

מבוא להצפנה - תרגיל 6 - מגיש: נתאי יחזקאלי

1.

א.

הרצתי קוד קצר במקטע $Q1 - a$ ולכן אני פשוט אקח את החישובים שפוסלים. נסתכל על 96: הראשוניים שמחלקים את 96 הם 2, 3:

$$2^{\frac{96}{2}} \equiv 2^{48} \equiv 1 \pmod{97}$$

ולכן הוא לא יוצר.

$$3^{\frac{96}{2}} \equiv 3^{48} \equiv 1 \pmod{97}$$

ולכן גם 3 אינו יוצר של \mathbb{Z}_{97}^* .

$$4^{\frac{96}{2}} \equiv 4^{48} \equiv 1 \pmod{97}$$

ולכן גם הוא לא יוצר.

לעומת זאת:

$$5^{\frac{96}{2}} \equiv 96 \pmod{97} \quad 5^{\frac{96}{3}} \equiv 35 \pmod{97}$$

ולכן 5 הוא היוצר הכי קטן של \mathbb{Z}_{97}^* .

ב.

התשובה לשאלה היא: $\varphi(\varphi(97)) = \varphi(96)$

$$96 = 2^5 \cdot 3$$

↓

$$\varphi(96) = (2^5 - 2^4) (3^1 - 3^0) = 16 \cdot 2 = 32$$

ג.

יש לנו ארבעה משוואות:

$$5^{48} \equiv 2^5 \cdot 3 \pmod{97}$$

$$5^{52} \equiv 2 \cdot 3^3 \pmod{97}$$

$$5^{66} \equiv 2 \cdot 5 \cdot 7 \pmod{97}$$

$$5^{72} \equiv 3 \cdot 5^2 \pmod{97}$$

ולכן: הכל mod96.

$$\begin{aligned}48 &= 5 \cdot L_5(2) + L_5(3) \\52 &= L_5(2) + 3 \cdot L_5(3) \\66 &= L_5(2) + L_5(5) + L_5(7) \\72 &= L_5(3) + 2 \cdot L_5(5)\end{aligned}$$

אנחנו יודעים כי $L_5(5) = 1$ ולכן:

$$72 = L_5(3) + 2 \Rightarrow \boxed{L_5(3) = 70}$$

כעת:

$$52 = L_5(2) + 18 \Rightarrow \boxed{L_5(2) = 34}$$

בדיקה: אם נציב את שני הנתונים האחרונים במשוואה הראשונה אכן נקבל 48 (⊙).

$$66 = 34 + 1 + L_5(7) \Rightarrow \boxed{L_5(7) = 31}$$

כעת נעבור לשלב הבא:
נחפש r כך ש- $5^r \cdot 31$:
עבור $r = 2$

$$31 \cdot 5^2 = 2^5 \cdot 3 \pmod{97}$$

ולכן:

$$L_5(31) + 2 \cdot L_5(5) = 5 \cdot L_5(2) + L_5(3) \iff L_5(31) = 5 \cdot 34 + 70 - 2 = 46 \pmod{96}$$

.ד

את החלק הזה מחשב קטע הקוד Q1 - d:

$$\lceil \sqrt{97} \rceil = 10$$

כעת: $5^{-10} \pmod{96} = 11$.
 אחרי שנרץ את הפונקציה $\text{bsgs}(5,31,97)$ נקבל כפלט $x = 46$.
 ואכן:

$$5^{46} \equiv 31 \pmod{97}$$

2.
 א.
 ע"פ ההגדרה:

$$\delta = (x - k\gamma) \cdot a^{-1} \iff a\delta = x - k\gamma \iff x = a\delta + k\gamma$$

בוב שרוצה לחשב את החתימה בעזרת המפתח הציבורי ובעזרת $\text{sig}(x)$ בודק האם: $\beta^\delta \cdot \gamma^\gamma \equiv \alpha^x \pmod{p}$.
 הסבר (נכונות הבדיקה):

$$\beta^\delta \cdot \gamma^\gamma = (\alpha^a)^\delta \cdot (\alpha^k)^\gamma = \alpha^{a\delta+k\gamma} = \alpha^x \pmod{p}$$

לבוב יש את $\alpha, \beta, p, \gamma, \delta, x$ ולכן הוא יכול לחשב את מה שצריך כדי לבדוק האם $\beta^\delta \cdot \gamma^\gamma \equiv \alpha^x \pmod{p}$.
 מפתח ציבורי $\text{sig}(x)$

ב. היתרון החישובי הוא בכך ש- a הוא המפתח הסודי של אליס, כלומר, מספיק לחשב פעם אחת את a^{-1} (וישנו כזה כי $a \in \mathbb{Z}_{p-1}^*$). לעומת זאת, בחתימת אל-גמל הרגילה, יש צורך לחשב כל פעם מחדש את k^{-1} (כי צריך כל פעם לתת k אחר).

ג. נסמן: $\text{sig}(x_1) = (\gamma, \delta_1)$, $\text{sig}(x_2) = (\gamma, \delta_2)$ כאשר נתון לנו שה- k זהה בשני המקרים. כמו-כן גם γ זהה בשני המקרים היות ו- $\gamma = \alpha^k$ ו- α הוא חלק מהמפתח הציבורי של אליס (ולכן הוא נשאר זהה) ו- k זהה (נתון כחלק מתנאי השאלה).
 כעת, ע"פ הנוסחאות שבשאלה:

$$\begin{aligned}
\delta_1 &= (x_1 - k\gamma) \cdot a^{-1} \\
\delta_2 &= (x_2 - k\gamma) \cdot a^{-1} \\
&\Updownarrow \\
\delta_1 - \delta_2 &= (x_1 - k\gamma) \cdot a^{-1} - (x_2 - k\gamma) \cdot a^{-1} = \\
&= a^{-1}(x_1 - k\gamma - x_2 + k\gamma) = a^{-1}(x_1 - x_2) \\
&\Updownarrow \\
\delta_1 - \delta_2 &= a^{-1}(x_1 - x_2)
\end{aligned}$$

ולכן:

$$a^{-1} = \frac{\delta_1 - \delta_2}{x_1 - x_2} \iff a = \frac{x_1 - x_2}{\delta_1 - \delta_2}$$

ואנחנו יודעים כי ל- a יש הופכי היות ו- $a \in \mathbb{Z}_{p-1}^*$.

נתון לנו כי $p = 71$

$$a = \frac{75 - 78 \equiv -3 \equiv 68 \pmod{71}}{66 - 75 \equiv -9 \equiv 62 \pmod{71}} = 62^{-1} \cdot 68 = 24$$

את ההופכי 62 ואת התוצאה הסופית חישבתי בקוד בחלק d - Q2.

כל החישובים נמצאים ב-Q3.

נסתכל על הטבלה הבאה:

b	15919	15704	4681
$b \pmod{151}$	64	0	0
$b \pmod{167}$	54	6	5

כעת, נשים לב כי $p \equiv 3 \pmod{4}$ וגם $q \equiv 3 \pmod{4}$, לכן, כל מה שעלינו לעשות הוא עבור כל b ועבור כל p (סה"כ שש אפשריות, היות ויש לנו שני מספרים ראשוניים):

אם $b \equiv 0 \pmod{p}$ - אזי יש לנו רק שורש אחד והוא 0. אחרת, נחשב:

$$x = b^{\frac{p+1}{4}} \pmod{p}$$

ולאחר מכן נבדוק האם $x^2 = b \pmod{p}$. אם כן - אזי $\pm x$ הם שורשים של $b \pmod{p}$.

אם לא נבדוק האם $x^2 = -b \pmod{p}$ - ואז יש לנו רק שורש אחד. לבסוף, אחרי שיהיו לנו את כל האינצידים (שלושה, אחד עבור כל b - נחשב את עבור משפט השאריות הסיני).

כעת נחשב בנפרד עבור כל b :

$$\underline{b = 15919, p = 151}$$

$$x \equiv 64^{\frac{p+1}{4}} \equiv 64^{38} \pmod{151} = 8$$

וכעת נבדוק:

$$8^2 = 64 \checkmark$$

ולכן ± 8 הם שורשים ריבועיים.

$$\underline{b = 15919, p = 167}$$

$$x \equiv 54^{\frac{p+1}{4}} \pmod{167} \equiv 87 \pmod{167}$$

ואכן:

$$87^2 \pmod{167} \equiv 54 \checkmark$$

ולכן עלינו לפתור אבעה משוואות באמצעות משפט השאריות הסיני. במקרה ויש לנו 0, למשל: $4681 \equiv 0 \pmod{151}$ אזי ישנו רק שורש יחיד והוא - 0. אחרת - אין שורשים! השורשים כולם מחושבים ב-Q3 ואני אציג כאן רק את התוצאות הסופיות:

15919	15704	4681
± 13447	± 17063	-
± 11937	± 8154	-
± 13280	-	-
± 11770	-	-

.4

בוב מנצח:

1. בוב בוחר את $a = 8154$ ושולח לאליס את המספר: $b = 15704 = a^2$.

2. אליס מחשבת את השורשים של b ומקבלת: 17063, 8154.

3. אליס שולחת לבוב את $c = 17063$.

4. בוב כי אכן: $c^2 = b$ אבל היות ו- $c \neq a$ אזי הוא מודיע לאליס כי היא הפסידה.

אליס מנצחת:

בדיוק אותו פרוטוקול כמו מקודם, רק שהפעם אליס בוחרת: $c = 8154$.

בוב מוודא כי אכן $c^2 = b$ ומודיע לאליס שהיא ניצחה היות ו- $c = a$.

הערה 1. בחרתי את 15704 כי יש לו שני שורשים ולכן ההסתברות שאליס תבחר בשורש שבו בחר באופן אקראי היא $\frac{1}{2}$. לעומת זאת, אם הייתי בוחר ב-15919 אזי היו ארבעה שורשים ולכן הסיכוי שאליס הייתה בוחרת בשורש שבו בחר היא $\frac{1}{4}$.