2/1/13

קריפטוגרפיה: תרגיל 5

הגשה: יום ד' 16.1.13 ב- 16:10 בשיעור.

שאלה 1

סעיף א

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

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 2

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 $x^w \equiv -1 \pmod p$.

סעיף ב

הראו כי $w^{w-1} \equiv 2 \pmod p$.

סעיף ג

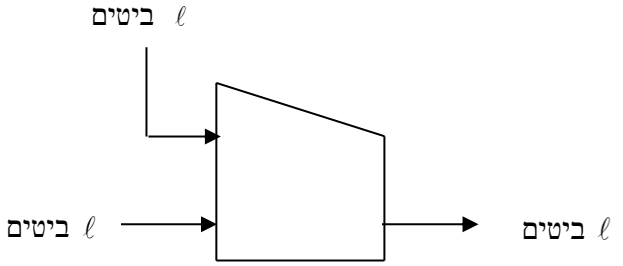
מתקיף מחזיק במפתח ציבורי $(p,2,B)$ של מערכת החתימה של ElGamal. הראו איך במתקיף יכול לחשב ביעילות z כך ש- $2^{wz} \equiv B^w \pmod p$.

סעיף ד

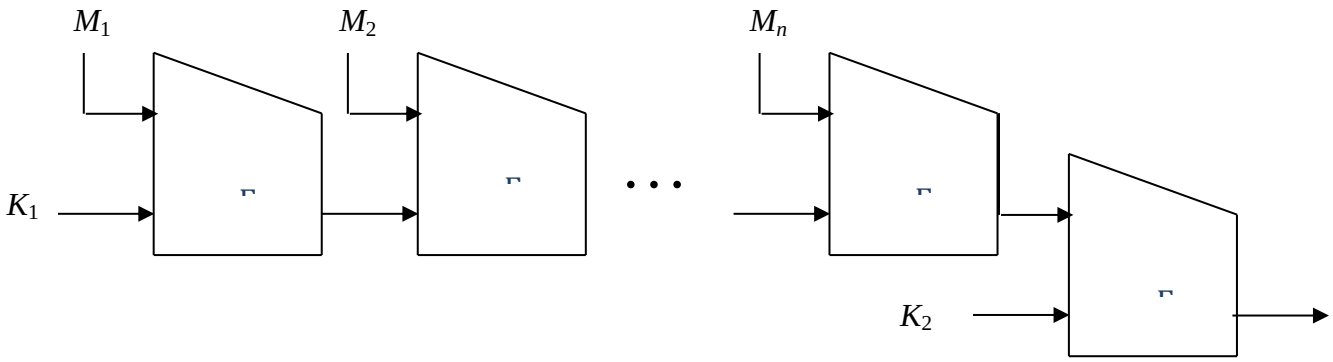
יהי $m \in \mathbb{z}_p^*$ מסמך כלשהו. נגדיר $\delta \leftarrow (w-1)(m-wz) \mod (p-1)$ כאשר z הוא הערך שחושב בסעיף ד. הוכיחו כי (w,δ) היא חתימה חוקית על m עבור המפתח הציבורי $(p,2,B)$.

שאלה 3

בשאלה זו נדון במערכת האותנטיקציה NMAC הבאה (שתוארה בהרצאות). המערכת משתמשת בפונקציית דחיסה $F: \{0,1\}^\ell \times \{0,1\}^\ell \to \{0,1\}^\ell$ המתוארת בציור הבא:



נניח כי לכל $k \in \{0,1\}^{\ell}$ הפונקציה $F(M,k)$, כפונקציה של M, היא פונקציה חד-חד ערכית ועל. הודעה מורכבת ממספר כלשהו של בלוקים, כל אחד באורך ℓ בדיוק. לחשב אותנטיקציה של הודעה המורכבת מ- n בלוקים, כל אחד עם ℓ ביטים, משתמשים ב- $n+1$ פונקציות דחיסה ובמפתח $\langle k_1, k_2 \rangle$ עם 2ℓ ביטים, עפ"י המתואר בציור הבא:



כלומר נגדיר $y_0 = k_1$ ו- $y_i \leftarrow F(M_i, y_{i-1})$ והפלט הוא: $\text{NMAC}((M_1, \ldots, M_n), (k_1, k_2)) = F(y_n, k_2)$. שימו לב כי לא משרשרים את אורך ההודעה בבלוק האחרון. בשאלה זו נראה מדוע ℓ צריך להיות גדול.

סעיף א

עבור NMAC עם מפתח $\langle k_1, k_2 \rangle$ ו- $n=2$, זוג הודעות $\langle M_1, M_2 \rangle$ ן- $\langle M'_1, M'_2 \rangle$ מתנגשות אם

$$\text{NMAC}(\langle M_1, M_2 \rangle, \langle k_1, k_2 \rangle) = \text{NMAC}(\langle M'_1, M'_2 \rangle, \langle k_1, k_2 \rangle)$$.

הוכיחו כי אם $\langle M_1, M_2 \rangle$ ו- $\langle M'_1, M'_2 \rangle$ מתנגשות אזי $F(M_2, F(M_1, k_1)) = F(M'_2, F(M'_1, k_1))$.

סעיף ב

כמה הודעות עם שני בלוקים יש להגריל מתוך $\{0,1\}^{2\ell}$ כך שבהסתברות לפחות 3/4 נקבל התנגשות?

סעיף ג

הוכיחו כי אם $F(M_2, F(M_1, k_1)) = F(M'_2, F(M'_1, k_1))$ אזי לכל M_3 מתקיים

$$\text{NMAC}(\langle M_1, M_2, M_3 \rangle, \langle k_1, k_2 \rangle) = \text{NMAC}(\langle M'_1, M'_2, M_3 \rangle, \langle k_1, k_2 \rangle)$$.

סעיף ד

נסמן ב- S את המספר שחישבתם בסעיף ב. הראו איך אפשר לשבור את NMAC ע"י $O(S)$ הודעות, כלומר השובר יכול לבקש אותנטיקציה של $O(S)$ מסמכים כרצונו ואח"כ למצוא בהסתברות 3/4 הודעה ואותנטיקציה חוקית שלה (כאשר ההודעה אינה אחת מההודעות שעליהם קיבל אותנטיקציה).

שאלה 4

נסתכל על מערכת האותנטיקציה הבאה:

- יצירת המפתחות: יהי p ראשוני גדול. המפתח הוא שני איברים $a,b \in \mathbf{Z}_p$ המוגרלים בהתפלגות אחידה ובאופן בלתי תלוי.
- האותנטיקציה של הודעה $x \in \mathbf{Z}_p$ היא $\text{AUTH}(x,(a,b)) = (ax+b) \bmod p$.

סעיף א

הראו כי איב היכולה לבקש אותנטיקציה של הודעה אחת $x \in \mathbf{Z}_p$ (אך אינה יודעת מהו המפתח), אינה יכולה לייצר בהסתברות גדולה מ- $1/p$ זוג $y, z \in \mathbf{Z}_p$ כך ש- $\boldsymbol{y \neq x}$ ו- $z = \mathrm{AUTH}(y,(a,b))$.

סעיף ב

הראו כי איב הרואה אותנטיקציה של שתי הודעות $x, x' \in \mathbf{Z}_p$ כך ש- $\boldsymbol{x \neq x'}$ (אך אינה יודעת מהו המפתח) יכולה לחשב את המפתח בצורה יעילה.

סעיף ג

בנו מערכת אותנטיקציה בה איב היכולה לבקש אותנטיקציה של t הודעות (אך אינה יודעת מהו המפתח) אינה יכולה לייצר בהסתברות גדולה מ- $1/p$ זוג $y, z \in \mathbf{Z}_p$ כך ש- y שונה מההודעות שאיב ביקשה ו- $\boldsymbol{z = AUTH(y,k)}$. הוכיחו בנייתכם.