

קריפטאנליזה של מערכות הצפנה סימטריות – תרגיל בית מס' 2

להגשה: 6.5.15

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

1. שאלה זו והבאות אחריה עוסקות בצופן DES.

סטודנט בקורס "קריפטוגרפיה לא מודרנית" שניתן באוניברסיטת טהרן הציע לשנות את פונקציית ההרחבה E בה משתמשים בתחילת פונקציית השלב של DES לטבלה הבאה:

16	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	1
32	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	17

(סדר המשבצות בטבלה הוא לפי סדר השורות, ומשמאל לימין בכל שורה. כלומר, 48 הביטים המתקבלים הינם, משמאל לימין, ביטים 16,1,2,3,4,5,4,5 וכו' מתוך 32 ביטי הכניסה ל E).

הראו תקיפה על הצופן המתקבל שדורשת 2^{54} הצפנות בלבד.

(רמז: השתמשו בפונקציה החדשה E, ביחד עם תכונה של בחירת תתי המפתחות של DES, כדי למצוא "תכונת השלמה" נוספת של הצופן החדש, הדומה במקצת לתכונה שמצאתם בתרגיל 1 שאלה 2).

2. נניח שיש בידכם תקיפה על שלושה שלבי DES שדורשת שלושה נתונים 2^{10} הצפנות. (תקיפה כזו חלקכם מצאתם בתרגיל 1 שאלה 4). נתבונן בארבעה שלבי DES.

- א. השתמשו בתקיפה על שלושה שלבי DES כדי לבנות תקיפה על ארבעה שלבי DES שדורשת 2^{60} הצפנות לכל היותר.
- ב. למה התקיפה שמצאתם בסעיף א' אינה מעניינת?
- ג. השתמשו ב chosen plaintexts כדי לשפר את התקיפה כך שתדרוש 2^{44} הצפנות לכל היותר.
- ד. (*) מצאו תקיפה יעילה הרבה יותר על ארבעה שלבי DES.

3. על מנת להתגונן מפני תקיפת הזזה (זו התקיפה בה עסקנו בתרגיל 1 שאלה 5א) הוחלט להשתמש בכל מפתחות הסיבוב של DES **באותו מפתח**, אבל להוסיף פעולה נוספת של הוספת קבוע בסוף כל פונקציית שלב. סדרת 16 הקבועים שנבחרו היא: $a,b,c,d,d,c,b,a,a,b,c,d,d,c,b,a$ כאשר a,b,c,d מילים שונות בנות 32 ביט כל אחת.

- א. מדוע תקיפת הזזה לא עובדת כנגד הצופן שהתקבל?
- ב. הציעו **תקיפת זיהוי** על הצופן שהתקבל שדורשת לכל היותר 2^{35} נתונים וזמן. (תקיפת זיהוי היא תקיפה בה אתם מקבלים לידיכם צופן בתור קופסה שחורה, ואתם רוצים לגלות האם הצופן הוא גרסת DES שתוארה בשאלה או צופן אקראי שאין לו תכונות מיוחדות. מותר לכם לבקש מהקופסה השחורה להצפין/לפענח ערכים לבחירתכם, ובסופו של דבר עליכם לנחש האם הצופן שבקופסה הוא גרסת DES שלנו או לא. אתם אמורים לצדוק בהסתברות קרובה ל 1).

(רמז: חישוב מה קורה אם במהלך תהליך ההצפנה, הערך לאחר שמונה שלבים הוא מהצורה (x,x) כאשר x מילה של 32 ביט, כלומר אם החצי השמאלי שווה לחצי הימני אחרי 8 שלבים.)

4. מערכת ההצפנה אבן-מנסור (Even-Mansour) מוגדרת בצורה הבאה:
 $E(P) = K_2 + f(P + K_1) +$
 היא פעולת קסור, ו- K_1, K_2 הינם זוג מפתחות בלתי תלויים. גודל הקלט, כל אחד מהמפתחות, והפלט הוא n ביטים. הציעו תקיפה על המערכת שדורשת בערך $2^{n/2}$ נתונים וזמן, ללא קשר למידת ה"מסובכות" של הפונקציה f .

(רמז: חישוב מה קורה אם זוג קלטים P, P' מקיים $P'=K+P$. כיצד תוכלו לגלות ביעילות האם זוג קלטים מקיים תופעה זו? כמה קלטים צריך כדי שביניהם יהיה זוג שמקיים את התופעה?).

5. שאלה זו עוסקת בהמרת זמן/זכרון. נתונה פונקציה f מ- n ביטים ל- n ביטים שהיא "חד-כיוונית", כלומר קל לחשב את $f(x)$ וקשה לחשב את $f^{-1}(x)$. נניח שהתוקף מקבל D ערכים x_1, \dots, x_D ומטרתו היא לחשב את f^{-1} עבור **לפחות אחד מהם**. (נסו לחשוב על מצב בחיים בו תקיפה כזו תהיה רלוונטית). הציעו תקיפה שדורשת חישוב מקדים של $2^n/D$, זכרון של $2^n/D$, וזמן של D ומצליחה בהסתברות לא זניחה.

6. שאלה זו עוסקת בצופן AES. נתבונן בהצפנה של קבוצה של 256 קלטים, בהם כל הבתים חוץ מהשמאלי העליון שווים ל 0, והבית השמאלי העליון מקבל את כל 256 הערכים האפשריים.

א. נתבונן בקבוצת 256 הערכים המתקבלים לאחר **שני שלבים** מלאים של הצפנה. הוכיחו כי בכל אחד מ 16 בתי המצב, כל אחד מ 256 הערכים האפשריים מופיע בדיוק פעם אחת בקבוצת הערכים המוצפנים.

ב. נתבונן בקבוצת 256 הערכים המתקבלים לאחר **שלושה שלבים** מלאים של הצפנה. הוכיחו כי בכל אחד מ 16 בתי המצב, הקסור של 256 הערכים המתקבלים הוא 0.

ג. השתמשו בסעיף ב' כדי להציע תקיפה על 4 שלבי AES שדורשת 2^{20} הצפנות לכל היותר.

ד. הציעו תקיפה על 5 שלבי AES שדורשת 2^{52} הצפנות לכל היותר.

(רמז: הוסיפו שלב לתקיפה של סעיף ג', בדומה לשאלה 2' לעיל).

ה. הציעו תקיפה על 6 שלבי AES שדורשת 2^{84} הצפנות לכל היותר.

ו. (** שפרו את התקיפה על 6 שלבי AES כך שהיא תדרוש פחות מ 2^{50} הצפנות.

בהצלחה!