191631

No. of Printed Pages : 2

MMTE-006(P)

M. Sc. (Mathematics with Applications in Computer Science) M. Sc. (MACS)

Term-End Examination

December, 2018

CRYPTOGRAPHY

Time : 2 Hours *Maximum Marks : 40*

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

(ii) Answer both of them.

(iii) Remaining 10 marks are for viva-voce.

1. Write a program in 'C' language that does all the following : 15

   (i) Write the cipher text given below in a file.

   (ii) Read the input from the file.

   (iii) Decrypt the Vigenère cipher with the key "HENRY".

   (iv) Write the output in a file.

   (v) Encrypt the output file using Vigenère cipher with the same key and print the output.

   (vi) Check the output obtained with the given cipher text :

OIGYY	AWURJ	SPVMC	ALVJB	HCNEB	ZIRFJ
KETVU	PPYPC	HVYPM	UXUVT	PKVCD	LEFKF
PWAVG	NLOFS	YWNEB	ZELKM	TSEIM	DMFJY

2. (a) Write a program in GP that takes a natural number as input and performs the Rabin Miller test to check whether it is probably prime. It should do the following :

   (i) If the input is even, it should exit with a message saying that the given number is an even composite number.

   (ii) If the input is an odd natural number, it should print 1 if it is a composite number and 0 if it is a prime.

   Check your program with the numbers $n = 1238424253392448019$ and $n = 10234788937$ as inputs. 10

   (b) Write a program in GP that outputs a random prime of length 512 bits. 5