31/10/2012

קריפטוגרפיה: תרגיל 1

הגשה: יום ד' 14/11/12 ב- 16:10 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

UYINY ZUYIA CBDFV RSLPI WLYEM PWTBC HXPEN JBTOT
YTJWI OXEFU RECLB PEFDM SKLEU VPTOO EBQLR CRNSF
QSEXF IWTYZ NJENN GNZPL SWOJM NXMXP SRUKJ KCNOE
KVVSO GBEHO DPFIG IDQFJ ENNBP NRSKT PEKAW MSZGA
CUPJX PYXVC SUCCS SENCB SVXCR KPGID GQUYQ ATWSC
SSCMT RRDNI JCCIX KPEZE XQFEG ECKPD QUDMS JLOWM
PNREB ABEHB EAJEI SCMTJ XREOH CIDGQ UYXHO TPJWO
PXPNI RGIUV VLYOH VHOBJ VIREN PPDIS KVEKL EMPBC
PEXOF FJNKD JXETS VHRGR SXQCI DSVGI ESDZV TXUBM
PWHAW IHVHR YIEJF RSLHV WAXLN RWSDZ BEWID AZJXE
WAXVE ROQOR WTKBF FJCBQ TZWAV TBTVO CAUYM SCBBK
INOEB IONOE KVVSO GNRCO BKPIC BYWLV VTYTE TRNYV
XVHNO AERCI DAHFM NQBPS IAMPB CPEXO JEKTS UFGVE
CQEVR TLISR GKYJB DEICA DYIDE TFUXO FQTZX TRMCR
XTOZF UNEBA FPWHY ZFFRW OLOVW DKGBE HSEZW VCTRM
ERQAQ MEVWC BQCVH BIVFN NEBAF PKOFK IIMSM PSZWT
SMBJY NDPJE OALTF RWSKV EPWPE BUVVS KEBPM TVMBM
ISLMI ZRDKB MVESD LFRXH CNSFQ HKQUZ XOMIO RHADP
FJXOB ULZPL OLQVS PVMJE XHOKB IMBLM BEXHO VJKWL
KUNVH IXBPK LEEAF RWTMW BJXWR MSVMT VMGKE TVMBJ
XDOIE RRDYV FNSMK VJEGA XIERH IOLBW XEBLF SVICN
SFQTR MTKSR WAUIY CUPFI

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.

סעיף ב

הסבירו מדוע בפענוח ההודעה הנ"ל עבור אורך מפתח 3 התקבלה התפלגות לא אחידה על האותיות ולעומת זאת עבור אורך מפתח 5 התקבלה התפלגות די אחידה על האותיות.

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 $\{0,..., r\text{-}1\}$. ההצפנה היא כמו מקודם (כלומר, $\bmod t$). הראו כי לכל m,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 $|K| > |M|$.)

שאלה 4

נסתכל על מערכת הצפנה בה אלגוריתם הפענוח יכול להיות אקראי (לדוגמא, בהינתן מפתח וקריפטוגרמה האלגוריתם יכול בהסתברות מסוימת להחזיר הודעה אחת ובהסתברות המשלימה להחזיר הודעה אחרת). נחליש את דרישת הנכונות של מערכת הצפנה Gen,E,D לדרישה כי אלגוריתם הפענוח מפענח בהסתברות לפחות 1/2 , כלומר לכל הודעה m

$$\Pr[\ D(E(m,k)) = m\ ] \geq 1/2$$

כאשר ההסתברות היא מעל האקראיות של אלגוריתם הפענוח.

הראו כי במקרה זה לכל תחום הודעות $|M|>1$, כאשר $|M| = 2^t$ עבור t שלם, קיימת מערכת הצפנה מושלמת בה $|K| \leq \frac{1}{2}|M|$.