עמוס ביימל 26.5.03

קריפטוגרפיה: תרגיל 5

הגשה: יום ב' 9/6/03 ב- 18:00 בהרצאה.

שאלה 1

להזכירכם, במערכת החתימה RSA המפתח הפרטי הוא (N,d) והמפתח הציבורי הוא (N,e) כאשר N הוא מכפלה של שני ראשוניים גדולים ו- $ed \equiv 1(\bmod \varphi(N))$. החתימה על מסמך $M \in \mathbf{Z}_N$ היא $M^d \bmod N$. כפי שראינו בכיתה מערכת זו אינה עמידה להתקפת הודעה נבחרת בגלל התכונה הכיפלית של RSA (כלומר, $((M_1)^d (M_2)^d \equiv (M_1 M_2)^d (\bmod N)$). כדי להתגבר על תכונה זו הוצא לחתום על מסמך M על ידי $(M+1)^d \bmod N$.

סעיף א

איך מוודאים בצורה יעילה שחתימה היא חוקית?

סעיף ב

מערכת זאת אינה עמידה כנגד התקפת הודעה נבחרת. בהינתן מסמך M, מתקיף מגריל $M_1 \in \mathbf{Z}_N^*$ בהתפלגות אחידה, מחשב $M_2 \leftarrow (M+1)(M_1)^{-1} \bmod N$ ומבקש מהחותם החוקי לחתום על $M_1 - 1$ ועל $M_2 - 1$. הראו איך המתקיף יכול בצורה יעילה לחשב חתימה על M.

סעיף ג

הראו איך מתקיף יכול בצורה יעילה לחתום על מסמך נתון M בעזרת בקשה מהחותם החוקי לחתום על הודעה אקראית אחת.

שאלה 2

סעיף א

בשאלה זו נסתכל על מערכת החתימה של ElGamal כאשר מפתח הוידוא הוא (p,g,B). תהיינה m_2, m_1 הודעות ו- (γ_1,δ_1) , (γ_2,δ_2) חתימות על m_2, m_1 בהתאמה. איב הצליחה לחשב a כך ש- $\gamma_1 \equiv g^a \gamma_2 (\bmod p)$. הראו איך איב יכולה לחשב בצורה יעילה את מפתח החתימה הפרטי מתוך $\gamma_1, \delta_1, \gamma_2, \delta_2, m_1, m_2, p, g$ ו- a.

הערה: הניחו של- $(\gamma_1\delta_2 - \gamma_2\delta_1)$ קיים הופכי מודולו p-1.

סעיף ב

נתון כי בוב חתם על שתי הודעות בשיטת ElGamal כאשר בשני המקרים השתמש באותו מפתח פרטי ובאותו k. הראו איך איב יכולה לחשב בצורה יעילה את מפתח החתימה הפרטי מתוך שתי ההודעות, שתי החתימות והמפתח הציבורי.

שאלה 3

בשאלה זו נראה כי יש לבחור בזהירות את מפתח החתימה במערכת החתימה של ElGamal. יהי p ראשוני ו- w שלם כך ש- $p=2w+1$. נניח כי 2 ו- w הם יוצרים של $\mathbb{Z}_p^*$ (לדוגמא, 2 ו- 6 הם יוצרים של $\mathbb{Z}_{13}^*$).

סעיף א

הראו כי לכל $x \in \mathbb{Z}_p^*$ מתקיים $x^w \equiv 1 \pmod p$ או $x^w \equiv -1 \pmod p$ ו- $w^{w-1} \equiv 2 \pmod p$.

סעיף ב

יהי $(p,2,B)$ מפתח ציבורי במערכת החתימה של ElGamal. הראו איך למצוא ביעילות z כך ש- $2^{wz} \equiv B^w \pmod p$.

סעיף ג

יהי $m \in \mathbb{Z}_p^*$ מסמך כלשהו. נגדיר $\delta \leftarrow (w-1)(m-wz) \bmod (p-1)$ כאשר z הוא הערך שחושב בסעיף ד. הוכיחו כי (w,δ) היא חתימה חוקית על m.

שאלה 4

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-כיוונית או לא.

1. $g_1(x) = f(f(x))$
2. $g_2(x_1,x_2) = f(x_1), f(x_2)$
3. $g_3(x_1,x_2) = f(x_1) \oplus x_2$

<u>הערה</u>: פונקציה אחת אינה חד-כיוונית.

שאלה 5

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

סעיף א

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 $i \ge 0$ 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-כיוונית?

סעיף ב

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 $i \ge 0$ 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-כיוונית?

<u>הנחיות לשתי השאלות האחרונות</u>:

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