

קריפטאנליזה של מערכות הצפנה סימטריות – תרגיל בית מס' 4

להגשה: 17.6.15

זהו החלק הראשון של התרגיל. בעוד שבוע יעלה במקומו התרגיל המלא (שיכלול גם את החלק הזה וגם את החלק השני). 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 תלויים (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).

בהצלחה!