

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

00074

**Term-End Practical Examination****December, 2014****MMTE-005(P) : CODING THEORY***Time :  $1\frac{1}{2}$  hours**Maximum Marks : 40*


---

**Note :** *This question paper has **one** question worth 30 marks. The remaining 10 marks are for the viva-voce.*

---

1. (a) Write a C program for computing CRC with CRC polynomial  $x^5 + x + 1 \in F_2[x]$ . 10
- (b) Compute the CRC of the following message using the above programme : 10  
011001011011010101
- (c) Write a C program to find the minimum distance of the ternary code whose generator matrix is given below : 10

$$G = \begin{bmatrix} 1 & 0 & 0 & 1 & 2 & 1 \\ 0 & 1 & 0 & 2 & 2 & 1 \\ 0 & 0 & 1 & 1 & 2 & 2 \end{bmatrix}.$$


---

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

**M.Sc. (MACS)**

00274

**Term-End Practical Examination**

**December, 2014**

**MMTE-006(P) : CRYPTOGRAPHY**

*Time :  $1\frac{1}{2}$  hours*

*Maximum Marks : 40*

---

**Note :** *There are two questions in this paper totalling 30 marks. Answer both of them. Remaining 10 marks are for the viva-voce.*

---

1. Write a program in C language that encrypts (and therefore decrypts) using an affine cipher. It should prompt for the values of a and b and use the values to encrypt/decrypt text. Use it to decrypt the text given below which was encrypted with  $a = 17, b = 20$ . 15

FJKHA EYHTK XKTJY EZYHS AJUTF YZANK  
AFXAK TFYKV UQAHK QMOKZ BABKZ FQMPW  
ZOKAC

2. (a) Write a program in GP to create a set containing all the quadratic residues modulo 557. Check whether 171 and 438 are residues mod 557. 5
- (b) Write a program in GP that performs the Miller-Rabin test. Use it to check whether 10000007 passes the Miller-Rabin test. 10
-