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

Term-End Practical Examination

December, 2017

00343

MMTE-006(P) : CRYPTOGRAPHY

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

Note : *(i) This question paper has two questions worth 30 marks.*
(ii) Remaining 10 marks are for the viva-voce.

2. (a) Write a program in GP that carries out decryption of affine cipher. Use it to decrypt the text given below :

GHPMHSHTDBJDBGHSPFGYJOHLCEPGDHCOHWPOLGLWJHOOJCZJ

The encryption key is a = 5, b = 15. *8*

(b) Use GP to compute the following : *7*

(i) All irreducible polynomials of degree 3 over $\mathbf{Z}_5$.

(ii) Inverse of 1298 modulo 2053.

(iii) Factorise 3090359137 using Fermat's method.

2. Write a 'C' program that simulates an LFSR for the recurrence relation

$$x_{n+7} = x_{n+6} + x_{n+5} + x_{n+4} + x_{n+3} + x_{n+2} + x_{n+1} + x_n \pmod 2.$$

Find the output sequence of length 25 for the initial state vector (0, 1, 1, 1, 0, 0, 0). *15*