No. of Printed Pages : 2 **MMTE-006**

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

M.Sc. (MACS)

00553

Term-End Examination

December, 2013

MMTE-006 : CRYPTOGRAPHY

Time : 2 hours *Maximum Marks : 50*

Note : *Answer **any five** questions.*

*Calculators are **not** allowed.*

1. (a) Test the irreducibility of the following polynomial : 2

$f(x)=x^2+2x+6$ in $\mathbf{Z}_7$.

(b) For a RSA crypto system, given n = 221, e = 5, find d. Given ciphertext = 11, find the plain text for this system. 6

(c) Check whether 2 is a primitive root modulo 17. 2

2. (a) Given the values a = 161 and b = 28 find gcd (a, b) by using the Extended Euclidean algorithm and also find s and t where sa + tb = gcd(a, b). 5

(b) Given the initial sequence 110010111001, find the recurrence relation that generates it. 5

3. (a) Encrypt the message "The earth is beautiful" by using vigenere cipher with key "ballon". You may ignore the spaces. 2

(b) Encrypt the text "attack preplanned" using a shift transformation with shift parameter 15. You may ignore the spaces. **2**

(c) Check whether the following sequence passes poker test : **6**
1001 1101 1101 1011 0011 1101 0111 0100 0010 1100 0010 0101 You may like to use the following values:

$$\chi^2_{0.05,1} = 3.84146 \quad \chi^2_{0.05,3} = 7.81473$$

4. Briefly explain the following : **5x2=10**

(a) Ciphertext-only attack

(b) Known plain text attack

(c) Chosen-plain Text attack

(d) Confusion and diffusion in a crypto system

(e) Purpose of expansion permutation in DES

5. (a) Encrypt the plain Text $m = 1011000101001 \quad 010$ using Electronic code book mode for permutation cipher with block length 4 with the key **3**

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$

(b) Illustrate the Miller-Rabin algorithm by applying it on 561. **5**

(c) Define a strong prime. **2**

6. (a) Explain the Merkle-Damgard strengthening. Assuming a block size of 64 bits and that we use 8 bits to represent a character, what string will you get by applying Merkle-Damgard strengthening to the string "DIGITAL SIGNATURES" ? **4**

(b) Illustrate the Fermat factorisation method by applying it to factorise 66013. **6**