No. of Printed Pages : 2 **MMTE-006(P)(Set-I)**

M. SC. (MATHEMATICS WITH APPLICATIONS IN COMPUTER SCIENCE) [M SC.(MACS)]

Term-End Practical Examination

December, 2024

MMTE-006(P)(Set-I) : CRYPTOGRAPHY

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

Note : *(i) The question paper has two questions worth 30 marks.*

(ii) Attempt both of them.

(iii) The remaining 10 marks are for the viva-voce.

1. Write a 'C' program that encrypts and decrypts using Vigenère cipher. Use it to decrypt the following text which is encrypted using the Vigenère cipher with BIERCE as the key : 15

UWEGQ PPOMJ GMTBS CCCUP IWQYO LEKKS ONSIC JVBYI GSGNI EEI

2. (a) Write a program in GP that performs the Rabin-Miller test. 8

(b) Write a program in GP that prints all pairs of encryption-decryption exponents for the RSA cryptosystem with $p = 2039$, $q = 2741$. 7

× × × × × × ×