19/12/2013

קריפטוגרפיה: תרגיל 4

הגשה: יום ד' 1.1.14 ב- 14:10 בשיעור.

שאלה 1

תהי (Gen,E,D) מערכת הצפנה בטוחה כמו שהוגדרה בכיתה. נניח שאלגוריתם Gen מקבל קלט 1^n, יוצר מפתח ציבורי PK ופרטי SK, כל אחד עם n ביטים, כך שבעזרת PK מצפינים הודעות עם n ביטים.

סעיף א

תהי $\ell: \mathbb{N} \to \mathbb{N}$ פונקציה כך שהאלגוריתם ההצפנה האקראי E עם מפתח ציבורי והודעה, כל אחד עם n ביטים, משתמש ב $\ell(n)$ ביטים אקראיים כדי ליצר את הקריפטוגרמה. הודעה M הוצפנה על ידי אלגוריתם E לקריפטוגרמה C. הראו שמתקיף שמחזיק במפתח PK ובהודעה M (אבל אינו יודע מהו C) יכול בהסתברות לפחות $1/2^{\ell(n)}$ לנחש את C.

סעיף ב

הוכיחו במערכת הצפנה בטוחה כנגד התקפת הודעות נבחרות (Gen,E,D) מתקיים $c \log n \leq \ell(n)$ לכל קבוע $0 \leq c$.

שאלה 2

בכיתה הצגנו את הנחת הקושי של בעיית DDH בתת החבורה של השאריות הריבועיות עבור ראשוני בטוח. בשאלה זו תראו שהנחה דומה לא מתקיימת עבור החבורה $\mathbb{Z}_p^*$ עבור p ראשוני אקראי.

נגדיר את המשחק הבא:

(1) בחר באקראי ראשוני p בן n ביטים.

(2) בחר g יוצר של $\mathbb{Z}_p^*$.

(3) בחר באקראי $x, y \in \mathbb{Z}_{p-1}$ וחשב: $A = g^x \bmod p$, $B = g^y \bmod p$

(4) הגרל $d \in \{0,1\}$ באקראי.
אם $d = 1$ אזי חשב $C = g^{x \cdot y} \bmod p$.
אחרת הגרל $C \in \mathbb{Z}_p^*$ באקראי.

(5) היריב E מופעל על p, g, A, B, C ופולט ניחוש $\hat{d}$.
E מנצח אם $\hat{d} = d$.

הראו יריב E (אלג' הסתברותי פולינומיאלי ב n) כך ש

$$\Pr\left[\begin{matrix}\text{מנצח } E \\ \text{במשחק הנ"ל}\end{matrix}\right] \geq \frac{1}{2} + t$$

עבור $t > 0$ קבוע כלשהו.

שאלה 3

בשאלה זו תראו שבעיית הלוג הדיסקרטי ניתנת לרדוקציה אקראית. יהי p ראשוני ו- g יוצר של $\mathbb{Z}_p^*$.

סעיף א

הראו כי עבור $A, B, C \in \mathbb{Z}_p^*$ כך ש $C = A \cdot B$ מתקיים ש- $DL_g(C) = DL_g(A) + DL_g(B)$.

סעיף ב

i. הראו כי אם מגרילים $x \in \mathbb{Z}_{p-1}$ באקראי בהתפלגות אחידה, אזי $X = g^x \bmod p$ מתפלג אחיד ב $\mathbb{Z}_p^*$.

ii. נקבע $A \in \mathbb{Z}_p^*$ כלשהו. הראו כי אם מגרילים $y \in \mathbb{Z}_p^*$ באקראי בהתפלגות אחידה, אזי $z = y \cdot A \bmod p$ מתפלג אחיד ב $\mathbb{Z}_p^*$.

סעיף ג

הראו כי אם קיים אלגוריתם יעיל $\mathcal{A}$ שמוצא לוג דיסקרטי ל- $\frac{1}{2}$ מהאיברים ב- $\mathbb{Z}_p^*$, אזי קיים אלגוריתם אקראי יעיל $\mathcal{B}$ שמוצא לוג דיסקרטי לכל מספר ב- $\mathbb{Z}_p^*$ בהסתברות לפחות $\frac{1}{2}$.

כלומר, הראו אלג' $\mathcal{B}$ שבקלט p, g, A מוצא בהסתברות לפחות $\frac{1}{2}$ איבר a כך ש $A \equiv g^a \pmod p$.

שאלה 4

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- $\gamma_1 \equiv g^a \gamma_2 \pmod p$. הראו איך איב יכולה לחשב בצורה יעילה את מפתח החתימה הפרטי מתוך $p, g, m_1, m_2, \gamma_1, \delta_1, \gamma_2, \delta_2$ ו- a.

<u>הערה</u>: 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 5

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

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 ג

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.