M.Sc. (Mathematics with Applications in Computer Science)
Term End Examination
December 2020
MMTE-006, Cryptography

Time allowed: 1½ hours ***Maximum Marks 50***

Note: The question paper has two questions worth 20 marks each. Attempt both of them.

1) a) Write a programme in GP that returns a random irreducible polynomial of degree 20 over $\mathbb{Z}_7$. (9)

   b) Write a programme GP that carries out decryption of text encrypted using Vigenère cipher to encrypt the text (11)

   "DFQAAVJDPVHARGZNNZTLTMBTEGEABIAWIQMOIZQQFWGGNIUST"

   The key is "PSMITH".

2) Write a programme in 'C' language that outputs all 25 possible decryptions of the string (20)

   RCCZJNVCCKYRKVEUJNVCC

   which was encrypted using shift cipher.