No. of Printed Pages : **2**

MMTE-006 (P)

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

Term-End Practical Examination

December, 2013

MMTE-006 (P) : CRYPTOGRAPHY

Time : 1½ 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 for the Rabin Miller test. **8**

(b) Use GP to find :

(i) All the irreducible polynomials of degree 11 over $\mathbf{Z}_2$. **4**

(ii) Inverse of the matrix : **3**

$$\begin{bmatrix} \bar{5} & \bar{2} & \bar{1} \\ \bar{1} & \bar{2} & \bar{0} \\ \bar{2} & \bar{2} & \bar{0} \end{bmatrix} \in GL_2(\mathbf{Z}_7)$$

2. Write a programme in C language to encrypt and decrypt using Vigenere Cipher. **15**

Use it to :

(a) Encrypt the text :

"ALLISWELLTHATENDSWELL" using the key "SECRET".

(b) Decrypt the text. "ZLUYKLHNPLVKVWEZJHBTDLKXV UEQSKAUZP" which was encrypted using the key word "HAMLET".