21.12.2014

קריפטוגרפיה: תרגיל 4

<u>הגשה</u>: יום א' 4.1.15 לתא 78 בקומה 1 בניין 37 (שימו לב שרשום על התא "אורי שטמר"). ההגשה בזוגות או ביחידים.

שאלה 1

יהיו $p,q>2$ ראשוניים כך ש- 3 מחלק את $(p-1)$ ולא מחלק את $(q-1)$.

סעיף א

הוכיחו כי ל- 1 יש בדיוק 3 שורשים-שלישיים מודולו p. כלומר, הוכיחו כי למשוואה $x^3 \equiv 1 \pmod p$ ישנם בדיוק 3 פתרונות בתחום $\mathbb{Z}_p$.

סעיף ב

נתונים $a,b \in \mathbb{Z}_p^*$ כך ש- $b^3 \equiv a \pmod p$.
הוכיחו כי ל- a יש בדיוק 3 שורשים-שלישיים מודולו p.

סעיף ג

נתונים $a,b \in \mathbb{Z}_q^*$ כך ש- $b^3 \equiv a \pmod q$.
הוכיחו כי b הוא השורש-השלישי היחיד של a מודולו q.

סעיף ד

נסמן $N=pq$.
נתונים $a,b \in \mathbb{Z}_N^*$ כך ש- $b^3 \equiv a \pmod N$.
הוכיחו כי ל- a יש בדיוק 3 שורשים-שלישיים מודולו N.

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.

סעיף א

יהי $p>2$ ראשוני, g יוצר של $\mathbb{Z}_p^*$ ו- $A \in \mathbb{Z}_p^*$. הראו כי ניתן לחשב ביעילות את ה LSB של $\mathrm{DL}_g(A)$.

סעיף ב

<u>נגדיר את המשחק הבא:</u>

(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: $A = g^x \bmod p \quad , \quad B = g^y \bmod p$
(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

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

עבור $t>0$ קבוע כלשהו.

שאלה 3

יהיו p ו- q ראשוניים אי-זוגיים כך ש- $p = 2q + 1$.

סעיף א

יהיו (p, g, b) ו- (p, g, B) מפתח פרטי וציבורי בהתאמה עבור מערכת ההצפנה של ElGamal, כאשר $B \equiv g^b \ (mod\ p)$, ותהיינה $M_1, M_2 \in \mathbb{Z}_p^*$ שתי הודעות.

עבור $j = 1,2$ נסמן ב (A_j, C_j) הצפנה של M_j בעזרת מחרוזת אקראית a_j, כלומר $A_j \leftarrow g^{a_j} \ (mod\ p)$ ו- $C_j \leftarrow B^{a_j} \cdot M_j \ (mod\ p)$.

הוכיחו כי $(A_1 \cdot A_2, C_1 \cdot C_2)$ היא הצפנה חוקית של ההודעה $M_1 \cdot M_2$, כאשר כל הכפלים הם ב- $\mathbb{Z}_p^*$.

סעיף ב

הראו שמערכת ההצפנה של ElGamal אינה עמידה בפני התקפת קריפטוגרמה נבחרת (כפי שראינו בכיתה עבור RSA). מותר לבקש פענוח של צופן אחד בלבד.

שאלה 4

נתאר מערכת חתימה:

- אלגוריתם יצירת המפתחות זהה לאלגוריתם יצירת המפתחות במערכת החתימה של ElGamal. כלומר, בוחרים p ראשוני, g יוצר של $\mathbb{Z}_p^*$ ו- $b \in \{1, \dots, p-2\}$, ומחשבים $B \leftarrow g^b \bmod p$. מפתח החתימה הפרטי הוא (p, g, b) ומפתח הוידוא הציבורי הוא (p, g, B).
- תחום ההודעות הוא $\mathbb{Z}_{p-1}^*$.
- כדי לחתום על מסמך M מוצאים z כך ש- $z \cdot M \equiv b \pmod{p-1}$, והחתימה היא $S \leftarrow g^z \bmod p$
- אלגוריתם הוידוא מכריז כי S היא חתימה חוקית על מסמך M אם"ם $S^M \equiv B \pmod{p}$

תזכורת: חתימה היא חוקית אם אלגוריתם הוידוא מכריז כי חתומה זו חוקית.

סעיף א

הראו כי אלגוריתם הוידוא תקין, כלומר אם החתימה S חושבה ע"י אלגוריתם החתימה אזי החתימה חוקית.

סעיף ב

מערכת חתימה זו אינה בטוחה. הראו כיצד זייפן יכול לייצר חתימה חוקית לכל הודעה $M \in \mathbb{Z}_{p-1}^*$.