No. of Printed Pages : 1

MMTE-006(P)

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

M.Sc. (MACS)

00173

Term-End Practical Examination

December, 2015

MMTE-006(P) : CRYPTOGRAPHY

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

Note : *(i) This question paper has* ***two*** *questions worth 30 marks. Answer* ***both*** *of them.*

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

1. Write a program in 'C' language that decrypts text which is encrypted using the vigenère cipher. Verify the program by decrypting the following text which was encrypted using Vigenère cipher with 'CONFIDENTIAL' as the key word : 15

VVRSQ ZSAWM RPFVB BTRRT BPAOV CYNDH
MGKQE OVCRC IPMAX UYDGZ SNNHP GFGPF

2. (a) Write a program in GP that returns a random prime of length 256 bits. 5

(b) Find all the irreducible polynomials of degree 4 over $\mathbf{F}_3$, the finite field with three elements, using a program in GP. 3

(c) Write a program in GP that prints all possible decryptions of a given string that was encrypted, using the affine cipher. Verify the program by decrypting the text "OMBLYKGBSCOPIPJOTQBH", which was encrypted using the affine cipher. Also, find the decryption key. 7