עמוס ביימל

14.5.01

קריפטוגרפיה – תרגיל 5

הגשה ביום שני ה-4.6.01 בהרצאה.

שאלה 1 (שיטת החידות של מרקל)
תהי $f : \{1,\ldots,N^2\} \to \{1,\ldots,N^2\}$ פונקציה חד-כיוונית, שבנוסף היא חד-חד ערכית. נתאר שיטה להחלפת מפתחות בין אליס לבוב:

אליס: מגרילה באופן אחיד ובלתי תלוי N מפתחות $K_1,\ldots,K_N$ מהתחום $\{1,\ldots,N^2\}$, ושולחת לבוב את $f(K_1),\ldots,f(K_N)$.

בוב: מגריל מפתחות מ-$\{1,\ldots,N^2\}$ עד שהוא מוצא מפתח K כך ש- $f(K)$ נמצא ברשימה שאליס שלחה לו, ושולח לאליס את $f(K)$.

K הוא המפתח המשותף שאליס ובוב בוחרים.

1. הסבירו כיצד אליס יודעת מהו המפתח K.
2. הוכיחו כי בוב צריך לבחור $O(N)$ מפתחות כדי שימצא מפתח משותף בהסתברות לפחות $1/2$.
3. כמה מפתחות בממוצע צריך מאזין לבחור כדי שימצא את המפתח המשותף?

שאלה 2

בשאלה זו נתאר שלוש הצעות לפונקציות HASH קריפטוגרפיות. תהי G, E, D מערכת הצפנה עם מפתח פרטי, כאשר $|M| = |K| = |C|$. תהי $m = m_1 \circ m_1 \circ \ldots \circ m_k$ הודעה, ו-g_k הוא תוצאת ה-HASH. הוכיחו כי שלוש השיטות הבאות אינן אמינות, כלומר יש למצוא שתי הודעות באותו אורך שהפלט עליהן שווה.

1.

$$\begin{aligned} g_1 &= E(m_1, m_1) \\ g_2 &= E(m_2, g_1) \\ &\vdots \\ g_k &= E(m_k, g_{k-1}) \end{aligned}$$

2.

$$\begin{aligned} g_1 &= E(m_1, m_k) \\ g_2 &= E(m_2, g_1) \\ &\vdots \\ g_k &= E(m_k, g_{k-1}) \end{aligned}$$

3. תהי $p(m)$ פונקציה המחזירה את 56 הביטים הראשונים של m.

$$\begin{aligned} g_1 &= DES(m_1, p(m_1)) \oplus m_1 \\ g_2 &= DES(m_2, p(g_1)) \oplus m_2 \\ &\vdots \\ g_k &= DES(m_k, p(g_{k-1})) \oplus m_k \end{aligned}$$

רמז: השתמשו בתכונת ההשלמה של DES שתוארה בתרגיל 2 שאלה 1.

שאלה 3

תהי $f : \{0,1\}^n \to \{0,1\}^n$ פונקציה חד-כיוונית, שבנוסף היא חד-חד ערכית. הוכיחו עבור כל אחת מהפונקציות הבאות אם היא חד-כיונית או לא.

$$\begin{aligned} g_1(x) &\stackrel{\text{def}}{=} f(f(x)) \\ g_2(x_1, x_2) &\stackrel{\text{def}}{=} f(x_1), f(x_2) \\ g_3(x_1, x_2) &\stackrel{\text{def}}{=} f(x_1) \oplus x_2 \end{aligned}$$

הערה: פונקציה אחת אינה חד-כיונית.

שאלה 4

תהי $f : \{0,1\}^n \to \{0,1\}^n$ פונקציה חד-כיוונית, שבנוסף היא חד-חד ערכית. נסמן $m = 2n$.

1. נגדיר את הפונקציה $g : \{0,1\}^m \to \{0,1\}^m$ הבאה: בהינתן קלט x, y נאתחל $y_0 = y$ ו- $x_0 = x$ ועבור $0 \leq i$ נחשב $y_{i+1} = x_i \oplus f(y_i)$ ו- $x_{i+1} = y_i$. הפלט של g על קלט x, y הוא x_{16}, y_{16}. האם g היא פונקציה חד-כיונית?
2. נגדיר את הפונקציה $h : \{0,1\}^m \to \{0,1\}^m$ הבאה: בהינתן קלט x, y נאתחל $y_0 = y$ ו- $x_0 = x$ ועבור $0 \leq i$ נחשב $y_{i+1} = y_i \oplus f(x_i)$ ו- $x_{i+1} = y_i$. הפלט של h על קלט x, y הוא x_2, y_2. האם h היא פונקציה חד-כיונית?

<u>הנחיות לשתי השאלות האחרונות:</u>

1. כדי להוכיח שפונקציה g היא חד-כיונית יש להראות כי אם יש אלגוריתם המחשב את g^{-1} אזי יש אלגוריתם המחשב את f^{-1}.
2. כדי להוכיח שפונקציה g אינה חד-כיונית יש להראות אלגוריתם המחשב את g^{-1}.