Prof. Dr. Rudolf Mathar, Dr. Arash Behboodi, Jose Leon

Exercise 3

Friday, May 6, 2016

Problem 1. The plaintext hidden in the following ciphertext is part of a famous English play:

```
KPJDLCGS PVHQKWRK KCKRBKPJ DLCWILKR BGSKORKO VCVCNVEW OVQDLCIL YFIRRIGB
IVSXQKRB DLCSVCXX PKRAOWYX HMXIKKRG XLGCXGWI NVEWCQYX CNKVRC
```

(a) Determine the index of coincidence I_C. What can you derive from it[1]?

Problem 2. *(variance of the index of coincidence)* In Lemma 3.3 of the lecture notes, the expectation value of the index of coincidence was calculated for the ciphertext $(C_1, \ldots, C_n)$ with random variables $C_1, \ldots C_n$ i.i.d.

a) Derive the variance of the index of coincidence $\mathrm{Var}(I_C)$ for the model of Lemma 3.3.

Problem 3. The handling of long keys for Vernam ciphers is difficult. Therefore, autokey systems are proposed. For a given keyword $k = (k_0, \ldots, k_{n-1})$ and message $m = (m_0, \ldots, m_{l-1})$ the following two autokey systems are given.

$$c_i = \begin{cases} m_i + k_i \pmod{26} & 0 \le i \le n-1 \\ m_i + c_{i-n} \pmod{26} & n \le i \le l-1 \end{cases}$$

$$\hat{c}_i = \begin{cases} m_i + k_i \pmod{26} & 0 \le i \le n-1 \\ m_i + m_{i-n} \pmod{26} & n \le i \le l-1 \end{cases}$$

a) Describe a ciphertext-only attack on $\mathbf{c} = (c_0, \ldots, c_{l-1})$.

b) Decrypt the cryptogram $\mathbf{c}$=DLGVTYOACOUVCEZA.

c) Assume the keylength to be known. Describe a ciphertext-only attack on $\hat{\mathbf{c}} = (\hat{c}_0, \ldots, \hat{c}_{l-1})$.

d) Decrypt the cryptogram $\hat{\mathbf{c}}$=QEXYIRVESIUXXKQVFLHKG using keylength 2.

Problem 4. Find the key for the following Vigenère-ciphertext and explain your approach.

Hint: You should subtract 1 from the estimator of the keylength you obtained from this ciphertext.

[1] $I_C \approx 0.0385$: polyalphabetic and uniformly distributed; $I_C \approx 0.0668$: monoalphabetic and English

ISYUZPNEVO IQIKHWPGHG IHCERNPNFC HEBHATWSGO GCUMWKPQAW
RSCTAPMINH IZJXBXYYBH WPLXLEPWMB DCMHZXNCMP TWCXTBLXBB
SPYWKDFFWW QPNHSMAYVH XECGQPDYPV TCYFMKPLRG TYMXGGPDX
QIEBXWGZQG SKTXXBRPSX HBLXTAXYIM OCOPXFNDOK SAJXHWCZNW
FTLGUIIEIF CGCIPWSTYT BSEIWONTQH IAOOGPJCXX BBJMHIAXSB
ABPXBOIPJN FEZMXWHEII ZPNYUSUZLX HWPQHFAOJE OXYFRGJNWB
BREFROCOQB HWZOMQDXGX BILMXFXPMH TBPLXVDFMX VDWXXJTYNL
WCEBXWGNIG GTBOXBRPMM VTDYXJTYNL VPGYMSGCCY WTOBTJTEIK
HJCYWVPGYW SHELHMTOGX MTECPWAWHH HPENXAEENH SMAINBSEBX
AIZGXHWPSA OKPJKSHPHM SSWCMHAPVN HWZLKCGEIF OCJNASNHCE
ZHPYFZTDMM SGCCUZTEBT BQLLHEJPMA SGPUYHTCJX FWLJLGDXYB
BIPFESREGT MQPZHICOQA WRSQBZACYW IRPGTDWLHM OHXNHHWPWH
ABZHIZPNYL CBPCGHTWFX QIXIKSRLFF ADCYECVTWT ZPYXYOGWYL
GTIWBHPMFX HWLHFMDHHP VXNBPWAWJX FRPCOSXYNA SRTLVIBDNT
BRPMBRTEUB ZLTNAOLPHH HWTHZADCYM VPYUGCGOCG OGJMNQRPML
WDYIYJTCSG OIFLTZRLOL SHLHWSUQYV HHQLHABJCG TPYWRWLLMG
CIPXYCGEBX RDNCEWIJUG RWFGTBXESH TBJXBGEZMB HXZHFMIPHW
SGYYLGDQBX OGEQTGTGYG GDNIGGETWB CJDULHDXUD SBPNASYPMM
CUXSVCBAUG WDYMBKPDYL DTNCTZAJZI JIYDTEMPWI SNASHPCLDT
YNFCHEIYAN ECFSPYXGSK PLPOHDIAOE ASTGLSYGTT PXBBVLHWQP
CYLGXYAMVT XNAWHAYVIA TUKWIJIYQW LLTQIPLZFT HQBHWXSZFD
HNAOCOCGOC JGTBWZIWWS PLBJTOZKCB TNHBTZZFME CCGQXAUEGD
FLVSHZZIZT LMNFTEIMVD DYPVDSUOSR SYKWHSYWOC LZYSRECHBU
ZLMVTQUBHW QOEOCOMTUP NCHIHOIZWC PYWVPCXEMQ PUMHWPNKCJ
MFXCUPRIZP THBBVEBXBP EOKSDCNASX YNXBHTNRCU EBXUGLNBTX
NUMWDYNAIH OYKWKLVESI SYKSXDMHAT EBBBVTHMVT FHLSAQCLVP
YXLSAQMTQG TZBQXYAECK PIYOQCOMSL SCVVVSIXGS TLXQIWSMCI
SYASPCNHTW TGPVDSULVP OZKSFFYGHD NWTGXZHMCI PMMHWPJTZI
CSYFXPHWGW TJTBSRILGP XYKTXOYEWI JIYATCYFOC TGTFGTYWSP
CFROCOQTGW LJIMIZZBBS THFMLTZXOS TMICHTNBCC YIMICNIGUT
YCTZLTNAAN ZQGCQDYKJX YAFMELLMWP WCMMUZLWCB PMMWRAYMGH
SYECHEHHCE AIKHJYCMMD QJKCRFLBBV EBHGTZZMVT XILHPRLXSP
MFXYXTHISC LZPENXFLLM TFTXUKYPMF RZPCAXOCOV XOJECYIALH
BAPWYGHXCY EMQWUVYPYX LOVLWBIDDN HOCLMMCCTM AWCRXXUGPY
BBHAYTYXYA HTWTMBBIPF EWVPHVSBJQ BTTHBHOISY TFIHULBDEU
EWIEFXHXYW MIGPXPWISM NDTCMMWITI GAPOYYFTBO XBILFEIHTI
GHDEBXOCNC XBIAIIIALL GCITIGKWTW AFTRUKRTOU EZQWUVYRLN
LOHHCMQWPM BBSTMZIXDY GCIEBTHHSY POHPPXFHPL BCJDOICCEB
BGEZCGHPYX BATYNBCCEB XAPENXFPEU EZUZLGCQPN MSGCYTGDYN
AOCEBTHXEB TDEPHLXJDN GCLEIUSGPG XAQPLXREWO MCISCLKPDN
ASRLNLBPXY POHXSYOKZO KWIPJXHPYX IZPJGTHTTU ECCPZXRWTG
TBSSYTHIPH WSSXYPVTCY OSGTQXBILV HIIEBXVDFM XWIHULSKPH
PWISXBTUTW NZIJNAOITW HIAOJKSKPH MVXXZKCBQI ECLTHZATEB
KCJRBMVTDN KSTEMHIGQL BSCOMAWEWU LHTOCGHWTM FOCYYKTDCM
XJTCUEMTLL LRJCCGULSC VVBJAXBTCU EHTXJXFPXY GHPYXVVPCU
VHTCNAFDFA AHWPCGGICO FSCEUEWIJI YHWPZBSCOC GHTXYKOCNY
AOSTVEIHSN HQDYZXGHTN XLEPLBSCNY WOGLXBQPWU KOSTWTZPWN
XFPECHBUZL MVTHIKGTTA KSLOURPNOU RADCYFCDOS FCGPCKFXEU
UZTXIKSGPA TFSWYLGDQN ASUPYEWCRI YCISYKGXDO YTTCYWANDY
ETIZOLSXYN XAEPLTHTWU GUJLAXHDXS PWUPUMZTYA MVXPPXBDQZ
XFTOBXFEPL LCCLFOWDWY GQTXSISIDI YQDFLLSLPL XAPOYMCUPY
EHWPWAOCRY BBBJXBGEZM BHXZHBBDEI GZNYYZZTNN XRQFNBZAFM
XRISYFTDCJ EIIZBHKTGY KWHECEZGPN TWCPXLIUQC VWTYNKSVLL
WHDCYLHPTH FSUCIFWBLX XBDDWKIEPF HTBLFMFTLN BBVEBXFPMV
BHHEBXADYE XMDCYOSCEB XRDRQASCMS TQRTXXBIZL MVGZOZVPQZ
XQITIGHWPS VOBPCGANHU RPJEGRRXDY TGTRLXKJAI GATQIKKWLN
WWHPULSXDF BYTLFVCWZF TBSLNESCRN ASKPHIZJEI PVDHULBDHV
XQDXCGUDWX TBSNIGGTBO XBIWSLCBPQ AOIAYXJXDB XJTYJEIIZV
XUPYNHSMAY KWTYWXHWPY YTTNNLCUXS BZAEYFDTCI GSCTAAHGPN
NFCTHZVDXY FIRSCGHDIC VOIPXYFDXI GSDQGRVPFH MGPMINHIZQ
GWULHVWTON AOIEBXQPEU OCXOYWANAL XGTYWXWHPC SSSSCFKWPH

```
BBWTMYFXRB  MOIXSOWDWY  GQTSYBBUWC  VHTOULZXRB  MKDFHWIEZH
FMWLHWKXEB  AWHEYXHWEB  XTJCSHTPOY  FCCTHLHPYN  EMEZMLSHDY
WATTEGSLXS  LSAQHHZDYA  XFBJIKWVTH  TZHZOEGTPG  XRPEIGQTEI
MOZPCMGUWC  ZVIQLHABJV  HRNLHWOBZL  XHWLHYWTYX  BGWXUESKZF
XBRPABBCFL  MIGPXMVGTF  ESSPPXFNQC  USGZZFMUCU  FSXEIHYUCI
FANHUBGINI  THEZWDSILJ  XBZYCYSDAY  GSSTNZFPDJ  XRISYICDCV
XOHEVRHWPN  AFDLNTBSOY  EWQPLTHTWS  VIIZHXCUSC  LSNPMYFDXN
ASHZWDSITV  EIHSCUIGYC  LVJOXXFLSC  ESXAYGHWPX  TACLVESPEL
UMTOATFTWF  XBEZY
```

For the recommended computer assisted evaluation the above ciphertext is also available in the web.