No. of Printed Pages : 1

MMTE-006 (P)

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

Term-End Practical Examination

June, 2014

00206

MMTE-006 (P) : CRYPTOGRAPHY

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

***Note :** This question paper has **two** questions worth 30 marks. Remaining 10 marks are for the viva- voce.*

1. (a) Write a program in GP that returns a random irreducible polynomial of degree 20 over $\mathbf{Z}_7$. *7*

(b) Write a program in GP that carries out decryption in Vigenère cipher. Use it to decrypt the text "DFQAAVJDPVHARGZNNZTLTMBTEGEABIAWIQMOIZQQFWGGNIUST". The key is PSMITH. *8*

2. Write a program in C that reads a string and outputs all 25 possible decryptions and the keys. Use it to decrypt the text

"RCCZJNVCCKYRKVEUJNVCC".

Also find the encryption and decryption keys from the information manually. *15*