8.11.2014

קריפטוגרפיה: תרגיל 1

הגשה: יום א' 23.11.14 לתא 78 בקומה 1 בניין 37 (שימו לב שרשום על התא "אורי שטמר"). ההגשה בזוגות או ביחידים.

שאלה 1

פענחו את ההודעה הבאה המוצפנת בצופן Vigenere בעזרת ה applet בו השתמשנו בכיתה.

הערה: גרסאות חדשות של Java חוסמות את ה applet. אם אתם ניתקלים בבעייה, הפעילו את לוח הבקרה של Java, ובלשונית Security הוסיפו לרשימת האתרים המורשים את הכתובת:
http://math.ucsd.edu/~crypto/java/EARLYCIPHERS/Vigenere.html
(ניתן להגיע ללוח הבקרה ע"י Start → All Programs → Java → Configure Java)

UEKQG VFVMF ODMFT KIMIM YRLQM XCQFF RVOUD RNPAI GJTAH KUJKQ BVZKA TVETA RFWWQ JRBTQ XSCFY UJBAR GCTNK NVZSD GELYA ZYMDM TUBTQ XVEME TFBTU TXBTM ZJPQI ULTPZ UKPMH KXQHQ TKWFT KTPUX JFVOQ YYMSM BVPQD GCQFF RVZUP OEOTA UUWRD KUDQX BVBIT OTPEG OKMPT KIAAI KCTFT GKATQ CFCXP TVDQD CVIDM TPBTU TXMXE KJWET KNIEM RNIKE IRTXQ JCQFF RVZQP XZLUZ MYWAP UEMPM EYMDY UKPQD YRQPF UYMDO UDMXU ZKTQD KUZUP OEOTA UUPQD KZAMB OVKQA LTIWQ GELMN UKBXQ UWEUZ KKIWQ ZYMYF UPWGD MIIZP SFBTQ XJPQU YZTXM TUEQM QRVPF NVGIU RCLAT KIOAA JJMFA AKJQR UIMUF MVBET UKIZP CYMZK ULIDQ MFQZS CRTWZ OTMXK GELCG OVBXK GELPA TFBDG TFNRF NVXMF NFZKA ADIKR GCTMZ JSZQM QKPQN UKBXQ GELFT KEGAG XXZMZ JDWFT KIEUX RXMFZ UKPUZ MRVPI NVVKA AXWUZ ZFPQD XFWYP UEBRA XXMFF UJIKS UFLYA XEQZS GELPA TKXQQ VZVFA KMMDK IFZZQ XSMRA XVGAG JFQFU CZTXF GBMSD KRBOM XVAMU JCQFF RVZQP XZLUZ MYWAP ZFPQD SFBTQ XRVPS GMMTQ XYIZP UEQFF NVODM TUUAF NVZXU BVLAG ZZVFT KNWAP NRTRM RVISG KWZAY ZYMHU RCISQ GELVG YKIEX OKBXQ XVLDU JZVST UFLQZ ZVZQP ZYMIA UUIIA RWUQF NVZDQ JIQPU TXPAA JUQPZ UKSZA CNPMF GNQOW KUKDQ GKCDQ NVEME GELIM YEWFM ZRTXM LIIUP UWPUY MFWPP GPTUF ZCMDQ JIQPU TXPAA JJIUP NVBTM TBGAG QZVPX ENWXR CYQFT KIIIM EJWQM XCGXU ZKTQD KUZUP OEOTA UUBAY EXZMZ JDWFT KIAIT GKPMH KPWGS UKQZK ULZMB XFVOM QVIZP CZVQK KJBQD JRGIM YSIWU TXLMK YFXAA XJQOW MIIZP SFBTQ XZAFA NRDQE UDMFT OEOSA UUBAY GBMTQ XJBDA TXMDI NVZQP UVAKA AIODM TUUAF NVZXU BVTUF ZCMDQ JIQPU TXPAA JROAA JHCMD ZVZAR GCMMS AVNMD ZYMDA TZVFT KNWAP NVZTA AJMEF GELEG TUMDF NVBTD KVTMD MVWMW ZIMQE ZYMZG ZKZQQ YRZQV AJBNQ RFEKA AJCDQ RPUGE ZBVAI OKZQB RZMPX OKBXQ XVLDU JZVST UFL

סעיף א

- הסבירו בקצרה כיצד חשבתם את אורך המפתח.
- מהם טבלאות השכיחויות של האותיות בכל עמודה?
- הסבירו כיצד קבעתם את ההזזה הציקלית בכל עמודה.
- מהי ההודעה המפוענחת (אין צורך להעתיק את כולה, מספיקות 2 מילים כדי לתאר אותה)?

סעיף ב

נסו לפענח את ההודעה הנ"ל בעזרת מפתח באורך כפול. תארו מה קיבלתם והסבירו מדוע.

שאלה 2

בתרגיל זה תראו כי בטיחות מערכת הצפנה לא תלויה בהתפלגות על ההודעות.
נתונה מערכת הצפנה $\pi = (Gen, Enc, Dec)$ מעל מרחב הודעות צפנים ומפתחות $\mathbb{M}, \mathbb{C}, \mathbb{K}$ בהתאמה, ונתונה התפלגות $\mathfrak{D}_1$ מעל $\mathbb{M}$.
נסמן ב- M_1, C_1 משתנים מקריים המציינים את ההודעות והצפנים עפ"י ההתפלגות $\mathfrak{D}_1$.

נתון כי מתקיימים 2 התנאים הבאים:

א. לכל הודעה $m \in \mathbb{M}$ מתקיים: $\Pr[M_1 = m] > 0$
ב. לכל $m \in \mathbb{M}$ ולכל $c \in \mathbb{C}$ מתקיים: $\Pr[C_1 = c | M_1 = m] = \Pr[C_1 = c]$

הוכיחו כי π היא מערכת הצפנה עם בטיחות מושלמת.

שאלה 3

נתונה מערכת הצפנה $\pi = (Gen, Enc, Dec)$ כך שכל יריב מנצח במשחק ההבחנה מול π בהסתברות בדיוק $1/2$. הוכיחו כי ל- π יש בטיחות מושלמת.

שאלה 4

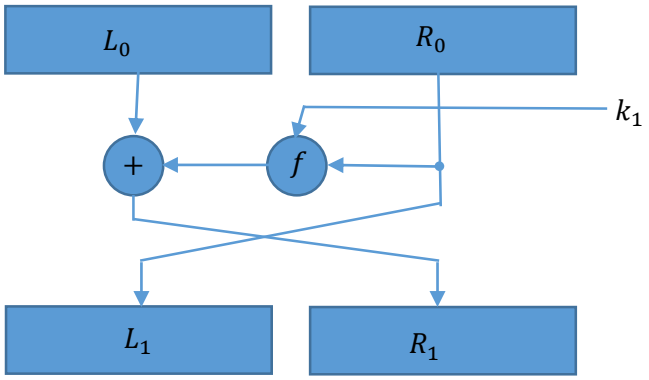
בשאלה זו תראו מתקפה על גרסה מוחלשת של DES המבצעת רק סיבוב אחד (במקום 16 סיבובים). לשם פשטות, נניח כי לא מתבצעים את הפרמוטציות IP ו- IP^{-1} בתחילת ובסוף התהליך. כלומר, עבור הודעה $x = L_0 R_0$ באורך 64 ביטים ועבור מפתח k_1 באורך 48 ביטים מקבלים הצפנה

$$y = L_1 R_1$$

כאשר

$$L_1 = R_0$$
$$R_1 = L_0 \oplus f(R_0, k_1)$$

וכאשר f היא הפונקצייה שהוגדרה בכיתה עבור מערכת DES.
בציור:



הראו מתקפת known plaintext אשר בהינתן זוג הודעה וצופן (x, y) מזהה קבוצה של 2^{16} מפתחות אפשריים כך שאחד מהם הוא המפתח הנכון.