Homework 3 in Cryptography I

Prof. Dr. Rudolf Mathar, Wolfgang Meyer zu Bergsten, Michael Reyer

11.11.2008

Exercise 7. 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 8. The permutation $\pi = (1)(2, 11, 5, 8)(3, 6, 7, 4)(9, 10)$ defines a permutation cipher with block length $k = 11$. Determine the number of character sequences of length 11 over the usual alphabet with 26 letters, whose cryptogram does not differ from the plaintext.

Hint: $(2, 11, 5, 8)$ means that position 2 is moved to position 11, 11 to 5, 5 to 8 and 8 to 2.

Exercise 9. Find the key for the following Vigenère-ciphertext. Explain your approach.

The ciphertext is also available on the exercise webpage.

Hint: You should subtract 1 from the estimator of the key-string length you obtained from this ciphertext.

```
ISYUZPNEVO  IQIKHWPGHG  IHCERNPNFC  HEBHATWSGO  GCUMWKPQAW  RSCTAPMINH
IZJXBXYYBH  WPLXLEPWMB  DCMHZXNCMP  TWCXTBLXBB  SPYWKDFFWW  QPNHSMAYVH
XECGQPDYPV  TCYFMKPLRG  TYMXGGPDXQ  IEBXWGZQGS  KTXXBRPSXH  BLXTAXYIMO
COPXFNDOKS  AJXHWCZNWF  TLGUIIEIFC  GCIPWSTYTB  SEIWONTQHI  AOOGPJCXXB
BJMHIAXSBA  BPXBOIPJNF  EZMXWHEIIZ  PNYUSUZLXH  WPQHFAOJEO  XYFRGJNWBB
REFROCOQBH  WZOMQDXGXB  ILMXFXPMHT  BPLXVDFMXV  DWXXJTYNLW  CEBXWGNIGG
TBOXBRPMMV  TDYXJTYNLV  PGYMSGCCYW  TOBTJTEIKH  JCYWVPGYWS  HELHMTOGXM
TECPWAWHHH  PENXAEENHS  MAINBSEBXA  IZGXHWPSAO  KPJKSHPHMS  SWCMHAPVNH
WZLKCGEIFO  CJNASNHCEZ  HPYFZTDMMS  GCCUZTEBTB  QLLHEJPMAS  GPUYHTCJXF
WLJLGDXYBB  IPFESREGTM  QPZHICOQAW  RSQBZACYWI  RPGTDWLHMO  HXNHHWPWHA
BZHIZPNYLC  BPCGHTWFXQ  IXIKSRLFFA  DCYECVTWTZ  PYXYOGWYLG  TIWBHPMFXH
WLHFMDHHPV  XNBPWAWJXF  RPCOSXYNAS  RTLVIBDNTB  RPMBRTEUBZ  LTNAOLPHHH
WTHZADCYMV  PYUGCGOCGO  GJMNQRPMLW  DYIYJTCSGO  IFLTZRLOLS  HLHWSUQYVH
HQLHABJCGT  PYWRWLLMGC  IPXYCGEBXR  DNCEWIJUGR  WFGTBXESHT  BJXBGEZMBH
XZHFMIPHWS  GYYLGDQBXO  GEQTGTGYGG  DNIGGETWBC  JDULHDXUDS  BPNASYPMMC
UXSVCBAUGW  DYMBKPDYLD  TNCTZAJZHB  SZZTBXXUEG  PYXPOHTHWI  ARYWPNXSIO
GPHMGLTNAO  VCYTHKLLBS  IJIYDTEMPW  ISNASHPCLD  TYNFCHEIYA  NECFSPYXGS
KPLPOHDIAO  EASTGLSYGT  TPXBBVLHWQ  PCYLGXYAMV  TXNAWHAYVI  ATUKWIJIYQ
```

WLLTQIPLZF THQBHWXSZF DHNAOCOCGO CJGTBWZIWW SPLBJTOZKC BTNHBTZZFM
ECCGQXAUEG DFLVSHZZIZ TLMNFTEIMV DDYPVDSUOS RSYKWHSYWO CLZYSRECHB
UZLMVTQUBH WQOEOCOMTU PNCHIHOIZW CPYWVPCXEM QPUMHWPNKC JMFXCUPRIZ
PTHBBVEBXB PEOKSDCNAS XYNXBHTNRC UEBXUGLNBT XNUMWDYNAI HOYKWKLVES
ISYKSXDMHA TEBBBVTHMV TFHLSAQCLV PYXLSAQMTQ GTZBQXYAEC KPIYOQCOMS
LSCVVVSIXG STLXQIWSMC ISYASPCNHT WTGPVDSULV POZKSFFYGH DNWTGXZHMC
IPMMHWPJTZ ICSYFXPHWG WTJTBSRILG PXYKTXOYEW IJIYATCYFO CTGTFGTYWS
PCFROCOQTG WLJIMIZZBB STHFMLTZXO STMICHTNBC CYIMICNIGU TYCTZLTNAA
NZQGCQDYKJ XYAFMELLMW PWCMMUZLWC BPMMWRAYMG HSYECHEHHC EAIKHJYCMM
DQJKCRFLBB VEBHGTZZMV TXILHPRLXS PMFXYXYXPS WLDUWGOSZC AOFBGWLFBB
TOOZFPMBBH HLSFOAWMHB ZPYTBSLCTH ISCLZPENXF LLMTFTXUKY PMFRZPCAXO
COVXOJECYI ALHBAPWYGH XCYEMQWUVY PYXLOVLWBI DDNHOCLMMC CTMAWCRXXU
GPYBBHAYTY XYAHTWTMBB IPFEWVPHVS BJQBTTHBHO ISYTFIHULB DEUEWIEFXH
XYWMIGPXPW ISMNDTCMMW ITIGAPOYYF TBOXBILFEI HTIGHDEBXO CNCXBIAIII
ALLGCITIGK WTWAFTRUKR TOUEZQWUVY RLNLOHHCMQ WPMBBSTMZI XDYGCIEBTH
HSYPOHPPXF HPLBCJDOIC CEBBGEZCGH PYXBATYNBC CEBXAPENXF PEUEZUZLGC
QPNMSGCYTG DYNAOCEBTH XEBTDEPHLX JDNGCLEIUS GPGXAQPLXR EWOMCISCLK
PDNASRLNLB PXYPOHXSYO KZOKWIPJXH PYXIZPJGTH TTUECCPZXR WTGTBSSYTH
IPHWSSXYPV TCYOSGTQXB ILVHIIEBXV DFMXWIHULS KPHPWISXBT UTWNZIJNAO
ITWHIAOJKS KPHMVXXZKC BQIECLTHZA TEBKCJRBMV TDNKSTEMHI GQLBSCOMAW
EWULHTOCGH WTMFOCYYKT DCMXJTCUEM TLLLRJCCGU LSCVVBJAXB TCUEHTXJXF
PXYGHPYXVV PCUVHTCNAF DFAAHWPCGG ICOFSCEUEW IJIYHWPZBS COCGHTXYKO
CNYAOSTVEI HSNHQDYZXG HTNXLEPLBS CNYWOGLXBQ PWUKOSTWTZ PWNXFPECHB
UZLMVTHIKG TTAKSLOURP NOURADCYFC DOSFCGPCKF XEUUZTXIKS GPATFSWYLG
DQNASUPYEW CRIYCISYKG XDOYTTCYWA NDYETIZOLS XYNXAEPLTH TWUGUJLAXH
DXSPWUPUMZ TYAMVXPPXB DQZXFTOBXF EPLLCCLFOW DWYGQTXSIS IDIYQDFLLS
LPLXAPOYMC UPYEHWPWAO CRYBBBJXBG EZMBHXZHBB DEIGZNYYZZ TNNXRQFNBZ
AFMXRISYFT DCJEIIZBHK TGYKWHECEZ GPNTWCPXLI UQCVWTYNKS VLLWHDCYLH
PTHFSUCIFW BLXXBDDWKI EPFHTBLFMF TLNBBVEBXF PMVBHHEBXA DYEXMDCYOS
CEBXRDRQAS CMSTQRTXXB IZLMVGZOZV PQZXQITIGH WPSVOBPCGA NHURPJEGRR
XDYTGTRLXK JAIGATQIKK WLNWWHPULS XDFBYTLFVC WZFTBSLNES CRNASKPHIZ
JEIPVDHULB DHVXQDXCGU DWXTBSNIGG TBOXBIWSLC BPQAOIAYXJ XDBXJTYJEI
IZVXUPYNHS MAYKWTYWXH WPYYTTNNLC UXSBZAEYFD TCIGSCTAAH GPNNFCTHZV
DXYFIRSCGH DICVOIPXYF DXIGSDQGRV PFHMGPMINH IZQGWULHVW TONAOIEBXQ
PEUOCXOYWA NALXGTYWXW HPCSSSSCFK WPHBBWTMYF XRBMOIXSOW DWYGQTSYBB
UWCVHTOULZ XRBMKDFHWI EZHFMWLHWK XEBAWHEYXH WEBXTJCSHT POYFCCTHLH
PYNEMEZMLS HDYWATTEGS LXSLSAQHHZ DYAXFBJIKW VTHTZHZOEG TPGXRPEIGQ
TEIMOZPCMG UWCZVIQLHA BJVHRNLHWO BZLXHWLHYW TYXBGWXUES KZFXBRPABB
CFLMIGPXMV GTFESSPPXF NQCUSGZZFM UCUFSXEIHY UCIFANHUBG INITHEZWDS
ILJXBZYCYS DAYGSSTNZF PDJXRISYIC DCVXOHEVRH WPNAFDLNTB SOYEWQPLTH
TWSVIIZHXC USCLSNPMYF DXNASHZWDS ITVEIHSCUI GYCLVJOXXF LSCESXAYGH
WPXTACLVES PELUMTOATF TWFXBEZY