No. of Printed Pages : 1 **MMTE-006(P)**

00263

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

M.Sc. (MACS)

Term-End Practical Examination

June, 2015

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 the viva-voce.

1. Write a program that encrypts (and therefore decrypts) using Vigenere cipher. Use it to decrypt the following text which was encrypted with Vigenere cipher using the key 'ATTACK' : *15*

```
TAXNK  GOGWE  TODAH  WNYNZ  BHCNT  HEIXO
IMKIG  NTHXX  CWIGX  MACEE  YIHOL  MFYRE
LLXIE
```

2. (a) Use GP to calculate the following : *1+1+3*

(i) Inverse of 449 modulo 809

(ii) Factors of $x^9 + 5x^8 + 6x + 5$ in $\mathbf{F}_{811}$ [x]

(iii) All integers from 1 to 10,000 which are ≡ 7 (83)

(b) Write a program in GP that outputs a random irreducible polynomial of degree 15 over $\mathbf{F}_{47}$. *10*