No. of Printed Pages : 2

MMTE-006 (P)

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

00480

Term-End Examination

August, 2011

MMTE-006 (P) : CRYPTOGRAPHY PRACTICALS

Time : 1½ hours *Maximum Marks : 40*

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

---

1. (a) Write a C-programme that encrypts using affine cipher. Use it to decrypt the following text which was encrypted using affine cipher with the key a = 5, b = 8. **15**

OCURI LLVAZ HLIMV APHIW LOCUR ILLMA
AVZAZ RCCVX OCURI LLHWM RZWVH PIVSC
IVXAV ZRCUC IUIVX ASCIV UOCUR ILLHW
MRZOW ZRMPA OWVMS AVHWX CVSCI VXMPA
OWVMU ZPCVM ZRWVZ RCIWP OCURI LLXCH
CVXAE PWULI VXORI ZCJCP ZRCSA UZQIY
NCOCU RILLH WMRZA VNCIS RCULI VXWVM
MPAEV XUWVH WCLXU WVUZP CCZUI VXAVZ
RCRWL LUOCU RILLV CJCPU EPPCV XCPIV
XCJCV WHORW SRWXA VAZHA PZRCQ AQCVZ
NCLWC JCZRW UWULI VXAPI LIPMC FIPZA
HWZOC PCUEN BEMIZ CXIVX UZIPJ WVMZR
CVAEP CQFWP CNCYA VXZRC UCIUI PQCXI
VXMEI PXCXN YZRCN PWZWU RHLCC ZOWLL
SIPPY AVZRC UZPEM MLCEV ZWLWV MAXUM
AAXZW QCZRC VCUOA PLXOW ZRILL WZUFA
OCPIV XQWMR ZUCZU HAPZR ZAZRC LWNCP
IZWAV IVXPC USECA HZRCA LX

(b) Write a C-programme that simulates a LFSR. It should take an initial state vector $(x_1, x_2, x_3, \ldots\ldots x_k)$ and the co-efficients $a_0, a_1, \ldots\ldots, a_{k-1}$ of a polynomial $x^k + a_{k-1}\, x^{k-1} + \ldots\ldots + a_1 x + a_0$ and the number of terms *l* of the pseudo random bit sequence as input and output *l* terms of the Pseudo-Random Bit sequence. Use your programme to generate 100 terms of the pseudo random bit sequence, given the polynomial $x^7 + x^6 + x^5 + x^4 + 1 \in \mathbb{Z}_2[x]$ and the state vector (0, 0, 1, 1, 0, 1, 1). **15**