Homework 4 in Cryptography I

Prof. Dr. Rudolf Mathar, Michael Reyer, Henning Maier

05.05.2011

Exercise 11. Show that the set of regular $n \times n$ matrices over a field K together with the usual matrix multiplication is a group. Is it an abelian group?

Exercise 12. 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.

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

2.
$$c_i = \begin{cases} m_i + k_i \pmod{26} & 0 \leq i \leq n-1 \\ m_i + m_{i-n} \pmod{26} & n \leq i \leq l-1 \end{cases}$$

(a) Describe a ciphertext-only attack on method 1.

(b) Decrypt DLGVTYOACOUVCEZA which is encrypted with method 1.

(c) Assume the keylength to be known. Describe a ciphertext-only attack on method 2.

(d) Decrypt QEXYIRVESIUXXKQVFLHKG which is encrypted with method 2. using keylength 2.

Exercise 13. Find the key for the following Vigenère-ciphertext. 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 computer assisted evaluation the above ciphertext is also available in the web.