עמוס ביימל **19.03.02**

קריפטוגרפיה: תרגיל 1

הגשה: יום ג' 9/04/02 בהרצאה. ההגשה בזוגות.

שאלה 1

פענחו את ההודעה הבאה המוצפנת בצופן Vigenere.

```
WMOQR PSIEM WMPVV URLOH ZQGPJ ZMPXS FRWDQ LMILG
GLUMW ZSQBR WNPPP JPUWA FVQAH PWIVF LZVKP TIHBW
VAXLO SJXIS FHQPZ LSMWG WUPFA UREII LUTWP QIFMN
TIZHM NFEVP ALTEA QGCFX IDCQP VBTIO VGLQR PWIZE
EQUIZ FLPEY KPMPE ZQSIY FVMIE DSIKM PWFHB AGZVV
BMROT IVFXZ SSUQS YBHQB PZNEB UGXJW AUSYU LMDIS
FXIXO PEXWQ BAFVB EMYUL MOVJQ XWSVL QLQOH PQEZF
QPOXW RXSFT IBEWD IDDML QIWBP PXIZQ XLMOQ ZKLCS
CFEMP SSNCL ESKFS CBRLY EEIQI FMNBM VZEXF HRNTZ
SXMDL TTFWA OLOHK AREJE VQHEI IUAWE BGKGV LUIND
IBVIV OCEBF TQWPW IZBYM MMATI OIMAY IEISL AJHSM
BURRB GQBLP SAIEE DVFAF MEVXQ ARTOA PUGSB KQHIY
MIBFI CNMOT XMFIV OMAII ZQHHJ XPMRJ PRMAJ PMIDQ
ROJJN QVPOX TQXEF VAMRO JRETM NIEAU RRMIT QXEFV
WRXSF GZKTE PKZMQ XJKPF VPQVM EIYUE VKSYF SNQPP
WIVPM QGIZQ REMIB FICTS NFLPD PMMVA MEQZX PYXXD
EEUPQ WIDPQ IZCZU LMDWA PVBQV DVRJD ILLEJ XINJT
PQVDX IZQXS FSZQX TDETX CAFVN QGECY BATPS EBUSY
BPTKM XQVIO XTDET TMDTC AFIXE IUMRO FHSQC EBFTQ
WEIEB IICFG IDVTF HIDSF OHJKX SFWMZ HPSEV PXSFV
MOITW IZQVC PVAUR POGZK TEJSV IICFE TESPB WQXCX
BHMFL ZVKPT MDTCA FIXXE AZSEV WMPZP SCUGG SIMAN
SZLII DRPEL QYXSF XQFPP PJNMX SFVWR QZEIZ ZGCZT
BAKCB TPKED TSWZE DWMOQ RPSIZ QXFSR MPXZQ EZUWS
FAZAX PBFWA OZOLQ EWEVH QQWZG GQBLP SWCZH PSXPQ
XTUPM MXCFE BUWPP RAQGC FXEDM EJROU XNPRB MMYFH
BTIGJ KMZIC FXINP PBYET MNIAI EEXFX PAHZG HWGFW
FWCNW EJXCF MZOSZ BSWZE TBLLC IBUGT UAIEX SFJQD
WEHVM MXNSC XFSRS EXTMN JRDQR EJSVE MYDIR GPTVW
KQEDB VIZHE IIUQX SPHET MNIAI EYWUM UMXPM CBAHC
JZMMP XPWBM PWPXP QVDGV WYXSF JQQPO QVIFX SJWAK
WEFQE MWUVW BMRPW STHIX FRBAJ APVBQ VDTCA FIXQS
ZFICE IUMRO FHNAV LTTMO MLMOM KXLCP MNYEW MOQRP
SIIEO PEJWD EVFCE AVOUL IFEAF VAARN PYTPV PNIUN
ICJRP UWSFE L
```

יש להראות:

1. כיצד חשבתם את אורך המפתח?
   רמז: חפשו, למשל, את המחרוזות WMOQR ו- LOH.
2. מהם טבלאות השכיחויות של האותיות בכל עמודה?
3. כיצד קבעתם את ההזזה הציקלית בכל עמודה?
4. מהי ההודעה המפוענחת?

הערה: קובץ עם הקריפטוגרמה נמצא באתר הקורס.

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, $\bmod t$). האם המערכת המתקבלת 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 שאינה בזבזנית בה ההתפלגות על המפתחות אינה אחידה. (כמובן, במערכת זו $|M| < |K|$.)

שאלה 4

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