MMTE-006(P)

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

Term-End Practical Examination

June, 2018

□□□96

MMTE-006(P) : CRYPTOGRAPHY

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

Note : (i)   *There are two questions in this paper, totalling 30 marks. Answer **both** of them.*

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

1. Write a program in C language that encrypts and decrypts text using Vigenère Cipher. Use it to decrypt the following text which is encrypted using Vigenère cipher using the key BIERCE :

   UWEGQPPOMJGMTBSCCCUPIWQYOLEKKSONSICJVBYIGSGNIEEI   *15*

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

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