

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

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

Term-End Practical Examination

December, 2024

MMTE-006(P)(Set-II) : 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 therefore decrypts) using Vigenère cipher. Use it to decrypt the following text which was encrypted with Vigenère cipher using the key
ATTACK : 15

GKTMO KRBLT JOSXM OHZIM YANVS
 MAOWQ HMYUN VYIKE RKRXW FQBTA
 XSGVF FTDGW AG

2. (a) Use GP to compute the following :

(i) Inverse of 449 modulo 809. 1

(ii) Factors of $x^9 + 5x^8 + 6x + 5$ in $\mathbf{F}_{811}$. 1

(iii) All integers from 1 to 10,000 which are
 $\equiv 7 \pmod{83}$. 3

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

× × × × × × ×