מחלקה למדעי המחשב

13/02/25 ט"ו בשבט תשפ"ה
09 : 00 – 12 : 00

קריפטוגרפיה

מועד א'

מרצה: ד"ר ירמיהו מילר.

תשפ"ה סמסטר א'

השאלון מכיל 12 **עמודים (כולל עמוד זה וכולל דף נוסחאות).**

בהצלחה!

==========

הנחיות למדור בחינות שאלוני בחינה

- לשאלון הבחינה יש לצרף מחברת.
- ניתן להשתמש במחשבון מדעי לא גרפי עם צג קטן.

חומר עזר

- דפי נוסחאות של הקורס (8 עמודים בפורמט $A4$), מצורפים לשאלון.

אחר / הערות יש לענות על השאלות באופן הבא:

- יש לנמק היטב כל שלב של פתרון. תשובה ללא הסבר וללא נימוק, אפילו נכונה, לא תתקבל.
- יש לפתור 4 מתוך 5 השאלות הבאות. משקל כל שאלה 25 נקודות.
- סדר התשובות אינו משנה, אך יש לרשום ליד כל תשובה את מספרה.
- הסבירו היטב את מהלך הפתרון.

==========

שאלה 1 (25 נקודות)

א) (8 נק') נתון המפתח הציבורי הבא של צופן El-Gamal:

$$K = (\alpha = 10, \quad a = 35, \quad p = 37, \quad d = 2) \ .$$

ב) (8 נק') נתון הטקסט גלוי $\mathrm{x} = 12$. אליס מצפינה את הטקסט גלוי הזה עם צופן El-Gamal ועם המפתח K. הוכיחו כי הטקסט המוצפן המתקבל הוא $(y_1, y_2) = (26, 9)$. בוב מקבל את הטקסט המוצפן ואת המפתח הציבורי מאליס ואז הוא מפענח את הטקסט המוצפן.
הוכיחו כי הטקסט גלוי שהוא מקבל הוא $\mathrm{x} = 12$.

ג) (9 נק') יהיו a, b, c, d, m שלמים. הוכיחו את הטענה הבאה:
אם $a \equiv b \mod m$ ו- $c \equiv d \mod m$ אז $ab \equiv cd \mod m$.

שאלה 2 (25 נקודות)

תהי X האלפבית $X = \{\mathtt{a}, \mathtt{b}, \mathtt{c}, \mathtt{d}, \mathtt{e}, \mathtt{f}\}$ ותהי פונקצית ההסתברות של האלפבית X

$$P_X(\mathtt{a}) = \frac{4}{15} \ , \quad P_X(\mathtt{b}) = \frac{2}{15} \ , \quad P_X(\mathtt{c}) = \frac{1}{15} \ , \quad P_X(\mathtt{d}) = \frac{1}{3} \ , \quad P_X(\mathtt{e}) = \frac{1}{30} \ , \quad P_X(\mathtt{f}) = \frac{1}{6} \ .$$

א) (10 נק')
מצאו הצפנה בינארית של האלפבית X עבורה תוחלת אורך ההצפנה של האותיות תהיה מינימלית.

ב) (5 נק')
חשבו את תוחלת אורך ההצפנה שמצאתם בסעיף א' ומצאו חסם עליון וחסם תחתון של תוחלת אורך ההצפנה.

ג) (10 נק')
תהי $X = \{a_1, \ldots, a_n\}$ אלפבית בעלת פונקצית ההסתברות

$$P_X(a_1) = p_1 \ , \quad P_X(a_2) = p_2 \ , \quad \cdots \quad P_X(a_k) = p_k \ ,$$

כאשר $0 < p_i < 1$ לכל $1 \le i \le k$.
נניח שאנחנו מצפינים את האותיות עם הצפנה בינארית. יהי n_i את האורך ההצפנה של $\mathtt{a}_i$ לכל $1 \le i \le k$.
הוכיחו את הטענה הבאה:
אם $p_1 \ge p_2 \ge \ldots \ge p_k$ אז ההצפנה הבינארית היחידה שמבטיחה התוחלת אורך ההצפנה המינימלית מקיימת את התנאי הבא:

$$n_1 \le n_2 \le \ldots \le n_k \ .$$

שאלה 3 (25 נקודות)

יהיו p, q מספרים ראשוניים שמוגדרים $p = 7, q = 11$, ויהי b מספר שלם שמוגדר להיות $b = 17$.
יהי (p, q, b) המפתח הציבורי של צופן RSA.

א) (8 נק')
אליס מצפינה את הטקסט גלוי $\mathrm{x} = 12$ באמצעות צופן RSA עם המפתח הזה.
הוכיחו כי הטקסט המוצפן המתקבל הוא $\mathrm{y} = 45$.

ב) (8 נק')
בוב מקבל את הטקסט המוצפן $\mathrm{y} = 45$ והמפתח הציבורי $(p = 7, q = 11, b = 17)$ מאליס.
בוב מפענח את הטקסט המוצפן הזה באמצעות המפתח הציבורי אשר הוא קיבל מאליס.
הוכיחו כי הטקסט גלוי שבוב מקבל בחזרה הוא $\mathrm{x} = 12$.

ג) (9 נק')
יהיו r, s מספרים ראשוניים ותהי ϕ פונקצית אוילר. הוכיחו את הטענה הבאה:

$$\phi\left(r^2 s\right) = \left(r^2 - r\right)(s - 1) \ .$$

שאלה 4

אליס שולחת לבוב את הטקסט המוצפן `BYNI` אשר הוצפן ע"י צופן היל עם המפתח $k = \begin{pmatrix} 1 & 8 \\ 2 & 5 \end{pmatrix}$.

א) (11 נק') חשבו את הטקסט גלוי המקורי של הטקסט המוצפן הזה.

ב) (10 נק') נתון צופן פייסטאל בעל פונקצית ליבה

$$f\left(x_1 x_2 x_3 x_4 x_5 \ , \ \pi\right) = x_{\pi(1)} x_{\pi(2)} x_{\pi(3)} x_{\pi(4)} x_{\pi(5)} \ .$$

יהי המפתח ההתחלתי התמורה:

$$\pi_0 = (135)(24)$$

ויהי כל תת-מפתח k_i $(i = 1, 2, 3)$ התמורה המתקבלת על ידי ביצוע i פעמים את התמורה π_0.
חשבו את הטקסט המוצפן של הטקסט גלוי `0010111001`.

ג) (4 נק') יהי p מספר ראשוני ו- n שלם. הוכיחו את הטענה הבאה:
אם p לא מחלק את n אז $\phi(pn) = (p - 1)\phi(n)$ כאשר ϕ פונקצית אוילר.

שאלה 5 (25 נקודות)

אליס הצפינה את הטקסט גלוי x עם צופן אפיני, עם המפתח $(5, 13)$ ושלחה את הטקסט המוצפן הבא לבוב: SHWNKKD.

א) (6 נק') הוכיחו כי ניתן לפענח כל טקסט אשר הוצפן על ידי צופן אפיני עם המפתח הזה.

ב) (7 נק') חשבו את הטקסט גלוי אשר אליס שלחה לבוב.

ג) (6 נק') הוכיחו שאם a, b שלמים וקיימים שלמים s, t כך ש- $sa + tb = 1$ אז a, b זרים.

ד) (6 נק') יהיו a, b שלמים. נגדיר $r = \frac{a}{\gcd(a,b)}$ ו- $s = \frac{b}{\gcd(a,b)}$.
הוכיחו כי r ו- s זרים.

פתרונות

שאלה 1

א) (8 נק')

$$\beta = \alpha^a \mod p = 10^{35} \mod 37 .$$

$$35 = 32 + 2 + 1.$$

$$\begin{aligned}
10 \mod 37 &= 10 , \\
10^2 \mod 37 &= 100 \mod 37 = 26 , \\
10^4 \mod 37 &= 26^2 \mod 37 = 10 , \\
10^8 \mod 37 &= 10^2 \mod 37 = 26 , \\
10^{16} \mod 37 &= 26^2 \mod 37 = 10 , \\
10^{32} \mod 37 &= 10^2 \mod 37 = 26 .
\end{aligned}$$

לכן

$$10^{35} \mod 37 = 10^{32}10^2 10^1 \mod 37 = (26)(26)(10) \mod 37 = 26 .$$

ז"א $\beta = 26$.

$$y_1 = \alpha^d \mod p = 10^2 \mod 37 = 26$$

$$\begin{aligned}
y_2 &= x\beta^d \mod p \\
&= (12)(26^2) \mod 37 \\
&= (12 \mod 37)(26^2 \mod 37) \\
&= (12)(10) \mod 37 \\
&= 9
\end{aligned}$$

ב) (8 נק')

$(y_1, y_2) = (3, 42)$.

$$x = (y_1^a)^{-1} \cdot y_2 \mod p = (26^{35})^{-1} \cdot 9 \mod 37$$

$$(26^{35})^{-1} \mod 37 \overset{\text{משפט פרמה}}{=} 26^{37-1-35} \mod 37 = 26 \mod 37 = 26 .$$

ולכן

$$x = (y_1^a)^{-1} \cdot y_2 \mod p = (26^{35})^{-1} \cdot 9 \mod 37 = (26)(9) \mod 37 = 234 \mod 37 = 12 .$$

ג) (9 נק')

נתון:

$c \equiv d \mod m$ -ו $a \equiv b \mod m$.

צריך להוכיח:

$ab \equiv cd \mod m$.

הוכחה:

$a \equiv b \mod m \Leftarrow$ קיים q_1 שלם כך ש-

(*1) $a = q_1 m + b$.

$c \equiv d \mod m \Leftarrow$ קיים q_2 שלם כך ש-

(*2) $c = q_2 m + d$.

נכפיל את המשוואות (*1) ו- (*2):

$$ac = (q_1 q_2 m + b q_2 + d q_1)\, m + bd = Qm + bd$$

כאשר $Q := q_1 q_2 m + b q_2 + d q_1$.
$\Leftarrow \exists Q$ שלם כך ש- $ac = Qm + bd \Leftarrow acbd \mod m$.

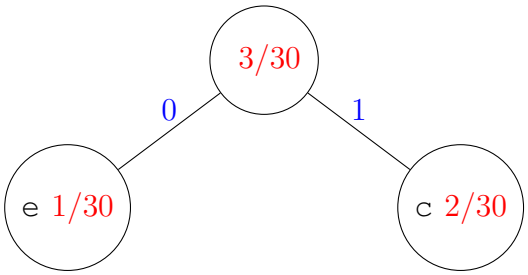
שאלה 2

א) (10 נק')

שלב 1)

e	c	b	f	a	d
$\frac{1}{30}$	$\frac{2}{30}$	$\frac{4}{30}$	$\frac{5}{30}$	$\frac{8}{30}$	$\frac{10}{30}$

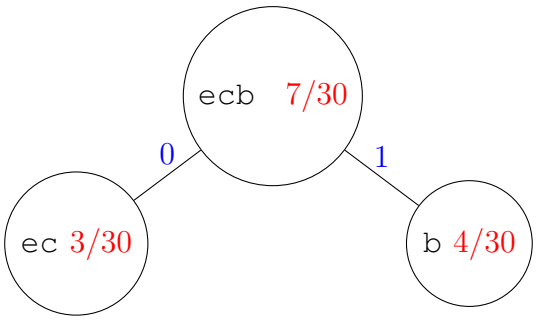
שלב 2)



e	c	b	f	a	d
$\frac{1}{30}$	$\frac{2}{30}$	$\frac{4}{30}$	$\frac{5}{30}$	$\frac{8}{30}$	$\frac{10}{30}$
0	1				
$\frac{3}{30}$		$\frac{4}{30}$	$\frac{5}{30}$	$\frac{8}{30}$	$\frac{10}{30}$

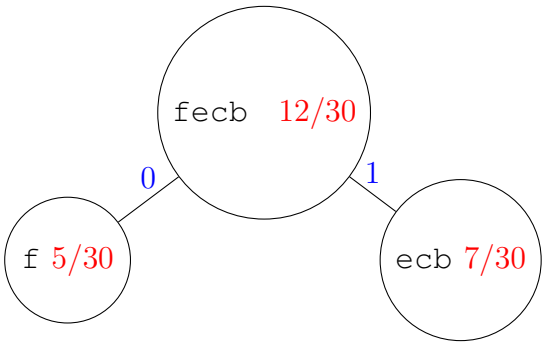
שלב 3)

ec	b	f	a	d
$\frac{3}{30}$	$\frac{4}{30}$	$\frac{5}{30}$	$\frac{8}{30}$	$\frac{10}{30}$
0	1			
$\frac{7}{30}$		$\frac{5}{30}$	$\frac{8}{30}$	$\frac{10}{30}$



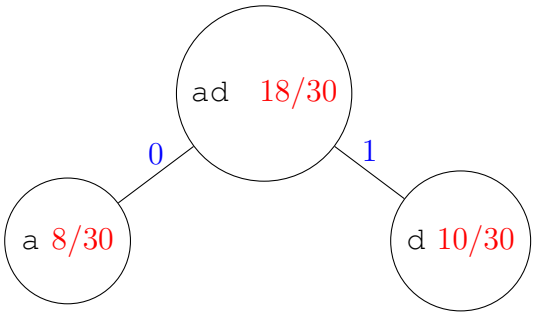
שלב 4)

f	ecb	a	d
$\frac{5}{30}$	$\frac{7}{30}$	$\frac{8}{30}$	$\frac{10}{30}$
0	1		
$\frac{12}{30}$		$\frac{8}{30}$	$\frac{10}{30}$

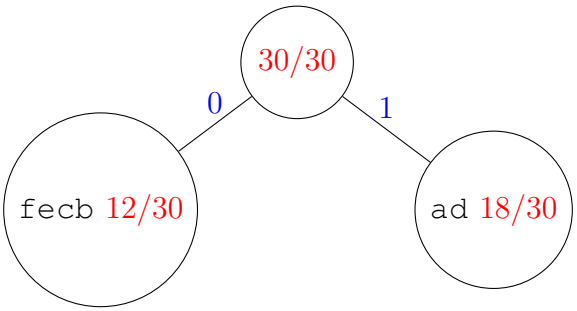


שלב 5)

a	d	fecb
$\frac{8}{30}$	$\frac{10}{30}$	$\frac{12}{30}$
0	1	
$\frac{18}{30}$		$\frac{12}{30}$

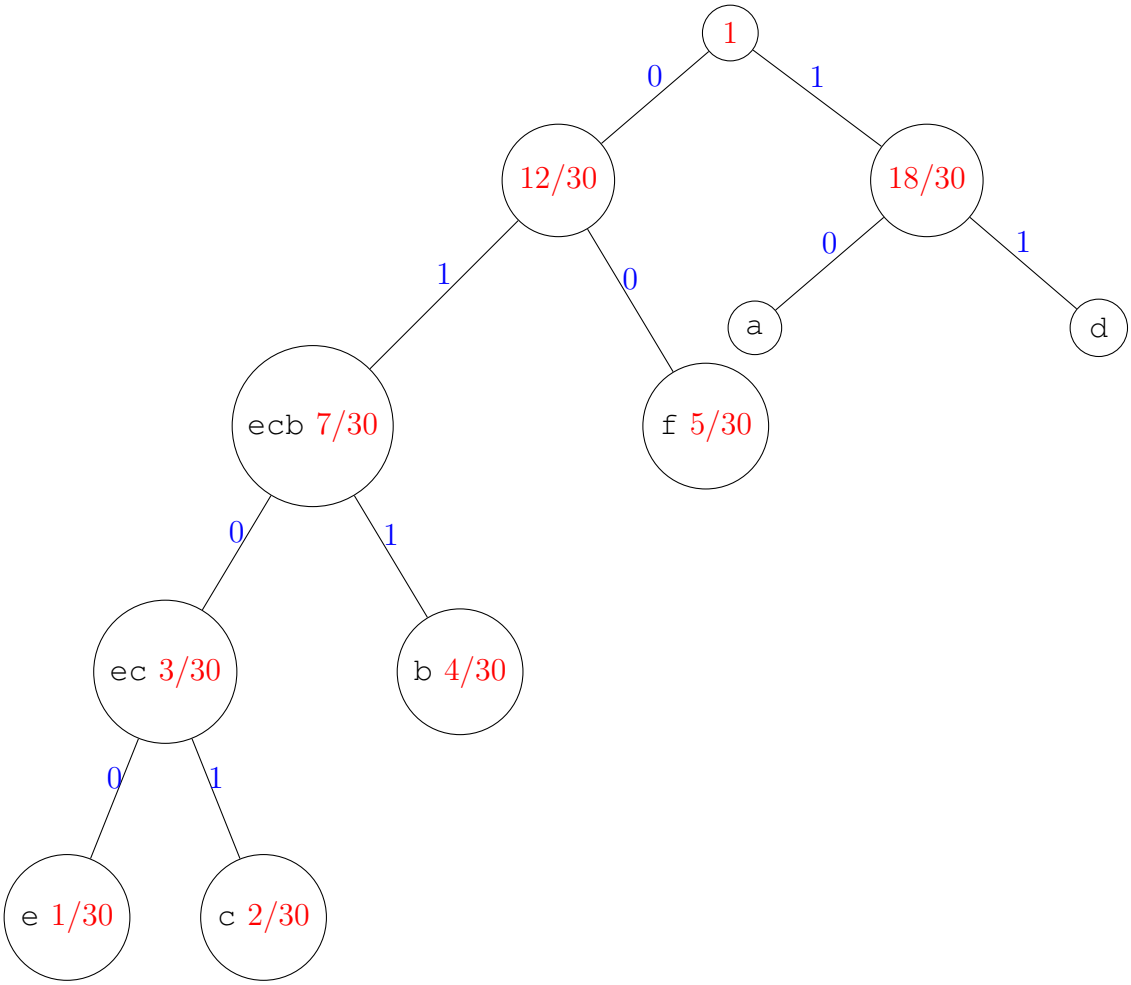


שלב 6)



fecb	ad
$\frac{12}{30}$	$\frac{18}{30}$
0	1
$\frac{30}{30}$	

שלב 7)



שלב 8)

a	10
b	011
c	0101
d	11
e	0100
f	00

ב) (5 נק')

x	$f(x)$	$\lvert f(x)\rvert$
a	10	2
b	011	3
c	0101	4
d	11	2
e	0100	4
f	00	2

$$\begin{aligned}
l(f) =& P_X(\mathtt{a})\,|f(\mathtt{a})| + P_X(\mathtt{b})\,|f(\mathtt{b})| + P_X(\mathtt{c})\,|f(\mathtt{c})| + P_X(\mathtt{d})\,|f(\mathtt{d})| + P_X(\mathtt{e})\,|f(\mathtt{e})| + P_X(\mathtt{f})\,|f(\mathtt{f})| \\
=& \frac{4}{15}(2) + \frac{2}{15}(3) + \frac{1}{15}(4) + \frac{1}{3}(2) + \frac{1}{30}(4) + \frac{1}{6}(2) \\
=& \frac{16}{30} + \frac{12}{30} + \frac{8}{30} + \frac{20}{30} + \frac{4}{30} + \frac{10}{30} \\
=& \frac{7}{3}\ .
\end{aligned}$$

$$\begin{aligned}
H[X] =& -P_X(\mathtt{a})\log_2 P_X(\mathtt{a}) - P_X(\mathtt{b})\log_2 P_X(\mathtt{b}) - P_X(\mathtt{c})\log_2 P_X(\mathtt{c}) - P_X(\mathtt{d})\log_2 P_X(\mathtt{d}) \\
& - P_X(\mathtt{e})\log_2 P_X(\mathtt{e}) - P_X(\mathtt{f})\log_2 P_X(\mathtt{f}) \\
=& -\frac{4}{15}\log_2\frac{4}{15} - \frac{2}{15}\log_2\frac{2}{15} - \frac{1}{15}\log_2\frac{1}{15} - \frac{1}{3}\log_2\frac{1}{3} - \frac{1}{30}\log_2\frac{1}{30} - \frac{1}{6}\log_2\frac{1}{6} \\
=& 2.279
\end{aligned}$$

$$H[X] \le l(f) \le H[X]+1 \quad \Rightarrow \quad 2.279 \le 2.33 \le 3.279$$

מתקיים.

ג) (10 נק') נניח בשלילה שקיימת תמורה $\{n_{i_1},\ldots,n_{i_k}\}$ של $\{n_1,\ldots,n_k\}$. כך שהתוחלת

$$E = n_{i_1}p_1 + \ldots + n_{i_{j-1}}p_{j-1} + n_{i_j}p_j + \ldots + n_{i_k}p_k\ .$$

היא מינימלית.

ללא הגבלת הכלליות נניח כי $n_1 = n_{i_j}$. אזי

$$E = n_{i_1}p_1 + \ldots + n_{i_{j-1}}p_{j-1} + n_1 p_j + \ldots + n_{i_k}p_k \ .$$

$n_1 = \min(n_1, \ldots, n_k)$ אז בהכרח $n_{i_{j-1}} \geq n_1$.
בנוסף $p_1 \geq p_2 \geq \cdots \geq p_k$ לכן $p_{j-1} \geq p_j$.
לכן לפי משפט **??**:

$$n_{i_{j-1}}p_{j-1} + n_1 p_j \geq n_1 p_{j-1} + n_{i_{j-1}}p_j \ . \qquad \textbf{(1*)}$$

לכן אם נחליף n_1 עם $n_{i_{j-1}}$ ב- E נקבל את התוחלת החדשה

$$E' = n_{i_1}p_1 + \ldots + n_1 p_{j-1} + n_{i_{j-1}}p_j + \ldots + n_{i_k}p_k$$

כך שלפי (1*):

$$E' = n_{i_1}p_1 + \ldots + n_1 p_{j-1} + n_{i_{j-1}}p_j + \ldots + n_{i_k}p_k \leq n_{i_1}p_1 + \ldots + n_{i_{j-1}}p_{j-1} + n_1 p_j + \ldots + n_{i_k}p_k = E$$

ז"א $E' \leq E$ בסתירה לכך כי E התוחלת המינימלית.

שאלה 3 (25 נקודות)

א)

$$n = pq = 7 \times 11 = 77$$
$$\phi(n) = \phi(pq) = (p-1)(q-1) = 10 \times 6 = 60 \ .$$

$a = 17^{-1} \mod 60$. נשתמש באלגוריתם של אוקלידס:

שיטה 1

$$\begin{aligned} r_0 &= 60, & r_1 &= 17 \ , \\ s_0 &= 1 \ , & s_1 &= 0 \ , \\ t_0 &= 0 \ , & t_1 &= 1 \ . \end{aligned}$$

שלב $i = 1$:	$r_2 = 60 - 3 \cdot 17 = 9$	$s_2 = 1 - 3 \cdot 0 = 1$	$t_2 = 0 - 3 \cdot 1 = -3$	$q_1 = 3$
שלב $i = 2$:	$r_3 = 17 - 1 \cdot 9 = 8$	$s_3 = 0 - 1 \cdot 1 = -1$	$t_3 = 1 - 1 \cdot (-3) = 4$	$q_2 = 1$
שלב $i = 3$:	$r_4 = 9 - 1 \cdot 8 = 1$	$s_4 = 1 - 1 \cdot (-1) = 2$	$t_4 = -3 - 1 \cdot (4) = -7$	$q_3 = 1$
שלב $i = 4$:	$r_5 = 8 - 8 \cdot 1 = 0$	$s_5 = -1 - 8 \cdot 2 = -17$	$t_5 = 4 - 8 \cdot (-7) = 60$	$q_4 = 8$

$$\gcd(17,60) = r_4 = 1\ , \qquad s = s_4 = 2\ , \qquad t = t_4 = -7\ .$$

$$2(60) - 7(17) = 1\ .$$

מכאן

$$-7(17) = 1 - 2(60) \quad \Rightarrow \quad -7(17) = 1 \mod 60 \quad \Rightarrow \quad 17^{-1} \equiv -7 \mod 60 = 53\ .$$

$$y = x^b \mod n = 12^{17} \mod 77\ .$$

$$12^{17} = 12^{16+1}$$

$$\begin{aligned}
12 \mod 77 &= && && = 12\ ,\\
12^2 \mod 77 &= 144 \mod 187 && && = 67\ .\\
12^4 \mod 77 &= 67^2 \mod 77 && && = 23\ .\\
12^8 \mod 77 &= 23^2 \mod 77 &= 529 \mod 77 && = 67\ .\\
12^{16} \mod 77 &= 67^2 \mod 77 &= 4489 \mod 187 && = 23\ .
\end{aligned}$$

$$12^{17} \mod 187 = (12^{16})(12^1) \mod 187 = (23)(12) \mod 77 = 45\ .$$

לכן הטקסט מוצפן $y = 45$.

ב)

$$y \mod p = 45 \mod 7 = 3\ , \quad a \mod (p-1) = 53 \mod 16 = 5\ .$$

לכן

$$x_1 = (y \mod p)^{a \mod (p-1)} \mod p = 3^5 \mod 7 = 243 \mod 7 = 5\ .$$

$$y \mod q = 45 \mod 11 = 1\ , \quad a \mod (q-1) = 53 \mod 10 = 3\ .$$

לכן

$$x_2 = (y \mod q)^{a \mod (q-1)} \mod q = 1^3 \mod 11 = 1\ .$$

$$\begin{aligned}
x &= x_1 \mod p = 5 \mod 7\ ,\\
x &= x_2 \mod q = 1 \mod 11\ .
\end{aligned}$$

נסמן: $m_1 = 7, m_2 = 11, a_1 = 5, a_2 = 1$.

$$\begin{aligned}
x &= a_1 \mod m_1 = 5 \mod 7\ ,\\
x &= a_2 \mod m_2 = 1 \mod 11\ .
\end{aligned}$$

נפתור ע"י משפט השאריות הסינית:

$$M = m_1 m_2 = 77, \quad M_1 = \frac{M}{m_1} = 11, \quad M_2 = \frac{M}{m_1} = 7.$$

$$y_1 = M_1^{-1} \mod m_1 = 11^{-1} \mod 7 = 2$$

$$y_2 = M_2^{-1} \mod m_2 = 7^{-1} \mod 11 = 8$$

$$\begin{aligned} a_1 M_1 y_1 + a_2 M_2 y_2 \mod M &= 166 \mod 77 \\ &= 12 \ . \end{aligned}$$

ג) פירוק לראשונים של $r^s s$:

$$r^2 s = r^2 s^1 \ .$$

לכן

$$\phi\left(r^2 s\right) = \left(r^2 - r\right)(s-1) \ .$$

שאלה 4 (25 נקודות)

א) (11 נק') $|k| = -11 \mod 26 = 15$. $\gcd(|k|, 26) = 1$ לכן ההופכי של $|k|$ קיימת. $|k|^{-1} \mod 26 = 15^{-1} \mod 26 = 7$. נחשב את המטריצה של קופקטורים:

$$C_{11} = 5 \ , \qquad C_{12} = -2 \ , \qquad C_{21} = -8 \ , \qquad C_{22} = 1 \ .$$

מכאן

$$\text{adj}(k) = C^t = \begin{pmatrix} 5 & -2 \\ -8 & 1 \end{pmatrix}^t \mod 26 = \begin{pmatrix} 5 & -8 \\ -2 & 1 \end{pmatrix}^t \mod 26 = \begin{pmatrix} 5 & 18 \\ 24 & 1 \end{pmatrix}$$

לכן

$$k^{-1} \mod 26 = |k|^{-1}\text{adj}(k) \mod 26 = 7 \begin{pmatrix} 5 & 28 \\ 24 & 1 \end{pmatrix} \mod 26 = \begin{pmatrix} 35 & 126 \\ 168 & 7 \end{pmatrix} \mod 26 = \begin{pmatrix} 9 & 22 \\ 12 & 7 \end{pmatrix} .$$

$$\begin{pmatrix} 1 & 24 \end{pmatrix} \begin{pmatrix} 9 & 22 \\ 12 & 7 \end{pmatrix} \mod 26 = \begin{pmatrix} 297 & 190 \end{pmatrix} \mod 26 = \begin{pmatrix} 11 & 8 \end{pmatrix}$$

$\mathtt{y} \in C$	B	Y	N	I
$y \in \mathbb{Z}_{26}$	1	24	13	8

$$\begin{pmatrix} 13 & 8 \end{pmatrix} \begin{pmatrix} 9 & 22 \\ 12 & 7 \end{pmatrix} \mod 26 = \begin{pmatrix} 213 & 342 \end{pmatrix} \mod 26 = \begin{pmatrix} 5 & 4 \end{pmatrix}$$

$\mathtt{y} \in C$	B	Y	N	I
$y \in \mathbb{Z}_{26}$	1	24	13	8
$x \in \mathbb{Z}_{26}$	11	8	5	4
$\mathtt{x} \in P$	l	i	f	e

ב) (10 נק')
$L_0 = 00101$ ו- $R_0 = 11001$. התת מפתחות הם

$$k_1 = (135)(24)\ , \qquad k_2 = (153)(2)(4)\ , \qquad k_3 = (1)(3)(5)(24)\ .$$

מכאן

$$L_1 = R_0 = 11001\ .$$
$$R_1 = L_0 \oplus f\left(R_0, k_1\right) = 00101 \oplus 00111 = 00010\ .$$

$$L_2 = R_1 = 00010\ .$$
$$R_2 = L_1 \oplus f\left(R_1, k_2\right) = 11001 \oplus 00010 = 11011\ .$$

$$L_3 = R_2 = 11011\ .$$
$$R_3 = L_2 \oplus f\left(R_2, k_3\right) = 00010 \oplus 11011 = 11001\ .$$
$$y = R_3 L_3 = 1100111011$$

ג) (4 נק') אם $p \nmid n$ אז p לא מופיע לפירוק לראשוניים של n. ז"א אם הפירוק לראשוניים של n הוא

$$n = p_1^{e_1} p_2^{e_2} \cdot p_k^{e_k}$$

אז $p \neq p_i$ לכל $1 \leq i \leq k$. לכן הפיקור לראשוניים של pn הוא

$$pn = p^1 p_1^{e_1} p_2^{e_2} \cdot p_k^{e_k}\ .$$

מכאן הפונקציית אוילר עבור pn היא

$$\phi(pn) = \left(p^1 - p^0\right)\left(p_1^{e_1} - p_1^{e_1 - 1}\right) \cdots \left(p_k^{e_k} - p_k^{e_k - 1}\right)\ .$$

אבל הפונקציית אוילר של p היה $\phi(p) = p-1$ והפונקציית אוילר של n הוא $\left(p_1^{e_1} - p_1^{e_1-1}\right) \cdots \left(p_k^{e_k} - p_k^{e_k-1}\right)$ לכן

$$\phi(pn) = (p-1)\phi(n)\ .$$

שאלה 5 (25 נקודות)

א) (6 נק') נתון המפתח של צופן אפיני $a = 5, b = 13$.
הכלל מפענח הינו $d_k(y) = a^{-1}(y-b) \mod 26$.
$\gcd(a, 26) = \gcd(5, 26) = 1$ לכן a^{-1} קיימת לכן הכלל מפענח קיים.

ב) (7 נק')

$$\begin{aligned} d_k(y) =& a^{-1}(y-b) \mod 26 = 5^{-5}(y-13) \mod 26 = 21(y-13) \mod 26 \\ =& 21y - 273 \mod 26 = 21y + 13 \mod 26\ . \end{aligned}$$

$y \in C$	S	H	W	N	K	K	D
$y \in \mathbb{Z}_{26}$	18	7	22	13	10	10	3
$x \in \mathbb{Z}_{26}$	1	4	7	0	15	15	24
$x \in P$	b	e	h	a	p	p	y

ג) (6 נק') נניח בשלילה ש- $\gcd(a,b) = d \neq 1$.
$\Leftarrow$ שלם ו- $\frac{a}{d}$ שלם.
נחלק את $sa + tb = 1$ ב- d:

$$sa + tb = 1 \quad \Rightarrow \quad s\frac{a}{d} + t\frac{b}{d} = \frac{1}{d} \ .$$

$\frac{a}{d}$ ו- $\frac{b}{d}$ שלמים $\Leftarrow$ הצד שמאול שלם $\Leftarrow$ הצד ימין שלם $\Leftarrow$ $\frac{1}{d}$ שלם. סתירה!

ד) (6 נק') לפי משפט אוקלידס קיימים שלמים s, t, d עבורם

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

נחלק ב- d:

$$s\frac{a}{d} + t\frac{b}{d} = 1 \ .$$

לכן לפי משפט אוקלידס: $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1 \Leftarrow \gcd\left(\frac{a}{\gcd(a,b)}, \frac{b}{\gcd(a,b)}\right) = 1 \Leftarrow$ ו- $\frac{a}{\gcd(a,b)}$ זרים.