Homework 3 in Advanced Methods of Cryptography

Prof. Dr. Rudolf Mathar, Markus Rothe, Milan Zivkovic

15.05.2014

Exercise 9. 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.

Exercise 10. 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.

```
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.

Exercise 11. 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]?

Exercise 12.

Let X, Y be random variables with support $\mathcal{X} = \{x_1, \ldots, x_m\}$ and $\mathcal{Y} = \{y_1, \ldots, y_d\}$. Assume that X, Y are distributed by $P(X = x_i) = p_i$ and $P(Y = y_j) = q_j$.

Let (X, Y) be the corresponding two-dimensional random variable with distribution $P(X = x_i, Y = y_j) = p_{ij}$.

Prove the following statements from Theorem 4.3:

(a) $0 \leq H(X)$ with equality if and only if $P(X = x_i) = 1$ for some i.

(b) $H(X) \leq \log m$ with equality if and only if $P(X = x_i) = \frac{1}{m}$ for all i.

(c) $H(X \mid Y) \leq H(X)$ with equality if and only if X and Y are stochastically independent (conditioning reduces entropy).

(d) $H(X, Y) = H(X) + H(Y \mid X)$ (chainrule of entropies).

(e) $H(X, Y) \leq H(X) + H(Y)$ with equality iff X and Y are stochastically independent.

Hint (a): $\ln z \leq z - 1$ for all $z > 0$ with equality if and only if $z = 1$.

Hint (b),(c): If f is a convex function, the Jensen inequality $f(E(X)) \leq E(f(X))$ holds.

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