שאלה 1 (25 נקודות)

נתון קבוצת טקסט גלוי $X = \{\mathtt{a}, \mathtt{b}, \mathtt{c}\}$, קבוצת טקסט מוצפן $Y = \{\mathtt{Q}, \mathtt{R}, \mathtt{S}\}$, והמפתחות $K = \{k_1, k_2, k_3\}$. פונקציית הסתברות של הטקסט גלוי היא

$$P_X(\mathtt{a}) = \frac{1}{10} \ , \qquad P_X(\mathtt{b}) = \frac{1}{5} \ , \qquad P_X(\mathtt{c}) = \frac{7}{10} \ ,$$

ופונקציית הסתברות של המפתחות היא

$$P_K(k_1) = \frac{1}{8} \ , \qquad P_K(k_2) = \frac{1}{4} \ , \qquad P_K(k_3) = \frac{5}{8} \ .$$

הכלל מצפין של הקריפטו-מערכת הוא

$$e_{k_i}(x) = \Big((x+i) \mod 3\Big) + 16 \ .$$

א) הרכיבו את המטריצת הצפנה של קריפטו-מערכת זו.

ב) מצאו את פונקצית הסתברות של הטקסט מוצפן Y.

ג) הוכיחו או הפריכו על ידי דוגמה נגדית: לקריפטו-מערכת זו יש סודיות מושלמת.

שאלה 2 (25 נקודות)

א) אליס שולחת לבוב הטקסט מוצפן הבא

$$\mathtt{OHIHERAWDUOYGNIO} \ .$$

אליס הצפינה את ההודעה באמצעות צופן תמורה עם המפתח $\pi = (4321)$. מצאו את הטקסט גלוי.

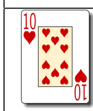
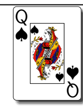
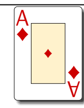
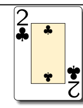
ב) נתונה אלפיבית בעלת 40 תווים. ונתונה הצפנה בעלת כלל מצפין

$$e_k(x) = ax + b$$

כאשר $x \in \mathbb{Z}_{40}$ ו- $k = (a, b), a, b \in \mathbb{Z}_{40}$ מפתח של ההצפנה. עבור אילו ערכי a, b ההצפנה ניתנת לפענח וכמה מפתחות חוקיים קיימים? רשמו את הכלל מפענח המתאים.

שאלה 3 (25 נקודות)

בחפיסת קלפים יש 10 קלפי מלך לב, 20 קלפי שתיים תלתן, 30 קלפי אס יהלום, 15 קלפי מלכה עלה, ו- 25 קלפי עשר לב:

25	15	30	20	10
				

א) מצאו הצפנת האפמן של כל אחד של הקלפים.

ב) מצאו את האנטרופיה של ההצפנה.

ג) הוכיחו: לצופן קיסר יש סודיות מושלמת.

שאלה 4 (25 נקודות)

א) חשבו את האיבר ההופכי $17^{-1} \mod 101$.

ב) פתרו את המערכת הבאה:

$$x \equiv 12 \mod 25 \ ,$$
$$x \equiv 9 \mod 26 \ ,$$
$$x \equiv 23 \mod 27 \ .$$

ג) הוכיחו: לכל ראשוניים a, b, הכמות של שלמים אשר זרים ל- ab וקטן מ- ab שווה ל- $(a-1)(b-1)$.

שאלה 5 (25 נקודות)

א) אליס מצפינה טקסט גלוי 10 ביטים באמצעות צופן פייסטל בעל 3 מחזורים. המפתח ההתחלתי k נתון על ידי התמורה

$$\pi = (134)(25) \ .$$

התזמון מפתחות הוא כך: כל תת-מפתח k_i $(1 \le i \le 3)$ מתקבל על ידי ההרכבה i- פעמים של התמורה π. מצאו את הטקסט מוצפן של הטקסט הגלוי `0010011001`.

ב) חשבו את $200^{-1} \mod 3$.

פתרונות

שאלה 1

א)

$$
\begin{aligned}
e_{k_1}(\texttt{a}) =& e_{k_1}(0) = \big((0+1) \mod 3\big) + 16 = 1 + 16 = 17 \to \texttt{R} \ , \\
e_{k_2}(\texttt{a}) =& e_{k_2}(0) = \big((0+2) \mod 3\big) + 16 = 2 + 16 = 18 \to \texttt{S} \ , \\
e_{k_3}(\texttt{a}) =& e_{k_3}(0) = \big((0+3) \mod 3\big) + 16 = 0 + 16 = 16 \to \texttt{Q} \ , \\
e_{k_1}(\texttt{b}) =& e_{k_1}(1) = \big((1+1) \mod 3\big) + 16 = 2 + 16 = 18 \to \texttt{S} \ , \\
e_{k_2}(\texttt{b}) =& e_{k_2}(1) = \big((1+2) \mod 3\big) + 16 = 0 + 16 = 16 \to \texttt{Q} \ , \\
e_{k_3}(\texttt{b}) =& e_{k_3}(1) = \big((3+1) \mod 3\big) + 16 = 1 + 16 = 17 \to \texttt{R} \ , \\
e_{k_1}(\texttt{c}) =& e_{k_1}(2) = \big((2+1) \mod 3\big) + 16 = 0 + 16 = 16 \to \texttt{Q} \ , \\
e_{k_2}(\texttt{c}) =& e_{k_2}(2) = \big((2+2) \mod 3\big) + 16 = 1 + 16 = 17 \to \texttt{R} \ , \\
e_{k_3}(\texttt{c}) =& e_{k_3}(2) = \big((3+2) \mod 3\big) + 16 = 2 + 16 = 18 \to \texttt{S} \ .
\end{aligned}
$$

	a	b	c
k_1	R	S	Q
k_2	S	Q	R
k_3	Q	R	S

ב)

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

$$
\begin{aligned}
P_Y(\texttt{R}) =& \sum_{k\in k_1,k_2,k_3} P(K=k_i)\, P(X=d_{k_i}(\texttt{R})) \\
=& P(K=k_1)\, P(X=d_{k_1}(\texttt{R})) + P(K=k_2)\, P(X=d_{k_2}(\texttt{R})) + P(K=k_3)\, P(X=d_{k_3}(\texttt{R})) \\
=& P(K=k_1)\, P(X=\texttt{a}) + P(K=k_2)\, P(X=\texttt{c}) + P(K=k_3)\, P(X=\texttt{b}) \\
=& \frac{1}{8}\cdot\frac{1}{10} + \frac{1}{4}\cdot\frac{7}{10} + \frac{5}{8}\cdot\frac{1}{5} \\
=& \frac{5}{16} \ .
\end{aligned}
$$

$$
\begin{aligned}
P_Y(\mathtt{S}) = & \sum_{k\in k_1,k_2,k_3} P(K=k_i)\, P(X=d_{k_i}(\mathtt{S})) \\
= & P(K=k_1)\, P(X=d_{k_1}(\mathtt{S})) + P(K=k_2)\, P(X=d_{k_2}(\mathtt{S})) + P(K=k_3)\, P(X=d_{k_3}(\mathtt{S})) \\
= & P(K=k_1)\, P(X=\mathtt{b}) + P(K=k_2)\, P(X=\mathtt{a}) + P(K=k_3)\, P(X=\mathtt{c}) \\
= & \frac{1}{8}\cdot\frac{1}{5} + \frac{1}{4}\cdot\frac{1}{10} + \frac{5}{8}\cdot\frac{7}{10} \\
= & \frac{39}{80}\ .
\end{aligned}
$$

$$
\begin{aligned}
P_Y(\mathtt{Q}) = & \sum_{k\in k_1,k_2,k_3} P(K=k_i)\, P(X=d_{k_i}(\mathtt{S})) \\
= & P(K=k_1)\, P(X=d_{k_1}(\mathtt{Q})) + P(K=k_2)\, P(X=d_{k_2}(\mathtt{Q})) + P(K=k_3)\, P(X=d_{k_3}(\mathtt{Q})) \\
= & P(K=k_1)\, P(X=\mathtt{c}) + P(K=k_2)\, P(X=\mathtt{b}) + P(K=k_3)\, P(X=\mathtt{a}) \\
= & \frac{1}{8}\cdot\frac{7}{10} + \frac{1}{4}\cdot\frac{1}{5} + \frac{5}{8}\cdot\frac{1}{10} \\
= & \frac{1}{5}\ .
\end{aligned}
$$

ג) לקריפטו-מערכת יש סודיות מושלמת אם התנאי $P(Y=y|X=x)=P(Y=y)$ מתקיים. תנאי השקול לזה הוא $P(X=x|Y=y)=P(X=x)$.

בדף נוסחאות: $P(Y=y|X=x)=\sum\limits_{\substack{k\in K\\ x=d_k(y)}} P(K=k_i)$.

לכן

$$P(Y=\mathtt{Q}|X=\mathtt{a}) = \sum_{\substack{k\in\{k_1,k_2,k_3\}\\ \mathtt{a}=d_{k_i}(\mathtt{Q})}} P(K=k_i) = P(K=k_1) = \frac{1}{8}\ .$$

$$P(Y=\mathtt{Q}) = \frac{1}{5}\ .$$

הרי $\frac{1}{5}=P(Y=\mathtt{Q}) \neq P(Y=\mathtt{Q}|X=\mathtt{a}) = \frac{1}{8}$ לכן לקריפטו-מערכת אין סודיות מושלמת.

שאלה 2 **(25 נקודות)**

א) $\pi = (4321)$, ז"א

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

ומכאן

$$\pi^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \ .$$

x $\in P$	O	H	I	H	E	R	A	W	D	U	O	Y	G	N	I	O
$x \in \mathbb{Z}_{26}$	14	7	8	7	4	17	0	22	3	20	14	24	6	13	8	14
$y = d_k(x)$	7	8	7	14	22	0	17	4	24	14	20	3	14	8	13	6
y $\in C$	h	i	h	o	w	a	r	e	y	o	u	d	o	i	n	g

ב) לכל $x, y \in \mathbb{Z}_{40}$:

$$y = ax + b \quad \Rightarrow \quad ax = y - b \quad \Rightarrow \quad x = a^{-1}(y-b) \ .$$

ז"א

$$d_k(y) = a^{-1}(y-b) \ .$$

b כל איבר ב- $\mathbb{Z}_{40}$, ז"א $b = 0, 1, \ldots, 39$.

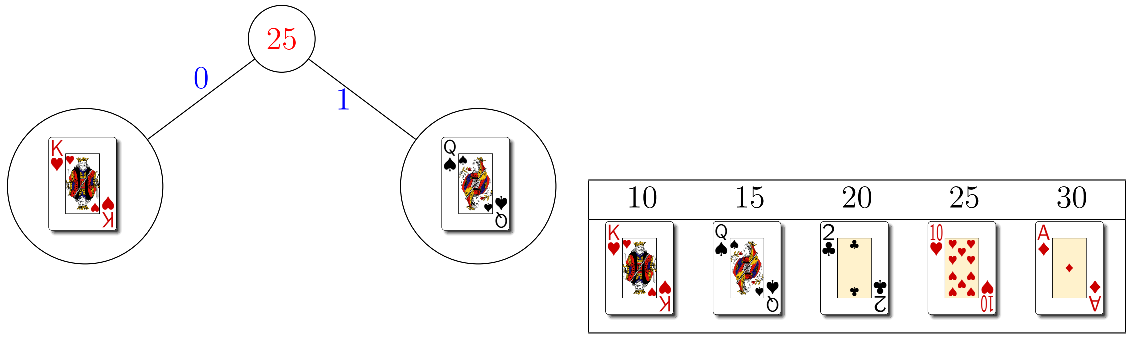
a איבר הפיך ב- $\mathbb{Z}_{40}$ אם ורק אם a זר ביחס ל- 40 (כלומר אס"ם $\gcd(a,40) = 1$).
קיימים $\phi(40)$ שלמים זרים ביחס ל-40.

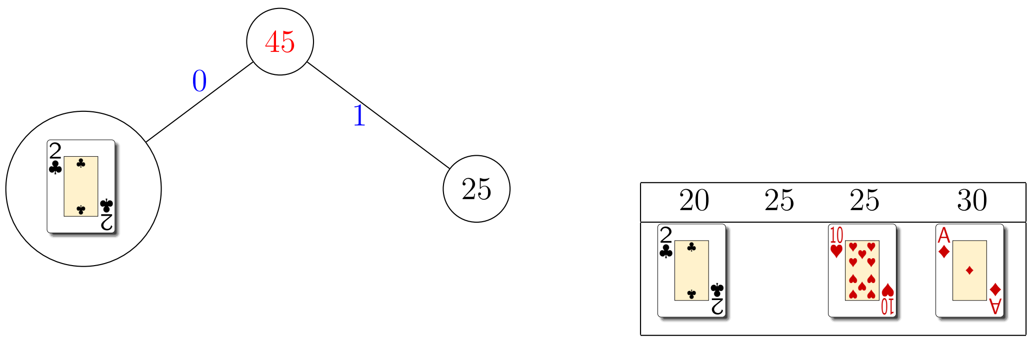
$$40 = 2^3 5^1 \quad \Rightarrow \quad \phi(40) = \left(2^3 - 2^2\right)\left(5^1 - 5^0\right) = 4 \cdot 4 = 16 \ .$$

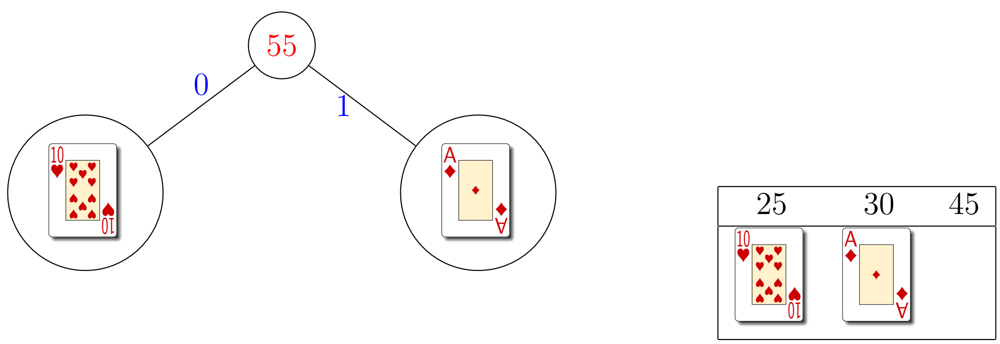
לכן קיימים 16 ערכים אפשריים ל- a. לפיכך קיימים $40 \times 16 = 840$ מפתחות אפשריים.

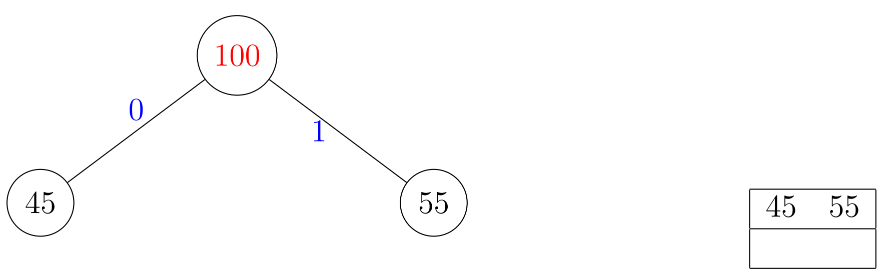
שאלה 3 (25 נקודות)

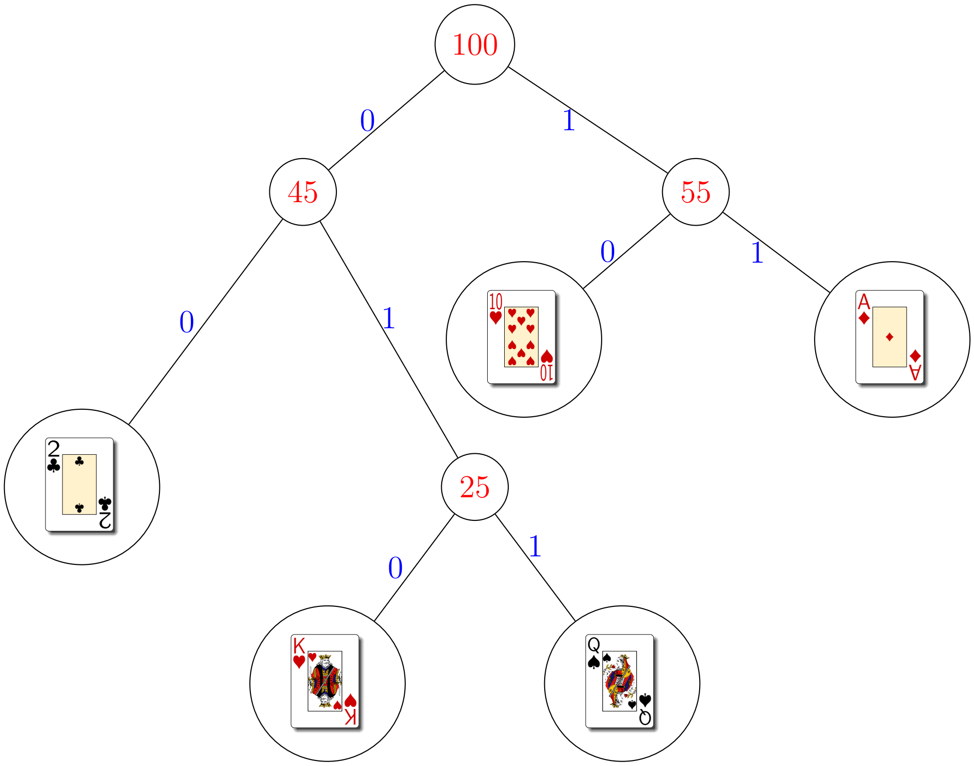
א)

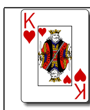
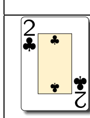
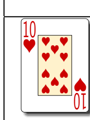
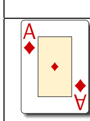

25
0
1
10 15 20 25 30


45
0
1
25
20 25 25 30

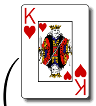
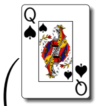
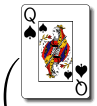
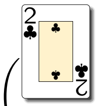
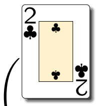

55
0
1
25 30 45

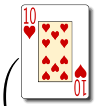
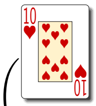
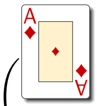
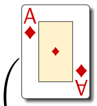

100
0
1
45
55
45 55



	010
	011
	00
	10
	11

ב)

$H[X] = -P_X\Big($  $\Big) \ln_2 P_X\Big($  $\Big) - P_X\Big($  $\Big) \ln_2 P_X\Big($  $\Big) - P_X\Big($  $\Big) \ln_2 P_X\Big($  $\Big)$

$- P_X\Big($  $\Big) \ln_2 P_X\Big($  $\Big) - P_X\Big($  $\Big) \ln_2 P_X\Big($  $\Big)$

$$\begin{aligned}
&= -\frac{10}{100}\ln_2\left(\frac{10}{100}\right) - \frac{15}{100}\ln_2\left(\frac{15}{100}\right) - \frac{20}{100}\ln_2\left(\frac{20}{100}\right) - \frac{25}{100}\ln_2\left(\frac{25}{100}\right) - \frac{30}{100}\ln_2\left(\frac{30}{100}\right)\\
&=0.332193 + 0.410545 + 0.464386 + 0.5 + 0.52109\\
&=2.22821 \ .
\end{aligned}$$

ג) צופן קיסר:

$$e_k(x) = x + k \mod 26 \ , \qquad\qquad d_k(y) = y - k \mod 26 \ .$$

יש סודיות מושלמת $\Leftrightarrow P(Y = y|X = x) = P(Y = y)$.

<u>צד שמאל</u>

מדף הנוסחאות:

$$P(Y = y|X = x) = \sum_{\substack{k\in\mathbb{Z}_{26}\\ x=d_k(y)}} P(K = k)$$

התנאי $x = d_k(y)$ אומר ש- $x = y - k \Leftarrow k = y - x$.
לכל x ו- y, מתוך כל האיברים בסכום בצד ימין יש רק k אחד עבורו $k = y - x$. לכן

$$P(Y = y|X = x) = P(k = y - x) = \frac{1}{26} \ . \qquad \textbf{(\#1)}$$

<u>צד ימין</u>

$$P(Y=y) = \sum_{k\in\mathbb{Z}_{26}} P(K=k)P\left(X=d_k(y)\right) \qquad \text{(דף נוסחאות)}$$

$$= \sum_{k\in\mathbb{Z}_{26}} \left(\frac{1}{26}\right) P\left(X=y-k \mod 26\right) \qquad (d_k(y)=y-k \mod 26)$$

$$= \left(\frac{1}{26}\right) \sum_{k\in\mathbb{Z}_{26}} P\left(X=y-k \mod 26\right) \ .$$

הסכום מעל k אומר שהארגומנט $X=y-k \mod 26$ עובר דרך כל איבר ב- $\mathbb{Z}_{26}$. ז"א הסכום ניתן לרשום בצורה $\sum\limits_{k\in\mathbb{Z}_{26}} P(X=k)$. זה פשוט סכום ההסתברויות ש- X שווה לכל איבר ב- $\mathbb{Z}_{26}$, אשר שווה ל- 1 לפי תכונת הנרמול של הסתברות. לכן

$$P(Y=y) = \left(\frac{1}{26}\right)\cdot 1 = \frac{1}{26} \ . \qquad \textbf{(\#2)}$$

לפי **(#1)** ו- **(#2)**, $P(Y=y|X=x)=\frac{1}{26}=P(Y=y)$ לכל x,y $\Leftarrow$ $\exists$ סודיות מושלמת.

<u>שאלה 4</u> (25 נקודות)

א) <u>שחטה 1</u>

$a=101, b=17$.

$$\begin{aligned} r_0 &= a=101\ , & r_1 &= b=17\ ,\\ s_0 &= 1\ , & s_1 &= 0\ ,\\ t_0 &= 0\ , & t_1 &= 1\ . \end{aligned}$$

שלב $i=1$:	$r_2=101-5\cdot 17=16$	$s_2=1-5\cdot 0=1$	$t_2=0-5\cdot 1=-5$	$q_1=5$
שלב $i=2$:	$r_3=17-1\cdot 16=1$	$s_3=0-1\cdot 1=-1$	$t_3=1-1\cdot(-5)=6$	$q_2=1$
שלב $i=3$:	$r_4=16-16\cdot 1=0$	$s_4=1-16\cdot(-1)=17$	$t_4=-5-16\cdot(6)=-101$	$q_3=16$

$$\gcd(a,b)=r_3=1\ , \qquad x=s_3=-1\ , \qquad y=t_3=6\ .$$

$$ax + by = -1(101) + 6(17) = 1 \ .$$

מכאן

$$6(17) = 1 + 1(101) \quad \Rightarrow \quad 6(17) = 1 \mod 101 \quad \Rightarrow \quad 17^{-1} = 101 \mod 6 \ .$$

<u>שיטה 2</u>

$$\begin{aligned} 101 =& 5(17) + 16 \\ 17 =& 1(16) + 1 \\ 16 =& 16(1) + 0 \ . \end{aligned}$$

$$\begin{aligned} 1 =& 17 - 1(16) \\ =& 17 - 1(101 - 5(17)) \\ =& 6(17) - 1(101) \ . \end{aligned}$$

לכן $17^{-1} \mod 101 = 6$.

ב)

$$\begin{aligned} x \equiv& 12 \mod 25 \ , \\ x \equiv& 9 \mod 26 \ , \\ x \equiv& 23 \mod 27 \ . \end{aligned}$$

נסמן

$$a_1 = 12 \ , \quad a_2 = 9 \ , \quad a_3 = 23 \ , \quad m_1 = 25 \ , \quad m_2 = 26 \ , \quad m_3 = 27 \ .$$

$$M = m_1 m_2 m_3 = 17550 \ , \quad M_1 = \frac{M}{m_1} = 702 \ , \quad M_2 = \frac{M}{m_2} = 675 \ , \quad M_3 = \frac{M}{m_3} = 650 \ .$$

$$y_1 = M_1^{-1} \mod m_1 = 702^{-1} \mod 25$$

$$\begin{aligned} 702 =& 28(25) + 2 \\ 25 =& 12(2) + 1 \\ 2 =& 2(1) + 0 \ . \end{aligned}$$

$$\begin{aligned} 1 =& 25 - 12(2) \\ =& 25 - 12(702 - 28(25)) \\ =& 337(25) - 12(702) \ . \end{aligned}$$

לכן $y_1 = 702^{-1} \mod 25 = -12 \mod 25 = 13$.

$$y_2 = M_2^{-1} \mod m_2 = 675^{-1} \mod 26$$

$$\begin{aligned} 675 =& 25(26) + 25 \\ 26 =& 1(25) + 1 \\ 25 =& 25(1) + 0 \ . \end{aligned}$$

$$\begin{aligned} 1 =& 26 - 1(25) \\ =& 26 - 1(675 - 25(26)) \\ =& 26(26) - 1(675) \ . \end{aligned}$$

לכן $y_2 = 675^{-1} \mod 26 = -1 \mod 26 = 25$.

$$y_3 = M_3^{-1} \mod m_3 = 650^{-1} \mod 27$$

$$\begin{aligned} 650 =& 24(27) + 2 \\ 27 =& 13(2) + 1 \\ 2 =& 2(1) + 0 \ . \end{aligned}$$

$$\begin{aligned} 1 =& 27 - 13(2) \\ =& 27 - 13(650 - 24(27)) \\ =& 25(27) - 13(650) \ . \end{aligned}$$

לכן $y_3 = 650^{-1} \mod 27 = -13 \mod 27 = 14$.

$$\begin{aligned} x =& a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3 \\ =& 12(702)(13) + 9(675)(25) + 23(650)(14) \mod 17550 \\ =& 470687 \mod 17550 \\ =& 14387 \ . \end{aligned}$$

ג) a ו- b ראשוניים לכן הפירוק לראשוניים של השלם ab הוא פשוט

$$ab = a^1 b^1 \ .$$

מכאן הפונקציית אוילר של ab היא

$$\phi(ab) = \left(a^1 - a^{1-1}\right)\left(b^1 - b^{1-1}\right) = (a-1)(b-1) \ .$$

כנדרש.

<u>שאלה 5</u> (25 נקודות)

א) $L_0 = 00100$ ו- $R_0 = 11001$. התת מפתחות הם

$$k_1 = (134)(25)\ , \qquad k_2 = (143)(2)(5)\ , \qquad k_3 = (1)(3)(4)(25)\ .$$

מכאן

$$L_1 = R_0 = 11001\ .$$
$$R_1 = L_0 \oplus f(R_0, k_1) = 00100 \oplus 01011 = 01111\ .$$

$$L_2 = R_1 = 01111\ .$$
$$R_2 = L_1 \oplus f(R_1, k_2) = 11001 \oplus 11011 = 00010\ .$$

$$L_3 = R_2 = 00010\ .$$
$$R_3 = L_2 \oplus f(R_2, k_3) = 01111 \oplus 00010 = 01101\ .$$
$$y = R_3 L_3 = 00010\ \ 01101\ .$$

ב) <u>שחטה 1</u>

$a = 200, b = 3$.

$$\begin{aligned} r_0 &= a = 200\ , \qquad & r_1 &= b = 3\ ,\\ s_0 &= 1\ , & s_1 &= 0\ ,\\ t_0 &= 0\ , & t_1 &= 1\ . \end{aligned}$$

$q_1 = 66$	$t_2 = 0 - 66 \cdot 1 = -66$	$s_2 = 1 - 66 \cdot 0 = 1$	$r_2 = 200 - 66 \cdot 3 = 2$	שלב $i = 1$:
$q_2 = 1$	$t_3 = 1 - 1 \cdot (-66) = 67$	$s_3 = 0 - 1 \cdot 1 = -1$	$r_3 = 3 - 1 \cdot 2 = 1$	שלב $i = 2$:
$q_3 = 2$	$t_4 = -66 - 2 \cdot (67) = -200$	$s_4 = 1 - 2 \cdot (-1) = 3$	$r_4 = 2 - 2 \cdot 1 = 0$	שלב $i = 3$:

$$\gcd(a, b) = r_3 = 1\ , \qquad x = s_3 = -1\ , \qquad y = t_3 = 67\ .$$

מכאן

$$ax + by = d \quad \Rightarrow \quad (-1)200 + 67(3) = 1\ .$$

$(-1)(200) = 1 - (67)3 \Leftarrow (-1)(200) \equiv 1 \mod 3 \Leftarrow 200^{-1} \mod 3 = -1 \mod 3 = 2$.

<u>שחטה 2</u>

$$\begin{aligned} 200 =& 66(3) + 2 \\ 3 =& 1(2) + 1 \\ 2 =& 2(1) + 0\ . \end{aligned}$$

$$\begin{aligned} 1 =& 3 - 1(2) \\ =& 3 - 1(200 - 66(3)) = \quad 67(3) - 1(200)\ . \end{aligned}$$

מכאן $200^{-1} \mod 3 = -1 \mod 3 = 2$.