CS290, Cryptanalysis, Spring, 2013, Homework 1

John Manferdelli

1. Calculate freq distribution and index of coincidence of the following three mono-alphabetic substitutions and recover the plaintext. Aside from the word breaks, how do you know it is not a transposition?
   a. UW ZTWITJDD N UVRTP ONEE OJNTRHI HJJPD UW OJ TJEJNDJP
   b. ZWT EAUKJ OUY JPHDNCJ FENSAYT O UOSAKOZANUOC ETVTETUGT FNAUZ
   c. GF QFIDOAX GWU AUPULBU FD GWU GWOAV TLPP TULAOIN GRAI RCBOVU VFJI AFGLGU LIV POBGUI QLAUDRPPH
2. How many alphabets in:

KONKA NMRZO PHNON AYEPP FHHBF YHBTA OLDET KMBHV

WBRAT EGHYE HMFHX HPVXU FUKLE OYAAM LHIYX YNUMA

TAMHU NMUAM TAFEK ATAMI AODDM SFHPE UFYRF HDKMD

MIGHZ DALFO EKFHX ADUMO YABUX YMOQR XDMSM OUNZZ

IHBJT HXZFR XAOHX KNUMT MIGSK HXAAL WATEM YGTAA

TAMPE NHATI GNUNX CQRLL QNTUK BHKKB NAXIX KANXA

UMXVD AGVFH XYIIM OAUMP FWTZM UGABO ESKOK ATEPP

POPVD MTFNE FHDYT BZTIV XLRAA MLHGN MWALE FEHXP

EAGKY AKFMN WATEP PPOPK AUZSM SBZML EAALW HNONA

UNMOM TUVAK POUCA PEMHZ FLRHF RNLNO HRIIM OEOFL

ETKLF CALDS TZUST PPBXM ARXUA WMOQW TFFHT AFHXI

AODDU NWZGP BZFHB ZFOFH ZDFLR ONUPT ALYOG LKTAH

FTALD OUIQR LOUDB UFHXJ MVXHZ DBAYA WLGSK POHPL

SOMZU XMOAU LHZDW VXLTY EAIPQ CXHXL ZVXDB AIALH

ZAPMG LLPSH MVRMH UQYPO QNBAI ALWUL XKGPP LXLCB

PGXAT AMJTE KOQTH VWIMH ZDIBF IMVGT TAUNM LDELA

MNWPF FXAOH XKGST KALEH DAWHK AIPQC XHXLM OQYXH

DRHBZ DFVDE MOMNT IADRJ AUEKF EESIH TAFOW VIIMO

FHXDU DHDPO NNXAL ZTEMV AKFLR OKOQR LVZAG KMLEV

IEWZT EPVGL WZUVB SUZXT QBNAU TPHER HBSHE PHIGN

UNMOQ HHBEE TSXTA LFIFL OOGZU DXYUN ZOAWW PEMTS

DEZBX AKHZD WLOEG AFHXD UDHDI ALPZA ESTEK DMYLH

ZDLVI HXUUC HBXDG AETTU PIMUA LHUSE KPXIM VGTBN

ATBUF OFFAL WYMGL HZDFF EUZHD HHNEH XHPAZ HUNTU

PWTZR RXLMN WZMTB ZRIXK NUMAA MLHIY XYTEA BZTXK

YENWM NWZMI WOQWT ZSOBU STHZF AKAMB TUPOY YABUL

DSTUP IFPSH MQAIG PRIPV GLWNA BTJWT HATEP PPOPH

ZDULD ELWQC MHNLX ZAIPL ZTUHO K

3. How hard is the above poly-alphabet to break if you know the first three lines are:

YOUDO NTKNO WABOU TMEWI THOUT YOUHA VEREA DABOO

KBYTH ENAME OFTHE ADVEN TURES OFTOM SAWYE RBUTT

HATAI NTNOM ATTER THATB OOKWA SMADE BYMRM ARKTW