

## תרגיל בית 8 במבנים אלגבריים 89-214 סמסטר א' תשפ"ג

**שאלה 1** (חימום). נניח ואליס הגרילה ראשוני מאוד גדול  $p$ . האם יש בעיה שהיא תבחר את  $n = p^2$  כחלק מהמפתח הציבורי שלה באלגוריתם RSA?

**שאלה 2**. קודדו ב-ASCII את האות הראשונה של שמכם באנגלית למספר, שאותו נסמן  $\lambda$ . קודדו גם את האות הקטנה המתאימה ל- $\lambda$  למספר ואותו נסמן  $\lambda$ . חשבו בשיטה של חישוב חזקה בעזרת ריבועים את  $\lambda^\lambda \pmod{1001}$ . לדוגמה אם שמכם הוא זרובבל הקידוד של Z הוא 90 והקידוד של z הוא 122. אתם מתבקשים לחשב את  $90^{122} \pmod{1001}$ . מותר להשתמש במחשבון (כולל בפונקציית המודולו) לחישובי הביניים, שאותם צריך לפרט.

**שאלה 3**. ידוע כי  $p = 257$  הוא ראשוני ושהחבורה  $U_{257}$  היא ציקלית. בעזרת הנתונים

$$89 \equiv 214^{186} \pmod{257} \quad 99 \equiv 214^{90} \pmod{257} \quad U_{257} = \langle 214 \rangle$$

מצאו  $0 \leq x < 257$  כך ש- $99 \equiv 89^x \pmod{257}$ .

אל תשברו את בעיית הלוגריתם הבדיד הזו בכוח, אלא במוח. רמז: מתישהו תצטרכו את אלגוריתם אוקלידס המורחב בחבורה אחרת, ולא הרבה מעבר לזה. דרך הפתרון צריכה לעבוד גם עבור  $p$ - $x$  גדולים.

**שאלה 4**. אליס ובוב רצו לשלוח זה לזה הודעות מוצפנות עם RSA. שניהם השתמשו במעריך ההצפנה  $e = 7$ . אליס הגרילה את הראשוניים  $p, q$  ובוב הגריל את הראשוניים  $p', q'$  ויצרו את המפתחות הציבוריים שלהם

$$n = pq = 38009, \quad n' = p'q' = 34427$$

בשאלה הזו אפשר להשתמש במחשבון פשוט לחישובי הביניים, אבל צריך לפרט אותם.

א. בוב רצה לשלוח לאליס את מספר הקורס 214 באופן מוצפן. הראו איך בוב יצפין את ההודעה. (כדאי לוודא אחר כך שאליס מצליחה לפענח את ההודעה נכון, אבל זה לא חלק מהשאלה.)

ב. בחרו מילה בת שלוש אותיות באנגלית וקודדו אותה ל-ASCII. עזרו לאליס למצוא דרך לקודד את המילה ולשלוח אותה לבוב באופן מוצפן עם שליחת שתי הודעות בלבד. הראו את ההודעות המוצפנות שאליס שלחה. שימו לב שמותר לאליס ובוב לתאם מראש את דרך הקידוד (כלומר אתם בונים פרוטוקול תקשורת שבו מסבירים איך נראית הודעה).

ג. המחשבים של אליס ובוב לא טובים בהגרלת ראשוניים, ומבלי לדעת חלק מהראשוניים  $p, q, p', q'$  שהגרילו לא שונים זה מזה. מצאו את המפתח הפרטי  $d$  של אליס ואת המפתח הפרטי  $d'$  של בוב בעזרת חישוב  $\gcd(n, n')$ .

**שאלה 5** (תכנות). ממשו בעצמכם פונקציה בשם  $\text{superpower}(x, k, n)$  המקבלת מספרים טבעיים  $x, k, n$  ומחשבת את  $x^k \pmod{n}$  לפי שיטת העלאה בחזקה בעזרת ריבועים, ובכל פעם שאתם מכפילים או מעלים בריבוע הדפיסו

$$x^i = y \pmod{n}$$

כאשר במקום  $x, i, y, n$  מופיעים המספרים המתאימים. למשל  $x$  ו- $n$  הם הפרמטרים לפונקציה וזהים בכל השורות, ואילו רק בשורה האחרונה  $i$  הוא  $k$ . מספר השורות לא אמור לעלות על  $2 \log_2 k$ . דוגמה להרצה של  $\text{superpower}(89, 11, 101)$ :

$$\begin{aligned} 89^1 &= 89 \pmod{101} \\ 89^2 &= 43 \pmod{101} \\ 89^4 &= 31 \pmod{101} \\ 89^5 &= 32 \pmod{101} \\ 89^{10} &= 14 \pmod{101} \\ 89^{11} &= 34 \pmod{101} \end{aligned}$$

נסו להריץ את  $\text{superpower}(x, k, 89214)$  עבור מספרים "גדולים" יחסית  $x, k$  שעבורם אתם עדיין יכולים לוודא את הפתרון.

**שאלה 6** (רשות). בעזרת שיטת צעדי גמד וצעדי ענק שראינו בכיתה מצאו את הפתרון למשוואה  $71 \equiv 7^x \pmod{101}$  ופתרון למשוואה  $72 \equiv 7^y \pmod{101}$ . קצת יותר קשה: משני הפתרונות האלו מצאו פתרון למשוואה  $71 \equiv 72^z \pmod{101}$ , וכנראה בדרך תצטרכו את החבורה  $U_{\varphi(101)}$ . הפתרונות צריכים לקיים  $0 \leq x, y, z < 101$ .

**שאלה 7** (אתגר). בעיית הלוגריתם הבדיד ל- $S_n$  אומרת שבהנתן תמורה  $\sigma \in S_n$  ותמורה  $\tau \in \langle \sigma \rangle$  יש למצוא מספר שלם  $x$  כך ש- $\tau = \sigma^x$ .

א. יהיו  $a_1, a_2, m_1, m_2$  שלמים המקיימים  $a_1 \equiv a_2 \pmod{\gcd(m_1, m_2)}$ . הוכיחו שלמשוואות

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \end{cases}$$

יש פתרון משותף. הדרכה אפשרית: הוכיחו כי  $a_1 - a_2 = k \cdot \gcd(m_1, m_2)$  עבור  $k$  שלם כלשהו. לפי איפיון הממ"מ כצירוף לינארי, קיימים מקדמים  $s_1, s_2$  המקיימים

$$s_1 m_1 + s_2 m_2 = \gcd(m_1, m_2)$$

שמוצאים אותם בעזרת אלגוריתם אוקלידס המורחב. הסבירו למה  $-k s_1 m_1 + a_1 = k s_2 m_2 + a_2$  ומה אפשר לעשות עם זה. כהערת אגב, זאת גרסה (מעט משוכללת) של משפט השאריות הסיני, והפתרון שמוצאים הוא יחיד עד כדי שקילות מודולו  $\text{lcm}(m_1, m_2)$ .

ב. הציעו אלגוריתם לפתרון בעיית הלוגריתם הבדיד ל- $S_n$ , שיהיה יעיל גם לחבורה גדולה כמו  $S_{300}$  (שיש בה איברים מסדר שגדול מ- $10^{17}$ ). רמז: אינדוקציה בסעיף הקודם.

ג. הסבירו איך האלגוריתם שלכם יפעל במקרה שבו  $\sigma$  היא מחזור מאורך 100 ובמקרה שבו  $\sigma$  היא מכפלה של 50 מחזורים זרים שחצי מהם מאורך 3 וחצי מהם מאורך 2.

ד. נבחר את התמורה

$$\sigma = (7, 8, 9, 10)(1, 3, 11, 13, 4)(5, 2, 6, 18, 17, 16) \in S_{18}$$

הראו איך האלגוריתם שלכם מהסעיף השני מוצא (באופן יעיל ולא נאיבי) את  $x$  עבור התמורה

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 \\ 11 & 16 & 13 & 3 & 17 & 5 & 9 & 10 & 7 & 8 & 4 & 12 & 1 & 14 & 15 & 18 & 6 & 2 \end{pmatrix} \in \langle \sigma \rangle$$

בהצלחה!