

קריפטאנליזה של מערכות הצפנה סימטריות – תרגיל בית מס' 3

להגשה: 27.5.15

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 עוסקת בצופן השטף RC4. השאלה כוללת רכיב **תכנות** ולכן היא רשות למי שאינו יודע לתכנת.

א. מצאו **תקיפת זיהוי** על מחרוזת הפלט של RC4 שדורשת פחות מ 2^{20} נתונים וזמן.

[הדרכה: כתבו תכנית שמחשבת את מחרוזת הפלט בהינתן המפתח הסודי. כעת, נסו אפשרויות שונות של המפתח וחשבו סטטיסטיקה על הפלט, למשל: באיזה חלק מהמקרים הבית הראשון של הפלט שווה ל-0, וכד'. כדי שיקל עליכם לזהות, כדאי לעשות סטטיסטיקה על הרבה מקרים, לפחות כמה אלפים].

ב. מה ניתן לעשות כדי להתגונן מפני תקיפת זיהוי זו?

ג. (***) מצאו תקיפת זיהוי אחרת שההגנה שתיארתם בסעיף ב' לא יעילה נגדה.

2. מצאו תקיפת מפגש באמצע על **שלושה** שלבי AES, שדורשת פחות מ-10 נתונים ולכל היותר 2^{45} הצפנות.

3. שאלה זו עוסקת בתקיפות מפגש באמצע על DES.

א. מצאו תקיפת מפגש באמצע על **ארבעה** שלבי DES, שדורשת פחות מ-10 נתונים ולכל היותר 2^{40} הצפנות.

ב. (***) מצאו תקיפת מפגש באמצע על **חמישה** שלבי DES, שדורשת פחות מ-10 נתונים ולכל היותר 2^{50} הצפנות.

ג. (***) מצאו תקיפת מפגש באמצע על **שישה** שלבי AES, שדורשת פחות מ-10 נתונים ולכל היותר 2^{53} הצפנות.

4. שאלה זו עוסקת בצופן GOST, סטנדרט הצפנה של רוסיה. את מבנה הצופן ניתן למצוא בוויקיפדיה.

א. נתבונן ב**שמונה** השלבים הראשונים של הצופן (עם סדרת המפתחות (K_1, K_2, \dots, K_8)). מצאו תקיפה על גרסה זו שדורשת **שני** זוגות קלט/פלט בלבד

ובערך 2^{128} הצפנות. הסבירו למה תקיפה זו היא **אופטימלית**, במובן זה שכל תקיפה עם שני נתונים על גרסה זו חייבת לדרוש 2^{128} הצפנות לפחות.

ב. מצאו דרך להוריד את סיבוכיות הזיכרון של התקיפה שהצעתם בסעיף א' ל- 2^{64} .

ג. נתבונן ב- **16** השלבים הראשונים של GOST (עם סדרת המפתחות $(K_1, K_2, \dots, K_8, K_1, K_2, \dots, K_8)$). מצאו תקיפה על גרסה זו שדורשת **זוג קלט/פלט אחד** בלבד ובערך 2^{192} הצפנות. הסבירו למה תקיפה זו היא **אופטימלית**, במובן זה שכל תקיפה עם נתון בודד על גרסה זו חייבת לדרוש 2^{192} הצפנות לפחות.

[רמז: השתמשו בשיטה שראיתם בשאלה 2 ג' בתרגיל מס' 2: במקום לנחש מפתח, נחשו ערך ביניים של ההצפנה, לאחר 8 שלבי הצפנה.]

ד. מצאו תקיפה על GOST המלא (כל 32 השלבים) שדורשת בערך 2^{32} נתונים ו- 2^{224} הצפנות.

[רמז: תחילה נסו "לבטל" את 16 השלבים האחרונים של ההצפנה בעזרת שיטה דומה לשאלה 3 בתרגיל מס' 2, ואחר כך השתמשו בסעיף ד' כדי לתקוף את 16 השלבים הנותרים.]

5. נתבונן בצופן דמוי DES בן **שבעה שלבים** בו אורך הבלוק הוא $n/2$ ביטים ואורך כל מפתח סיבוב הוא $n/2$ ביטים גם כן. מפתחות הסיבוב הינם בלתי תלויים, ופונקציית הסיבוב היא "חד כיוונית" (במובן זה שאפשר להפעיל אותה בקלות אם יודעים את מפתח הסיבוב ולא ניתן להפעיל אותה אם לא יודעים את כל מפתח הסיבוב).

א. מצאו תקיפת מפגש באמצע על הצופן שדורשת נתונים בודדים ובערך $2^{3n/2}$ זמן וזיכרון.

ב. מצאו תקיפת dissection על הצופן שדורשת נתונים בודדים, בערך 2^{2n} זמן ובערך 2^n זיכרון.

ג. (*) מצאו תקיפה על הצופן שדורשת נתונים בודדים, בערך $2^{3n/2}$ זמן ובערך 2^n זיכרון.

[רמז: נסו לשלב ביחד אלמנטים מהתקיפות של סעיפים א' וב'.]

6. שאלה זו עוסקת בצופן AES, וממשיכה את שאלה 6 מתרגיל 2. 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 בסדרת 256 הערכים המתקבלים בבית מסוים לאחר שלושה שלבים מלאים של הצפנה (מסודרים לפי סדר הערכים של הבית הלא-קבוע בקלט: תחילה הערך שמתאים ל-0 בבית הלא קבוע, אחר כך זה שמתאים ל-1, וכו'). נתייחס אל הסדרה כאל וקטור בינארי באורך $8 \cdot 256 = 2048$ ביטים. הוכיחו כי הווקטור הזה יכול לקבל לכל היותר 2^{72} ערכים אפשריים.
- [רמז: הוכיחו שאפשר להגדיר 9 משתנים בגודל בית כל אחד (שהינם תלויים במפתח הסודי ובערך הבתים הקבועים בקבוצת הקלטים), כך שאם יודעים את ערכי כל 9 המשתנים, יודעים את סדרת 256 הערכים במלואה].
- ב. (*) נתבונן בסדרת 256 הערכים המתקבלים בבית מסוים לאחר ארבעה שלבים מלאים של הצפנה. נתייחס אל הסדרה כאל וקטור בינארי באורך $8 \cdot 256 = 2048$ ביטים. הוכיחו כי הווקטור הזה יכול לקבל לכל היותר 2^{200} ערכים אפשריים.
- [רמז: הוכיחו שאפשר להגדיר 25 משתנים בגודל בית כל אחד (שהינם תלויים במפתח הסודי ובערך הבתים הקבועים בקבוצת הקלטים), כך שאם יודעים את ערכי כל 25 המשתנים, יודעים את סדרת 256 הערכים במלואה].
- ג. השתמשו בסעיף ב' כדי להציע תקיפה על 6 שלבי AES שדורשת כ- 2^{40} הצפנות ו- 2^{200} תאי זכרון. (כמובן שהתקיפה רלוונטית רק אם אורך המפתח הוא מעל 200 ביטים).
- ד. הציעו תקיפה על 8 שלבי AES שדורשת 2^{210} הצפנות לכל היותר.
- [רמז: הוסיפו שני שלבים לתקיפה של סעיף ג', בדומה לשאלה 6 בתרגיל 2].
- ה. (***) שפרו את התקיפה על 8 שלבי AES כך שהיא תדרוש פחות מ- 2^{180} הצפנות.

בהצלחה!