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

June, 2025

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

Time : 1½ Hours *Maximum Marks : 40*

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

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

1. Write a program in C language that decrypt text which is encrypted using the affine cipher. Verify that program by decrypting the following text which was encrypted using affine cipher with the key (11, 10) : 15

   ULSKA LJCVC ALINL UMCAU LSKAL JCSIP

ALINL UMCAU LSKAL JCKYC INSUA RIMUL

2. (a) Write a program in GP that prints all the squares modulo a given prime. It should print each square only once. 3

(b) Suppose we take A = 1, B = 2, ... , Z = 26, and consider 'HELLO' as a number in base 27. Then 'HELLO', when converted to a number, gives $8+5\cdot 27+12\cdot(27)^2 +12\cdot(27)^3+15\cdot(27)^4$ = 8216702. We can convert this back to text also. 8

Write programmes in GP that convert from text to number and number to text.

(c) Let $p=4294967311$, $q=4294968317$, $n=pq$, $e=17$. A certain text T was converted to a number and encrypted by raising it to the power e, modulo (n). The number obtained is 12006217362570451251. Find the plain-text T, by using GP. 4

× × × × ×