בס"ד

קריפטאנאליזה של מערכות הצפנה סימטריות – תרגיל בית מס' 1

להגשה: 15.4.15

השאלות המסומנות ב (*) הינן קשות יותר ואינן חובה. השאלות המסומנות ב (**) קשות מאוד. השאלות המסומנות ב (!) הן ככלל שאלות שאני לא יודע לפתור.

1. פענחו את צופן ההחלפה הבא. (הטקסט אינו מכיל סימני פיסוק ורווחים בין מילים שונות. שני הקטעים הם חלק מאותו טקסט (עם הפסקה של כמה פסקאות ביניהם).

בגויר אוגצח קסנקס רסתמר בסנתי בסמקת דתסות כלרדס מדרדת סקמרל רדבסכ רכררח תקקרת דקקצז דרדבס ריולז פרדוב תדצגת קררקת זצצגל תאררק תסתור אצנתצ קזתצת גדפהו ספהור קסלרי כרצגכ ואסתט צסנסנ קקגוי תבזכס עותנא קוצסג קתלרק בזצגו יתדהע תורתת צגכמצ קדהצס תקדחת סצאתב צגוית תצכמא בדתזס גדכרו תדתסק מרלרד קדתזח אוסרפ שתורת קפתוד רעסכד ותסרס תמרקב זצמתו צאתבת צסגכע בקתצמ דקסנד רחסתב מתותד סגכות לרקאב תצגוי קבסקת לרקתכ צתירק קנהרצ רקתקט רלרקס הורכת לאקתד סכרתא הדקסנ בורדב לתזהו רקתנו רקתסח רקתרא תבטמצ תסתצז סאצרש נצקאח תתדוב תדתאת כואצת קתקטל נצניק תקברג בוזדס חרמקס צזצדת אברסג ויתלת אגלהא תצניק גתדקק צזדרד.

...

צהרזז לדזלפ לתגלת כבורק תנידס נקליר טרסרא תבסנב ורתסד לתנסס ירתלר דברתק פרתקס קלמשס בורשר נצגוי ראוגצ תבדתח העזתד לתסשב נרדתס סרפשת ורדתנ צרפתמ סכצשד ניודס גתקתד סקגתכ מתדגל תקזור ערקבע גדנצס חקדקמ רלסרס תמרדב גוירא וגצסר גקמרל דראוגצ.

2. שאלה זו והבאות אחריה עוסקות בצופן DES. חומר נוסף על הצופן (כולל הגדרה מלאה של הטבלאות בהן הוא משתמש) ניתן למצוא בוויקיפדיה, וכן באתר: http://en.wikipedia.org/wiki/DES_supplementary_material.
נסמן ב $E_K(P) = C$ את ההצפנה של הקלט P באמצעות המפתח K שמובילה לפלט C. [זהו סימון קבוע בו נשתמש גם בהמשך.] עבור וקטור בינארי $x = (x_1, \dots, x_n) \in \{0,1\}^n$, נסמן ב- $\bar{x}$ את הוקטור "המשלים" $\bar{x} = (1 - x_1, \dots, 1 - x_n)$.

א. הוכיחו את הטענה הבאה, שנקראת "תכונת ההשלמה של DES": לכל P ולכל K מתקיים $E_K(P) = \overline{E_{\bar{K}}(\bar{P})}$.

ב. השתמשו בתכונת ההשלמה כדי להציע תקיפה על DES שדורשת נתונים של 2 chosen plaintexts וסיבוכיות זמן של בערך 2^{55} הצפנות.

3. הציעו תקיפה טובה ככל הניתן על **שני** שלבי DES שדורשת **זוג קלט/פלט אחד בלבד**. [יעד המינימום הוא שהסיבוכיות לא תעלה על 2^{16}, אבל כנראה אפשר להשיג סיבוכיות טובה בהרבה.]

4. הציעו תקיפה טובה ככל הניתן על **שלושה** שלבי DES. [יעד המינימום הוא שהסיבוכיות הכוללת לא תעלה על 2^{30} הצפנות. ניתן להשיג סיבוכיות טובה בהרבה.]

5. בשאלה זו נעסוק בגרסאות של DES בהן משנים את מנגנון קביעת מפתחות הסיבוב.

א. נניח שמפתח ההצפנה K הינו באורך 48 ביטים, ו**כל מפתחות הסיבוב שווים ל K.** הראו שניתן לשבור את הצופן DES המלא (16 שלבים) בתקיפה שהסיבוכיות הכוללת שלה לא עולה על 2^{34} הצפנות DES.
[רמז: חישבו מה קורה אם עבור שני זוגות קלט/פלט $(\mathrm{P}, C), (P', C')$, ההצפנה של P על ידי **שלב אחד** של DES (עם המפתח K) שווה ל P'.]

ב. (*) בתנאים של סעיף א', מצאו תקיפה שדורשת לכל היותר 2^{18} הצפנות, אם לתוקף מותר להשתמש ב chosen plaintexts.

ג. (**) נניח שמפתח ההצפנה K הינו (K_1, K_2) כאשר כל אחד מ K_1, K_2 הוא באורך 48 ביטים, ושמפתחות הסיבוב הם K_1, K_2 **לסירוגין**. הראו שניתן לשבור את הצופן DES המלא (16 שלבים) בתקיפה שהסיבוכיות הכוללת שלה לא עולה על 2^{34} הצפנות DES.

ד. (**) נניח שמפתח ההצפנה K הינו (K_1, K_2, K_3, K_4) כאשר כל אחד מ K_1, K_2, K_3, K_4 הוא באורך 48 ביטים, ושמפתחות הסיבוב הם K_1, K_2, K_3, K_4 **לסירוגין**. הראו שניתן לשבור את הצופן DES המלא (16 שלבים) בתקיפה שהסיבוכיות הכוללת שלה לא עולה על 2^{34} הצפנות DES.

ה. (!) אותה שאלה כמו סעיף ד', אבל עם שלושה מפתחות (K_1, K_2, K_3).

6. שאלה זו עוסקת בצופן AES. חומר נוסף על הצופן ניתן למצוא בוויקיפדיה. לשם פשטות, נניח שהמפתח הוא בגודל 128 ביטים ושכמות השלבים היא 10. נעסוק בגרסאות של AES בהן חלק מהפעולות מושמטות. "תקיפה" פירושה אלגוריתם שמאפשר למצוא את המפתח או לפחות יכולת להצפין ולפענח כל הודעה.

א. נניח שהשמיטו מ AES את פעולת **SubBytes** (בכל השלבים). מצאו את התקיפה הטובה ביותר שתוכלו על הצופן המתקבל. [דרישת מינימום: 2^{24} פעולות לכל היותר.]

ב. נניח שהשמיטו מ AES את פעולת **MixColumns** (בכל השלבים). מצאו את התקיפה הטובה ביותר שתוכלו על הצופן המתקבל. [דרישת מינימום: 2^{14} הצפנות לכל היותר.]

ג. נניח שהשמיטו מ AES את פעולת **ShiftRows** (בכל השלבים). מצאו את התקיפה הטובה ביותר שתוכלו על הצופן המתקבל. [דרישת מינימום: 2^{36} הצפנות לכל היותר.]

ד. (*) נניח ששינו את אלגוריתם קביעת המפתח כך שהמפתח שווה ל **K** בכל השלבים. מצאו את התקיפה הטובה ביותר שתוכלו על הצופן המתקבל. [דרישת מינימום: 2^{70} הצפנות לכל היותר.]

בהצלחה!