* *Maximum Marks : 50*

***Note :*** *Answer **any five** out of **six** questions. Calculators are **not** allowed.*

**1.** (a) Define the following terms : **6**

(i) Probabilistic algorithm.

(ii) Yes-biased Monte Carlo algorithm.

(iii) Las-Vegas algorithm.

(iv) A sub-exponential time algorithm.

(b) State the different modes of operation of block ciphers. Explain the encryption and decryption procedures in ECB an CBC modes of operation. **4**

**2.** (a) Explain, with diagram, the Matyas-Meyer-Oseas method and Miyaguchi Preneel method for constructing compression function from a block cipher. **5**

(b) Let $n = 17.23 = 391$. Is 15 a valid encryption exponent for an RSA crypto system with $n$ as the modulus ? If yes, find the decryption exponent. If no, choose a valid encryption exponent of your own and find the decryption exponent. 3

(c) Encrypt the text MEET AT NOON using affine cipher with key (5, 2). 2

3. (a) For the initial segment of bits 011 001 00 of sequence of period 15, find the recurrences that generates it ? 5

(b) If $f(x) = x^3 + x^2 + 2x + 2$ and $g(x) = x^3 + 5x^2 + 10x + 6$ are polynomials in $Q(x)$, use the extended euclidean algorithm to find $P(x)$ and $q(x)$ in $Q(x)$ such that $P(x)\ f(x) + q(x)\ g(x) = h(x)$ where $h(x)$ is the gcd of $f(x)$ and $g(x)$. 5

4. (a) Explain the construction of the S-box in the AES algorithm. 4

(b) Explain the principles of confusion and diffusion used in design of ciphers. 2

(c) (i) The following cipher text was encrypted using a simple columnar transformation cipher with 7 columns : 4

ROAT EHRO TETN UAEC RDRE NQSX TUAY Decrypt the text.

(ii) Is simple columnar transposition a transposition cipher or a substitution cipher ? Justify your answer.

5. (a) Illustrate the algorithm for multiplication in finite fields using the elements $x^2+x+1+[f(x)]$ and $x^2+x+2+[f(x)]$ in the finite field $\frac{\mathbb{Z}_3[x]}{[f(x)]}$ where $f(x)$ is the polynomial $x^3+2x^2+1 \in \mathbb{Z}_3[x]$. 5

(b) Explain the Runs test for random sequences. Apply test for the following sequence : 5

11101000010110101110000011 11100010111000001110111000
01001001001011101100000011 01001100110001010011110111
01001000111100110001100011 11001000001010011001001000
0011011100

You may use the following values :
$\chi^2_{0.05,3}=7.81473$, $\chi^2_{0.05,4}=9.48773$,
$\chi^2_{0.05,5}=11.0705$

6. (a) Check whether the number 353 is a strong pseudo prime the base 2. 4

(b) Check whether the polynomial $x^2+x-1$ is irreducible over $Z/3[x]$. If it is irreducible, check whether it is Primitive. 3

(c) Explain the Diffie-Hellman key exhange protocol. 3