No. of Printed Pages : 1

MMTE-006(P)

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

00346

Term-End Practical Examination

December, 2016

MMTE-006(P) : CRYPTOGRAPHY

Time : $1\frac{1}{2}$ Hours *Maximum Marks : 40*

Note : *(i) There are two questions in this paper, totalling 30 marks. Answer* ***both*** *of them.*

(ii) Remaining 10 marks are for viva-voce.

1. Write a program in 'C' language that simulates an LFSR. It should take an initial state vector $(x_0, x_1, ..., x_k)$ and the coefficients $a_0, a_1, ..., a_{k-1}$ of the recurrence

$$x_{n+k} = a_{k-1}\ x_{n+k-1} + a_{k-2}\ x_{n+k-2} + ... + a_0x_0 \text{ (mod 2)},$$

the number of terms l of pseudo-random bit sequence as input and output l terms of the pseudo-random bit sequence. Use it to generate first 20 terms of the sequence given by $x_{n+6} \equiv x_n + x_{n+2} + x_{n+3} + x_{n+5}$ and initial vector (0, 1, 1, 0, 1). *15*

2. (a) Write a program in GP that performs Rabin Miller test. Use it to check whether the number n = 12083810075737055857 is a prime number. *10*

(b) Write a function in GP that converts a text to a number by considering the text as a number in base 27 with A = 1, B = 2, ..., Z = 26. Use this function to convert the text "THISISATEST" into a number.

Then, encrypt the number using RSA algorithm with

p = 15838626342085188689

q = 12648755071576652143

e = 27628987

Find d, decrypt and check your answer. *5*