11.5.2015

קריפטוגרפיה: תרגיל 1

הגשה: יום ד' 18.11.15 בשעה 14:10 בהרצאה. ההגשה בזוגות או ביחידים.

שאלה 1

ההודעה crypto הוצפנה לקריפטוגרמה RJZJNH ע"י צופן Hill כאשר המפתח הוא מטריצה 2×2.

סעיף א

מצאו את מפתח ההצפנה. יש להראות את החישובים שבצעתם.

סעיף ב

הסבירו מדוע המפתח הוא אכן מטריצה 2×2.

שאלה 2

היזכרו בהגדרת הבטיחות שניתנה בכיתה עבור מערכת הצפנה $\pi = (\text{Gen}, \text{Enc}, \text{Dec})$.

משחק הבחנה א:

1. המצפין מחשב $K \leftarrow \text{Gen}$.
2. היריב $\mathcal{A}$ פולט זוג מסרים m_0, m_1 ממרחב המסרים של מערכת ההצפנה.
3. המצפין מגריל בהתפלגות אחידה $b \in \{0,1\}$, ומחשב $c \leftarrow \text{Enc}(m_b, K)$.
4. היריב $\mathcal{A}$ מקבל את הקריפטוגרמה c ופולט $\hat{b} \in \{0,1\}$. היריב $\mathcal{A}$ מנצח אם $\hat{b} = b$.

הגדרה א:

מערכת π היא בטוחה אם לכל יריב הסתברותי $\mathcal{A}$

$$\Pr\left[\begin{matrix}\text{מנצח } \mathcal{A} \\ \text{במשחק א}\end{matrix}\right] = \frac{1}{2}.$$

סעיף א

סטודנט בקורס טען שאפשר לפשט את משחק ההבחנה באופן הבא:
במקום לאפשר ליריב לבחור זוג מסרים m_0, m_1, נאפשר לו לבחור רק מסר אחד m. על מנת לנצח במשחק היריב יידרש להבחין בין הצפנה של m לבין הצפנה של 1 (הניחו כי 1 נמצא במרחב המסרים של המערכת). באופן פורמלי:

משחק הבחנה ב:

1. המצפין מחשב $K \leftarrow \text{Gen}$.
2. היריב $\mathcal{B}$ פולט מסר m ממרחב המסרים של מערכת ההצפנה.
3. המצפין מגריל בהתפלגות אחידה $b \in \{0,1\}$.
   אם $b = 0$ אז מחשבים קריפטוגרמה $c \leftarrow \text{Enc}(m, K)$.
   אם $b = 1$ אז מחשבים קריפטוגרמה $c \leftarrow \text{Enc}(1, K)$.
4. היריב $\mathcal{B}$ מקבל את הקריפטוגרמה c ופולט $\hat{b} \in \{0,1\}$. היריב $\mathcal{B}$ מנצח אם $\hat{b} = b$.

הגדרה ב:

מערכת π היא בטוחה אם לכל יריב הסתברותי $\mathcal{B}$

$$\Pr\left[\begin{matrix}\text{מנצח } \mathcal{B} \\ \text{במשחק ב}\end{matrix}\right] = \frac{1}{2}.$$

הוכיחו כי אם π אינה בטוחה לפי הגדרה ב אזי π אינה בטוחה לפי הגדרה א.
הדרכה: הניחו כי קיים יריב $\mathcal{B}$ המנצח במשחק ב בהסת' $> \frac{1}{2}$ והראו בעזרתו יריב $\mathcal{A}$ למשחק א.

סעיף ב

סטודנט אחר בקורס טען שאפשר לפשט עוד יותר את משחק ההבחנה:
לא נאפשר ליריב לבחור מסרים כלל, ועל מנת לנצח במשחק היריב יידרש להבחין בין הצפנה של 1 לבין הצפנה של 2 (הניחו כי 1 ו- 2 נמצאים במרחב המסרים של המערכת). באופן פורמלי:

משחק הבחנה ג:

1. המצפין מחשב $K \leftarrow \text{Gen}$.
2. המצפין מגריל בהתפלגות אחידה $b \in \{0,1\}$.
   אם $b = 0$ אז מחשבים קריפטוגרמה $c \leftarrow \text{Enc}(1, K)$.
   אם $b = 1$ אז מחשבים קריפטוגרמה $c \leftarrow \text{Enc}(2, K)$.
3. היריב $\mathcal{B}$ מקבל את הקריפטוגרמה c ופולט $\hat{b} \in \{0,1\}$. היריב $\mathcal{B}$ מנצח אם $\hat{b} = b$.

הגדרה ג:

מערכת π היא בטוחה אם לכל יריב הסתברותי $\mathcal{B}$

$$\Pr\left[\begin{matrix}\mathcal{B}\text{ מנצח}\\ \text{במשחק ג}\end{matrix}\right] = \frac{1}{2}.$$

הראו כי קיימת מערכת הצפנה אשר בטוחה לפי הגדרה ג <u>ולא</u> בטוחה לפי הגדרה א.
<u>רמז</u>: ניתן להתחיל ממערכת הצפנה הבטוחה לפי הגדרה א ולשנות אותה בהתאם.

שאלה 3

נתונה מערכת הצפנה $\pi = (Gen, Enc, Dec)$ כך <u>שכל</u> יריב מנצח במשחק ההבחנה א מול π בהסתברות בדיוק $1/2$. הוכיחו כי ל- π יש בטיחות מושלמת.

שאלה 4

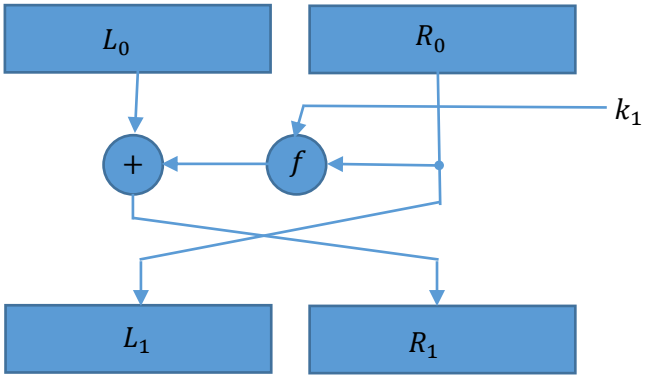
בשאלה זו תראו מתקפה על גרסה מוחלשת של DES המבצעת רק סיבוב אחד (במקום 16 סיבובים). לשם פשטות, נניח כי לא מתבצעים את הפרמוטציות IP ו- IP^{-1} בתחילת ובסוף התהליך. כלומר, עבור הודעה $x = L_0R_0$ באורך 64 ביטים ועבור מפתח k_1 באורך 48 ביטים מקבלים הצפנה

$$y = L_1R_1$$

כאשר

$$L_1 = R_0$$
$$R_1 = L_0 \oplus f(R_0, k_1)$$

וכאשר f היא הפונקצייה שהוגדרה בכיתה עבור מערכת DES.
בציור:



הראו מתקפת known plaintext אשר בהינתן זוג הודעה וצופן (x, y) מזהה קבוצה של 2^{16} מפתחות אפשריים כך שאחד מהם הוא המפתח הנכון.