המחלקה למדעי המחשב

01/03/2026 י"ב באדר תשפ"ו
09 : 00 – 12 : 00

# קריפטוגרפיה למדמ"ח

מועד ב'
ד"ר ירמיהו מילר.

תשפ"ו סמסטר א'

**השאלון מכיל 4 עמודים (כולל עמוד זה).**

## בהצלחה!

==========

**הנחיות לסטודנטים כולל חומרי עזר**

- ניתן להשתמש במחשבון מדעי לא גרפי עם צג קטן.
- ניתן להשתמש בדפי נוסחאות (13 עמודים בפורמט $A4$) מצורפים לשאלון.
- יש לענות על השאלות במחברת בלבד.

**הנחיות למדור בחינות**

- לשאלון הבחינה יש לצרף מחברת.

**אחר / הערות**

- סטודנטים במתווה **רגיל**: נדרשים לפתור 4 **מתוך השאלות** 1 **עד** 5.
- סטודנטים במתווה **מילואים**: נדרשים לפתור 4 **מתוך השאלות** 1 **עד** 6.
- יש לנמק היטב כל שלב של פתרון. תשובה ללא הסבר וללא נימוק, אפילו נכונה, לא תתקבל.
- סדר התשובות אינו משנה, אך יש לרשום ליד כל תשובה את מספרה.
- יש לרשום בראש המחברת איזה שאלות לבדוק.

==========



המכללה האקדמית להנדסה סמי שמעון
קמפוס באר שבע ביאליק פינת בזל 84100 | קמפוס אשדוד ז'בוטינסקי 84, 77245 | www.sce.ac.il | חייג: *מספר

## שאלה 1 (25 נקודות)

**א) (5 נק')**
בוב בונה מפתח ציבורי הבא של צופן RSA:

$$(b = 31, n = pq) \ , \quad p = 37 \ , q = 41 \ .$$

חשבו את המפתח סודי.

**ב) (7 נק')**
אליס מצפינה את ההודעה BCCI. הוכיחו כי הטקסט מוצפן המתקבל הוא GJJ.

**ג) (8 נק')**
הוכיחו כי כאשר בוב מפענח את הטקסט מוצפן GJJ שמצאתם בסעיף ב' הוא יקבל את הטקסט הגלוי BCII.

**ד) (5 נק')**
הוכיחו או הפריכו ע"י דוגמה נגדית את הטענה הבאה:
ליחס שקילות מודולרי $ax \equiv y \pmod{m}$ קיים פתרון יחיד $x \in \mathbb{Z}_m$ אם ורק אם $\gcd(a, m) = 1$.

## שאלה 2 (25 נקודות)

יהי $X = \{\mathrm{q}, \mathrm{r}, \mathrm{s}\}$ קבוצת טקסט גלוי עם פונקצית הסתברות

$$P_X(\mathrm{q}) = \frac{1}{3} \ , \qquad P_X(\mathrm{r}) = \frac{1}{4} \ , \qquad P_X(\mathrm{s}) = \frac{5}{12} \ .$$

יהי $K = \{k_1, k_2, k_3, k_4\}$ קבוצת מפתחות בעלת פונקצית הסתברות

$$P_K(k_i) = \frac{1}{4}$$

לכל $k_i \in K$. יהי $Y = \{\mathrm{A}, \mathrm{B}, \mathrm{C}\}$ קבוצת טקטסט מוצפן. נגדיר הכלל מצפין

$$e_{k_i}(x) = 2x + i \mod 3$$

לכל $x \in \mathbb{Z}_{26}$ ולכל $i \in \{1, 2, 3, 4\}$.

**א) (8 נק')**
מצאו את $P_Y(y)$ לכל $y \in Y$.

**ב) (8 נק')**
הוכיחו או הפריכו על ידי דוגמה נגדית: לקריפטו-מערכת זו יש סודיות מושלמת.



המכללה האקדמית להנדסה סמי שמעון
קמפוס באר שבע ביאליק פינת בזל 84100 | קמפוס אשדוד ז'בוטינסקי 84, 77245 | www.sce.ac.il | חייג: *מספרים

**ג) (5 נק')**
יהיו $a, b$ שלמים.
הוכיחו או הפריכו ע"י דוגמה נגדית את הטענה הבאה:
$d = \gcd(a, b)$ אם ורק אם לכל מחלק משותף $c$ של $a$ ו- $b$: $c \mid d$.

**ד) (4 נק')**
הוכיחו או הפריכו ע"י דוגמה נגדית את הטענה הבאה:
אם $a, b$ שלמים וגם $b \neq 0$ אז $\gcd(a, b) = \gcd(b, a \bmod b)$.

## שאלה 3 (25 נקודות)

**א) (8 נק')**
הטקסט הבא הוצפן ע"י צופן וויג'נר עם המפתח `goodluck`:

$y = \texttt{RWGWPHVYZVSKPUTD}$ .

חשבו את הטקסט הגלוי המקורי.

**ב) (8 נק')** הוכיחו כי צופן וויג'נר ניתן לפענוח.

**ג) (4 נק')** תהי $\pi : \Sigma \to \Sigma$ תמורה על האלפבית $\Sigma$.
הוכיחו או הפריכו ע"י דוגמה נגדית את הטענה הבאה:
$\pi \in [z_1^{n_1} \dots z_k^{n_k}]$ אם ורק אם $\pi^{-1} \in [z_1^{n_1} \dots z_k^{n_k}]$.
כלומר לתמורה $\pi$ ולתמורה ההופכית $\pi^{-1}$ יש אותו פירוק למחזורים.

**ד) (5 נק')** יהיו $a, b, m$ שלמים חיוביים.
הוכיחו או הפריכו ע"י דוגמה נגדית את הטענה הבאה:
$a \equiv b \pmod{m}$ אם ורק אם $a \bmod m = b \bmod m$.

## שאלה 4

**א) (11 נק')** הטקסט הבא הוצפן ע"י צופן היל עם המפתח $k = \begin{pmatrix} \texttt{B} & \texttt{D} & \texttt{B} \\ \texttt{B} & \texttt{A} & \texttt{B} \\ \texttt{B} & \texttt{B} & \texttt{A} \end{pmatrix}$:

$y = \texttt{CQHJMJIFB}$ .

חשבו את הטקסט הגלוי.

**ב) (9 נק')** הוכיחו כי צופן היל ניתן לפענוח.

**ג) (5 נק')** הוכיחו או הפריכו ע"י דוגמה נגדית את הטענה הבאה:
צופן אניגמה הוא תמורה משקפת.



המכללה האקדמית להנדסה סמי שמעון
קמפוס באר שבע ביאליק פינת בזל 84100 | קמפוס אשדוד ז'בוטינסקי 84, 77245 | www.sce.ac.il | חייג: *מסמסם

## שאלה 5 (25 נקודות)

**א) (10 נק')**
אליס שולחת את הטקסט המוצפן הבא לבוב:

CVLCBKDIVTLNQV .

הטקסט הוצפן ע"י צופן אפיני עם המפתח $(a = 11, b = 3)$. חשבו את הטקסט גלוי המקורי אשר אליס שלחה לבוב.

**ב) (8 נק')**
נתון הכלל מצפין הבא מעל אלפבית של אורך $p$ כאשר $p$ מספר ראשוני.

$$\forall x \in \mathbb{Z}_p : \quad e_k(x) = ax + b \bmod p \ ,$$

כאשר $a, b$ שלמים.
הוכיחו או הפריכו ע"י דוגמה נגדית את הטענה הבאה:
לכל $a, b$ הצופן ניתן לפענוח.

**ג) (7 נק')**
יהיו $a, b, c$ שלמים. הוכיחו או הפריכו ע"י דוגמה נגדית את הטענה הבאה:
אם $a \equiv b \pmod{c}$ אז לכל $n > 1$: $a^n \equiv b^n \pmod{c}$.

## שאלה 6 (25 נקודות) שאלת בחירה לסטודנטים במתווה מילואים בלבד

**א) (13 נקודות)** פתרו את המערכת יחסים שקילות הבאה:

$$\begin{aligned} 13x &\equiv 4 \mod 99 \\ 15x &\equiv 56 \mod 101 \ . \end{aligned}$$

**ב) (12 נקודות)**
יהיו $a, b, m$ שלמים חיוביים. הוכיחו או הפריכו ע"י דוגמה נגדית את הטענה הבאה:
אם $m \mid a$ וגם $m \mid b$ אז $\gcd\left(\frac{a}{m}, \frac{b}{m}\right) = \frac{\gcd(a,b)}{m}$.



המכללה האקדמית להנדסה סמי שמעון
קמפוס באר שבע ביאליק פינת בזל 84100 | קמפוס אשדוד ז'בוטינסקי 84, 77245 | www.sce.ac.il | חייג: *מהפנים

# תוכן העניינים


1 תורת המספרים 5

2 חוגים 7

3 צפני בסיסיים 8

4 צופן RSA 9

5 צופן ElGamal 10

6 צופן אניגמה 10

7 תורת שאנון וסודיות מושלמת 12

8 צופן פייסטל 13

9 צופן IDEA 14

10 צופן DES 15


# 1 תורת המספרים

$m \mid a$ אם ורק אם קיים שלם $q$ כך ש $a = qm$.

קיים שלם $q$ כך ש: $a = qm + b \iff m \mid a - b \iff a \equiv b \pmod{m}$

אם $a, b$ שלמים חיוביים אז השארית של $a$ בחלוקה ב- $b$, מסומנת $a \bmod b$ היא

$$a \bmod b = a - b \left\lfloor \frac{a}{b} \right\rfloor \ .$$

**משפט החילוק של אוקלידס**: לכל זוג שלמים $a, b$ קיימים שלמים $q, r$ כך ש:

$$a = qb + r \ , \qquad 0 \le r < |b| \ .$$

אם $a, b \ge 0$ אזי $q = \left\lfloor \frac{a}{b} \right\rfloor$ ו- $r = a \bmod b$.

**האלגוריתם של אוקלידס:** לכל שלמים $a, b$ ($a \ge b \ge 0$) האלגוריתם הבא נותן את $\gcd(a, b)$.

**Algorithm 1** האלגוריתם של אוקלידס

**Input:** Integers $a, b$ .
$r_0 \leftarrow a, \quad r_1 \leftarrow b, \quad n \leftarrow 1$
**while** $r_n \neq 0$ **do**
  $q_n \leftarrow \left\lfloor \frac{r_{n-1}}{r_n} \right\rfloor$
  $r_{n+1} \leftarrow r_{n-1} - q_n r_n$
  $n \leftarrow n + 1$
**end while**
$n \leftarrow n - 1$
**Output:** $r_n = \gcd(a, b)$

| שלב | $q_n$ | $r_n$ |
|---|---|---|
| $n = 1$ | $q_1 = \lfloor \frac{r_0}{r_1} \rfloor$ | $r_2 = r_0 - q_1 r_1$ |
| $n = 2$ | $q_2 = \lfloor \frac{r_1}{r_2} \rfloor$ | $r_3 = r_1 - q_2 r_2$ |
| $\vdots$ | | |
| $n - 1$ | $q_{n-1} = \lfloor \frac{r_{n-2}}{r_{n-1}} \rfloor$ | $r_n = r_{n-2} - q_{n-1} r_{n-1}$ |
| $n$ | $q_n = \lfloor \frac{r_{n-1}}{r_n} \rfloor$ | $r_{n+1} = r_{n-1} - q_n r_n$ |

**משפט בז'ו:** לכל זוג שלמים $a, b$ קיימים שלמים $s, t, d$ כך ש:

$$sa + tb = d \ , \qquad d = \gcd(a, b) \ .$$

בהינתן $a \geq b \geq 0$ **האלגוריתם המוכלל של אוקלידס** נותן את השלמים $(s, t, d)$ בפירוק $sa + tb = d$ באופן הבא:

**Algorithm 2** האלגוריתם המוכלל של אוקלידס

**Input:** Integers $a, b$ .
$r_0 \leftarrow a, \quad r_1 \leftarrow b$
$s_0 \leftarrow 1, \quad s_1 \leftarrow 0$
$t_0 \leftarrow 0, \quad t_1 \leftarrow 1, \quad n \leftarrow 1$
**while** $r_n \neq 0$ **do**
  $q_n \leftarrow \left\lfloor \frac{r_{n-1}}{r_n} \right\rfloor$
  $r_{n+1} \leftarrow r_{n-1} - q_n r_n$
  $s_{n+1} \leftarrow s_{n-1} - q_n s_n$
  $t_{n+1} \leftarrow t_{n-1} - q_n t_n$
  $n \leftarrow n + 1$
**end while**
$n \leftarrow n - 1$
**Output:** $d = r_n, s = s_n, t = t_n$

| שלב | $q_n$ | $r_n$ | $s_n$ | $t_n$ |
|---|---|---|---|---|
| $n = 1$ | $q_1 = \lfloor \frac{r_0}{r_1} \rfloor$ | $r_2 = r_0 - q_1 r_1$ | $s_2 = s_0 - q_1 s_1$ | $t_2 = t_0 - q_1 t_1$ |
| $n = 2$ | $q_2 = \lfloor \frac{r_1}{r_2} \rfloor$ | $r_3 = r_1 - q_2 r_2$ | $s_3 = s_1 - q_2 s_2$ | $t_3 = t_1 - q_2 t_2$ |
| $\vdots$ | | | | |
| $n - 1$ | $q_{n-1} = \lfloor \frac{r_{n-2}}{r_{n-1}} \rfloor$ | $r_n = r_{n-2} - q_{n-1} r_{n-1}$ | $s_n = s_{n-2} - q_{n-1} s_{n-1}$ | $t_n = t_{n-2} - q_{n-1} t_{n-1}$ |
| $n$ | $q_n = \lfloor \frac{r_{n-1}}{r_n} \rfloor$ | $r_{n+1} = r_{n-1} - q_n r_n$ | $s_{n+1} = s_{n-1} - q_n s_n$ | $t_{n+1} = t_{n-1} - q_n t_n$ |

שני מספרים שלמים $a, b$ נקראים **מספרים זרים** אם $\gcd(a,b)=1$.

**משפט הפירוק לראשוניים**:
לכל שלם חיובי $m$ קיים מספרים ראשוניים $p_1, p_2, \ldots, p_n$ ושלמים אי-שליליים $e_1, \ldots, e_n$ כך שניתן לרשום $m$ כפירוק לראשוניים בצורה הבאה:

$$m = p_1^{e_1} \times p_2^{e_2} \ldots p_n^{e_n} \ .$$

**פונקצית אוילר:**
אם הפירוק לראשוניים של מספר שלם $m$ הוא $m = \prod_{i=1}^{n} p_i^{e_i}$, אז המספר של שלמים אשר זרים ביחס ל- $m$ וקטן ממנו ניתן על ידי הנוסחה

$$\phi(m) = \prod_{i=1}^{n} \left(p_i^{e_i} - p_i^{e_i-1}\right) \ .$$

אם $p$ מספר ראשוני אז: $\phi(p) = p-1.$
אם $p$ מספר ראשוני אז: $\phi\left(p^n\right) = p^n - p^{n-1}.$
אם $s, t$ שלמים זרים (כלומר $\gcd(s,t)=1$) אז: $\phi\left(s \cdot t\right) = \phi(s)\phi(t).$
אם $p$ ו- $q$ מספרים ראשוניים שונים אז: $\phi(p \cdot q) = (p-1)(q-1).$

**משפט הקטן של פרמה:**
אם $p$ מספר ראשוני אז לכל $a$ שלם התנאים הבאים מתקיימים:

$$a^p \equiv a \pmod p \ , \qquad a^{p-1} \equiv 1 \pmod p \ , \qquad a^{-1} \equiv a^{p-2} \pmod p \ .$$

**משפט אוילר:** אם $n$ שלם חיובי ו- $a \in \mathbb{Z}_n$ וגם $\gcd(a,n)=1$ אז $a^{\phi(n)} \equiv 1 \pmod n$ וגם $a^{-1} \equiv a^{\phi(n)-1} \pmod n$.

**משפט השאריות הסיני**: יהיו $m_1, \ldots, m_r$ שלמים זרים בזוגות ו- $a_1, \ldots, a_r$ שלמים. אזי למערכת

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_r \pmod{m_r} \end{aligned}$$

קיים פתרון יחיד מודולו $M = m_1 m_2 \cdots m_r$ שהוא

$$x \equiv \sum_{i=1}^{r} a_i M_i y_i \pmod M$$

כאשר $M_i = \dfrac{M}{m_i}$ ו- $y_i = M_i^{-1} \mod m_i$ לכל $1 \le i \le r$.

## 2 חוגים

**חוג $\mathbb{Z}_m$**: אם $m$ שלם חיובי אז החוג $\mathbb{Z}_m$ מוגדר $\mathbb{Z}_m \triangleq \{0, 1, \ldots, m-1\}$.
לכל שלם $b$ נתאים איבר $a \in \mathbb{Z}_m$ לפי התנאי: $a \equiv b \pmod m$.

**איבר הופכי של איבר חוג:**
לכל $a \in \mathbb{Z}_m$ אם קיים שלם $x$ כך ש: $ax \equiv 1 \pmod m$ אז אומרים כי $x$ האיבר ההופכי של $a$ ב- $\mathbb{Z}_m$,

מסומן $a^{-1} \in \mathbb{Z}_m$.

**תניא לקיום איבר הופכי בחוג:** נתון $a \in \mathbb{Z}_m$ קיים איבר הופכי $a^{-1}$ אם ורק אם $\gcd(a,m)=1$.

**הקופקטור** ה- $ij$ של מטריצה $A$ שווה לדטרמיננטת המטריצה המתקלת אחרי מחיקת שורת $i$ ועמודת $j$:

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1j} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2j} & \cdots & a_{2n} \\ \vdots & & & & & \\ a_{i1} & a_{i2} & \cdots & a_{ij} & \cdots & a_{in} \\ \vdots & & & & & \\ a_{n1} & a_{n2} & \cdots & a_{nj} & \cdots & a_{nn} \end{pmatrix} \quad \Rightarrow \quad C_{ij} = (-1)^{i+j} \begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1j} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2j} & \cdots & a_{2n} \\ \vdots & & & & & \\ a_{i1} & a_{i2} & \cdots & a_{ij} & \cdots & a_{in} \\ \vdots & & & & & \\ a_{n1} & a_{n2} & \cdots & a_{nj} & \cdots & a_{nn} \end{vmatrix}$$

**מטריצת הקופקטורים** של מטריצה $A$ היא המטריצה שבה רכיב ה-$ij$ הוא הקופקטור ה- $ij$ של $A$:

$$C = \begin{pmatrix} C_{11} & \cdots & C_{1n} \\ \vdots & \ddots & \vdots \\ C_{n1} & \cdots & C_{nn} \end{pmatrix} .$$

**נוסחת קריימר למטריצה הופכית:** $A^{-1} = (\det A)^{-1} C^t$.

**איברים הפיכים ב-** $\mathbb{Z}_{26}$:

| $a$ | 1 | 3 | 5 | 7 | 9 | 11 | 15 | 17 | 19 | 21 | 23 | 25 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $a^{-1}$ | 1 | 9 | 21 | 15 | 3 | 19 | 7 | 23 | 11 | 5 | 17 | 25 |

## 3 צפני בסיסיים

**ערכים הקריפטוגרפיים של האותיות:**

| a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

**לוח הכפל של** 26:

| $m$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $26 \times m$ | 26 | 52 | 78 | 104 | 130 | 156 | 182 | 208 | 234 | 260 | 286 | 312 | 338 | 364 | 390 |

| $m$ | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $26 \times m$ | 416 | 442 | 468 | 494 | 520 | 546 | 572 | 598 | 624 | 650 | 676 | 702 | 728 | 754 | 780 |

**צפנים בסיסיים:**

| צופן | כלל מצפין | כלל מפענח | מפתח |
|---|---|---|---|
| קיסר | $e_k(x) = x + k \bmod 26$ | $d_k(x) = x - k \bmod 26$ | $k \in \mathbb{Z}_{26}$ |
| תמורה | $e_\pi(x_1 \dots x_m) = x_{\pi(1)} \dots x_{\pi(m)} \bmod 26$ | $d_\pi(y_1 \dots y_m) = y_{\pi^{-1}(1)} \dots y_{\pi^{-1}(m)} \bmod 26$ | $\pi$ תמורה של אורך $m$ |
| החלפה | $e_\pi(x) = \pi(x) \bmod 26$ | $d_\pi(y) = \pi^{-1}(y) \bmod 26$ | $\pi$ תמורה של אורך 26 |
| אפיני | $e_k(x) = (ax + b) \bmod 26$ | $d_k(y) = a^{-1}(y - b) \bmod 26$ | $k = (a, b)$, $\gcd(a, 26) = 1.$ |
| ויז'נר | $e_k(x_1, \dots, x_m) = (x_1 + k_1, \dots, x_m + k_m) \bmod 26$ | $d_k(y_1, \dots, y_m) = (y_1 - k_1, \dots, y_m - k_m) \bmod 26$ | $k = (k_1, \dots, k_m) \in \mathbb{Z}_{26}^m$ |
| היל | $e_k(x_1 \dots x_m) = (x_1 \dots x_m) \cdot k \bmod 26$ | $d_k(y_1 \dots y_m) = (y_1 \dots y_m) \cdot k^{-1} \bmod 26$ | $k \in \mathbb{Z}_{26}^{m \times m}$ $\gcd(\det(k), 26) = 1.$ |

## 4 צופן RSA

- מפתח ציבורי: $(b, n)$ כאשר $n = pq$ כאשר $p, q$ מספרים ראשוניים שונים.
- מפתח סודי: $(a, p, q)$ כאשר $a \equiv b^{-1} \pmod{\phi(n)}$, כאשר $\phi$ הפונקצית אוילר של $n$.

  בגלל ש- $n = pq$ כאשר $p, q$ מספרים שלמים אז $\phi(n) = \phi(pq) = (p-1)(q-1)$.

  לכן: $a \equiv b^{-1} \pmod{(p-1)(q-1)}$.
- כלל מצפין: $e_k(x) = x^b \bmod n$ לכל מספר שלם $x$.
- כלל מפענח: $d_k(y) = y^a \bmod n$ לכל מספר שלם $y$.

**שיטת הריבועיים לחישוב חזקה מודולרית:**

בהינתן $y = x^b \bmod n$. יהי $b = b_k \dots b_1 b_0$ הייצוג ביניארי של $b$. אזי קיים אלגוריתם הנקרא שיטת הריבועיים שנותן ערך של $y = x^b \bmod n$ באופן הבא:

**Algorithm 3** האלגוריתם שיטת הריבועיים

**Input:** Integers $x, b_0, \ldots, b_k, n$ .
$i \leftarrow 1$
$z_0 \leftarrow x$
**while** $i \leq k$ **do**
  $z_i \leftarrow z_{i-1}^2 \bmod n$
**end while**
$i \leftarrow 0$
$y \leftarrow 1$
**while** $i \leq k$ **do**
  **if** $b_i = 1$ **then**
    $y \leftarrow z_i y \bmod n$
  **end if**
**end while**
**return:** $y$ $\triangleright\ y = x^b \bmod n$

**האלגוריתם לפענוח של צופן RSA** :

האלגוריתם הבא נותן את הפתרון $x$ של הכלל מפענח $x = y^a \bmod n$ לפי השלבים הבאים:

**שלב [1]** מחשבים $y \bmod p$ ו- $a \bmod (p-1)$ ואז מחשבים $x_1 = (y \bmod p)^{a \bmod (p-1)} \bmod p.$

**שלב [2]** מחשבים $y \bmod q$ ו- $a \bmod (q-1)$ ואז מחשבים $x_2 = (y \bmod q)^{a \bmod (q-1)} \bmod q.$

**שלב [3]** בעזרת המשפט השאריות הסיני פותרים את המערכת $\left\{ \begin{array}{ll} x = & x_1 \bmod p \\ x = & x_2 \bmod q \end{array} \right\}.$

## 5 צופן ElGamal

- המפתח הוא $k = (p, a, \alpha, d)$ כאשר:
  - $p$ מספר ראשוני
  - $a, d, \alpha$ מספרים שלמים חיוביים עבורם $2 \leq a, d, \alpha \leq p-2$.
- $\beta = \alpha^a \bmod p$.
- כלל מצפין: $y_1 = \alpha^d \bmod p, \quad y_2 = x\beta^d \bmod p$ לכל $x$ שלם חיובי.
- כלל מפענח: $x = (y_1^a)^{-1}\, y_2 \bmod p$ לכל שלמים חיוביים $y_1, y_2$.

## 6 צופן אניגמה

**תמורה** על קבוצה סופית $\Sigma = \{x_1, \ldots, x_n\}$ היא פונקציה $\pi : \Sigma \to \Sigma$ חד-חד ערכית ו"על" $\Sigma$.

- **על $\Sigma$:** לכל $y \in \Sigma$ קיים $x \in \Sigma$ כך ש: $y = \Sigma(x)$.
- **חד-חד-ערכית:** לכל $x, y \in \Sigma$ מתקיים:

$$x \neq y \quad \Rightarrow \quad \Sigma(x) \neq \pi(y) \ .$$

**התמורה הזהות** מסומנת $\mathrm{id} : \Sigma \to \Sigma$ ומוגדרת כך שלכל $x \in \Sigma$: $\mathrm{id}(x) = x$.

**תמורה הופכית**: אם $\pi : \Sigma \to \Sigma$ תמורה על הקבוצה $\Sigma$, התמורה ההופכית מסומנת $\pi^{-1}$ מקיימת את התנאי:

$$\forall x \in \Sigma \qquad \pi\pi^{-1}(x) = x = \pi^{-1}\pi(x) \ .$$

תמורה $\rho : \Sigma \to \Sigma$ היא **תמורה משקפת** אם התנאי הזה מתקיים:

$$\forall x, y \in \Sigma : \qquad \rho(x) = y \quad \Longleftrightarrow \quad \rho(y) = x \ .$$

**הגלגלים ומשקף הקבוע של צופן אניגמה:**

| $x$ | $A$ | $B$ | $C$ | $D$ | $E$ | $F$ | $G$ | $H$ | $I$ | $J$ | $K$ | $L$ | $M$ | $N$ | $O$ | $P$ | $Q$ | $R$ | $S$ | $T$ | $U$ | $V$ | $W$ | $X$ | $Y$ | $Z$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $\alpha_1(x)$ | $E$ | $K$ | $M$ | $F$ | $L$ | $G$ | $D$ | $Q$ | $V$ | $Z$ | $N$ | $T$ | $O$ | $W$ | $Y$ | $H$ | $X$ | $U$ | $S$ | $P$ | $A$ | $I$ | $B$ | $R$ | $C$ | $J$ |
| $\alpha_2(x)$ | $A$ | $J$ | $D$ | $K$ | $S$ | $I$ | $R$ | $U$ | $X$ | $B$ | $L$ | $H$ | $W$ | $T$ | $M$ | $C$ | $Q$ | $G$ | $Z$ | $N$ | $P$ | $Y$ | $F$ | $V$ | $O$ | $E$ |
| $\alpha_3(x)$ | $B$ | $D$ | $F$ | $H$ | $J$ | $L$ | $C$ | $P$ | $R$ | $T$ | $X$ | $V$ | $Z$ | $N$ | $Y$ | $E$ | $I$ | $W$ | $G$ | $A$ | $K$ | $M$ | $U$ | $S$ | $Q$ | $O$ |
| $\rho(x)$ | $Y$ | $R$ | $U$ | $H$ | $Q$ | $S$ | $L$ | $D$ | $P$ | $X$ | $N$ | $G$ | $O$ | $K$ | $M$ | $I$ | $E$ | $B$ | $F$ | $Z$ | $C$ | $W$ | $V$ | $J$ | $A$ | $T$ |

**כלל מצפין וכלל מפענח של צופן אניגמה:**

- בהינתן מילה $x_1 x_2 \ldots x_k$ של טקסט גלוי, הכלל מצפין של האות ה- $i$ הוא: $e(x_i) = \Delta_i(x_i)$
  כאשר $\Delta_i$ היא התמורה הכתובה למטה.
- בהינתן מילה $y_1 y_2 \ldots y_k$ של טקסט מוצפן הכלל מפענח של האות ה- $i$ הוא: $d(y_i) = \Delta_i(y_i)$.
- לכל $i$ שלם:

$$\Delta_i = \tau_i^{-1} \, \rho \, \tau_i \ ,$$

כאשר

- $\rho$ היא התמורה המשקפת הקבועה של צופן אניגמה,
-

$$\tau_i = \sigma_{-i} \, \alpha_3 \, \sigma_i \, \alpha_2 \, \alpha_1 \, \pi \ , \qquad \tau_i^{-1} = \pi \, \alpha_1^{-1} \, \alpha_2^{-1} \, \sigma_{-i} \, \alpha_3^{-1} \ \sigma_i$$

כאשר $\alpha_1, \alpha_2, \alpha_3$ הן התמורות של הגלגלים של צופן אניגמה הנתונות בטבלה למעלה, $\pi$ היא תמורה המשקפת המשתנה,

- $\sigma_i$ היא תמורה הזזה של $i$ אותיות קדימה באלפבית: $\sigma_i(x) = x + i \bmod 26$,
- $\sigma_{-i}$ היא תמורה הזזה של $i$ אותיות אחורה באלפבית: $\sigma_{-i}(x) = x - i \bmod 26$.

**מילה משוכפלת** היא מילה סימטרית של טקסט גלוי באורך 6 אותיות מהצורה:

$$xyzxyz \ .$$

**מילה אופיינית** היא ההצפנה של מילה משוכפלת ע"י צופן אניגמה:

$$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \Delta_1(x)\Delta_2(y)\Delta_3(z)\Delta_4(x)\Delta_5(y)\Delta_6(z) \ .$$

**משפט רייבסקי I:** יהי $\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6$ מילה אופיינית של צופן האניגמה. אזי:

$$\sigma_4 = \Delta_4\Delta_1\left(\sigma_1\right) \ , \quad \sigma_5 = \Delta_5\Delta_2\left(\sigma_2\right) \ , \quad \sigma_6 = \Delta_6\Delta_3\left(\sigma_3\right) \ .$$

**משפט רייבסקי II:**

עבור כל אחת של התמורות $\Delta_4\Delta_1$, $\Delta_5\Delta_2$, $\Delta_6\Delta_3$ של צופן אניגמה, קיים סידור של הפירוק לראשונים שנקרא **סדר רייבסקי** כך שהתנאים הבאים מתקיימים:

- לכל זוג מחרוזות $\begin{pmatrix} a_1 & a_2 & \cdots a_{k-1} & a_k \end{pmatrix} \begin{pmatrix} b_1 & b_2 & \cdots b_{k-1} & b_k \end{pmatrix}$ ב- $\Delta_4\Delta_1$:
  $$b_k = \Delta_1\left(a_1\right) \ , \quad b_{k-1} = \Delta_1\left(a_2\right) \ , \quad \ldots \quad , b_2 = \Delta_1\left(a_{k-1}\right) \ , \quad b_1 = \Delta_1\left(a_k\right) \ .$$
- לכל זוג מחרוזות $\begin{pmatrix} a_1 & a_2 & \cdots a_{k-1} & a_k \end{pmatrix} \begin{pmatrix} b_1 & b_2 & \cdots b_{k-1} & b_k \end{pmatrix}$ ב- $\Delta_5\Delta_2$:
  $$b_k = \Delta_1\left(a_1\right) \ , \quad b_{k-1} = \Delta_1\left(a_2\right) \ , \quad \ldots \quad , b_2 = \Delta_1\left(a_{k-1}\right) \ , \quad b_1 = \Delta_1\left(a_k\right) \ .$$
- לכל זוג מחרוזות $\begin{pmatrix} a_1 & a_2 & \cdots a_{k-1} & a_k \end{pmatrix} \begin{pmatrix} b_1 & b_2 & \cdots b_{k-1} & b_k \end{pmatrix}$ ב- $\Delta_6\Delta_3$:
  $$b_k = \Delta_1\left(a_1\right) \ , \quad b_{k-1} = \Delta_1\left(a_2\right) \ , \quad \ldots \quad , b_2 = \Delta_1\left(a_{k-1}\right) \ , \quad b_1 = \Delta_1\left(a_k\right) \ .$$

# 7 תורת שאנון וסודיות מושלמת

**הסתברויות של האותיות:**

| אות | הסתברות | אות | הסתברות | אות | הסתברות | אות | הסתברות | אות | הסתברות |
|---|---|---|---|---|---|---|---|---|---|
| a | 0.082 | f | 0.022 | k | 0.008 | p | 0.019 | u | 0.028 |
| b | 0.015 | g | 0.02 | l | 0.04 | q | 0.001 | v | 0.01 |
| c | 0.028 | h | 0.061 | m | 0.024 | r | 0.06 | w | 0.023 |
| d | 0.043 | i | 0.07 | n | 0.067 | s | 0.063 | x | 0.001 |
| e | 0.127 | j | 0.002 | o | 0.075 | t | 0.091 | y | 0.02 |
| | | | | | | | | z | 0.001 |

**קבוצות תדירויות של האותיות בטקטס:**

| | אות | הסתברות |
|---|---|---|
| 1. | e | $p = 0.127$ |
| 2. | t,a,o,i,n,s,h,r | $0.06 \lessapprox p \lessapprox 0.09$ |
| 3. | d,l | $p \approx 0.04$ |
| 4. | c,u,m,w,f,g,y,p,b | $0.015 \lessapprox p \lessapprox 0.028$ |
| 5. | v,k,j,x,q,z | $p < 0.01$ |

**זוגות האותיות הנפוצים ביותר:**

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| th | he | in | er | an | re | ed | on | es | st |
| en | at | to | nt | ha | nd | ou | ea | ng | as |
| or | ti | is | et | it | ar | te | se | hi | of |

**שלשות של אותיות הנפוצים ביותר:**

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| the | ing | and | her | ere | ent | tha | nth | was | eth | for | dth |

**מידע** של מ"מ בדיד $X$: $I_X(x) = -\log_2(P_X(x))$.

**אנטרופיה** של מ"מ בדיד $X$: $H[X] = -\sum_{i=1}^{N} P_X(x_i)\log_2(P_X(x_i))$.

**נוסחת בייס**:

$$P(X=x|Y=y)P(Y=y) = P(X=x \cap Y=y) = P(Y=y|X=x)P(X=x) \ .$$

**סודיות**:

נתונה קריפטו-מערכת בעלת קבוצת טקסט גלוי $X$, קבוצת טקסט מוצפן $Y$ וקבוצת מפתחות $K$, כלל מצפין $y = e_k(x)$ וכלל מפענח $x = d_k(y)$.

$$P(Y=y)=\sum_{k\in K}P(K=k)P\left(X=d_k(y)\right)\ ,$$

$$P(Y=y|X=x)=\sum_{\substack{k\in K\\ x=d_k(y)}}P(K=k)\ ,$$

$$P(X=x|Y=y)=\frac{P(X=x)\sum_{\substack{k\in K\\ x=d_k(y)}}P(K=k)}{\sum_{k\in K}P(K=k)P\left(X=d_k(y)\right)}\ .$$

**סודיות מושלמת**: לקריפטו-מערכת יש סודיות מושלמת אם התנאי הבא מתקיים:

$$P(X=x|Y=y)=P(X=x)\qquad\Longleftrightarrow\qquad P(Y=y|X=x)=P(Y=y)\ .$$

**אנטרופיה מותנית**:

$$H(X|Y=y)=-\sum_{x\in X}P(X=x|Y=y)\log_2 P(X=x|Y=y)\ ,$$

$$H(X|Y)=-\sum_{y\in Y}\sum_{x\in X}P(Y=y)P(X=x|Y=y)\log_2 P(X=x|Y=y)\ ,$$

$$H(X,Y)=H(Y)+H(X|Y)\ ,\qquad H(X|Y)\le H(X)\ .$$

**משפט האנטרופיה לקריפו-מערכת:**

$$H(K|C)=H(K)+H(P)-H(C)\ .$$

**טבלת אמת**:

| $p$ | $q$ | $p\wedge q$ | $p\vee q$ | $\sim p$ | $p\oplus q$ |
|---|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 0 | 0 |
| 1 | 0 | 0 | 1 | 0 | 1 |
| 0 | 1 | 0 | 1 | 1 | 1 |
| 0 | 0 | 0 | 0 | 1 | 0 |

# 8 צופן פייסטל

**ספרות הקסדצימליות**:

| hex | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| binary | 0000 | 0001 | 0010 | 0011 | 0100 | 0101 | 0110 | 0111 |
| hex | 8 | 9 | A | B | C | D | E | F |
| binary | 1000 | 1001 | 1010 | 1011 | 1100 | 1101 | 1110 | 1111 |

**משוואות פייסטל להצפנה:**
נתון טקטסט גלוי $x = L_0R_0$. לכל $1 \le i \le N$:

$$L_i = R_{i-1} \ , \qquad R_i = L_{i-1} \oplus f(R_{i-1}, k_i) \ , \qquad y = R_N L_N \ .$$

**משוואות פייסטל לפענוח:**
נתון טקטסט גלוי $y = R_N L_N$. לכל $1 \le i \le N$:

$$R_i = L_{i+1} \ , \qquad L_i = R_{i+1} \oplus f(R_i, k_{i+1}) \ , \qquad x = L_0 R_0 \ .$$

# 9 צופן IDEA

**תזמון מפתח של IDEA**

| $r$ | $k_1$ | $k_2$ | $k_3$ | $k_4$ | $k_5$ | $k_6$ |
|---|---|---|---|---|---|---|
| 1 | $0-15$ | $16-31$ | $32-47$ | $48-63$ | $64-79$ | $80-95$ |
| 2 | $96-111$ | $112-127$ | $25-40$ | $41-56$ | $57-72$ | $73-88$ |
| 3 | $89-104$ | $105-120$ | $121-8$ | $9-24$ | $50-65$ | $66-81$ |
| 4 | $82-97$ | $98-113$ | $114-1$ | $2-17$ | $18-33$ | $34-49$ |
| 5 | $75-90$ | $91-106$ | $107-122$ | $123-10$ | $11-26$ | $27-42$ |
| 6 | $43-58$ | $59-74$ | $100-115$ | $116-3$ | $4-19$ | $20-35$ |
| 7 | $36-51$ | $52-67$ | $68-83$ | $84-99$ | $125-12$ | $13-28$ |
| 8 | $29-44$ | $45-60$ | $61-76$ | $77-92$ | $93-108$ | $109-124$ |
| 9 | $22-37$ | $38-53$ | $54-69$ | $70-85$ | $-$ | $-$ |

**אלגוריתם הצפנת IDEA**

- נתון טקסט גלוי $P \in \{0,1\}^{64}$. של אורך 64 ביטים.
- מחלקים $P$ לארבע בלוקים $P_i \in \{0,1\}^{16}$: $P = P_1P_2P_3P_4$.
- בתחילת מחזור ה- $r$ ($1 \le r \le 9$) מסמנים את הטקסט מוצפן המתקבל ממחזור הקודם (מחזור $r-1$) ב- $C^{(r)}$, מלבד מ- $C^{(1)} = X$.
- כל מחזור $r$ מורכב מהשלבים הבאים:

$$Y_1 = C_1^{(r)} \odot k_1^{(r)} = C_1^{(r)} \cdot k_1^{(r)} \mod (2^{16}+1) \qquad [1]$$

$$Y_2 = C_2^{(r)} \boxplus k_2^{(r)} = C_2^{(r)} + k_2^{(r)} \mod 2^{16} \qquad [2]$$

$$Y_3 = C_3^{(r)} \boxplus k_3^{(r)} = C_3^{(r)} + k_3^{(r)} \mod 2^{16} \qquad [3]$$

$$Y_4 = C_4^{(r)} \odot k_4^{(r)} = C_4^{(r)} \cdot k_4^{(r)} \mod (2^{16}+1) \qquad [4]$$

$$Y_5 = Y_1 \oplus Y_3 \qquad [5]$$

$$Y_6 = Y_2 \oplus Y_4 \qquad [6]$$

$$Y_7 = Y_5 \odot k_5^{(r)} = Y_5 \cdot k_5^{(r)} \mod (2^{16}+1) \qquad [7]$$

$$Y_8 = Y_6 \boxplus Y_7 = Y_6 + Y_7 \mod 2^{16} \qquad [8]$$

$$Y_9 = Y_8 \odot k_6^{(r)} = Y_8 \cdot k_6^{(r)} \mod 2^{16}+1 \qquad [9]$$

$$Y_{10} = Y_7 \boxplus Y_9 = Y_7 + Y_9 \mod 2^{16} \qquad [10]$$

$$C_1^{(r+1)} = Y_1 \oplus Y_9 \qquad [11]$$

$$C_2^{(r+1)} = Y_3 \oplus Y_9 \qquad [12]$$

$$C_3^{(r+1)} = Y_2 \oplus Y_{10} \qquad [13]$$

$C_4^{(r+1)} = Y_4 \oplus Y_{10}$ [14]

- בכדי לקבל את הטקסט מוצפן הסופי, אחרי ביצוע של כל המחזורים $r$ מבצעים את השלב התפוקה:

$C_1 = C_1^{(9)} \odot k_1^{(9)} = C_1^{(9)} \cdot k_1^{(9)} \mod 2^{16}+1$ [1]

$C_2 = C_3^{(9)} \boxplus k_2^{(9)} = C_3^{(9)} + k_2^{(9)} \mod 2^{16}$ [2]

$C_3 = C_2^{(9)} \boxplus k_3^{(9)} = C_2^{(9)} + k_3^{(9)} \mod 2^{16}$ [3]

$C_4 = C_4^{(9)} \odot k_4^{(9)} = C_4^{(9)} \cdot k_4^{(9)} \mod 2^{16}+1$ [4]

- לבסוף הטקסט מוצפן 64- ביטים מתקבל מהארבע בלוקים 16- ביטים $C = C_1C_2C_3C_4$.

**מפתחות פענוח של IDEA**

$$DK_1^{(1)} = \left(K_1^{(9)}\right)^{-1} , \quad DK_2^{(1)} = -\left(K_2^{(9)}\right) , \quad DK_3^{(1)} = -\left(K_3^{(9)}\right) , \quad DK_4^{(1)} = \left(K_4^{(9)}\right)^{-1} ,$$
$$DK_5^{(1)} = K_5^{(8)} , \quad DK_6^{(1)} = K_6^{(8)} .$$

## 10 צופן DES

**אלגוריתם הצפנת DES :** נתון טקסט גלוי 64 ביטים $x = x_1 \dots x_{64}$.

**שלב [1]** מבצעים $IP(x_1, x_2, \dots, x_{64})$ כאשר $IP$ התמורה הסטטית ההתחלתית:

$$IP = \begin{pmatrix} 58 & 50 & 42 & 34 & 26 & 18 & 10 & 2 & 60 & 52 & 44 & 36 & 28 & 20 & 12 & 4 \\ 62 & 54 & 46 & 38 & 30 & 22 & 14 & 6 & 64 & 56 & 48 & 40 & 32 & 24 & 16 & 8 \\ 57 & 49 & 41 & 33 & 25 & 17 & 9 & 1 & 59 & 51 & 43 & 35 & 27 & 19 & 11 & 3 \\ 61 & 53 & 45 & 37 & 29 & 21 & 13 & 5 & 63 & 55 & 47 & 39 & 31 & 23 & 15 & 7 \end{pmatrix}.$$

**שלב [2]** מחלקים $IP(x) = L_0R_0$ לשניים. $L_0$ כאשר ה-32 ביטים הראשונים של $x_0$ ו- $R_0$ ה- 32 האחרונים:

$$L_0 = x_{58}, x_{50}, x_{42}, x_{34}, x_{26}, x_{18}, x_{10}, x_2, x_{60}, x_{52}, x_{44}, x_{36}, x_{28}, x_{20}, x_{12}, x_4$$
$$x_{62}, x_{54}, x_{46}, x_{38}, x_{30}, x_{22}, x_{14}, x_6, x_{64}, x_{56}, x_{48}, x_{40}, x_{32}, x_{24}, x_{16}, x_8 ,$$

$$R_0 = x_{57}, x_{49}, x_{41}, x_{33}, x_{25}, x_{17}, x_9, x_1, x_{59}, x_{51}, x_{43}, x_{35}, x_{27}, x_{19}, x_{11}, x_3$$
$$x_{61}, x_{53}, x_{45}, x_{37}, x_{29}, x_{21}, x_{13}, x_5, x_{63}, x_{55}, x_{47}, x_{39}, x_{31}, x_{23}, x_{15}, x_7 .$$

**שלב [3]** מבצעים 16 מחזורים של אלגוריתם פייסטל: $L_i = R_{i-1} , \qquad R_i = L_{i-1} \oplus f\left(R_{i-1}, k_i\right).$

כאשר $k_1, \dots, k_{16}$ תת-מפתחות כל אחד 48 ביטים שמתקבלים ממפתח התחלתי $k$.

**שלב [4]** $y = IP^{-1}\left(R_{16}L_{16}\right)$ כאשר $IP^{-1}$ התמורה ההופכית:

$$IP^{-1} = \begin{pmatrix} 40 & 8 & 48 & 16 & 56 & 24 & 64 & 32 & 39 & 7 & 47 & 15 & 55 & 23 & 63 & 31 \\ 38 & 6 & 46 & 14 & 54 & 22 & 62 & 30 & 37 & 5 & 45 & 13 & 53 & 21 & 61 & 29 \\ 36 & 4 & 44 & 12 & 53 & 20 & 60 & 28 & 35 & 3 & 43 & 11 & 51 & 19 & 59 & 27 \\ 34 & 2 & 42 & 10 & 50 & 18 & 58 & 26 & 33 & 1 & 41 & 9 & 49 & 17 & 57 & 25 \end{pmatrix}$$

**הפונקציית ליבה של DES**

$$f : \{0,1\}^{32} \times \{0,1\}^{48} \to \{0,1\}^{32}.$$

נסמן הארגומנטים של $f$ ב- $f(A, J)$ כאשר $A \in \{0,1\}^{32}$, $J \in \{0,1\}^{48}$. $f$ מתוארת על ידי האלגוריתם הבא:

**שלב [1]** מגדילים $A$ לרצף 48 ביטים באמצעות התמורה ההגדלה

$$E = \begin{pmatrix} 32 & 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 6 & 7 & 8 & 9 \\ 8 & 9 & 10 & 11 & 12 & 13 \\ 12 & 13 & 14 & 15 & 16 & 17 \\ 16 & 17 & 18 & 19 & 20 & 21 \\ 20 & 21 & 22 & 23 & 24 & 25 \\ 24 & 25 & 26 & 27 & 28 & 29 \\ 28 & 29 & 30 & 31 & 32 & 1 \end{pmatrix}$$

**שלב [2]** מחשבים $E(A) \oplus J$ ורושמים התשובה כשירשור של שמונה רצפים 6 ביטים:

$$B = B_1B_2B_3B_4B_5B_6B_7B_8 \ , \qquad B_j \in \{0,1\}^6 \ .$$

**שלב [3]** רושמים $B_j = b_1b_2b_3b_4b_5b_6$ כאשר $b_i \in \{0,1\}$.

**שלב [4]** בשלב זה משתמשים ההחלפות $S_1, \ldots, S_8$. כל $S_j$ היא מטריצה מסדר $4\times16$ שנתון למטה. לכל $1 \le j \le 8$:

$$C_j = \left(S_j(r,c)\right)_2 \ , \qquad r = (b_1b_6)_{10} \ , \qquad c = (b_2b_3b_4b_5)_{10}$$

כאשר $r$ בספרות דצמליות, $c$ בספרות דצמליות, ו- $S_j(r,c)$ האיבר בשורה $r$ ועמודה $c$ של המטריצה $S_j$. לבסוף ממירים $C_j$ לספרות ביניאריות.

**שלב [5]** $f(A,J) = P(C_1C_2C_3C_4C_5C_6C_7C_8)$ כאשר $P$ התמורה

$$P = \begin{pmatrix} 16 & 7 & 20 & 21 \\ 29 & 12 & 28 & 17 \\ 1 & 15 & 23 & 26 \\ 5 & 18 & 31 & 10 \\ 2 & 8 & 24 & 14 \\ 32 & 27 & 3 & 9 \\ 19 & 13 & 30 & 6 \\ 22 & 11 & 4 & 25 \end{pmatrix}.$$

**התזמון המפתח של DES:** נתון מפתח התחלתי 64 ביטים, $k$.

**שלב [1]** מבצעים התמורה

$$PC_1 = \begin{pmatrix} 57 & 49 & 41 & 33 & 25 & 17 & 9 \\ 1 & 58 & 50 & 42 & 34 & 26 & 18 \\ 10 & 2 & 59 & 51 & 43 & 35 & 27 \\ 19 & 11 & 3 & 60 & 52 & 44 & 36 \\ 63 & 55 & 47 & 39 & 31 & 23 & 15 \\ 7 & 62 & 54 & 46 & 38 & 30 & 22 \\ 14 & 6 & 61 & 53 & 45 & 37 & 29 \\ 21 & 13 & 5 & 28 & 20 & 12 & 4 \end{pmatrix}$$

**שלב [2]** נסמן $PC_1(k) = C_0D_0$ כאשר $C_0$ ה- 28 ביטים הראשונים ו- $D_0$ ה- 28 ביטים האחרונים.

**שלב [3]** לכל $1 \le i \le 16$, מחשבים $C_i = LS_i\left(C_{i-1}\right) \ , \qquad D_i = LS_i\left(D_{i-1}\right) \ , \qquad k_i = PC_2\left(C_iD_i\right).$

כאשר $LS_i = \begin{cases} \text{הזזה מקום אחת שמאולה} & i = 1,2,9,16, \\ \text{הזזה שתי מקומות שמאלה} & i = 3,4,5,6,7,8,10,11,12,13,14,15 \ , \end{cases}$ ו- $PC_2$ התמורה

$$PC_2 = \begin{pmatrix} 14 & 17 & 11 & 24 & 1 & 5 \\ 3 & 28 & 15 & 6 & 21 & 10 \\ 23 & 19 & 12 & 4 & 26 & 8 \\ 16 & 7 & 27 & 20 & 13 & 2 \\ 41 & 52 & 31 & 37 & 47 & 55 \\ 30 & 40 & 51 & 45 & 33 & 48 \\ 44 & 49 & 39 & 56 & 34 & 53 \\ 46 & 42 & 50 & 36 & 29 & 32 \end{pmatrix}.$$

**הבלוקים של ההחלפות של DES**

| | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $S_1$ | 14 | 4 | 13 | 1 | 2 | 15 | 11 | 8 | 3 | 10 | 6 | 12 | 5 | 9 | 0 | 7 |
| | 0 | 15 | 7 | 4 | 14 | 2 | 13 | 1 | 10 | 6 | 12 | 11 | 9 | 5 | 3 | 8 |
| | 4 | 1 | 14 | 8 | 13 | 6 | 2 | 11 | 15 | 12 | 9 | 7 | 3 | 10 | 5 | 0 |
| | 15 | 12 | 8 | 2 | 4 | 9 | 1 | 7 | 5 | 11 | 3 | 14 | 10 | 0 | 6 | 13 |
| $S_2$ | 15 | 1 | 8 | 14 | 6 | 11 | 3 | 4 | 9 | 7 | 2 | 13 | 12 | 0 | 5 | 10 |
| | 3 | 13 | 4 | 7 | 15 | 2 | 8 | 14 | 12 | 0 | 1 | 10 | 6 | 9 | 11 | 5 |
| | 0 | 14 | 7 | 11 | 10 | 4 | 13 | 1 | 5 | 8 | 12 | 6 | 9 | 3 | 2 | 15 |
| | 13 | 8 | 10 | 1 | 3 | 15 | 4 | 2 | 11 | 6 | 7 | 12 | 0 | 5 | 14 | 9 |
| $S_3$ | 10 | 0 | 9 | 14 | 6 | 3 | 15 | 5 | 1 | 13 | 12 | 7 | 11 | 4 | 2 | 8 |
| | 13 | 7 | 0 | 9 | 3 | 4 | 6 | 10 | 2 | 8 | 5 | 14 | 12 | 11 | 15 | 1 |
| | 13 | 6 | 4 | 9 | 8 | 15 | 3 | 0 | 11 | 1 | 2 | 12 | 5 | 10 | 14 | 7 |
| | 1 | 10 | 13 | 0 | 6 | 9 | 8 | 7 | 4 | 15 | 14 | 3 | 11 | 5 | 2 | 12 |
| $S_4$ | 7 | 13 | 14 | 3 | 0 | 6 | 9 | 10 | 1 | 2 | 8 | 5 | 11 | 12 | 4 | 15 |
| | 13 | 8 | 11 | 5 | 6 | 15 | 0 | 3 | 4 | 7 | 2 | 12 | 1 | 10 | 14 | 9 |
| | 10 | 6 | 9 | 0 | 12 | 11 | 7 | 13 | 15 | 1 | 3 | 14 | 5 | 2 | 8 | 4 |
| | 3 | 15 | 0 | 6 | 10 | 1 | 13 | 8 | 9 | 4 | 5 | 11 | 12 | 7 | 2 | 14 |
| $S_5$ | 2 | 12 | 4 | 1 | 7 | 10 | 11 | 6 | 8 | 5 | 3 | 15 | 13 | 0 | 14 | 9 |
| | 14 | 11 | 2 | 12 | 4 | 7 | 13 | 1 | 5 | 0 | 15 | 10 | 3 | 9 | 8 | 6 |
| | 4 | 2 | 1 | 11 | 10 | 13 | 7 | 8 | 15 | 9 | 12 | 5 | 6 | 3 | 0 | 14 |
| | 11 | 8 | 12 | 7 | 1 | 14 | 2 | 13 | 6 | 15 | 0 | 9 | 10 | 4 | 5 | 3 |
| $S_6$ | 12 | 1 | 10 | 15 | 9 | 2 | 6 | 8 | 0 | 13 | 3 | 4 | 14 | 7 | 5 | 11 |
| | 10 | 15 | 4 | 2 | 7 | 12 | 9 | 5 | 6 | 1 | 13 | 14 | 0 | 11 | 3 | 8 |
| | 9 | 14 | 15 | 5 | 2 | 8 | 12 | 3 | 7 | 0 | 4 | 10 | 1 | 13 | 11 | 6 |
| | 4 | 3 | 2 | 12 | 9 | 5 | 15 | 10 | 11 | 14 | 1 | 7 | 6 | 0 | 8 | 13 |
| $S_7$ | 4 | 11 | 2 | 14 | 15 | 0 | 8 | 13 | 3 | 12 | 9 | 7 | 5 | 10 | 6 | 1 |
| | 13 | 0 | 11 | 7 | 4 | 9 | 1 | 10 | 14 | 3 | 5 | 12 | 2 | 15 | 8 | 6 |
| | 1 | 4 | 11 | 13 | 12 | 3 | 7 | 14 | 10 | 15 | 6 | 8 | 0 | 5 | 9 | 2 |
| | 6 | 11 | 13 | 8 | 1 | 4 | 10 | 7 | 9 | 5 | 0 | 15 | 14 | 2 | 3 | 12 |
| $S_8$ | 13 | 2 | 8 | 4 | 6 | 15 | 11 | 1 | 10 | 9 | 3 | 14 | 5 | 0 | 12 | 7 |
| | 1 | 15 | 13 | 8 | 10 | 3 | 7 | 4 | 12 | 5 | 6 | 11 | 0 | 14 | 9 | 2 |
| | 7 | 11 | 4 | 1 | 9 | 12 | 14 | 2 | 0 | 6 | 10 | 13 | 15 | 3 | 5 | 8 |
| | 2 | 1 | 14 | 7 | 4 | 10 | 8 | 13 | 15 | 12 | 9 | 0 | 3 | 5 | 6 | 11 |

# פתרונות

## שאלה 1

**א)**

$$n = pq = 37 \times 41 = 1517$$

$$\phi(n) = \phi(pq) = (p-1)(q-1) = 36 \times 40 = 1440 \ .$$

$a = b^{-1} \bmod \phi(n) = 31^{-1} \bmod 1440$. נחשב את $31^{-1} \bmod 1440$ בעזרת האלגוריתם המוכלל של אוקלידס. נסמן $A = 1440, B = 31$.

$$\begin{aligned} r_0 &= A = 1440 \ , & r_1 &= B = 31 \ , \\ s_0 &= 1 \ , & s_1 &= 0 \ , \\ t_0 &= 0 \ , & t_1 &= 1 \ . \end{aligned}$$

| | | | | |
|---|---|---|---|---|
| שלב $i = 1$: | $t_2 = 0 - 46 \cdot 1 = -46$ | $s_2 = 1 - 46 \cdot 0 = 1$ | $r_2 = 1440 - 46 \cdot 31 = 14$ | $q_1 = 46$ |
| שלב $i = 2$: | $t_3 = 1 - 2 \cdot (-46) = 93$ | $s_3 = 0 - 2 \cdot 1 = -2$ | $r_3 = 31 - 2 \cdot 14 = 3$ | $q_2 = 2$ |
| שלב $i = 3$: | $t_4 = -46 - 4 \cdot (93) = -418$ | $s_4 = 1 - 4 \cdot (-2) = 9$ | $r_4 = 14 - 4 \cdot 3 = 2$ | $q_3 = 4$ |
| שלב $i = 4$: | $t_5 = 93 - 1 \cdot (-418) = 511$ | $s_5 = -2 - 1 \cdot (9) = -11$ | $r_5 = 3 - 1 \cdot 2 = 1$ | $q_4 = 1$ |
| שלב $i = 5$: | $t_6 = -418 - 2 \cdot (511) = -1440$ | $s_6 = 9 - 2 \cdot (-11) = 31$ | $r_6 = 2 - 2 \cdot 1 = 0$ | $q_5 = 2$ |

$$\gcd(a, b) = r_5 = 1 \ , \qquad s = s_5 = -11 \ , \qquad y = t_5 = 511 \ .$$

$$(-11)(1440) + (511)(31) = 1 \ .$$

מכאן

$$31^{-1} \equiv 511 \mod 1440 \ .$$

לכן $a = b^{-1} \bmod \phi(n) = 31^{-1} \bmod 1440 = 511$.

**ב)** $\texttt{BCCI} \to 1228$. ההצפנה ניתנת ע"י הכלל מצפין:

$$y = x^b \bmod n = 1228^{31} \bmod 1517 \ .$$

נחשב את החזקה המודולרית בעזרת השיטת הריבועיים באופן הבא.

$$b = 31 = 16 + 8 + 4 + 2 + 1 = [11111]_2 = b_4 b3 b_2 b_1 b_0 \ .$$

$i \leftarrow 0, z_0 \leftarrow 1228 \bmod n = 1228$.

$$\begin{aligned}
z_1 =& z_0^2 \bmod n &&= (1228)^2 \bmod 1517 &&= 86\\
z_2 =& z_1^2 \bmod n &&= (86)^2 \bmod 1517 &&= 1328\\
z_3 =& z_2^2 \bmod n &&= (1328)^2 \bmod 1517 &&= 830\\
z_4 =& z_3^2 \bmod n &&= (830)^2 \bmod 1517 &&= 182\ .
\end{aligned}$$

$i \leftarrow 0, y \leftarrow 1$.

$$\begin{aligned}
y \leftarrow& (y)(z_0) \bmod n &&= (1228) \bmod 1517 &&= 1228\\
y \leftarrow& (y)(z_1) \bmod n &&= (1228)(86) \bmod 1517 &&= 935\\
y \leftarrow& (y)(z_2) \bmod n &&= (935)(1328) \bmod 1517 &&= 774\\
y \leftarrow& (y)(z_3) \bmod n &&= (774)(830) \bmod 1517 &&= 729\\
y \leftarrow& (y)(z_4) \bmod n &&= (729)(182) \bmod 1517 &&= 699\ .
\end{aligned}$$

לכן הטקסט מוצפן הינו $y = 699 \rightarrow \texttt{GJJ}$.

**ג)** $y = \texttt{GJJ} \rightarrow 699$. נחשב את הטקסט הגלוי המקורי:

$$y \bmod p = 699 \bmod 37 = 33\ , \qquad a \bmod (p-1) = 511 \bmod 36 = 7\ .$$

לכן

$$\begin{aligned}
x_1 =& (y \bmod p)^{a \bmod (p-1)} \bmod p\\
=& 33^7 \bmod 37\\
=& \left(33^2 \bmod 37\right)\left(33^2 \bmod 37\right)\left(33^2 \bmod 37\right)(33 \bmod 37) \bmod 37\\
=& \left(16^2 \bmod 37\right)((16)(37) \bmod 37) \bmod 37\\
=& (34)(10) \bmod 37\\
=& 7\ .
\end{aligned}$$

בנוסף

$$y \bmod q = 699 \bmod 41 = 2\ , \qquad a \bmod (q-1) = 511 \bmod 40 = 31\ .$$

לכן

$$x_2 = (y \bmod q)^{a \bmod (q-1)} \bmod q = 2^{31} \bmod 41 = 39$$

$$\begin{aligned}
x_2 =& (y \bmod q)^{a \bmod (q-1)} \bmod q\\
=& 2^{31} \bmod 41\\
=& \left(2^8 \bmod 41\right)\left(2^8 \bmod 41\right)\left(2^8 \bmod 41\right)\left(2^7 \bmod 41\right) \bmod 41\\
=& (10)(10)(10)(5) \bmod 41\\
=& 39\ .
\end{aligned}$$

לבסוף עלינו לפתור את המערכת הבאה:

$$\begin{aligned}
x =& x_1 \bmod p &&= 7 \bmod 37\ ,\\
x =& x_2 \bmod q &&= 39 \bmod 41\ .
\end{aligned}$$

נתפור את המערכת הזאת בעזרת המשפט השאריות הסיני. נסמן $a_1 = 7$, $m_1 = 37$, $a_2 = 39$, $m_2 = 41$.

$$M = m_1 m_2 = (37)(41) = 1517 \ , \qquad M_1 = \frac{M}{m_1} = 41 \ , \qquad M_2 = \frac{M}{m_2} = 37 \ .$$

מכיוון ש: $10(37) - 9(41) = 1$ אז $37^{-1} \equiv 10 \bmod 41$ ו- $41^{-1} \equiv -9 \bmod 37 \equiv 28 \bmod 37$.
לפיכך: $y_1 = M_1^{-1} \bmod m_1 = 41^{-1} \mod 37 = 28$ ו- $y_2 = M_2^{-1} \bmod m_2 = 37^{-1} \mod 41 = 10$.
לכן

$$\begin{aligned} x =& a_1 M_1 y_1 + a_2 M_2 y_2 \mod M \\ =& 7(41)(28) + 39(37)(10) \mod 1517 \\ =& 22466 \mod 1517 \\ =& 1228 \to \texttt{BCCI} \ . \end{aligned}$$

**ד)** <u>כיוון $\Leftarrow$</u>

נניח בשלילה כי למשוואה $ax \equiv y \pmod m$ יש פתרון יחיד $x = x_1$ אבל $\gcd(a, m) = d > 1$.

אזי $ax_1 \equiv \pmod m$ ולכן קיים $q$ שלם עבורו $ax_1 = qm + y$.
לכן $\frac{am}{d}$ הוא שלם ולכן $ax_1 + \frac{am}{d} = qm + y + \frac{am}{d}$.
מכאן $a\left(x_1 + \frac{m}{d}\right) = \left(q + \frac{a}{d}\right) m + y$, ז"א קיים שלם $Q = q + \frac{a}{d}$ כך ש-

$$a\left(x_1 + \frac{m}{d}\right) = Qm + y \quad \Rightarrow \quad a\left(x_1 + \frac{m}{d}\right) \equiv y \pmod m$$

ולכן $ax_2 \equiv y \pmod m$ כאשר $x_2 = x_1 + \frac{m}{d}$.
לכן $x_2$ הוא גם פתרון, בסתירה לכך שיש רק פתרון יחיד.

<u>כיוון $\Rightarrow$</u>

ננחיח ש: $\gcd(a, m) = 1$ ונניח בשלילה כי יש שני פתרונות $x_1 \not\equiv x_2 \pmod{26}$. כלומר:

$$ax_1 \equiv y \pmod m \quad \text{ו-} \quad ax_2 \equiv y \pmod m \ .$$

לפי טרנזיטיביות $ax_1 \equiv ax_2 \pmod m$ ולכן $m \mid a(x_1 - x_2)$.
$\gcd(a, m) = 1$ לכן $m \nmid a$ לכן $m \mid x_1 - x_2$ לכן $x_1 \equiv x_2 \pmod{26}$, בסתירה לכך ש- $x_1 \not\equiv x_2 \pmod{26}$.

## שאלה 2

**א)**

$$
\begin{aligned}
2(16)+1 \mod 3 &= 33 \mod 3 = 0\\
2(16)+2 \mod 3 &= 34 \mod 3 = 1\\
2(16)+3 \mod 3 &= 35 \mod 3 = 2\\
2(16)+4 \mod 3 &= 36 \mod 3 = 0
\end{aligned}
$$

$$
\begin{aligned}
2(17)+1 \mod 3 &= 35 \mod 3 = 2\\
2(17)+2 \mod 3 &= 36 \mod 3 = 0\\
2(17)+3 \mod 3 &= 37 \mod 3 = 1\\
2(17)+4 \mod 3 &= 38 \mod 3 = 2
\end{aligned}
$$

$$
\begin{aligned}
2(18)+1 \mod 3 &= 37 \mod 3 = 1\\
2(18)+2 \mod 3 &= 38 \mod 3 = 2\\
2(18)+3 \mod 3 &= 39 \mod 3 = 0\\
2(18)+4 \mod 3 &= 40 \mod 3 = 1
\end{aligned}
$$

| $K \backslash X$ | q | r | s |
|---|---|---|---|
| $k_1$ | a | c | b |
| $k_2$ | b | a | c |
| $k_3$ | c | b | a |
| $k_4$ | a | c | b |

$$
\begin{aligned}
P_Y(\mathtt{a}) =& P_K(k_1)P_X(\mathtt{q}) + P_K(k_2)P_X(\mathtt{r}) + P_K(k_3)P_X(\mathtt{s}) + P_K(k_4)P_X(\mathtt{q})\\
=& \left(\frac{1}{4}\right)\left(\frac{1}{3}\right) + \left(\frac{1}{4}\right)\left(\frac{1}{4}\right) + \left(\frac{1}{4}\right)\left(\frac{5}{12}\right) + \left(\frac{1}{4}\right)\left(\frac{1}{3}\right)\\
=& \frac{1}{3} \quad .
\end{aligned}
$$

$$
\begin{aligned}
P_Y(\mathtt{b}) =& P_K(k_1)P_X(\mathtt{s}) + P_K(k_2)P_X(\mathtt{q}) + P_K(k_3)P_X(\mathtt{r}) + P_K(k_4)P_X(\mathtt{s})\\
=& \left(\frac{1}{4}\right)\left(\frac{5}{12}\right) + \left(\frac{1}{4}\right)\left(\frac{1}{3}\right) + \left(\frac{1}{4}\right)\left(\frac{1}{4}\right) + \left(\frac{1}{4}\right)\left(\frac{5}{12}\right)\\
=& \frac{17}{48} \quad .
\end{aligned}
$$

$$
\begin{aligned}
P_Y(\mathtt{c}) =& P_K(k_1)P_X(\mathtt{r}) + P_K(k_2)P_X(\mathtt{s}) + P_K(k_3)P_X(\mathtt{q}) + P_K(k_4)P_X(\mathtt{r})\\
=& \left(\frac{1}{4}\right)\left(\frac{1}{4}\right) + \left(\frac{1}{4}\right)\left(\frac{5}{12}\right) + \left(\frac{1}{4}\right)\left(\frac{1}{3}\right) + \left(\frac{1}{4}\right)\left(\frac{1}{4}\right)\\
=& \frac{5}{16} \quad .
\end{aligned}
$$

**ב)**

$$P(X=\mathtt{q}|Y=\mathtt{b}) = \frac{P(Y=\mathtt{b}|X=\mathtt{q})P(X=\mathtt{q})}{P(Y=\mathtt{b})} = \frac{P_X(\mathtt{q})P_K(k_2)}{P_Y(\mathtt{b})} = \frac{\left(\frac{1}{3}\right)\left(\frac{1}{4}\right)}{\left(\frac{17}{48}\right)} = \frac{4}{17}$$

$$P(X=\mathtt{r}|Y=\mathtt{c}) = \frac{P(Y=\mathtt{c}|X=\mathtt{r})P(X=\mathtt{r})}{P(Y=\mathtt{c})} = \frac{P_X(\mathtt{r})\left(P_K(k_1)+P_K(k_4)\right)}{P_Y(\mathtt{c})} = \frac{\left(\frac{1}{4}\right)\left(\frac{1}{4}+\frac{1}{4}\right)}{\left(\frac{5}{16}\right)} = \frac{2}{5}$$

דוגמה נגדית:

$$\frac{4}{17} = P(X=\mathtt{q}|Y=\mathtt{b}) \neq P(X=\mathtt{q}) = \frac{1}{3}\ .$$

לכן לקריפטו-מערכת אין סודיות מושלמת.

**ג)** <u>כיוון $\Leftarrow$</u>

יהי $d=\gcd(a,b)$. נניח כי $c|a$ וגם $c|b$. אזי קיימים שלמים $a'$ ו- $b'$ עבורם $a=ca'$ ו- $b=cb'$. לפי משפט בז'ו קיימים שלמים $s,t$ עבורם

$$d = sa+tb = sca'+tcb' = c\left(sa'+tb'\right)\ .$$

לכן לכל מחלק משותף $c$ של $a$ ו- $b$ מתקיים $c|d$.

<u>כיוון $\Rightarrow$</u>

נניח שעבור כל מחלק משותף $c$ של $a$ ו- $b$ מתקיים $c|d'$.

$\Leftarrow d'=qc \Leftarrow d'\leq c$.

מכיוון ש- $c|a$ ו- $c|b$ אזי $c\leq\gcd(a,b)$, בגלל ש- $\gcd(a,b)$ הוא המחלק המשותף הגדול ביותר של $a$ ו- $b$.

$\Leftarrow d'\leq c\leq\gcd(a,b) \Leftarrow d'\leq\gcd(a,b)$.

מצד שני, $\gcd(a,b)$ הוא עצמו מחלק משותף של $a$ ו- $b$, לכן לפי ההנחה ההתחלתית, $\gcd(a,b)\mid d'$ $\Leftarrow$ קיים שלם $Q$ עבורו $d'=Q\gcd(a,b) \Leftarrow \gcd(a,b)\leq d'$.

ז"א קיבלנו ש- $d'\leq\gcd(a,b)$ וגם $\gcd(a,b)\leq d'$ לכן בהכרח $d'=\gcd(a,b)$.

**ד)**

ראשית נוכיח כי $\gcd(a,b)\mid\gcd(b,a \bmod b)$.

לפי המשפט החילוק של אוקלידיס (משפט קיימים שלמים $q,r$ עבורם

$$a=qb+r=\left\lfloor\frac{a}{b}\right\rfloor b+(a \bmod b) \quad\Rightarrow\quad a \bmod b = a-\left\lfloor\frac{a}{b}\right\rfloor b\ .$$

לכן אם $d=\gcd(a,b)$ אזי $d \mid a$ ו- $d \mid b \Leftarrow d \mid (a \bmod b) \Leftarrow d \mid \gcd(b, a \bmod b)$.

כעת נוכיח כי $\gcd(b, a \bmod b) \mid \gcd(a,b)$.

נסמן $d=\gcd(b, a \bmod b)$. לכן $d \mid b$ ו- $d \mid (a \bmod b)$. לפי המשפט החילוק של אוקלידיס קיימים שלמים $q, r$ עבורם

$$a = qb + r = \left\lfloor \frac{a}{b} \right\rfloor b + (a \bmod b)$$

לכו $d \mid a$. ז"א $d \mid a$ וגם $d \mid b \Leftarrow d \mid \gcd(a,b)$.

הוכחנו כי $\gcd(b, a \bmod b) \mid \gcd(a,b)$ ו- $\gcd(a,b) \mid \gcd(b, a \bmod b)$ לפיכך :

$$\gcd(a,b) = \gcd(b, a \bmod b) \ .$$

## שאלה 3 (25 נקודות)

**א) (8 נק')**

המפתח הוא `goodluck`. לכן:

$$k_1 = 6, \quad k_2 = 14, \quad k_3 = 14, \quad k_4 = 3, \quad k_5 = 11, \quad k_6 = 20, \quad k_7 = 2, \quad k_8 = 10 \ .$$

$$\begin{aligned} e_k(\texttt{RWGWPHVY}) =& e_k(17, 22, 6, 22, 15, 7, 21, 24) \\ =& (17-6, 22-14, 6-14, 22-3, 15-11, 7-20, 21-2, 24-10) \bmod 26 \\ =& (11, 8, 18, 19, 4, 13, 19, 14) \bmod 26 \\ =& \texttt{LISTENTO} \end{aligned}$$

$$\begin{aligned} e_k(\texttt{ZVSKPUTD}) =& e_k(25, 21, 18, 10, 15, 20, 19, 3) \\ =& (25-6, 21-14, 18-14, 10-3, 15-11, 20-20, 19-2, 3-10) \bmod 26 \\ =& (19, 7, 4, 7, 4, 0, 17, 19) \bmod 26 \\ =& \texttt{THEHEART} \end{aligned}$$

הטקסט הגלוי המקורי הוא:

$$x = \texttt{listen to the heart} \ .$$

**ב) (8 נק')**

אם $k \in \mathbb{Z}_{26}^m$ אז לכל $x \in \mathbb{Z}_{26}^m$:

$$\begin{aligned} d_k(e_k(x)) =& d_k\big( (x_1+k_1 \ , \ x_2+k_2 \ , \ x_3+k_3, \quad \dots \quad , \ x_m+k_m \ ) \bmod 26 \big) \\ =& d_k\big( \ (x_1+k_1) \bmod 26 \ , \ (x_2+k_2) \bmod 26 \ , \quad \dots \quad , \ (x_m+k_m) \bmod 26 \ \big) \\ =& \big( \ \big[(x_1+k_1) \bmod 26 - k_1\big] \bmod 26 \ , \quad \dots \quad , \ \big[(x_m+k_m) \bmod 26\big] \bmod 26 \ \big) \ . \end{aligned}$$

כעת נוכיח כי $[(x+k) \bmod \bmod m - k] \bmod m = x \bmod m$:
לפי משפט החילוק של אוקלידס קיימים שלמים $q_1, r_1$ כך ש:

$$x + k = q_1 m + r_1 \ , \quad 0 \le r_1 < m \ ,$$

כאשר $q_1 = \left\lfloor \frac{x+k}{m} \right\rfloor$ וגם $r_1 = (x+k) \bmod m$. מכאן:

$$((x+k) \bmod m) - k = r_1 - k = x - q_1 m \ .$$

ז"א קיים שלם $Q = -q_1$ כך ש:

$$((x+k) \bmod m) - k = Qm + x$$

ולכן

$$((x+k) \bmod m) - k \equiv x \pmod m$$

ולפיכך, מכיוון שהשני שלמים $((x+k) \bmod m) - k$ ו- $x$ שקולים מודולריים ביחס ל- $m$, אז בהכרח יש להם אותה שארית בחלוקה ב- $m$:

$$[((x+k) \bmod m) - k] \bmod m = x \bmod m \ .$$

לכן:

$$d_k\left(e_k(x)\right) = \left( x_1 \bmod 26 \ , \quad \ldots \quad , \ x_m \bmod 26 \right) \bmod 26 = \left( x_1 \ , \quad \ldots \quad , \ x_m\right) \bmod 26 \ .$$

**ג)** <u>**כיוון** $\Leftarrow$</u>

נניח כי $\pi \in [z_1^{n_1} \ldots z_k^{n_k}]$. תהי $\pi_{i_j,z_j}$ מחזור באורך $z_j$ לכל $1 \le i_j \le n_j$, לכל $1 \le j \le k$. אזי:

$$\pi = \prod_{j=1}^{k} \prod_{i_j=1}^{n_j} \pi_{i_j,z_j} \ .$$

לכן

$$\pi^{-1} = \prod_{j=1}^{k} \prod_{i_j=1}^{n_j} \pi_{i_j,z_j}^{-1} \ .$$

מכיוון שהתמורה ההופכית של מחזור באורך $z$ הוא גם מחזור באורך $z$ אזי

$$\pi^{-1} \in [z_1^{n_1} \ldots z_k^{n_k}] \ .$$

<u>**כיוון** $\Rightarrow$</u>

**ד)**

<u>כיוון $\Leftarrow$</u>

נניח ש- $a \equiv b \pmod m$. אזי קיים שלם $Q$ כך ש:

$$a = qm + b \ .$$

לפי משפט החילוק של אוקלידס,

$$b = \bar{q}m = r_1 \ , \qquad r_1 = b \bmod m \ .$$

לכן

$$a = (q + \bar{q})\, m + r_1 = Qm + r_1$$

כאשר $Q = q + \bar{q}$ שלם ו- $0 \le r_1 < b$ הוא השארית $r_1 = b \bmod m$. מכאן נובע ש:

$$a \bmod m = a - m \left\lfloor \frac{a}{m} \right\rfloor = Qm + r_1 - Qm = r_1$$

ז"א $a \bmod m = r_1 = \bmod m$.

<u>כיוון $\Rightarrow$</u>

נניח ש- $a \bmod m = b \bmod m$. אזי

$$a - m \left\lfloor \frac{a}{m} \right\rfloor = b - m \left\lfloor \frac{b}{m} \right\rfloor \qquad \Rightarrow \qquad a = \left( \left\lfloor \frac{a}{m} \right\rfloor - \left\lfloor \frac{b}{m} \right\rfloor \right) m + b \qquad \Rightarrow \qquad a = qm + b$$

כלומר קיים שלם $q = \left\lfloor \frac{a}{m} \right\rfloor - \left\lfloor \frac{b}{m} \right\rfloor$ עבורו $a = qn + b$ ולכן $a \equiv b \pmod m$.

## <u>שאלה 4</u> (25 נקודות)

$$k = \begin{pmatrix} \mathtt{B} & \mathtt{D} & \mathtt{B} \\ \mathtt{B} & \mathtt{A} & \mathtt{B} \\ \mathtt{B} & \mathtt{B} & \mathtt{A} \end{pmatrix} \to \begin{pmatrix} 1 & 3 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$$

| $\mathtt{y} \in C$ | C | Q | H | J | M | J | I | F | B |
|---|---|---|---|---|---|---|---|---|---|
| $y \in \mathbb{Z}_{26}$ | 2 | 16 | 7 | 9 | 12 | 9 | 8 | 6 | 2 |

הדטרמיננטה של $k$ היא $\det \ k \bmod 26 = 3$.
$\gcd(3, 26) = 1$ לכן המטריצה הפיכה ב- $\mathbb{Z}_{26}$.

$$\begin{pmatrix} 1 & 3 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix} \quad \Rightarrow \quad C_{11} = (-1)^{1+1} \begin{vmatrix} 0 & 1 \\ 1 & 0 \end{vmatrix} \bmod 26 = -1 \bmod 26 = 25 \ .$$

$$\begin{pmatrix} 1 & 3 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix} \quad \Rightarrow \quad C_{12} = (-1)^{1+2} \begin{vmatrix} 1 & 1 \\ 1 & 0 \end{vmatrix} \bmod 26 = 1 \bmod 26 = 1 \ .$$

$$\begin{pmatrix} 1 & 3 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix} \quad \Rightarrow \quad C_{13} = (-1)^{1+3} \begin{vmatrix} 1 & 0 \\ 1 & 1 \end{vmatrix} \bmod 26 = 1 \bmod 26 = 1 \ .$$

$$\begin{pmatrix} 1 & 3 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix} \quad \Rightarrow \quad C_{21} = (-1)^{2+1} \begin{vmatrix} 3 & 1 \\ 1 & 0 \end{vmatrix} \bmod 26 = 1 \bmod 26 = 1 \ .$$

$$\begin{pmatrix} 1 & 3 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix} \quad \Rightarrow \quad C_{22} = (-1)^{2+2} \begin{vmatrix} 1 & 1 \\ 1 & 0 \end{vmatrix} \bmod 26 = -1 \bmod 26 = 25 \ .$$

$$\begin{pmatrix} 1 & 3 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix} \quad \Rightarrow \quad C_{23} = (-1)^{2+3} \begin{vmatrix} 1 & 3 \\ 1 & 1 \end{vmatrix} \bmod 26 = -2 \bmod 26 = 24 \ .$$

$$\begin{pmatrix} 1 & 3 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix} \quad \Rightarrow \quad C_{31} = (-1)^{3+1} \begin{vmatrix} 3 & 1 \\ 0 & 1 \end{vmatrix} \bmod 26 = 3 \bmod 26 = 3 \ .$$

$$\begin{pmatrix} 1 & 3 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix} \quad \Rightarrow \quad C_{32} = (-1)^{3+2} \begin{vmatrix} 1 & 1 \\ 1 & 1 \end{vmatrix} \bmod 26 = 0 \bmod 26 = 0 \ .$$

$$\begin{pmatrix} 1 & 3 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix} \quad \Rightarrow \quad C_{33} = (-1)^{3+3} \begin{vmatrix} 1 & 3 \\ 0 & 1 \end{vmatrix} \bmod 26 = -3 \bmod 26 = 23 \ .$$

$$C = \begin{pmatrix} C_{11} & C_{12} & C_{13} \\ C_{21} & C_{22} & C_{23} \\ C_{31} & C_{32} & C_{33} \end{pmatrix} = \begin{pmatrix} 25 & 1 & 1 \\ 1 & 25 & 2 \\ 3 & 0 & 23 \end{pmatrix} \ .$$

$$\mathrm{adj}(A) = C^t = \begin{pmatrix} 25 & 1 & 3 \\ 1 & 25 & 0 \\ 1 & 2 & 23 \end{pmatrix} \ .$$

$$k^{-1} \bmod 26 = (\det \ k)^{-1} \, \mathrm{adj}(k) \ .$$

$$(\det\ k)^{-1} \bmod 26 = 3^{-1} \bmod 26 = 9\ .$$

$$k^{-1} = 9\begin{pmatrix} 25 & 1 & 3 \\ 1 & 25 & 0 \\ 1 & 2 & 23 \end{pmatrix} = \begin{pmatrix} 225 & 9 & 27 \\ 9 & 225 & 0 \\ 9 & 18 & 207 \end{pmatrix} \bmod 26 = \begin{pmatrix} 17 & 9 & 1 \\ 9 & 17 & 0 \\ 9 & 18 & 25 \end{pmatrix}$$

$$(2,16,7)\cdot k^{-1} = (241,416,177) \bmod 26 = (7,0,21)$$

$$(9,12,9)\cdot k^{-1} = (342,447,234) \bmod 26 = (4,5,0)$$

$$(8,5,1)\cdot k^{-1} = (190,175,33) \bmod 26 = (8,19,7)$$

| y $\in C$ | C | Q | H | J | M | J | I | F | B |
|---|---|---|---|---|---|---|---|---|---|
| $y \in \mathbb{Z}_{26}$ | 2 | 16 | 7 | 9 | 12 | 9 | 8 | 5 | 1 |
| $x \in \mathbb{Z}_{26}$ | 7 | 0 | 21 | 4 | 5 | 0 | 8 | 19 | 7 |
| x $\in P$ | h | a | v | e | f | a | i | t | h |

**א)** נסמן $y = e_k(x)$:

$$\begin{aligned} d_k(y) =& yk^{-1} \bmod 26 \\ =& (xk \bmod 26)\, k^{-1} \bmod 26\ . \end{aligned}$$

לכל שלמים $a$ ו- $b$ מתקיים $((a \bmod m)\, b) \bmod m = ab \bmod m$ לכן:

$$d_k(y) = xkk^{-1} \bmod 26 = x \bmod 26\ ,$$

לפיכך:

$$d_k\big(e_k(x)\big) = x \bmod 26\ .$$

**ב)** לכל מילה $x = x_1x_2\ldots x_n$ הכלל מצפין של האות ה- $i$ הוא:

$$e_k(x_i) = \Delta_i(x_i)$$

כאשר $\Delta_i = \tau_i^{-1}\rho\tau_i$ כאשר $\rho$ הוא תמורה משקפת קבועה של צופן אניגמה ו- $\tau_i$ תמורה מורכבת. מכאן:

$$\begin{aligned} \Delta_i^2 =& \tau_i^{-1}\rho\tau_i\tau_i^{-1}\rho\tau_i && \text{(ההגדרה של הכלל מצפין של צופן אניגמה)} \\ =& \tau_i^{-1}\rho\mathrm{id}\rho\tau_i && \text{(ההגדרה של תמורה הופכית)} \\ =& \tau_i^{-1}\rho^2\tau_i && \text{(ההגדרה של תמורה הזהות)} \\ =& \tau_i^{-1}\mathrm{id}\tau_i && \text{($\rho$ תמורה משקפת)} \\ =& \tau_i^{-1}\tau_i \\ =& \mathrm{id}\ . \end{aligned}$$

## שאלה 5 (25 נקודות)

**א) (10 נק')** נתון המפתח של צופן אפיני $a = 11, b = 3$.
הכלל מפענח הינו $d_k(y) = a^{-1}(y - b) \bmod 26$.
$\gcd(a, 26) = \gcd(11, 26) = 1$ לכן $a^{-1}$ קיימת לכן הכלל מפענח קיים:

$$a^{-1} \equiv 19 \bmod 26 \ .$$

$$d_k(y) = a^{-1}(y - b) \bmod 26 = 19(y - 3) \bmod 26 = 19y - 57 \bmod 26 = 19y + 21 \bmod 26 \ .$$

$$\begin{aligned}
d_k(\texttt{C}) &= d_k(2) &&= 19(2) + 21 \bmod 26 = 7 \ , \\
d_k(\texttt{V}) &= d_k(21) &&= 19(21) + 21 \bmod 26 = 4 \ , \\
d_k(\texttt{L}) &= d_k(11) &&= 19(11) + 21 \bmod 26 = 22 \ , \\
d_k(\texttt{B}) &= d_k(1) &&= 19(1) + 21 \bmod 26 = 14 \ , \\
d_k(\texttt{K}) &= d_k(10) &&= 19(10) + 21 \bmod 26 = 3 \ , \\
d_k(\texttt{D}) &= d_k(3) &&= 19(3) + 21 \bmod 26 = 0 \ , \\
d_k(\texttt{I}) &= d_k(23) &&= 19(8) + 21 \bmod 26 = 17 \ , \\
d_k(\texttt{T}) &= d_k(20) &&= 19(19) + 21 \bmod 26 = 18 \ , \\
d_k(\texttt{N}) &= d_k(13) &&= 19(13) + 21 \bmod 26 = 8 \ , \\
d_k(\texttt{Q}) &= d_k(16) &&= 19(16) + 21 \bmod 26 = 13 \ ,
\end{aligned}$$

| $\texttt{y} \in C$ | C | V | L | C | B | K | D | I | V | T | L | N | Q | V |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $y \in \mathbb{Z}_{26}$ | 2 | 21 | 11 | 2 | 1 | 10 | 3 | 8 | 21 | 19 | 11 | 13 | 16 | 21 |
| $x \in \mathbb{Z}_{26}$ | 7 | 4 | 22 | 7 | 14 | 3 | 0 | 17 | 4 | 18 | 22 | 8 | 13 | 18 |
| $\texttt{x} \in P$ | h | e | w | h | o | d | a | r | e | s | w | i | n | s |

**ב) (8 נק')** הטענה נכונה. הפונקציה ההופכית היא $d_k(y) = a^{-1}(y - b) \bmod p$.
ז"א קיים כלל מצפין $\iff$ קיים האיבר ההופכי $a^{-1}$ ב- $\mathbb{Z}_p$ $\iff$ $\gcd(a, p) = 1$.
מכיוון ש- $p$ מספר ראשוני אזי לכל $a \in \mathbb{Z}_p$ מתקיים $\gcd(a, p) = 1$ לכן לכל $a \in \mathbb{Z}_p$ קיים איבר הפוכי $a^{-1}$ לכן לכל $a \in \mathbb{Z}_p$ קיים כלל מצפין.

**ג) (7 נק')** אם $a \equiv b \pmod{c}$ אז קיים שלם $q$:

$$a = qc + b \ .$$

לכן

$$a^n = (qc + b)^n = \left( \sum_{k=1}^{n} \binom{n}{k} q^k c^{k-1} b^{n-k} \right) c + b^n = Qc + b^n$$

כאשר $Q$ שלם. לכן קיים שלם $Q$ כך ש:

$$a^n = Qc + b^n \quad \Rightarrow \quad a^n \equiv b^n \pmod{c} \ .$$

## שאלה 6

**א) (13 נקודות)**

ראשית נחשב את ההופכי המודולרי של 13 ביחס ל- 99 בעזרת האלגוריתם המכולל של אוקלידס באופן הבא.

נסמן: $a = 99, b = 13$.

אתחול:

$$\begin{aligned} r_0 &= a = 99 \ , & r_1 &= b = 13 \ , \\ s_0 &= 1 \ , & s_1 &= 0 \ , \\ t_0 &= 0 \ , & t_1 &= 1 \ . \end{aligned}$$

| | | | | |
|---|---|---|---|---|
| שלב $k = 1$: | $t_2 = 0 - 7 \cdot 1 = -7$ | $s_2 = 1 - 7 \cdot 0 = 1$ | $r_2 = 99 - 7 \cdot 13 = 8$ | $q_1 = 7$ |
| שלב $k = 2$: | $t_3 = 1 - 1 \cdot (-7) = 8$ | $s_3 = 0 - 1 \cdot 1 = -1$ | $r_3 = 13 - 1 \cdot 8 = 5$ | $q_2 = 1$ |
| שלב $k = 3$: | $t_4 = -7 - 1 \cdot (8) = -15$ | $s_4 = 1 - 1 \cdot (-1) = 2$ | $r_4 = 8 - 1 \cdot 5 = 3$ | $q_3 = 1$ |
| שלב $k = 4$: | $t_5 = 8 - 1 \cdot (-15) = 23$ | $s_5 = -1 - 1 \cdot 2 = -3$ | $r_5 = 5 - 1 \cdot 3 = 2$ | $q_4 = 1$ |
| שלב $k = 5$: | $t_6 = -15 - 1 \cdot (23) = -38$ | $s_6 = 2 - 1 \cdot (-3) = 5$ | $r_6 = 3 - 1 \cdot 2 = 1$ | $q_5 = 1$ |
| שלב $k = 6$: | $t_7 = 23 - 2 \cdot (-38) = 99$ | $s_7 = -3 - 2 \cdot (5) = -13$ | $r_7 = 2 - 2 \cdot 1 = 0$ | $q_6 = 2$ |

$$\gcd(a, b) = r_6 = 1 \ , \qquad s = s_6 = 5 \ , \qquad t = t_6 = -38 \ .$$

$$sa + tb = 5(99) - 38(13) = 1 \ .$$

לכן

$$13^{-1} \equiv -38 \pmod{99} = 61 \pmod{99} \ .$$

□

כעת נחשב את ההופכי המודולרי של 15 ביחס ל- 101 בעזרת האלגוריתם המוכלל של אוקלידס באופן הבא.

נסמן: $a = 101, b = 15$.

אתחול:

$$\begin{aligned} r_0 &= a = 101 \ , & r_1 &= b = 15 \ , \\ s_0 &= 1 \ , & s_1 &= 0 \ , \\ t_0 &= 0 \ , & t_1 &= 1 \ . \end{aligned}$$

| | | | | |
|---|---|---|---|---|
| שלב $k=1$: | $t_2 = 0 - 6 \cdot 1 = -6$ | $s_2 = 1 - 6 \cdot 0 = 1$ | $r_2 = 101 - 6 \cdot 15 = 11$ | $q_1 = 6$ |
| שלב $k=2$: | $t_3 = 1 - 1 \cdot (-6) = 7$ | $s_3 = 0 - 1 \cdot 1 = -1$ | $r_3 = 15 - 1 \cdot 11 = 4$ | $q_2 = 1$ |
| שלב $k=3$: | $t_4 = -6 - 2 \cdot (7) = -20$ | $s_4 = 1 - 2 \cdot (-1) = 3$ | $r_4 = 11 - 2 \cdot 4 = 3$ | $q_3 = 2$ |
| שלב $k=4$: | $t_5 = 7 - 1 \cdot (-20) = 27$ | $s_5 = -1 - 1 \cdot 3 = -4$ | $r_5 = 4 - 1 \cdot 3 = 1$ | $q_4 = 1$ |
| שלב $k=5$: | $t_6 = -20 - 3 \cdot (27) = -101$ | $s_6 = 3 - 3 \cdot (-4) = 15$ | $r_6 = 3 - 3 \cdot 1 = 0$ | $q_5 = 3$ |

$$\gcd(a,b) = r_6 = 1 \ , \qquad s = s_5 = -4 \ , \qquad t = t_5 = 27 \ .$$

$$sa + tb = -4(101) + 27(15) = 1 \ .$$

לכן

$$15^{-1} \equiv 27 \pmod{101} \ .$$

ראשית נחשב את ההופכי המודולרי של 13 ביחס ל- 99 בעזרת האלגוריתם המכולל של אוקלידס באופן הבא.

נסמן: $a = 99, b = 13$.

אתחול:

$$\begin{aligned} r_0 &= a = 99 \ , & r_1 &= b = 13 \ , \\ s_0 &= 1 \ , & s_1 &= 0 \ , \\ t_0 &= 0 \ , & t_1 &= 1 \ . \end{aligned}$$

| | | | | |
|---|---|---|---|---|
| שלב $k=1$: | $t_2 = 0 - 7 \cdot 1 = -7$ | $s_2 = 1 - 7 \cdot 0 = 1$ | $r_2 = 99 - 7 \cdot 13 = 8$ | $q_1 = 7$ |
| שלב $k=2$: | $t_3 = 1 - 1 \cdot (-7) = 8$ | $s_3 = 0 - 1 \cdot 1 = -1$ | $r_3 = 13 - 1 \cdot 8 = 5$ | $q_2 = 1$ |
| שלב $k=3$: | $t_4 = -7 - 1 \cdot (8) = -15$ | $s_4 = 1 - 1 \cdot (-1) = 2$ | $r_4 = 8 - 1 \cdot 5 = 3$ | $q_3 = 1$ |
| שלב $k=4$: | $t_5 = 8 - 1 \cdot (-15) = 23$ | $s_5 = -1 - 1 \cdot 2 = -3$ | $r_5 = 5 - 1 \cdot 3 = 2$ | $q_4 = 1$ |
| שלב $k=5$: | $t_6 = -15 - 1 \cdot (23) = -38$ | $s_6 = 2 - 1 \cdot (-3) = 5$ | $r_6 = 3 - 1 \cdot 2 = 1$ | $q_5 = 1$ |
| שלב $k=6$: | $t_7 = 23 - 2 \cdot (-38) = 99$ | $s_7 = -3 - 2 \cdot (5) = -13$ | $r_7 = 2 - 2 \cdot 1 = 0$ | $q_6 = 2$ |

$$\gcd(a,b) = r_6 = 1 \ , \qquad s = s_6 = 5 \ , \qquad t = t_6 = -38 \ .$$

$$sa + tb = 5(99) - 38(13) = 1 \ .$$

לכן

$$13^{-1} \equiv -38 \pmod{99} = 61 \pmod{99} \ .$$

□

כעת נחשב את ההופכי המודולרי של 15 ביחס ל- 101 בעזרת האלגוריתם המוכלל של אוקלידס באופן הבא.

נסמן: $a = 101, b = 15$.

אתחול:

$$\begin{aligned} r_0 =& a = 101 \ , & r_1 &= b = 15 \ , \\ s_0 =& 1 \ , & s_1 &= 0 \ , \\ t_0 =& 0 \ , & t_1 &= 1 \ . \end{aligned}$$

| | | | | |
|---|---|---|---|---|
| $q_1 = 6$ | $r_2 = 101 - 6 \cdot 15 = 11$ | $s_2 = 1 - 6 \cdot 0 = 1$ | $t_2 = 0 - 6 \cdot 1 = -6$ | שלב $k = 1$: |
| $q_2 = 1$ | $r_3 = 15 - 1 \cdot 11 = 4$ | $s_3 = 0 - 1 \cdot 1 = -1$ | $t_3 = 1 - 1 \cdot (-6) = 7$ | שלב $k = 2$: |
| $q_3 = 2$ | $r_4 = 11 - 2 \cdot 4 = 3$ | $s_4 = 1 - 2 \cdot (-1) = 3$ | $t_4 = -6 - 2 \cdot (7) = -20$ | שלב $k = 3$: |
| $q_4 = 1$ | $r_5 = 4 - 1 \cdot 3 = 1$ | $s_5 = -1 - 1 \cdot 3 = -4$ | $t_5 = 7 - 1 \cdot (-20) = 27$ | שלב $k = 4$: |
| $q_5 = 3$ | $r_6 = 3 - 3 \cdot 1 = 0$ | $s_6 = 3 - 3 \cdot (-4) = 15$ | $t_6 = -20 - 3 \cdot (27) = -101$ | שלב $k = 5$: |

$$\gcd(a,b) = r_6 = 1 \ , \qquad s = s_5 = -4 \ , \qquad t = t_5 = 27 \ .$$

$$sa + tb = -4(101) + 27(15) = 1 \ .$$

לכן

$$15^{-1} \equiv 27 \pmod{101} \ .$$

$$13^{-1} \cdot 13x \equiv 61 \cdot 4 \pmod{99} \quad \Rightarrow \quad x \equiv 244 \pmod{99} = 46 \pmod{99}$$

$$15^{-1} \cdot 15x \equiv 27 \cdot 56 \pmod{101} \quad \Rightarrow \quad x \equiv 1512 \pmod{101} = 98 \pmod{101}$$

כעת נפתור את המערכת

$$\begin{aligned} x =& 46 \bmod 99 \ , \\ x =& 98 \bmod 101 \ , \end{aligned}$$

בעזרת המשפט השאריות הסיני.
נסמן

$$a_1 = 46\ , \quad m_1 = 99\ , \quad a_2 = 98\ , \quad m_2 = 101\ , \quad M = m_1 m_2 = 9999\ , \quad M_1 = \frac{M}{m_1} = 101\ , \quad M_2 = \frac{M}{m_2} = 99\ .$$

$$y_1 = M_1^{-1} \pmod{m}_1 = 101^{-1} \pmod{99} = 50\ , \qquad y_2 = M_2^{-1} \pmod{m}_2 = 99^{-1} \pmod{101} = 50\ .$$

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 \bmod M = 717400 \bmod 9999 = 7471\ .$$

$$13^{-1} \cdot 13x \equiv 61 \cdot 4 \pmod{99} \quad \Rightarrow \quad x \equiv 244 \pmod{99} = 46 \pmod{99}$$

$$15^{-1} \cdot 15x \equiv 27 \cdot 56 \pmod{101} \quad \Rightarrow \quad x \equiv 1512 \pmod{101} = 98 \pmod{101}$$

כעת נפתור את המערכת

$$x = 46 \bmod 99\ ,$$
$$x = 98 \bmod 101\ ,$$

בעזרת המשפט השאריות הסיני.
נסמן

$$a_1 = 46\ , \quad m_1 = 99\ , \quad a_2 = 98\ , \quad m_2 = 101\ , \quad M = m_1 m_2 = 9999\ , \quad M_1 = \frac{M}{m_1} = 101\ , \quad M_2 = \frac{M}{m_2} = 99\ .$$

$$y_1 = M_1^{-1} \pmod{m}_1 = 101^{-1} \pmod{99} = 50\ , \qquad y_2 = M_2^{-1} \pmod{m}_2 = 99^{-1} \pmod{101} = 50\ .$$

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 \bmod M = 717400 \bmod 9999 = 7471\ .$$

**ב) (12 נקודות)**

יהי $d = \gcd(a, b)$.
$\exists$ שלמים $s, t$ כך ש-

$$sa + tb = d\ . \qquad (*)$$

נחלק (*) ב- $m$ ונקבל

$$s\left(\frac{a}{m}\right) + t\left(\frac{b}{m}\right) = \frac{d}{m}\ . \qquad (**)$$

נשים לב $m \mid a$ ו- $m \mid b$. לכן $\frac{a}{m}$ שלם ו- $\frac{b}{m}$ שלם.
ז"א המספר בצד שמאל הוא שלם.
לכן המספר בצד ימין, $\frac{d}{m}$, הוא בהכרח שלם.
לכן ולפי משפט בזו $\frac{d}{m} = \gcd\left(\frac{a}{m}, \frac{b}{m}\right)$.
לכן

$$\gcd\left(\frac{a}{m}, \frac{b}{m}\right) = \frac{\gcd(a,b)}{m} \ .$$