בס"ד

קריפטאנאליזה של מערכות הצפנה סימטריות – תרגיל בית מס' 4

להגשה: 17.6.15

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 במערכת אבן-מנסור (Even-Mansour) בעלת שלושה שלבים. כלומר, $E(P) = K_4 + F(K_3 + F(K_2 + F(K_1 + P)))$, כאשר F פונקציה **ידועה** ו- K_1, K_2, K_3, K_4 מפתחות בלתי תלויים. נניח שאורך הבלוק והאורך של כל מפתח הם n ביטים.

   א. מצאו תקיפה על המערכת שדורשת 2^{2n} זמן, 2^n זכרון ו- 4 זוגות קלט/פלט בלבד.

   ב. מצאו תקיפה על המערכת שדורשת $2^{1.5n}$ זמן, $2^{1.5n}$ זכרון ו- $2^{0.5n}$ נתונים (מסוג chosen plaintext).

   [רמז: ראשית, "פרקו" את פעולת הוספת המפתח K_1 לשתי פעולות, שבכל אחת מהן מוסיפים מפתח בגודל n/2 ביטים. כעת, השתמשו בשיטת splice-and-cut, כאשר "נקודת החיתוך" נמצאת בין שתי פעולות הוספת המפתח שהגדרתם.]

2. שאלה זו עוסקת בצופן DEAL. זהו צופן פייסטל בן 8 שלבים, עם בלוק באורך 128 ביטים ומפתח באורך 256 ביטים, בו פונקציית השלב היא הצפנת DES מלאה. פרטים נוספים על מבנה הצופן ניתן למצוא בוויקיפדיה. אנחנו נניח לשם הפשטות שמפתחות הסיבוב הינם באורך 56 ביטים כל אחד (כמו ב DEAL האמיתי) **והינם בלתי תלוים** (לא כמו בצופן האמיתי).

   א. מצאו תקיפה על 7 שלבי DEAL שדורשת לכל היותר 2^{170} הצפנות ו- 2^{170} זכרון.

   ב. מצאו תקיפה על 7 שלבי DEAL שדורשת לכל היותר 2^{242} הצפנות ו- 2^{114} זכרון.

   [רמז: השתמשו ב dissection].

   ג. (*)מצאו תקיפה על 7 שלבי DEAL שדורשת לכל היותר 2^{170} הצפנות ו- 2^{114} זכרון.

   ד. מצאו תקיפה על DEAL המלא (8 שלבים) שדורשת לכל היותר 2^{200} הצפנות ו- 2^{200} זכרון.

[רמז: השתמשו ברעיון של שאלה 1.]

ה. (*) מצאו תקיפה על DEAL המלא (8 שלבים) שדורשת לכל היותר 2^{200} הצפנות ו- 2^{150} זכרון.

3. שאלה זו עוסקת בצופן IDEA. ניתן למצוא את תיאור המבנה שלו בוויקיפדיה ובמסמכים אליהם וויקיפדיה מפנה. בצופן IDEA יש 8.5 שלבים, כאשר כל שלב מורכב מהוספת מפתח (בקסור או בחיבור מודולרי) וממבנה מסובך שנקרא MA. הדבר החשוב הוא **אלגוריתם בניית מפתחי הסיבוב:** כל מפתחות הסיבוב הם רצפי ביטים מתוך המפתח המקורי (מצאו באינטרנט את הטבלה המדויקת של הביטים שנלקחים בכל סיבוב).

נתבונן בגרסה חלקית של 4.5 שלבי IDEA שמתחילה **בתחילת השלב הרביעי** ומסתיימת **באמצע השלב השמיני**. מצאו תקיפה על גרסה זו שדורשת לכל היותר 2^{110} הצפנות. השתדלו שסיבוכיות הזכרון והנתונים תהיה קטנה ככל הניתן. (אפשרי ששתיהן יהיו פרקטיות).

4. שאלה זו והבאות אחריה עוסקות בקריפטאנאליזה דיפרנציאלית.

א. כתבו תכנית (באיזה שפת תכנות שתרצו) שמחשבת את טבלת ההתפלגות הדיפרנציאלית של הטבלה S_k של DES, כאשר k הספרה האחרונה בתעודת הזהות שלכם מודולו 8. מצאו את ההסתברות הגבוהה ביותר של מעבר דיפרנציאלי $a \to b$ דרך S_k ובדקו עבור כמה זוגות (a, b) היא מתקבלת.

ב. מצאו תכונה דיפרנציאלית איטרטיבית של שני שלבי DES (לא זאת שנראה בשיעור הקרוב). השתדלו שהסתברות התכונה תהיה גבוהה ככל הניתן. כמה שלבי DES אפשר לתקוף בעזרת התכונה שמצאתם?

ג. מצאו תכונה דיפרנציאלית של 5 שלבי DES עם הסתברות גבוהה ככל הניתן. [יש תכונה עם הסתברות גבוהה יותר מזאת שנראה בשיעור].

ד. השתמשו בתכונה שמצאתם (או בתכונה שנראה בשיעור אם לא פתרתם את ג') כדי להציע תקיפה על 6 שלבי DES.

5. שאלה זו עוסקת ב AES.

א. מצאו תכונה דיפרנציאלית של שלושה שלבי AES עם הסתברות $p \geq 2^{-63}$. [עדיף שתכתבו בעצמכם תכנית שמחשבת את טבלת ההתפלגות הדיפרנציאלית של SubBytes, אבל אתם יכולים גם לקחת מהאינטרנט.]

ב. השתמשו בתכונה שמצאתם כדי להציע תקיפה דיפרנציאלית על ארבעה שלבי AES בסיבוכיות קטנה מ 2^{80}.

[רמז: במקום לנחש את כל מפתח הסיבוב האחרון בבת אחת, נחשו בכל פעם בית אחד של המפתח ובדקו האם התחזית של הדיפרנציאל בבית מסוים מתקיימת, וכך תקטינו בכל פעם את כמות הזוגות שצריך לעבור עליהם.]

6. שאלה זו עוסקת בתכונות דיפרנציאליות איטרטיביות.

א. נניח שבצופן דמוי-DES, קיימת תכונה דיפרנציאלית $a \to 0$ של פונקציית השלב F שמתקיים בהסתברות p. מצאו תכונה דיפרנציאלית איטרטיבית טובה ככל הניתן של שני שלבי הצופן. כמה גבוהה צריכה להיות ההסתברות p כדי שניתן יהיה לתקוף בעזרת התכונה 16 שלבים של הצופן?

ב. נניח שבצופן דמוי-DES, קיימת תכונה דיפרנציאלית איטרטיבית $a \to a$ של פונקציית השלב F שמתקיימת בהסתברות p. מצאו תכונה דיפרנציאלית איטרטיבית טובה ככל הניתן של שלושה שלבי הצופן. כמה גבוהה צריכה להיות ההסתברות p כדי שניתן יהיה לתקוף בעזרת התכונה 16 שלבים של הצופן?

בהצלחה!