30/10/2013

קריפטוגרפיה: תרגיל 1

הגשה: יום ד' 13/11/13 ב- 14:10 בהרצאה. ההגשה בזוגות או ביחידים.

שאלה 1

פענחו את ההודעה הבאה המוצפנת בצופן Vigenere בעזרת ה aplet בו השתמשנו בכיתה הנמצא באתר הבא http://math.ucsd.edu/~crypto/java/EARLYCIPHERS/Vigenere.html

VRGLL XRZNJ EQKSJ BBPGS BJNQY HWFLB QKPQH FVQWW
MBFFH NDRFE VHPHH NUECO VXUWO WCJIF LVBPH VAWGQ
KPTNF VSORR RSEHD WLRFN HERRN DFSYX VVLLO CHRPQ
UOOEI RFFSY UIGDL HWSTV FTWJW SGZRH SRPNJ TSOWS
ADVBA HRGAG WAVMA LUSSR VYVAS SOINC RRZRG HERBP
VVRNR OHWLB KRRKF YZWAH OVYCH YWAGF LXBFI HVAKN
QKQXE SPHKU IQONF ZVRBO QSJDR QGOHW LRRVO MPKIJ
SFVEQ KGGAD KVXFM TUAVX GZNHP KIHKV BPHPY ATSJF
INYRB YBEAV VHOEV VLVGD FSHFG SNSEE LUORH GBECF
KPMFW QRWWE CSFGA GXUJB ICKXU WPCIS YGWEG KIKBG
TZADR QQNVK RXUWG KKEMT YRGPF SZHNB EHWVF GVAZS
EDQKE WLEWT ONGWG GBJAU EYDVB PHVAW GHNDJ SAPOJ
GMALH FJDPY GJSZW LBKRQ KXRGJ LGCRZ RJAAA QXFSA
RHLOR DLHDH MESYZ EHWNU PSOVX BZHBZ UIQKB TILPY
ABBOR JHKRF WFGBM AHOIV BEVBZ LZVVH OHVEE GHBZW
LROBF HGJEG ZIJGM FUYCO HHVFG SNFIC LVCJS SVFGG
PKIAK NOJGK PZDON HGBHL WJJIA LVFAG EGSSZ KZWNU
ECOVJ VTRFK SXVUP OXOIF LUOPF EEJLW JISEE NHERR
OWGKA HRGZR RWWEP WAHAU WBXGV AVMYA PCJYE YDRMC
LEALF HDHTB KGGXD VGGAU AOPZS AOJGE FZXOJ VSYLN
BEUIC GEHAG SAORR JHWQS LHDHH BUHAA QXCJB JEGMA
YRJEG IAURC BVYPZ JOODQ BFTHD HXEGI SKIJV DRGOX
TCDVS ZECZJ FBKZH RFNBZ LWQSG SZMEA MNFUP EXAAU
EWEZG AUPKI ZGFHN HGRFG HKSWR UESPI MYWFO PWVVT
HHAGX BLUSU HEEGY RSKMF LYSXO SJWEU AQORA GVWOI
KSARA UXUWU SWGSS LUSJV EGGYR NHTBJ GSNVA RVASO
GELSS HAURB GAWZR RGCAC SZLNL GVAUI CGEHE VEPUB
FZLRT LBDKO MGAPC WQHFS VRDLW NYRBY BMFFB HWXXU
GEWVH HGGGO LLRGG FWHLG BFIOH OILUB ALDRV WFKDH
RNKXS ZLJGZ RBODX NHCSZ LRGGG VAGEG SPSJW IEKNZ
AAEAV RFODM QFBHP RQLCA CSOIQ YRSWU PVWEH DLWLW
NFOHT NJNHA GSPMZ SJWEG ABBOX TCDVS ZECZJ FBKZH
RFQWO FPBKR RAYMQ WAQAR JCJVG IDRAK NCLHV NLRRL
USTJN APKEG LUSEQ XRDYW CHRPW PCISE AQPCJ GYPLR
RPRXN JTSPW LRMFS NVSSE VQNRW BXGUK RKYWL ODRSS
SPSXR SXHNZ PDPXQ BIPXF RKXML HEBDN BZDTC DRGAU
ZVURG SKIAL UOPSV BYEOI ZEFVV GYOSF WQPUW LRYHO
NGMNF ASSVT NHRFE QNHFR FASSE LRFOW LRJRG WLHVL
NZHRA RVGVA QWNLB QKOPR UGAWW IEANZ EQGYM QWJJW

RSEQD KMFLB FUWLR UBBPH RGGSS IDMYK SWHHX ESAGB
HVFSA RHLZR UUOPV AUAYS DDZVF TREUI PLNQY HWFLB
HDHGB ECOJL IFKRF RHVFS GHEPI FOVHD WLRSF GEVXN
FPSKI GBEZI JLGNL VCJSV BNVRA UWVFG VAXWN UPCNG
MAYGC PKIYS GSOWP RSXHD HRFSN BZEVV LNWJV KBNRF
JPIAL PCIPY AAPOP LSAKU SWGUH SEHAU WNJRQ KQHHU
GWJJW VEVZW USCWE OPLSA KGONJ IGAAU PKIHK RFORJ
NLYSW VXGOB CBWLR KRQKP TNFVS ODPGZ BICKX UAFHE
PIHFQ SNXXZ GFHOH GEWPM PKIVF SWHWV NLVCJ LWRKC
SYLEY DLGPU MXAAU XHGNM FSPKI AKNIJ GIESF SLDVN
LRDNR KESZY JRAAS FDNLW ZZNGB USALQ CKUEP URGOW
STGBU HHEAV LODRS HKRFW FGBMA HOWLE GHUDD GBMEH
WSTEG ISZSV BURGO WLRHB GPQSG WQOJG AUAYS PRTOJ
NGOLR GZRIO LRGWY ZEJIA URQKP QHFVH UGISW ARAGT
EAFAW QHFSV REWHV VACPW EEYRH WPIEA POJLR GWEBA
WYFWE GPKIA WJSOW TEGTF WPGBV RBWPI QEHGY XPNJF
KAHTF MCRWW ECWEH WLRVF THKWL RSPQK XRGKB TIDRL
SZSNL GNFFH DHTBK GOYNR BOYSZ JIQLU SIXWP MYONS
VBYEO IDGPG EREQK GGJSZ QIFVN MOOIN CVBRR PIWFO
LUSPW FGEQA UAPVP KIAKN OJGKP ZDWJW IEURD PFSZE
HBEFE GABBO RZRJF SWVAU WESHD BEWFH NLGGA BBODR
QGISN VMTZG OHOSJ LUSWJ IAUVS ODGPW FGPRM ALRZH
LKRFP SSLXU WNGAQ WNVBQ QPIAL FOXRY GLUSA IJBJG
FAIIE VVFAF XYQGC BXPYL NYAEY YCNQY HWFSA RDLKU
NBZQP IBHRF WWMBF FCJBE UGBOJ GKBGT ZAQIG OBFGV
XUWCC OWVRH BFPHH FMPVH DVTWF QWOIP GYZAF XVGAC
BLRGW EBAWG BFGSJ WABMY RXHMY DRUWO MALUS QQMGW
QGPDX RKOIP WLRGC SNDXV GAGPD ORHYO YHSIW EGADW
JZRFA WLRFF OEVEY DBKAG XBHES OXQRL UOPDR LGASQ
VMAYN TKUIV YARWW EYAAY EVESG ESEJR RJ

סעיף א

1. הסבירו בקצרה כיצד חשבתם את אורך המפתח.
2. מהם טבלאות השכיחויות של האותיות בכל עמודה?
3. הסבירו כיצד קבעתם את ההזזה הציקלית בכל עמודה.
4. מהי ההודעה המפוענחת?

ניתן לצרף צילומי מסך.

שאלה 2

בשאלה זו נתאר מערכת הצפנה. למערכת יש שני פרמטרים t ו- r כאשר $r < t$. קבוצת ההודעות היא $M=\{0,...,r\text{-}1\}$.
המפתח k נבחר בהתפלגות אחידה מתוך $K=\{0,...,t\text{-}1\}$. ההצפנה של הודעה m נעשית בצורה הבאה:

$$E(m,k) = (m+k) \bmod t$$

1. הוכיחו כי מערכת הצפנה זו היא מושלמת ביחס לכל התפלגות P_M.

2. נשנה את המערכת כך שהמפתח כעת יבחר בהתפלגות אחידה מתוך $\{0,..., r-1\}$. ההצפנה היא כמו מקודם (כלומר, $\bmod t$). הראו כי לכל t,r המערכת המתקבלת אינה מושלמת. יש להוכיח את תשובתכם.

שאלה 3

סעיף א

תהי M קבוצת הודעות ו- K קבוצת מפתחות כך ש- $|K|=|M|$. הוכיחו כי בכל מערכת הצפנה מושלמת ביחס להתפלגות האחידה מעל M ההתפלגות על המפתחות היא אחידה.

סעיף ב

מערכת הצפנה אינה בזבזנית אם לכל שני מפתחות k_1,k_2 קיימת לפחות הודעה אחת m כך ש- $E(m,k_1) \neq E(m,k_2)$. הראו מערכת הצפנה מושלמת ביחס להתפלגות האחידה מעל M שאינה בזבזנית בה ההתפלגות על המפתחות אינה אחידה. (כמובן, במערכת זו $|M| < |K|$.)

שאלה 4

עבור מחרוזת בינארית A, נסמן ב- $\bar{A}$ את המחרוזת המשלימה (כלומר, המחרוזת בה כל אפס מוחלף באחד ולהפך). הוכיחו כי $DES(\bar{m},\bar{k}) = \overline{DES(m,k)}$. הסתמכו על העובדה כי המפתח k_i בכל איטרציה הוא תת-קבוצה של הביטים של המפתח k.

סעיף ב

הראו, בעזרת סעיף א, איך לבצע התקפת חיפוש ממצה על DES המשתמשת ב 2^{55} הפעלות של DES. איזו סוג התקפה תיארתם?