בס"ד

קריפטאנאליזה של מערכות הצפנה סימטריות – תרגיל בית מס' 5

להגשה: 22.7.15

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 עוסקת בקריפטאנאליזה דיפרנציאלית. מפתחי הצפנים האיראנים המהוללים הצליחו לייצר טבלאות (S-boxes) עבור DES, שהן מושלמות מבחינה דיפרנציאלית. כלומר, בכל שורה ב DDT כל 16 האיברים שווים ל- 4. המפתחים החליפו את הטבלאות של DES בטבלאות החדשות והלכו לנוח על זרי הדפנה. עד שהם נחים, מצאו דרך לשבור את הצופן המלא שהתקבל (כל 16 השלבים) בסיבוכיות נתונים וזמן של 2^{35} לכל היותר.

[רמז: מצאו תכונה איטרטיבית בהסתברות טובה של הצופן החדש]

2. שאלה זו עוסקת במערכת אבן-מנסור (Even-Mansour), עם בלוק ומפתחות באורך n ביטים כל אחד. נתונים מספרים D,T המקיימים $D \leq T$ וכן $DT = 2^n$. מצאו תקיפה על מערכת אבן-מנסור עם סיבוכיות נתונים וזכרון D וסיבוכיות זמן T.

[רמז: תקיפה דיפרנציאלית]

3. שאלה זו עוסקת בתקיפת "דיפרנציאל בלתי אפשרי" (impossible differential).

א. נתבונן בצופן עם מבנה פייסטל של 5 שלבים (כמו 5 שלבי DES) בו פונקציית הסיבוב F היא <u>הפיכה</u> (בניגוד ל DES). נתבונן בזוג קלטים (P, P') עם הפרש $(0, a)$ (כלומר, החצי השמאלי של ההפרש הוא 0 והחצי הימני הוא הערך a (שמורכב מ- n/2 ביטים). הוכיחו ש<u>לא יתכן</u> שהפרש הפלטים המתאימים (C, C') שווה גם הוא ל $(0, a)$. [רמז: חשבו את ערכי ההפרשים בהתקדמות מצד הקלט ובהתקדמות מצד הפלט, ובדקו מה קורה באמצע.] תופעה זו נקראת "דיפרנציאל בלתי אפשרי".

ב. מצאו תקיפת זיהוי על 5 שלבי הצופן DEAL שדורשת לכל היותר 2^{66} נתונים והצפנות.

[רמז: השתמשו בסעיף א', התבוננו במבנים של 2^{64} נתונים ששווים בצד השמאלי שלהם, והשתמשו בטריק שראינו בפתרון תרגיל 2 שאלה 4].

ג. (*) מצאו תקיפה על 6 שלבי DEAL שדורשת לכל היותר 2^{70} נתונים ו- 2^{126} הצפנות.

ד. מצאו תכונה דיפרנציאלית בלתי אפשרית של מספר גדול ככל הניתן של שלבי DES. [שימו לב שפונקציית הסיבוב F של DES אינה הפיכה.]

4. שאלה זו והבאה אחריה עוסקות בקריפטאנאליזה לינארית.

א. כתבו תכנית (באיזה שפת תכנות שתרצו) שמחשבת את טבלת הקירובים הלינאריים (linear approximation table) של הטבלה S_k של DES, כאשר k הספרה האחרונה בתעודת הזהות שלכם מודולו 8. מצאו את ההטיה הגדולה ביותר של מעבר לינארי $a \to b$ דרך S_k ובדקו עבור כמה זוגות (a, b) היא מתקבלת.

ב. (*) מצאו תכונה לינארית איטרטיבית של שני שלבי DES (לא זאת שראינו בשיעור). השתדלו שהטייית התכונה תהיה גבוהה ככל הניתן. כמה שלבי DES אפשר לתקוף בעזרת התכונה שמצאתם?

ג. השתמשו בתכונה לינארית כרצונכם (אפשר לקחת מהאינטרנט) כדי להציע תקיפה על 6 שלבי DES.

5. התבוננו בצופן CTC שתיאורו מופיע בקישור הבא:
http://drops.dagstuhl.de/volltexte/2007/1013/pdf/07021.CourtoisNicolas.Paper.1013.pdf
(בעיקר סעיפים 2,7,13 בפרק 3). נתמקד בגרסת 255 ביטים של הצופן (הכוללת 85 טבלאות בכל שלב). מפתח הצופן טען שהוא בטוח כנגד תקיפות סטנדרטיות. מצאו תקיפה ששוברת מספר רב ככל הניתן של שלבים בסיבוכיות שלא עולה על 2^{30} נתונים והצפנות.
[רמז: מצאו תכונה לינארית איטרטיבית עם הטייה גדולה. אפשר לתקוף אפילו 14 שלבים!]

6. שאלה זו עוסקת בקריפטאנאליזה דיפרנציאלית-לינארית.

א. נתבונן בצופן בן שישה שלבים. נסמן את ערכי הביניים לאחר שלושה שלבי הצפנה ב X. נניח שקיימת תכונה דיפרנציאלית של שלושת השלבים הראשונים שמבטיחה שאם שני קלטים P, P' מקיימים $P + P' = a$ אז ערכי הביניים המתאימים מקיימים $X + X' = b$ בהסתברות 1. כמו כן, נניח שקיימת תכונה לינארית של שלושת השלבים האחרונים שאומרת ש:

$\Pr[C_{15} + C_2 + C_0 = X_1 + X_3] = \frac{1}{2} + q$. נתבונן בזוג קלטים המקיים $P + P' = a$. חשבו את ההסתברות $\Pr[C_{15} + C_2 + C_0 = C'_{15} + C'_2 + C'_0]$.

ב. מצאו תקיפת זיהוי על הצופן מסעיף א'. כמה נתונים דורשת התקיפה? (תקיפה מסוג זה נקראת תקיפה דיפרנציאלית-לינארית).

ג. הכלילו את טענת סעיף א' ותוצאת סעיף ב' למקרה בו התכונה הדיפרנציאלית מתקיימת רק בהסתברות p וחוזה את ההפרש $X + X'$ לא בכל הבלוק אלא רק בביטים 1,3 (ההפרש בביטים האחרים נותר לא ידוע). כמה נתונים דורשת התקיפה כעת?

ד. נתבונן ב 8 שלבי DES. תקפו גרסה זו של DES באמצעות תקיפה דיפרנציאלית, תקיפה לינארית, ותקיפה דיפרנציאלית-לינארית. מהי התקיפה הטובה ביותר שקיבלתם?

בהצלחה!