

## קריפטוגרפיה: תרגיל 4

הגשה: יום ד' 30.12.15 בשעה 14:10 בהרצאה. 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 ראשוני אקראי.

#### סעיף א

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

#### סעיף ב

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:  $A = g^x \pmod{p}$ ,  $B = g^y \pmod{p}$ .
  - (4) הגרל  $d \in \{0,1\}$  באקראי.
  - אם  $d = 1$  אזי חשב  $C = g^{x \cdot y} \pmod{p}$ .
  - 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

$$\Pr \left[ E \text{ מנצח} \mid \text{במשחק ה"ל} \right] \geq \frac{1}{2} + t$$

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  $B \equiv g^b \pmod{p}$ , ותהינה  $M_1, M_2 \in \mathbb{Z}_p^*$  שתי הודעות. עבור  $j = 1, 2$  נסמן ב- $(A_j, C_j)$  הצפנה של  $M_j$  בעזרת מחרוזת אקראית  $a_j$ , כלומר  $A_j \leftarrow g^{a_j} \pmod{p}$  ו- $C_j \leftarrow B^{a_j} \cdot M_j \pmod{p}$ . 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

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  $X = g^x \pmod{p}$  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  $z = y \cdot A \pmod{p}$  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 5

בשאלה זו תראו מתקפה על שיטת החתימה RSA Textbook.

#### סעיף א

הראו איך בהינתן המפתח הפומבי  $(N, e)$  והודעה אקראית  $m \in \mathbb{Z}_N^*$  ניתן לזייף (ביעילות) חתימה על  $m$ . לתוקף מותר לבקש חתימה על הודעה אחת (שונה מ- $m$ ).

#### סעיף ב

הסבירו מדוע (תחת הנחת הקושי של RSA) לא ניתן לבצע את הנ"ל מבלי לבקש אף חתימה.