PMAT 329   Introduction to Cryptography

ASSIGNMENT 1

- Set: Wednesday, September 29
- Due: Wednesday, October 13 in class ---   NO LATE ASSIGNMENTS ACCEPTED!

- Total: 60 points plus 5 bonus points

---

1. [12 points] Cryptanalyze the following ciphertext.
Show all your thinking.

```
TWOZW VHFWK LXOXG MAWBO AHLMB EXYHK VXXLM BFTMX
WTLHG XKXZB FXGMB GYTGM KRTGW MPHIE TMHHG LVTOT
EKRFH OBGZL HNMAH GZXMM RLUNK ZKHTW AXTWH YVHEN
FGGXT KBGZK HTWCN GVMBH GYBOX XBZAM SXKHX TLMHY
IBMSX KLVAH HEYBK XWNIH GURHN KITMK HELAT OXWXL
MKHRX WUKBW ZXLHO XKFTK LAVKX XDYKH FZKXX GFHNG
MMHTI HBGMT LYTKG HKMAT LMAXU KBWZX WNXPX LMHYI
BMSXK LVAHH EPBEE WXYXG WABEE YBOXX BZAML BQHGX
FBEXG HKMAH YZKXX GFHNG MBYYH KVXWM HKXMB KXPBE
EWXLM KHRUK BWZXL HNMAH YZKXX GFHNG MTGWW XETRK
XWLTM FTKLA VKXXD EHHFB LVTIM
```

2. [8 points] Which of the following represent selections of English
text enciphered monoalphabetically? Why?

(a) BQCKG WTNMC RZXUW EKACD SWAPO HLAIU

(b) KKPNV HHTZH TWEUH EYVAB YWKTQ MDALM

(c) QUXKG OYZNK RGTJU LZNKS UXTOT MIGRS

(d) AOZHO ZWSGW BHVSA SRWHS FFOBS OBGSO

3. [15 points] Cryptanalyze the following ciphertext.
Show all your reasoning.
Hint: The title of this text is "The CADBURY Caramilk Cryptogram."

```
GHPCS PCEPMPEGAL YRREH ,Y TO,T,LAWR ACE TAXAIRL YX,I HIALL
O,DDRXH AF,MR ERD,HPW,XH HOW YL,K PH EPMPERE PXY, AH
IAC^ HRTWP,CH AH WOR CGIFRX ,Y XRNGPXRE ERD,HPWH AW WOR
R,WW,I ,Y WOR ERD,HPW,X PH WOR TRCWXR FL,TB KPWO DLAWRH
RATO DX,SXRHHPMRL^ HDLPWWPCS WOR YL,K ,Y RPWORX
PCSXREPRCW PCW, WK, HWXRAIH GCWPL WOR XRNGPXRE CGIFRX
PH XRATORE WOR PCEPKPEGAL ERD,HPWH AXR HOABRC
W,SRWORX W Y,XI WOR T,IDLRWR YPCPHORE FAX
```

4. [15 points] Cryptanalyze the following Vignere cipher.
Show all your reasoning.
Hint: 7 alphabets were used to encipher the plaintext.

```
BIPIZ VYPVK JLXAD VUBPP QDVEY XTMIM TCLRV SIVKN SEBCP SNELX
WPCES CTMRD SIAGW ROCEL XWPCC YFCQP QDQGD BJVJF QBIMS YKACN
QBXEL XWPWZ VWPKE ODWAQ TGDZQ GGMRO ZTDTE KDSMF IPGYX KSCQB
KEMGC JWDLW AIJGM ZQWHU QBPEU RMUCT FDTQP PZVEP BKYYV WFCKB
PWEDZ GZCSL TKVSZ RLWIP IZYEP GPYHL SKMAY FGSCV QGAVG IMEDT
RXDZO KEMGC AVYCI VDVAY FVHGM OSDIK QGRRD CARIN WPEKJ ZGCEL
SITKW TXSRK GCDXG PCVRZ VAOMF ZPSHA MUSXM DPZNI TFEWI TNHEJ
TIPND SXIEC PBTJD LWMEW ZPDGP PELJZ GCELS CKCXM IMHMF DZMVT
VVSQC SCLER PGCIP GKFXZ DZKJL XADVQ PAIGE TGDCC ACOVY REACI
EMPWK IWCCJ WLTUC XOMLH QPPZV EPBKY YRGLB JOCIA HIYKJ XGEWT
DPGLX VHYCQ SIQQX PZWCN WBELW GBJOT FERZA ZESYG IRRTG KJJUI
DXWBK CXPBL TVFNL XSRWP DCSDP VFCZS LTKVS ZRLDB JOOEL PKQWX
YFXKC DTSFH BGBXM FPTUK YHDXV MCELS IAROP HACNQ BXELX WPPCS
EDVGV ZGSIQ QXESS CWVRP VAICU ODEKD XJSDX ARIVO OEDVW TSELE
PAVBT GLHMV YQVMA MUDZI FRZAZ ESJHK TKXFD TLCDL FWUWT OTXAH
AVYCI VDZVB LRKBQ VDPHL DIPYE LWGTQ MLXAD VCXOH WRZAZ EMLLP
GXYIW SMFPZ VHGWE ODWAC OKDPQ HAWAC PRUGG RDTSF IMERY MIJMU
DSEFR IPBPH MRMKX QSJBI VSZRW MXQCF VWHEK DSMFN WWBNS EBCPS
NELXW PCYIL LWTUL WOTTN KDTJD DKNPE KNAVO XFSHM HYCXZ TLGFP
PGEUG XESXT VEBJT LXWPZ CSYGI OCELW XJOMC CHIWI BLTZX KUEMW
QHBGW TWSKM TCLXA AMVYZ PXDZE YYXJD TNSYK SCLRB ZXWRB KXRMF
UWTWL XADVV RCSMV PGXNV QEBKY YFQPK QWMMF PBKYY SXEZQ QCEEB
QPQLR VHVCD PVEXV CVSEJ SECBP JWPBW BPWAI KCXPR UGGRD LRVSM
EBJTL XVHYC QSIQQ WLYLD UCDTG SATAK YHOXB JYFXA CBGBG IFIQQ
XMCLW MVOCQ ACINE DIJDZ CZAPA RIVSZ RMHQP QLRSA OQBTX ZBIPN
LOWNE JSNLA CLKFT HMPTK JPWLW MCVRS JXBJW ELWHC DCJWL TUGXN
VQEBU KATDX KCDTS FXVHY CQSIQ QXMIX DZGSE MKHMP DQVGB IVOCQ
ACINY CGGBX WDPVD DKCDT SFPVF OYXWG AAYFV VPBCM ZQEJV KMLXA
DVUXP XODZM KEXZT ZGMPM NXVID PVEXV CVZVU DUREE IJAWE KEMGC
BJODE ETSGI TWMHM FDZHW RZAZE XZTQP PZVEP BKYYE XIMTS EPWPD
GCELW CMVGZ VCXVC NOMLX WPDZX ZTINQ ZVAIP ODSIA QUUEM WQHBG
WAVGK QFODO WNOGX PVSIQ QXVIQ BIPKR IETVV FPVAU QEKEM GCIPN
ZTWGI VSZRS ANGKE YJTAV RLXWC PCXNI LWMDK DMURZ AZESY GIRRT
GKTKW BTXQD NVRPW MQAAC EIE
```

(There are a few errors in the cipher text --- correct them!)

5. Suppose you have received the following ciphertext

```
EHAYI HAOOM NSPCM YHYDF OSYUT CWCRV MQEHA YIHEY BMZPS
LZXOS WKIOZ COSEH BHWON KRUNS NNJIV DMQLG BGHRB MSKRJ
EGTCX VOSFC ZCMAM DVXRV IREQV HZZEN MKRHF UPWQQ EHMKI
RBMYM BMZPM JWOYI CWGEX ZKKKS UPRVI OOIFR JWEHX XUYJE
BUHRM KCDTV KKNNS LRAZH CWIRV DCCBA RNCED CPVPF EGTCZ
KJAXV WTBMY MBMZP OBEQL TBHEH XXPFK KMYDP LWOKI SXZNZ
VHWSE YVDEH BHNNQ WHRDE JQHWV DHPBP NZRNN ZDXAB LGZKD
YPCXM POGDW OHOVB BHLWV DNWLR
```

which you know was enciphered with a digraphic Hill cipher. Furthermore, you know that the text begins with the phrase "the only guide".

(a) [10 points] Find the decryption matrix.
(b) [5 Bonus points] Give the resulting plaintext.

Show all your work.