עבודת 2: תמורות, צופן אניגמה, קריפטו-אנליזה וצופן RSA

אופן כתיבת תשובות לשאלות

1) **יש להראות פתרון מלא.** הסבירו היטב את מהלך הפתרון.

2) יש לנמק היטב כל שלב של פתרון. תשובה ללא הסבר וללא נימוק, אפילו נכונה, לא תתקבל.

3) יש לרשום ליד כל תשובה את מספר של השאלה שעליה אתם עונים.

מועד הגשה

1) ההגשה היא עד סוף יום ההגשה, כלומר עד השעה 23:59 באותו היום. אל תחכו לרגע האחרון. תכננו את זמנכם בהתאם. הגישו לפני.

2) איחור במועד ההגשה יגרור הורדה של ציון, 5 נק' לכל יום איחור או חלק ממנו. בכל מקרה לא יהיה ניתן להגיש מעבר ל-2 ימי איחור ממועד ההגשה דלעיל.

אופן הגשה

1) קראו היטב את השאלות. עליכם לענות על כל השאלות בעבודה זו.

2) הגשת העבודה תהיה דרך אתר הקורס במודל בלבד. הגשת העבודה היא **ביחידים או בזוגות.**

3) כיצד להגיש?

א) יש לסרוק או להמיר את העבודה לקובץ pdf ולהגיש אותו (סריקה לא ברורה או מטושטשת לא תיבדק).

ב)
- במידה שאת.ה מגיש.ה פתרונות לבד אז בשם הקובץ שיוגש למערכת ההגשה יהיה מספר ת"ז ושם של המגיש ושם של העבודה. לדוגמה: עבודה2-ירמיהו-תז-123456789.pdf.
- במידה שאתם מגישים פתרונות כזוג אז בשם הקובץ שיוגש למערכת ההגשה יהיו מספרי ת"ז ושמות של המגישים ושם של העבודה. לדוגמה: עבודה2-ירמיהו-תז-123456789-גל-113114115.pdf

4) בקובץ המוגש יש להוסיף את התיעוד הבא בעמוד הראשון (בעברית או באנגלית, לבחירתכם). יש לשנות את השם לשם שלכם ואת תעודת הזהות לתעודת הזהות שלכם. ובמקום סולמית יש לכתוב את מספר העבודה.

Assignment: #
Author1: Israel Israeli, ID: 01234567
Author2: Dave David, ID: 8910111213

5) לאחר שהעליתם את הקבצים שלכם למודל, הורידו אותם מהמודל למחשב שלכם וודאו כי הקבצים תקינים וכי העליתם את הקבצים הנכונים והמלאים. לאחר תום מועד ההגשה לא יתקבלו ערעורים על כך שהעליתם קבצים לא תקינים או שהעליתם בטעות קבצים אחרים / לא נכונים.

שאלות

1) שאלות בנוגע העבודה יש לשאול בפורום באתר המודל של הקורס או בשעות קבלה של המתרגל/ת האחראי/ת בלבד. אין לשלוח שאלות במייל לא למתרגל האחראי ולא למתרגלים/מרצים אחרים.

2) ניתן לשאול שאלות הבהרה ומיקוד על המשימות שבעבודה במידה ומשימה מסוימת לא ברורה. לא ניתן לשאול על הפתרונות שלכם. לדוגמא, לא ניתן לשאול האם הפתרון שלי נכון, לא ניתן לשאול למה הפתרון לא עובד, וכדומה.

שונות

1) השאלות בעבודה זו הינן שוות משקל. כלומר, משקל כל שאלה הוא 100 חלקי מספר השאלות בעבודה.

2) בשאלה מרובת סעיפים, הסעיפים הם שווי משקל. כלומר משקל כל סעיף הוא משקל השאלה כולה חלקי מספר הסעיפים השאלה.

בהצלחה!

עבודת 2: תמורות, צופן אניגמה, קריפטו-אנליזה וצופן RSA

שאלה 1 (10 נקודות)

VSLBHPNAQRPELCGGUVFZRFFNTRCYRNFRJEVGRLBHEANZRURER

שאלה 2 (9 נקודות)

הטקסט הבא

BXNKJLGZ

הוצפן ע"י צופן אניגמה עם המשקפת המשתנה

$$\pi = \texttt{(AG)(XI)(LP)(HD)(ES)(TY)}\ .$$

מצאו את הטקסט הגלוי.

שאלה 3 (9 נקודות)

הטבלה הבאה מראה מילים אופייניות מהודעות מוצפנות מאותו יום.

WWODFS	TASEQM	JMKNZC	FSZWUW	JBPNLT	CFDXVR
DLVQMF	VBRULE	GTACDP	KYESTU	AZJLIV	IRLGNI
PEQIYH	XONKHK	UNBJWX	LVIHPY	ZCFRSL	BJXAEZ
OQYFCJ	MHGPOA	YDWMJB	QXCBGN	NKTVAG	HPHORD
RUUTKQ	SGMYXO	EIVZBF			

א) הוכיחו כי התמורות המתאימות של צופן אניגמה הן:

$$\Delta_4\Delta_1 = \texttt{(JNVU)(ZRTE)(GCXKSYMPI)(ALHOFWDQB)}\ ,$$
$$\Delta_5\Delta_2 = \texttt{(HO)(XG)(DJEYT)(MZIBL)(FVPRNW)(AQCSUK)}\ ,$$
$$\Delta_6\Delta_3 = \texttt{(MOS)(CNK)(BXZW)(TGAP)(FLIYJV)(QHDREU)}\ .$$

ב) נניח כי התמורות $\Delta_4\Delta_1$, $\Delta_5\Delta_2$, $\Delta_6\Delta_3$ הן בסדר רייבסקי. נתון הטקסט הבא שהוצפן ע"י צופן אניגמה:

MWORVZ

חשבו את הטקסט הגלוי.

שאלה 4 (9 נקודות)

הטקסט הבא הוצפן ע"י צופן אפיני:

```
BDHS CZTF ZX OZTZCFA ADYC RLXCF ZC OZMZYP XDTFDYF FOXFX
OZKF ADYC OZMF CUF SFXHOCX DK XDTFDYF FOXFX CUZYJZYP
ADYC RDSSB LQDHC CUF KHCHSF SFTFTQFS VDTIOFTFYCX KDSPFC
CUF ZYXHOCX ADYC RDSSB RULC DCUFS IFDIOF CUZYJ ZK
BDH XHVVFFA ZY CUZX CFOO TF UDR ADYC KDSPFC CD ULMF KHY
```

היעזרו בקריפטו-אנליזה כדי למצוא את הטקסט הגלוי.

שאלה 5 (9 נקודות)

תהי $\pi : \Sigma \to \Sigma$ תמורה מעל אלפבית Σ. הוכיחו או הפריכו ע"י דוגמה נגדית את הטענות הבאות:

א) אם π מחזור באורך k אזי $\pi^k = \mathrm{id}$.

ב) אם π מחזור באורך k אזי k הוא השלם הקטן ביותר עבורו $\pi^k = \mathrm{id}$.

שאלה 6 (9 נקודות)

תהי Σ אלפבית בעל n אותיות. כלומר $|\Sigma| = n$. נסמן ב- S_n הקבוצה של כל התמורות האפשריות מעל Σ.
הוכיחו את הטענה הבאה:
אם קיימת תמורה $\alpha \in S_n$ כך שלכל $\beta \in S_n$ מתקיים:

$$\alpha\beta = \beta\alpha$$

אז $\alpha = \mathrm{id}$.

שאלה 7 (9 נקודות)

אליס שולחת לבוב הודעה. אליס מצפינה את ההודעה ע"י צופן RSA עם הפרמטרים

$$b = 107 \ , \quad p = 73 \ , \quad q = 31 \ .$$

ההצפנה של ההודעה היא

$$y = \mathrm{DED} \ .$$

א) הוכיחו כי המפתח הציבורי הוא $(a, p, q) = (323, 73, 31)$.

ב) חשבו את הטקסט הגלוי שאליס שלחה.

שאלה 8 (9 נקודות)
פתרו את המערכת משוואות הבאה בעזרת המשפט השאריות הסיני:

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

שאלה 9 (9 נקודות)
פתרו את המערכת משוואות הבאה:

$$13x \equiv 4 \mod 99$$
$$15x \equiv 56 \mod 101 \ .$$

רמז: השתמשו באלגוריתם המוכלל של אוקליד ואחר כך המשפט השאירות הסיני.

שאלה 10 (9 נקודות)
בוב בונה מפתח ציבורי ומפתח סודי של צופן RSA עם הפרמטרים $p = 37$, $q = 41$ ו- $b = 31$.

א) חשבו את n, $\phi(n)$ ו- a.

ב) אליס מצפינה את הטקסט הגלוי `bcci`. מהי הטקסט מוצפן שהיא שולחת לבוב?

ג) הוכיחו שהפענוח של הטקסט מוצפן שמצאתם בסעיף ב' נותן `bcci`.

רמז:

$$(-11)(1440) + (511)(31) = 1 \ , \qquad (-9)(41) + (10)(37) = 1 \ .$$

שאלה 11 (9 נקודות)
נתון הטקסט גלוי

`thefutureisgood`

והטקסט מוצפן שלו

`FOPBVFWDFCCGMAT`

הטקסט הוצפן עם צופן היל. מצאו את המפתח.

פתרונות

שאלה 1

הטקסט הוצפן ע"י צופן הזזה עם המפתח $k=13$.

$$d_k(y)=y-k \bmod 26 \ .$$

y	V	S	L	B	H	P	N	A	Q	R	P	E	L	C	G	G	U	V	F	Z	R	F	F	N	T	R
y	21	18	11	1	7	15	13	0	16	17	15	4	11	2	6	6	20	21	5	25	17	5	5	13	19	17
$d_k(y)$	8	5	24	14	20	2	0	13	3	4	2	17	24	15	19	19	7	8	18	12	4	18	18	0	6	4
x	i	f	y	o	u	c	a	n	d	e	c	r	y	p	t	t	h	i	s	m	e	s	s	a	g	e

y	C	Y	R	N	F	R	J	E	V	G	R	L	B	H	E	A	N	Z	R	U	R	E	R
y	2	24	17	13	5	17	9	4	21	6	17	11	2	7	4	0	13	25	17	20	17	4	17
$d_k(y)$	15	11	4	0	18	4	22	17	8	19	4	24	15	20	17	13	0	12	4	7	4	17	4
x	p	l	e	a	s	e	w	r	i	t	e	y	o	u	r	n	a	m	e	h	e	r	e

שאלה 2

התמורות של צופן אניגמה הן:

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

הכלל מצפין והכלל מפענח של צופן אניגמה מוגדרים באופן הבא. נתון תמורה משקפת המשתנה (נתונה בשאלה)

$$\pi = \texttt{(AG)(XI)(LP)(HD)(ES)(TY)} \ .$$

לכל מילה $x_1x_2\ldots x_n$ של טקסטט גלוי, לכל $1\leq i\leq n$ הכלל מצפין הוא:

$$e\left(x_i\right)=\Delta_i\left(x_i\right)$$

ולכל לכל מילה $y_1y_2\ldots y_n$ של טקסטט מוצפן, לכל $1\leq i\leq n$ הכלל מפענח הוא:

$$d\left(y_i\right)=\Delta_i\left(y_i\right)$$

כאשר Δ_i היא התמורה המורכבת

$$\Delta_i=\pi\ \left[\alpha_3^i\right]^{-1}\ \alpha_2^{-1}\ \alpha_1^{-1}\ \rho\ \alpha_1\ \alpha_2\ \alpha_3^i\ \pi(x_i)$$

כאשר

$$\alpha_3^i=\sigma_{-i}\ \alpha_3\ \sigma_i\ , \qquad \left[\alpha_3^i\right]^{-1}=\sigma_{-i}\ \alpha_3^{-1}\ \sigma_i\ .$$

נתון הטקסט מוצפן:

$$\texttt{BXNKJLGZ} \ .$$

1) $\underline{y_1 = \mathtt{B}}$

$$B \xrightarrow{\pi} B \xrightarrow{\sigma_1} C \xrightarrow{\alpha_3} F \xrightarrow{\sigma_{-1}} E \xrightarrow{\alpha_2} S \xrightarrow{\alpha_1} S \xrightarrow{\rho} F$$
$$\xrightarrow{\alpha_1^{-1}} D \xrightarrow{\alpha_2^{-1}} C \xrightarrow{\sigma_1} D \xrightarrow{\alpha_3^{-1}} B \xrightarrow{\sigma_{-1}} A \xrightarrow{\pi} \color{red}{G}$$

2) $\underline{x_2 = \mathtt{X}}$

$$X \xrightarrow{\pi} I \xrightarrow{\sigma_2} K \xrightarrow{\alpha_3} X \xrightarrow{\sigma_{-2}} V \xrightarrow{\alpha_2} Y \xrightarrow{\alpha_1} C \xrightarrow{\rho} U$$
$$\xrightarrow{\alpha_1^{-1}} R \xrightarrow{\alpha_2^{-1}} G \xrightarrow{\sigma_2} I \xrightarrow{\alpha_3^{-1}} Q \xrightarrow{\sigma_{-2}} O \xrightarrow{\pi} \color{red}{O}$$

3) $\underline{x_3 = \mathtt{N}}$

$$N \xrightarrow{\pi} N \xrightarrow{\sigma_3} Q \xrightarrow{\alpha_3} I \xrightarrow{\sigma_{-3}} F \xrightarrow{\alpha_2} I \xrightarrow{\alpha_1} V \xrightarrow{\rho} W$$
$$\xrightarrow{\alpha_1^{-1}} N \xrightarrow{\alpha_2^{-1}} T \xrightarrow{\sigma_3} W \xrightarrow{\alpha_3^{-1}} R \xrightarrow{\sigma_{-3}} O \xrightarrow{\pi} \color{red}{O}$$

4) $\underline{x_4 = \mathtt{K}}$

$$K \xrightarrow{\pi} K \xrightarrow{\sigma_4} O \xrightarrow{\alpha_3} Y \xrightarrow{\sigma_{-4}} U \xrightarrow{\alpha_2} P \xrightarrow{\alpha_1} H \xrightarrow{\rho} D$$
$$\xrightarrow{\alpha_1^{-1}} G \xrightarrow{\alpha_2^{-1}} R \xrightarrow{\sigma_4} V \xrightarrow{\alpha_3^{-1}} L \xrightarrow{\sigma_{-4}} H \xrightarrow{\pi} \color{red}{D}$$

5) $\underline{x_5 = \mathtt{J}}$

$$J \xrightarrow{\pi} J \xrightarrow{\sigma_5} O \xrightarrow{\alpha_3} Y \xrightarrow{\sigma_{-5}} T \xrightarrow{\alpha_2} N \xrightarrow{\alpha_1} W \xrightarrow{\rho} V$$
$$\xrightarrow{\alpha_1^{-1}} I \xrightarrow{\alpha_2^{-1}} F \xrightarrow{\sigma_5} K \xrightarrow{\alpha_3^{-1}} U \xrightarrow{\sigma_{-5}} P \xrightarrow{\pi} \color{red}{L}$$

6) $\underline{x_6 = \mathtt{L}}$

$$L \xrightarrow{\pi} P \xrightarrow{\sigma_6} V \xrightarrow{\alpha_3} M \xrightarrow{\sigma_{-6}} G \xrightarrow{\alpha_2} R \xrightarrow{\alpha_1} U \xrightarrow{\rho} C$$
$$\xrightarrow{\alpha_1^{-1}} Y \xrightarrow{\alpha_2^{-1}} V \xrightarrow{\sigma_6} B \xrightarrow{\alpha_3^{-1}} A \xrightarrow{\sigma_{-6}} U \xrightarrow{\pi} \color{red}{U}$$

7) $\underline{x_7 = \mathtt{G}}$

$$G \xrightarrow{\pi} A \xrightarrow{\sigma_7} H \xrightarrow{\alpha_3} P \xrightarrow{\sigma_{-7}} I \xrightarrow{\alpha_2} X \xrightarrow{\alpha_1} R \xrightarrow{\rho} B$$
$$\xrightarrow{\alpha_1^{-1}} W \xrightarrow{\alpha_2^{-1}} M \xrightarrow{\sigma_7} T \xrightarrow{\alpha_3^{-1}} J \xrightarrow{\sigma_{-7}} C \xrightarrow{\pi} \color{red}{C}$$

8) $\underline{x_8 = \mathtt{Z}}$

$$Z \xrightarrow{\pi} Z \xrightarrow{\sigma_8} H \xrightarrow{\alpha_3} P \xrightarrow{\sigma_{-8}} H \xrightarrow{\alpha_2} U \xrightarrow{\alpha_1} A \xrightarrow{\rho} Y$$
$$\xrightarrow{\alpha_1^{-1}} O \xrightarrow{\alpha_2^{-1}} Y \xrightarrow{\sigma_8} G \xrightarrow{\alpha_3^{-1}} S \xrightarrow{\sigma_{-8}} K \xrightarrow{\pi} K$$

לפיכך הטקסט גלוי הוא: GOODLUCK .

שאלה 3

א) בהינתן מילה משוכפלת

$$xyz\ xyz$$

הטקסט המוצפן המתקבל ע"י צופן אניגמה הוא נקרא מילה אופיינית, אשר כתוב בביטוי הבא:

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

המשפט רייבסקי I נותן את היחסים הבאים:

$$\begin{aligned} \sigma_4 &= \Delta_4\Delta_1(\sigma_1)\ , \\ \sigma_5 &= \Delta_5\Delta_2(\sigma_2)\ , \\ \sigma_6 &= \Delta_6\Delta_3(\sigma_3)\ . \end{aligned}$$

לדוגמה, לפי המילה האופיינית הראשונה ברשימה נקבל:

$$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \mathtt{WWODFS} \quad\Rightarrow\quad \sigma_1 = \mathtt{W}\ , \sigma_4 = \mathtt{D} \quad\Rightarrow\quad \Delta_4\Delta_1(\mathtt{W}) = \mathtt{D}\ .$$

ז"א התמורה $\Delta_4\Delta_1$ על האות W פולטת D. בעזרת השיטה הזו על כל המילים האופיניות ברשימה נקבל

את התמורות של כל האותיות:

$$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \mathtt{WWODFS} \Rightarrow \sigma_1 = \mathtt{W}\ ,\ \sigma_4 = \mathtt{D} \Rightarrow \Delta_4\Delta_1(\mathtt{W}) = \mathtt{D}\ .$$
$$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \mathtt{DLVQMF} \Rightarrow \sigma_1 = \mathtt{D}\ ,\ \sigma_4 = \mathtt{Q} \Rightarrow \Delta_4\Delta_1(\mathtt{D}) = \mathtt{Q}\ .$$
$$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \mathtt{PEQIYH} \Rightarrow \sigma_1 = \mathtt{P}\ ,\ \sigma_4 = \mathtt{I} \Rightarrow \Delta_4\Delta_1(\mathtt{P}) = \mathtt{I}\ .$$
$$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \mathtt{OQYFCJ} \Rightarrow \sigma_1 = \mathtt{O}\ ,\ \sigma_4 = \mathtt{F} \Rightarrow \Delta_4\Delta_1(\mathtt{O}) = \mathtt{F}\ .$$
$$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \mathtt{RUUTKQ} \Rightarrow \sigma_1 = \mathtt{R}\ ,\ \sigma_4 = \mathtt{T} \Rightarrow \Delta_4\Delta_1(\mathtt{R}) = \mathtt{T}\ .$$
$$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \mathtt{TASEQM} \Rightarrow \sigma_1 = \mathtt{T}\ ,\ \sigma_4 = \mathtt{E} \Rightarrow \Delta_4\Delta_1(\mathtt{T}) = \mathtt{E}\ .$$
$$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \mathtt{VBRULE} \Rightarrow \sigma_1 = \mathtt{V}\ ,\ \sigma_4 = \mathtt{U} \Rightarrow \Delta_4\Delta_1(\mathtt{V}) = \mathtt{U}\ .$$
$$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \mathtt{XONKHK} \Rightarrow \sigma_1 = \mathtt{X}\ ,\ \sigma_4 = \mathtt{K} \Rightarrow \Delta_4\Delta_1(\mathtt{X}) = \mathtt{K}\ .$$
$$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \mathtt{MHGPOA} \Rightarrow \sigma_1 = \mathtt{M}\ ,\ \sigma_4 = \mathtt{P} \Rightarrow \Delta_4\Delta_1(\mathtt{M}) = \mathtt{P}\ .$$
$$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \mathtt{SGMYXO} \Rightarrow \sigma_1 = \mathtt{S}\ ,\ \sigma_4 = \mathtt{Y} \Rightarrow \Delta_4\Delta_1(\mathtt{S}) = \mathtt{Y}\ .$$
$$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \mathtt{JMKNZC} \Rightarrow \sigma_1 = \mathtt{J}\ ,\ \sigma_4 = \mathtt{N} \Rightarrow \Delta_4\Delta_1(\mathtt{J}) = \mathtt{N}\ .$$
$$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \mathtt{GTACDP} \Rightarrow \sigma_1 = \mathtt{G}\ ,\ \sigma_4 = \mathtt{C} \Rightarrow \Delta_4\Delta_1(\mathtt{G}) = \mathtt{C}\ .$$
$$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \mathtt{UNBJWX} \Rightarrow \sigma_1 = \mathtt{U}\ ,\ \sigma_4 = \mathtt{J} \Rightarrow \Delta_4\Delta_1(\mathtt{U}) = \mathtt{J}\ .$$
$$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \mathtt{YDWMJB} \Rightarrow \sigma_1 = \mathtt{Y}\ ,\ \sigma_4 = \mathtt{M} \Rightarrow \Delta_4\Delta_1(\mathtt{Y}) = \mathtt{M}\ .$$
$$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \mathtt{EIVZBF} \Rightarrow \sigma_1 = \mathtt{E}\ ,\ \sigma_4 = \mathtt{Z} \Rightarrow \Delta_4\Delta_1(\mathtt{E}) = \mathtt{Z}\ .$$
$$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \mathtt{FSZWUW} \Rightarrow \sigma_1 = \mathtt{F}\ ,\ \sigma_4 = \mathtt{W} \Rightarrow \Delta_4\Delta_1(\mathtt{F}) = \mathtt{W}\ .$$
$$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \mathtt{KYESTU} \Rightarrow \sigma_1 = \mathtt{K}\ ,\ \sigma_4 = \mathtt{S} \Rightarrow \Delta_4\Delta_1(\mathtt{K}) = \mathtt{S}\ .$$
$$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \mathtt{LVIHPY} \Rightarrow \sigma_1 = \mathtt{L}\ ,\ \sigma_4 = \mathtt{H} \Rightarrow \Delta_4\Delta_1(\mathtt{L}) = \mathtt{H}\ .$$
$$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \mathtt{QXCBGN} \Rightarrow \sigma_1 = \mathtt{Q}\ ,\ \sigma_4 = \mathtt{B} \Rightarrow \Delta_4\Delta_1(\mathtt{Q}) = \mathtt{B}\ .$$
$$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \mathtt{JBPNLT} \Rightarrow \sigma_1 = \mathtt{J}\ ,\ \sigma_4 = \mathtt{N} \Rightarrow \Delta_4\Delta_1(\mathtt{J}) = \mathtt{N}\ .$$
$$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \mathtt{AZJLIV} \Rightarrow \sigma_1 = \mathtt{A}\ ,\ \sigma_4 = \mathtt{L} \Rightarrow \Delta_4\Delta_1(\mathtt{A}) = \mathtt{L}\ .$$
$$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \mathtt{ZCFRSL} \Rightarrow \sigma_1 = \mathtt{Z}\ ,\ \sigma_4 = \mathtt{R} \Rightarrow \Delta_4\Delta_1(\mathtt{Z}) = \mathtt{R}\ .$$
$$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \mathtt{NKTVAG} \Rightarrow \sigma_1 = \mathtt{N}\ ,\ \sigma_4 = \mathtt{V} \Rightarrow \Delta_4\Delta_1(\mathtt{N}) = \mathtt{V}\ .$$
$$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \mathtt{CFDXVR} \Rightarrow \sigma_1 = \mathtt{C}\ ,\ \sigma_4 = \mathtt{X} \Rightarrow \Delta_4\Delta_1(\mathtt{C}) = \mathtt{X}\ .$$
$$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \mathtt{IRLGNI} \Rightarrow \sigma_1 = \mathtt{I}\ ,\ \sigma_4 = \mathtt{G} \Rightarrow \Delta_4\Delta_1(\mathtt{I}) = \mathtt{G}\ .$$
$$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \mathtt{BJXAEZ} \Rightarrow \sigma_1 = \mathtt{B}\ ,\ \sigma_4 = \mathtt{A} \Rightarrow \Delta_4\Delta_1(\mathtt{B}) = \mathtt{A}\ .$$
$$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \mathtt{HPHORD} \Rightarrow \sigma_1 = \mathtt{H}\ ,\ \sigma_4 = \mathtt{O} \Rightarrow \Delta_4\Delta_1(\mathtt{H}) = \mathtt{O}\ .$$

לפי התוצאות האלו נרשום את התמורה $\Delta_4\Delta_1$ בייצוג טבלה בטבלה הבאה:

x	$\Delta_4\Delta_1(x)$
A	L
B	A
C	X
D	Q
E	Z
F	W

x	$\Delta_4\Delta_1(x)$
G	C
H	O
I	G
J	N
K	S
L	H

x	$\Delta_4\Delta_1(x)$
M	P
N	V
O	F
P	I
Q	B
R	T

x	$\Delta_4\Delta_1(x)$
S	Y
T	E
U	J
V	U
W	D
X	K

x	$\Delta_4\Delta_1(x)$
Y	E
Z	R

לפי הטבלה, אפשר לפרק את התמורה למחזורים שלה ואז נקבל את הפירוק למחזורים הבא:

$$\Delta_4\Delta_1 = (\mathtt{JNVU})\,(\mathtt{ZRTE})\,(\mathtt{GCXKSYMPI})\,(\mathtt{ALHOFWDQB}) \quad ,$$

כנדרש.
מהמילה האופיינית הראשונה ברשימה, לפי משפט רייבסקי I נקבל:

$$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \mathtt{WWODFS} \quad\Rightarrow\quad \sigma_2 = \mathtt{W}\ , \sigma_5 = \mathtt{F} \quad\Rightarrow\quad \Delta_5\Delta_2\,(\mathtt{W}) = \mathtt{F}\ .$$

ז"א התמורה $\Delta_5\Delta_2$ על האות W פולטת F. בעזרת השיטה הזו על כל המילים האופיניות ברשימה נקבל את התמורות של כל האותיות:

$$\begin{array}{lllll}
\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = & \mathtt{WWODFS} & \Rightarrow\ \sigma_2 = \mathtt{W}\ , & \sigma_5 = \mathtt{F} & \Rightarrow\ \Delta_5\Delta_2\,(\mathtt{W}) = \mathtt{F}\ .\\
\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = & \mathtt{DLVQMF} & \Rightarrow\ \sigma_2 = \mathtt{L}\ , & \sigma_5 = \mathtt{M} & \Rightarrow\ \Delta_5\Delta_2\,(\mathtt{L}) = \mathtt{M}\ .\\
\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = & \mathtt{PEQIYH} & \Rightarrow\ \sigma_2 = \mathtt{E}\ , & \sigma_5 = \mathtt{Y} & \Rightarrow\ \Delta_5\Delta_2\,(\mathtt{E}) = \mathtt{Y}\ .\\
\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = & \mathtt{OQYFCJ} & \Rightarrow\ \sigma_2 = \mathtt{Q}\ , & \sigma_5 = \mathtt{C} & \Rightarrow\ \Delta_5\Delta_2\,(\mathtt{Q}) = \mathtt{C}\ .\\
\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = & \mathtt{RUUTKQ} & \Rightarrow\ \sigma_2 = \mathtt{U}\ , & \sigma_5 = \mathtt{K} & \Rightarrow\ \Delta_5\Delta_2\,(\mathtt{U}) = \mathtt{K}\ .\\
\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = & \mathtt{TASEQM} & \Rightarrow\ \sigma_2 = \mathtt{A}\ , & \sigma_5 = \mathtt{Q} & \Rightarrow\ \Delta_5\Delta_2\,(\mathtt{A}) = \mathtt{Q}\ .\\
\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = & \mathtt{VBRULE} & \Rightarrow\ \sigma_2 = \mathtt{B}\ , & \sigma_5 = \mathtt{L} & \Rightarrow\ \Delta_5\Delta_2\,(\mathtt{B}) = \mathtt{L}\ .\\
\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = & \mathtt{XONKHK} & \Rightarrow\ \sigma_2 = \mathtt{O}\ , & \sigma_5 = \mathtt{H} & \Rightarrow\ \Delta_5\Delta_2\,(\mathtt{O}) = \mathtt{H}\ .\\
\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = & \mathtt{MHGPOA} & \Rightarrow\ \sigma_2 = \mathtt{H}\ , & \sigma_5 = \mathtt{O} & \Rightarrow\ \Delta_5\Delta_2\,(\mathtt{H}) = \mathtt{O}\ .\\
\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = & \mathtt{SGMYXO} & \Rightarrow\ \sigma_2 = \mathtt{G}\ , & \sigma_5 = \mathtt{X} & \Rightarrow\ \Delta_5\Delta_2\,(\mathtt{G}) = \mathtt{X}\ .\\
\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = & \mathtt{JMKNZC} & \Rightarrow\ \sigma_2 = \mathtt{M}\ , & \sigma_5 = \mathtt{Z} & \Rightarrow\ \Delta_5\Delta_2\,(\mathtt{M}) = \mathtt{Z}\ .\\
\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = & \mathtt{GTACDP} & \Rightarrow\ \sigma_2 = \mathtt{T}\ , & \sigma_5 = \mathtt{D} & \Rightarrow\ \Delta_5\Delta_2\,(\mathtt{T}) = \mathtt{D}\ .\\
\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = & \mathtt{UNBJWX} & \Rightarrow\ \sigma_2 = \mathtt{N}\ , & \sigma_5 = \mathtt{W} & \Rightarrow\ \Delta_5\Delta_2\,(\mathtt{N}) = \mathtt{W}\ .\\
\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = & \mathtt{YDWMJR} & \Rightarrow\ \sigma_2 = \mathtt{D}\ , & \sigma_5 = \mathtt{J} & \Rightarrow\ \Delta_5\Delta_2\,(\mathtt{D}) = \mathtt{J}\ .\\
\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = & \mathtt{EIVZBF} & \Rightarrow\ \sigma_2 = \mathtt{I}\ , & \sigma_5 = \mathtt{B} & \Rightarrow\ \Delta_5\Delta_2\,(\mathtt{I}) = \mathtt{B}\ .\\
\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = & \mathtt{FSZWUW} & \Rightarrow\ \sigma_2 = \mathtt{S}\ , & \sigma_5 = \mathtt{U} & \Rightarrow\ \Delta_5\Delta_2\,(\mathtt{S}) = \mathtt{U}\ .\\
\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = & \mathtt{KYESTU} & \Rightarrow\ \sigma_2 = \mathtt{Y}\ , & \sigma_5 = \mathtt{T} & \Rightarrow\ \Delta_5\Delta_2\,(\mathtt{Y}) = \mathtt{T}\ .\\
\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = & \mathtt{LVIHPY} & \Rightarrow\ \sigma_2 = \mathtt{V}\ , & \sigma_5 = \mathtt{P} & \Rightarrow\ \Delta_5\Delta_2\,(\mathtt{V}) = \mathtt{P}\ .\\
\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = & \mathtt{QXCBGN} & \Rightarrow\ \sigma_2 = \mathtt{X}\ , & \sigma_5 = \mathtt{G} & \Rightarrow\ \Delta_5\Delta_2\,(\mathtt{X}) = \mathtt{G}\ .\\
\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = & \mathtt{JBPNLT} & \Rightarrow\ \sigma_2 = \mathtt{B}\ , & \sigma_5 = \mathtt{L} & \Rightarrow\ \Delta_5\Delta_2\,(\mathtt{B}) = \mathtt{L}\ .\\
\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = & \mathtt{AZJLIV} & \Rightarrow\ \sigma_2 = \mathtt{Z}\ , & \sigma_5 = \mathtt{I} & \Rightarrow\ \Delta_5\Delta_2\,(\mathtt{Z}) = \mathtt{I}\ .\\
\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = & \mathtt{ZCFRSL} & \Rightarrow\ \sigma_2 = \mathtt{C}\ , & \sigma_5 = \mathtt{S} & \Rightarrow\ \Delta_5\Delta_2\,(\mathtt{C}) = \mathtt{S}\ .\\
\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = & \mathtt{NKTVAG} & \Rightarrow\ \sigma_2 = \mathtt{K}\ , & \sigma_5 = \mathtt{A} & \Rightarrow\ \Delta_5\Delta_2\,(\mathtt{K}) = \mathtt{A}\ .\\
\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = & \mathtt{CFDXVR} & \Rightarrow\ \sigma_2 = \mathtt{F}\ , & \sigma_5 = \mathtt{V} & \Rightarrow\ \Delta_5\Delta_2\,(\mathtt{F}) = \mathtt{V}\ .\\
\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = & \mathtt{IRLGNI} & \Rightarrow\ \sigma_2 = \mathtt{R}\ , & \sigma_5 = \mathtt{N} & \Rightarrow\ \Delta_5\Delta_2\,(\mathtt{R}) = \mathtt{N}\ .\\
\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = & \mathtt{BJXAEZ} & \Rightarrow\ \sigma_2 = \mathtt{J}\ , & \sigma_5 = \mathtt{E} & \Rightarrow\ \Delta_5\Delta_2\,(\mathtt{J}) = \mathtt{E}\ .\\
\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = & \mathtt{HPHORD} & \Rightarrow\ \sigma_2 = \mathtt{P}\ , & \sigma_5 = \mathtt{R} & \Rightarrow\ \Delta_5\Delta_2\,(\mathtt{P}) = \mathtt{R}\ .
\end{array}$$

לפי התוצאות האלו נרשום את התמורה $\Delta_5\Delta_2$ בייצוג טבלה בטבלה הבאה:

x	$\Delta_5\Delta_2(x)$
A	Q
B	L
C	S
D	J
E	Y
F	V

x	$\Delta_5\Delta_2(x)$
G	X
H	O
I	B
J	E
K	A
L	M

x	$\Delta_5\Delta_2(x)$
M	Z
N	W
O	H
P	R
Q	C
R	N

x	$\Delta_5\Delta_2(x)$
S	U
T	D
U	K
V	P
W	F
X	G

x	$\Delta_5\Delta_2(x)$
Y	T
Z	I

לפי הטבלה, אפשר לפרק את התמורה למחזורים שלה ואז נקבל את הפירוק למחזורים הבא:

$$\Delta_5\Delta_2 = \texttt{(HO) (XG) (DJEYT) (MZIBL) (FVPRNW) (AQCSUK)} \ ,$$

כנדרש.
לפי המילה האופיינית הראשונה ברשימה, ממשפט רייבסקי I נקבל:

$$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \texttt{WWODFS} \quad \Rightarrow \quad \sigma_3 = \texttt{O} \ , \sigma_6 = \texttt{S} \quad \Rightarrow \quad \Delta_6\Delta_3\,(\texttt{O}) = \texttt{S} \ .$$

ז"א התמורה $\Delta_6\Delta_3$ על האות W פולטת F. בעזרת השיטה הזו על כל המילים האופיניות ברשימה נקבל את התמורות של כל האותיות:

$$\begin{aligned}
\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 &= \texttt{WWODFS} &&\Rightarrow \sigma_3 = \texttt{O}\ , &&\sigma_6 = \texttt{S} &&\Rightarrow \Delta_6\Delta_3\,(\texttt{O}) = \texttt{S}\ .\\
\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 &= \texttt{DLVQMF} &&\Rightarrow \sigma_3 = \texttt{V}\ , &&\sigma_6 = \texttt{F} &&\Rightarrow \Delta_6\Delta_3\,(\texttt{V}) = \texttt{F}\ .\\
\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 &= \texttt{PEQIYH} &&\Rightarrow \sigma_3 = \texttt{Q}\ , &&\sigma_6 = \texttt{H} &&\Rightarrow \Delta_6\Delta_3\,(\texttt{Q}) = \texttt{H}\ .\\
\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 &= \texttt{OQYFCJ} &&\Rightarrow \sigma_3 = \texttt{Y}\ , &&\sigma_6 = \texttt{J} &&\Rightarrow \Delta_6\Delta_3\,(\texttt{Y}) = \texttt{J}\ .\\
\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 &= \texttt{RUUTKQ} &&\Rightarrow \sigma_3 = \texttt{U}\ , &&\sigma_6 = \texttt{Q} &&\Rightarrow \Delta_6\Delta_3\,(\texttt{U}) = \texttt{Q}\ .\\
\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 &= \texttt{TASEQM} &&\Rightarrow \sigma_3 = \texttt{S}\ , &&\sigma_6 = \texttt{M} &&\Rightarrow \Delta_6\Delta_3\,(\texttt{S}) = \texttt{M}\ .\\
\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 &= \texttt{VBRULE} &&\Rightarrow \sigma_3 = \texttt{R}\ , &&\sigma_6 = \texttt{E} &&\Rightarrow \Delta_6\Delta_3\,(\texttt{R}) = \texttt{E}\ .\\
\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 &= \texttt{XONKHK} &&\Rightarrow \sigma_3 = \texttt{N}\ , &&\sigma_6 = \texttt{K} &&\Rightarrow \Delta_6\Delta_3\,(\texttt{N}) = \texttt{K}\ .\\
\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 &= \texttt{MHGPOA} &&\Rightarrow \sigma_3 = \texttt{G}\ , &&\sigma_6 = \texttt{A} &&\Rightarrow \Delta_6\Delta_3\,(\texttt{G}) = \texttt{A}\ .\\
\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 &= \texttt{SGMYXO} &&\Rightarrow \sigma_3 = \texttt{M}\ , &&\sigma_6 = \texttt{O} &&\Rightarrow \Delta_6\Delta_3\,(\texttt{M}) = \texttt{O}\ .\\
\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 &= \texttt{JMKNZC} &&\Rightarrow \sigma_3 = \texttt{K}\ , &&\sigma_6 = \texttt{C} &&\Rightarrow \Delta_6\Delta_3\,(\texttt{K}) = \texttt{C}\ .\\
\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 &= \texttt{GTACDP} &&\Rightarrow \sigma_3 = \texttt{A}\ , &&\sigma_6 = \texttt{P} &&\Rightarrow \Delta_6\Delta_3\,(\texttt{A}) = \texttt{P}\ .\\
\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 &= \texttt{UNBJWX} &&\Rightarrow \sigma_3 = \texttt{B}\ , &&\sigma_6 = \texttt{X} &&\Rightarrow \Delta_6\Delta_3\,(\texttt{B}) = \texttt{X}\ .\\
\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 &= \texttt{YDWMJB} &&\Rightarrow \sigma_3 = \texttt{W}\ , &&\sigma_6 = \texttt{B} &&\Rightarrow \Delta_6\Delta_3\,(\texttt{W}) = \texttt{B}\ .\\
\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 &= \texttt{EIVZBF} &&\Rightarrow \sigma_3 = \texttt{V}\ , &&\sigma_6 = \texttt{F} &&\Rightarrow \Delta_6\Delta_3\,(\texttt{V}) = \texttt{F}\ .\\
\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 &= \texttt{FSZWUW} &&\Rightarrow \sigma_3 = \texttt{Z}\ , &&\sigma_6 = \texttt{W} &&\Rightarrow \Delta_6\Delta_3\,(\texttt{Z}) = \texttt{W}\ .\\
\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 &= \texttt{KYESTU} &&\Rightarrow \sigma_3 = \texttt{E}\ , &&\sigma_6 = \texttt{U} &&\Rightarrow \Delta_6\Delta_3\,(\texttt{E}) = \texttt{U}\ .\\
\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 &= \texttt{LVIHPY} &&\Rightarrow \sigma_3 = \texttt{I}\ , &&\sigma_6 = \texttt{Y} &&\Rightarrow \Delta_6\Delta_3\,(\texttt{I}) = \texttt{Y}\ .\\
\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 &= \texttt{QXCBGN} &&\Rightarrow \sigma_3 = \texttt{C}\ , &&\sigma_6 = \texttt{N} &&\Rightarrow \Delta_6\Delta_3\,(\texttt{C}) = \texttt{N}\ .\\
\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 &= \texttt{JBPNLT} &&\Rightarrow \sigma_3 = \texttt{P}\ , &&\sigma_6 = \texttt{T} &&\Rightarrow \Delta_6\Delta_3\,(\texttt{P}) = \texttt{T}\ .\\
\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 &= \texttt{AZJLIV} &&\Rightarrow \sigma_3 = \texttt{J}\ , &&\sigma_6 = \texttt{V} &&\Rightarrow \Delta_6\Delta_3\,(\texttt{J}) = \texttt{V}\ .\\
\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 &= \texttt{ZCFRSL} &&\Rightarrow \sigma_3 = \texttt{F}\ , &&\sigma_6 = \texttt{L} &&\Rightarrow \Delta_6\Delta_3\,(\texttt{F}) = \texttt{L}\ .\\
\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 &= \texttt{NKTVAG} &&\Rightarrow \sigma_3 = \texttt{T}\ , &&\sigma_6 = \texttt{G} &&\Rightarrow \Delta_6\Delta_3\,(\texttt{T}) = \texttt{G}\ .\\
\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 &= \texttt{CFDXVR} &&\Rightarrow \sigma_3 = \texttt{D}\ , &&\sigma_6 = \texttt{R} &&\Rightarrow \Delta_6\Delta_3\,(\texttt{D}) = \texttt{R}\ .\\
\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 &= \texttt{IRLGNI} &&\Rightarrow \sigma_3 = \texttt{L}\ , &&\sigma_6 = \texttt{I} &&\Rightarrow \Delta_6\Delta_3\,(\texttt{L}) = \texttt{I}\ .\\
\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 &= \texttt{BJXAEZ} &&\Rightarrow \sigma_3 = \texttt{X}\ , &&\sigma_6 = \texttt{Z} &&\Rightarrow \Delta_6\Delta_3\,(\texttt{X}) = \texttt{Z}\ .\\
\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 &= \texttt{HPHORD} &&\Rightarrow \sigma_3 = \texttt{H}\ , &&\sigma_6 = \texttt{D} &&\Rightarrow \Delta_6\Delta_3\,(\texttt{H}) = \texttt{D}\ .
\end{aligned}$$

לפי התוצאות האלו נרשום את התמורה $\Delta_6\Delta_3$ בייצוג טבלה בטבלה הבאה:

x	$\Delta_6\Delta_3(x)$
A	P
B	X
C	N
D	R
E	U
F	L

x	$\Delta_6\Delta_3(x)$
G	A
H	D
I	Y
J	V
K	C
L	I

x	$\Delta_6\Delta_3(x)$
M	O
N	K
O	S
P	T
Q	H
R	E

x	$\Delta_6\Delta_3(x)$
S	M
T	G
U	Q
V	F
W	B
X	Z

x	$\Delta_6\Delta_3(x)$
Y	J
Z	W

לפי הטבלה, אפשר לפרק את התמורה למחזורים שלה ואז נקבל את הפירוק למחזורים הבא:

$$\Delta_6\Delta_3 = \texttt{(MOS)(CNK)(BXZW)(TGAP)(FLIYJV)(QHDREU)} \ ,$$

כנדרש.

ב) נתונות לנו את התמורות הבאות

$$\Delta_4\Delta_1 = \texttt{(JNVU)(ZRTE)(GCXKSYMPI)(ALHOFWDQB)} \ ,$$
$$\Delta_5\Delta_2 = \texttt{(HO)(XG)(DJEYT)(MZIBL)(FVPRNW)(AQCSUK)} \ ,$$
$$\Delta_6\Delta_3 = \texttt{(MOS)(CNK)(BXZW)(TGAP)(FLIYJV)(QHDREU)} \ .$$

ונתון לנו שהתמורות הן בסדר רייבסקי. ז"א אם $(a_1\ a_2\ \ldots\ a_k)(b_1\ b_2\ \ldots\ b_k) \in \Delta_4\Delta_1$ אז:

$$b_1 = \Delta_1(a_k), \quad b_2 = \Delta_1(a_{k-1}), \quad \ldots \quad , b_k = \Delta_1(a_1) \ .$$

אותו דבר מתקיים עבור $\Delta_5\Delta_2$ ו- $\Delta_6\Delta_3$.

נניח כי הטקסט MWORVZ הוצפן ע"י צופן אניגמה.

$$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \texttt{MWORVZ} = \Delta_1(x_1)\Delta_2(x_2)\Delta_3(x_3)\Delta_4(x_4)\Delta_5(x_5)\Delta_6(x_6) \ .$$

נחשב את הטקסט הגלוי $x_1x_2x_3x_4x_5x_6$ בעזרת משפט רייבסקי II באופן הבא:

אות #1)

$$\Delta_4\Delta_1 = \texttt{(JNVU)(ZRTE)(GCXKSYMPI)(ALHOFWDQB)} \xRightarrow{\text{משפט רייבסקי II}} H = \Delta_1(M)$$

לכן:

$$\sigma_1 = \Delta_1(x_1) = \texttt{M} \quad \Rightarrow \quad x_1 = \Delta_1(\texttt{M}) = \texttt{H} \ .$$

אות #2)

$$\Delta_5\Delta_2 = \texttt{(HO)(XG)(DJEYT)(MZIBL)(FVPRNW)(AQCSUK)} \xRightarrow{\text{משפט רייבסקי II}} A = \Delta_2(W)$$

לכן:

$$\sigma_2 = \Delta_2(x_2) = \texttt{W} \quad \Rightarrow \quad x_2 = \Delta_2(\texttt{W}) = \texttt{A} \ .$$

אות #3)

$$\Delta_6\Delta_3 = \texttt{(MOS) (CNK) (BXZW) (TGAP) (FLIYJV) (QHDREU)} \xrightarrow{\text{משפט רייבסקי II}} N = \Delta_3(O)$$

לכן:

$$\sigma_3 = \Delta_3(x_3) = \texttt{O} \quad \Rightarrow \quad x_3 = \Delta_3(\texttt{O}) = \texttt{N} \; .$$

אות #4)

$$\texttt{R} = \Delta_4\Delta_1(\texttt{Z}) \quad \Rightarrow \quad \Delta_4(\texttt{R}) = \Delta_1(\texttt{Z}) = \texttt{U}$$

$$\sigma_4 = \Delta_4(x_4) = \texttt{R} \quad \Rightarrow \quad x_4 = \Delta_4(\texttt{R}) = \texttt{U} \; .$$

אות #5)

$$\texttt{V} = \Delta_5\Delta_2(\texttt{F}) \quad \Rightarrow \quad \Delta_5(\texttt{V}) = \Delta_2(\texttt{F}) = \texttt{K}$$

$$\sigma_5 = \Delta_5(x_5) = \texttt{V} \quad \Rightarrow \quad x_5 = \Delta_5(\texttt{V}) = \texttt{K} \; .$$

אות #6)

$$\texttt{Z} = \Delta_6\Delta_3(\texttt{X}) \quad \Rightarrow \quad \Delta_6(\texttt{Z}) = \Delta_3(\texttt{X}) = \texttt{A}$$

$$\sigma_6 = \Delta_6(x_6) = \texttt{Z} \quad \Rightarrow \quad x_6 = \Delta_6(\texttt{Z}) = \texttt{A} \; .$$

לכן התשובה הסופית היא:

$$x_1x_2x_3x_4x_5x_6 = \text{HANUKA} \; .$$

שאלה 4

שלב 1) נרשום את התדירויות של האותיות המופיעות בטקסט מוצפן:

A	7	N	0
B	4	O	12
C	26	P	4
D	22	Q	2
E	0	R	5
F	33	S	12
G	0	T	8
H	9	U	10
I	3	V	3
J	2	W	0
K	7	X	15
L	4	Y	15
M	3	Z	16

שלב 2) נרשום את האותיות הנפוצות ביותר:

- F מופיעה 33 פעמים.
- C מופיעה 26 פעמים.
- D מופיעה 22 פעמים.
- Z מופיעה 16 פעמים.
- X, Y מופיעות 15 פעמים.
- O, S מופיעה 12 פעמים.

שלב 3) ננסה למצוא את המפתח $k=(a,b)$ ($a,b\in\mathbb{Z}_{26}$) של הכלל מצפין של הצופן אפיני

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

לכל $x\in\mathbb{Z}_{26}$ על ידי **התאמת אותיות הכי נפוצים.**

- נניח כי

$$\texttt{e}\xrightarrow{e_k}\texttt{F}\ ,\qquad \texttt{t}\xrightarrow{e_k}\texttt{C}\ .$$

- ז"א

$$\begin{aligned}e_k(4)&=5\\ e_k(19)&=2\ .\end{aligned}$$

- נציב $e_k=ax+b$ ונקבל

$$\begin{aligned}4a+b=5\ ,\\ 19a+b=2\ .\end{aligned}$$

כעת נפתור את המערת מעל $\mathbb{Z}_{26}$:

$$\left(\begin{array}{cc|c}4&1&5\\19&1&2\end{array}\right)\xrightarrow{R_2\to R_2-R_1}\left(\begin{array}{cc|c}4&1&5\\15&0&-3\end{array}\right)=\left(\begin{array}{cc|c}4&1&5\\15&0&23\end{array}\right)$$

$$\xrightarrow{R_2\to 15^{-1}R_2=7R_2}\left(\begin{array}{cc|c}4&1&5\\1&0&161\end{array}\right)=\left(\begin{array}{cc|c}4&1&5\\1&0&5\end{array}\right)$$

$$\xrightarrow{R_1\to R_1-4R_2}\left(\begin{array}{cc|c}0&1&-15\\1&0&5\end{array}\right)=\left(\begin{array}{cc|c}0&1&11\\1&0&5\end{array}\right)$$

$a=5, b=11$.

$\gcd(a,26)=1$ אז המפתח $k=(5,11)$ תקין.

- נבנה את הכלל מפענח עם המפתח המתקבל:

$$\begin{aligned} d_k(y) =& a^{-1}(y-b) \bmod 26 \\ =& 5^{-1}(y-11) \\ =& 21(y-11) \bmod 26 \\ =& 21y-231 \bmod 26 \\ =& 21y+3 \ . \end{aligned}$$

שלב 4) ננסה לפענח את הטקטסט מצפון עם הכלל מפענח

y $\in C$	B	D	H	S	C	Z	T	F	Z	X	O	Z	T	Z	C	F	A	A	D	Y
$y \in \mathbb{Z}_{26}$	1	3	7	18	2	25	19	5	25	23	14	25	19	25	2	5	0	0	3	24
$x = d_k(y) \in \mathbb{Z}_{26}$	24	14	20	17	19	8	12	4	8	18	11	8	12	8	19	4	3	3	14	13
x $\in P$	y	o	u	r	t	i	m	e	i	s	l	i	m	i	t	e	d	d	o	n

y $\in C$	C	R	L	X	C	F	Z	C	O	Z	M	Z	Y	P	X	D	T	F	D	Y
$y \in \mathbb{Z}_{26}$	2	17	11	23	2	5	25	2	14	25	12	25	24	15	23	3	19	5	3	24
$x = d_k(y) \in \mathbb{Z}_{26}$	19	22	0	18	19	4	8	19	11	8	21	8	13	6	18	14	12	4	14	13
x $\in P$	t	w	a	s	t	e	i	t	l	i	v	i	n	g	s	o	m	e	o	n

y $\in C$	F	F	O	X	F	X	O	Z	K	F	A	D	Y	C	O	Z	M	F	C	U
$y \in \mathbb{Z}_{26}$	5	5	14	23	5	23	14	25	10	5	0	3	24	2	14	25	12	5	2	20
$x = d_k(y) \in \mathbb{Z}_{26}$	4	4	11	18	4	18	11	8	5	4	3	14	13	19	11	8	21	4	19	7
x $\in P$	e	e	l	s	e	s	l	i	f	e	d	o	n	t	l	i	v	e	t	h

y $\in C$	F	S	F	X	H	O	C	X	D	K	X	D	T	F	D	Y	F	F	O	X
$y \in \mathbb{Z}_{26}$	5	18	5	23	7	14	2	23	3	10	23	3	19	5	3	24	5	5	14	23
$x = d_k(y) \in \mathbb{Z}_{26}$	4	17	4	18	20	11	19	18	14	5	18	14	12	4	14	13	4	4	11	18
x $\in P$	e	r	e	s	u	l	t	s	o	f	s	o	m	e	o	n	e	e	l	s

y $\in C$	F	X	C	U	Z	Y	J	Z	Y	P	A	D	Y	C	R	D	S	S	B	L
$y \in \mathbb{Z}_{26}$	5	23	2	20	25	24	9	25	24	15	0	3	24	2	17	3	18	18	1	11
$x = d_k(y) \in \mathbb{Z}_{26}$	4	18	19	7	8	13	10	8	13	6	3	14	13	19	22	14	17	17	24	0
x $\in P$	e	s	t	h	i	n	k	i	n	g	d	o	n	t	w	o	r	r	y	a

y $\in C$	Q	D	H	C	C	U	F	K	H	C	H	S	F	S	F	T	F	T	Q	F
$y \in \mathbb{Z}_{26}$	16	3	7	2	2	20	5	10	7	2	7	18	5	18	5	19	5	19	16	5
$x = d_k(y) \in \mathbb{Z}_{26}$	1	14	20	19	19	7	4	5	20	19	20	17	4	17	4	12	4	12	1	4
x $\in P$	b	o	u	t	t	h	e	f	u	t	u	r	e	r	e	m	e	m	b	e

y $\in C$	S	V	D	T	I	O	F	T	F	Y	C	X	K	D	S	P	F	C	C	U
$y \in \mathbb{Z}_{26}$	18	21	3	19	8	14	5	19	5	24	2	23	10	3	18	15	5	2	2	20
$x = d_k(y) \in \mathbb{Z}_{26}$	17	2	14	12	15	11	4	12	4	13	19	18	5	14	17	6	4	19	19	7
x $\in P$	r	c	o	m	p	l	e	m	e	n	t	s	f	o	r	g	e	t	t	h

y $\in C$	F	Z	Y	X	H	O	C	X	A	D	Y	C	R	D	S	S	B	R	U	L
$y \in \mathbb{Z}_{26}$	5	25	24	23	7	14	2	23	0	3	24	2	17	3	18	18	1	17	20	11
$x = d_k(y) \in \mathbb{Z}_{26}$	4	8	13	18	20	11	19	18	3	14	13	19	22	14	17	17	24	22	7	0
x $\in P$	e	i	n	s	u	l	t	s	d	o	n	t	w	o	r	r	y	w	h	a

y $\in C$	C	D	C	U	F	S	I	F	D	I	O	F	C	U	Z	Y	J	Z	K	B
$y \in \mathbb{Z}_{26}$	2	3	2	20	5	18	8	5	3	8	14	5	2	20	25	24	9	25	10	1
$x = d_k(y) \in \mathbb{Z}_{26}$	19	14	19	7	4	17	15	4	14	15	11	4	19	7	8	13	10	8	5	24
x $\in P$	t	o	t	h	e	r	p	e	o	p	l	e	t	h	i	n	k	i	f	y

y $\in C$	D	H	X	H	V	V	F	F	A	Z	Y	C	U	Z	X	C	F	O	O	T
$y \in \mathbb{Z}_{26}$	3	7	23	7	21	21	5	5	0	25	24	2	20	25	23	2	5	14	14	19
$x = d_k(y) \in \mathbb{Z}_{26}$	14	20	18	20	2	2	4	4	3	8	13	19	7	8	18	19	4	11	11	12
x $\in P$	o	u	s	u	c	c	e	e	d	i	n	t	h	i	s	t	e	l	l	m

y $\in C$	F	U	D	R	A	D	Y	C	K	D	S	P	F	C	C	D	U	L	M	F
$y \in \mathbb{Z}_{26}$	5	20	3	17	0	3	24	2	10	3	18	15	5	2	2	3	20	11	12	5
$x = d_k(y) \in \mathbb{Z}_{26}$	4	7	14	22	3	14	13	19	5	14	17	6	4	19	19	14	7	0	21	4
x $\in P$	e	h	o	w	d	o	n	t	f	o	r	g	e	t	t	o	h	a	v	e

y $\in C$	K	H	Y
$y \in \mathbb{Z}_{26}$	10	7	24
$x = d_k(y) \in \mathbb{Z}_{26}$	5	20	13
x $\in P$	f	u	n

שאלה 5

נניח כי $\pi : \Sigma \to \Sigma$ מחזור באורך k. ז"א הפירוק למחזורים של π הוא:

$$\pi = \left(a_1 \ a_2 \ a_{k-1} \ a_k\right) \ ,$$

או, כפונקציה מעל Σ:

$$\pi\left(a_1\right) = a_2, \quad \pi\left(a_2\right) = a_3, \quad \ldots \quad \pi\left(a_{k-1}\right) = a_k, \quad \pi\left(a_k\right) = a_1 \ .$$

אפשר לרשום את זה בביטוי יחיד:

$$\pi\left(a_i\right) = a_{(i \bmod k)+1} \ .$$

עבור π^2:

$$\pi^2\left(a_1\right) = a_3, \quad \pi^2\left(a_2\right) = a_4, \quad \ldots \quad \pi^2\left(a_{k-2}\right) = a_k \ , \quad \pi^2\left(a_{k-1}\right) = a_1 \ , \quad \pi^2\left(a_k\right) = a_2 \ .$$

ובאותה מידה אפשר לרשום π^2 בביטוי יחיד:

$$\pi^2\left(a_i\right) = a_{((i+1) \bmod k)+1} \ .$$

באופן כללי לכל $j \geq 0$ טבעי:

$$\pi^j\left(a_i\right) = a_{((i+j-1) \bmod k)+1} \ .$$

מכאן נציב $j = k$:

$$\pi^k\left(a_i\right) = a_{((i+k-1) \bmod k)+1} = a_{((i-1) \bmod k)+1} = \begin{cases} a_i & : i < k \\ a_k & : i = k \end{cases} \ .$$

ז"א לכל $1 \leq i \leq k$:

$$\pi^k(a_i) = a_i \quad \Rightarrow \quad \pi^k = \mathrm{id}$$

כנדרש.

שאלה 6 תהי Σ אלפבית עבורו $n = |\Sigma|$, ויהי S_n האוסף של כל התמורות מעל Σ.

הטענה: אם $\alpha : \Sigma \to \Sigma$ תמורה המקיימת $\alpha\beta = \beta\alpha$ לכל $\beta \in S_n$ אזי $\beta = \mathrm{id}$.

הוכחה:

נוכיח את הטענה דרך השלילה.

נניח בשלילה שקיימת תמורה $\alpha \neq \mathrm{id}$ כך ש- $\alpha\beta = \beta\alpha$ לכל $\beta \in S_n$.

מכיוון ש- $\alpha \neq \mathrm{id}$ אז קיים $x \in \Sigma$ עבורו $\alpha(x) = y \neq x$.

הטענה מתקיימת לכל $\beta \in S_n$, אז היא מתקיימת עבור התמורה הספציפית γ עבורה:

$$\gamma(y) = y \ , \quad \gamma(x) = z \neq x \ .$$

כלומר y נקודת שבת של γ ו- x נקודת זזה של γ.

מכיוון ש- $\alpha\gamma = \gamma\alpha$, אז עבור הנקודה x:

$$\alpha\gamma(x) = \gamma\alpha(x)$$

נציב $\alpha(x) = y$ ו- $\gamma(x) = z$:

$$\alpha(z) = \gamma(y)$$

נציב שוב $\gamma(y) = y$ ונקבל:

$$\alpha(z) = y \ .$$

זאת אומרת $\alpha(x) = y$ וגם $\alpha(z) = y$ וגם $z \neq x$. זאת אומרת α לא חד-חד ערכית, בסתירה לכך שתמורה היא פונקציה חד-חד-ערכית.

שאלה 7

א) המפתח הציבורי הוא (b, n). הפרמטר b כבר נתון בשאלה אז נשאר רק לחשב את n:

$$n = pq = 73 \times 31 = 2263 \ .$$

לכן המפתח הציבורי הוא

$$(b, n) = (107, 2263) \ .$$

כעת נחשב את המפתח הסודי (a, p, q). הראשוניים p, q נתונים בשאלה אז נשאר רק לחשב את a לפי הנוסחה $a = b^{-1} \pmod{\phi(n)}$, כאשר $\phi(n)$ הוא הפונקצית אוילר:

$$\phi(n) = \phi(pq) = (p-1)(q-1) = 72 \times 30 = 2160 \ .$$

לפיכך $a = 107^{-1} \pmod{2160}$. נחשב את $107^{-1} \pmod{2160}$ בעזרת האלגוריתם לאיבר ההופכי (ראו משפט **??**):

Algorithm 1 האלגוריתם לאיבר ההופכי

Input: Integers A, B .
$r_0 \leftarrow A$
$r_1 \leftarrow B$
$t_0 \leftarrow 0$
$t_1 \leftarrow 1$
$n \leftarrow 1$
while $r_n \neq 0$ **do**
  $q_n \leftarrow \left\lfloor \dfrac{r_{n-1}}{r_n} \right\rfloor$
  $r_{n+1} \leftarrow r_{n-1} - q_n r_n$
  $t_{n+1} \leftarrow t_{n-1} - q_n t_n$
  $n \leftarrow n+1$
end while
$n \leftarrow n-1$
if $r_n \neq 1$ **then**
  B has no inverse modulo A
else
  return: t_n $\qquad \triangleright\ t_n = B^{-1} \pmod{A}$
end if

נשים $A = 23940, B = 47$. נאתחל את המשתנים של האלגוריתם:

$$r_0 = A = 2160, \qquad r_1 = B = 107\ ,$$
$$t_0 = 0\ , \qquad t_1 = 1\ .$$

אזי האיטרציות של האלגוריתם הם כמפורט למטה:

שלב $n = 1$:	$t_2 = 0 - 20 \cdot 1 = -20$	$r_2 = 2160 - 20 \cdot 107 = 20$	$q_1 = 20$
שלב $n = 2$:	$t_3 = 1 - 5 \cdot (-20) = 101$	$r_3 = 107 - 5 \cdot 20 = 7$	$q_2 = 5$
שלב $n = 3$:	$t_4 = -20 - 2 \cdot (101) = -222$	$r_4 = 20 - 2 \cdot 7 = 6$	$q_3 = 2$
שלב $n = 4$:	$t_5 = 101 - 1 \cdot (-222) = 323$	$r_5 = 7 - 1 \cdot 6 = 1$	$q_4 = 1$
שלב $n = 5$:	$t_6 = -222 - 6 \cdot (323) = -2000$	$r_6 = 6 - 6 \cdot 1 = 0$	$q_5 = 6$

לפיכך $107^{-1} \equiv 323 \pmod{2160}$. לכן התשובה הסופית בשביל a היא:

$$a = 323\ .$$

ב) ראשית נרשום את הערכים של האותיות של הטקסט גלוי (אנחנו מתעלמים מספרות הפרדה בין אותיות):

$$y = \texttt{DED} \to 343 \ .$$

בסעיף הקודם קיבלנו את הפרמטרים $b = 107$, $p = 73$, $q = 31$ וחישבנו $n = 2263$, $\phi(n) = 2160$ והוכחנו כי $a = b^{-1} \bmod n = 323$. כעת נקח את הטקסט מוצפן $y = 343$ והמפתח הסודי $(a, p, q) = (323, 73, 31)$ ונחשב את הטקסט הגלוי המקורי שאליס שלחה, על פי הכלל מפענח $x = y^a \bmod n$. בפרט אנחנו נחשב את x מהכלל מפענח הזה בעזרת האלגוריתם הבא:

$$x_1 = \left[(y \bmod p)^{a \bmod (p-1)}\right] \bmod p \ ,$$
$$x_2 = \left[(y \bmod q)^{a \bmod (q-1)}\right] \bmod q \ .$$

ואז פוטרים את המערכת הבאה בעזרת המשפט השאריות הסיני:

$$x = x_1 \bmod p \ ,$$
$$x = x_2 \bmod q \ .$$

$$y \bmod p = 343 \bmod 73 = 51 \ , \qquad a \bmod (p-1) = 323 \bmod 70 = 43 \ .$$

לכן

$$x_1 = (y \bmod p)^{a \bmod (p-1)} \bmod p = 51^{43} \bmod 73 = 10$$

$$y \bmod q = 343 \bmod 31 = 2 \ , \qquad a \bmod (q-1) = 323 \bmod 30 = 23 \ .$$

לכן

$$x_2 = (y \bmod q)^{a \bmod (q-1)} \bmod q = 2^{23} \bmod 31 = 8$$

התשובה הסופית ניתנת ע"י הפתרון למערכת הבאה:

$$x = x_1 \bmod p = 10 \bmod 73$$
$$x = x_2 \bmod q = 8 \bmod 31$$

שניתן לפתור ע"י המשפט השאריות הסיני. נסמן $a_1 = 10$, $m_1 = 73$, $a_2 = 8$, $m_2 = 31$.

$$M = m_1 m_2 = (73)(31) = 2263 \ , \qquad M_1 = \frac{M}{m_1} = 31 \ , \qquad M_2 = \frac{M}{m_2} = 73 \ .$$

כעת נחשב $y_1 = M_1^{-1} \bmod m_1 = 73^{-1} \bmod 31$ ו- $y_2 = M_2^{-1} \bmod m_2 = 31^{-1} \bmod 73$.

נחשב את הפירוק אוקלידס של 73 ו- 31 בעזרתת האלגוריתם המוכלל של אוקלידס, ומהפריוק אוקלידס נמצא את האיברים ההופכיים המודולריים באופן הבא. נסמן: $A = 73, B = 31$.

$$r_0 = A = 73 \ , \qquad r_1 = B = 31 \ ,$$
$$s_0 = 1 \ , \qquad s_1 = 0 \ ,$$
$$t_0 = 0 \ , \qquad t_1 = 1 \ .$$

שלב $k=1$:	$t_2=0-2\cdot 1=-2$	$s_2=1-2\cdot 0=1$	$r_2=73-2\cdot 31=11$	$q_1=\left\lfloor\frac{r_0}{r_1}\right\rfloor=2$
שלב $k=2$:	$t_3=1-2\cdot(-2)=5$	$s_3=0-2\cdot 1=-2$	$r_3=31-2\cdot 11=9$	$q_2=\left\lfloor\frac{r_1}{r_2}\right\rfloor=2$
שלב $k=3$:	$t_4=-2-1\cdot(5)=-7$	$s_4=1-1\cdot(-2)=3$	$r_4=11-1\cdot 9=2$	$q_3=\left\lfloor\frac{r_2}{r_3}\right\rfloor=1$
שלב $k=4$:	$t_5=5-4\cdot(-7)=33$	$s_5=-2-4\cdot(3)=-14$	$r_5=9-4\cdot 2=1$	$q_4=\left\lfloor\frac{r_3}{r_4}\right\rfloor=4$
שלב $k=5$:	$t_6=-7-2\cdot(33)=-73$	$s_6=3-2\cdot(-14)=31$	$r_6=9-4\cdot 2=1$	$q_5=\left\lfloor\frac{r_4}{r_5}\right\rfloor=2$

$$\gcd(A,B)=r_5=1\ ,\qquad s=s_5=-14\ ,\qquad t=t_5=33\ .$$

$$sA+tB=-14(73)+33(31)=1\ .$$

לכן

$$\begin{aligned}&73^{-1}\equiv -14 \pmod{31}\equiv 17 \pmod{31}\\&31^{-1}\equiv 33 \pmod{73}\ .\end{aligned}$$

לכן

$$\begin{aligned}y_1&=M_1^{-1} \bmod m_1 &&=31^{-1} \bmod 73 &&\equiv 33 \bmod 73\\ y_2&=M_2^{-1} \bmod m_2 &&=73^{-1} \bmod 31 &&\equiv 17 \bmod 73\ .\end{aligned}$$

$$\begin{aligned}y=&a_1M_1y_1+a_2M_2y_2\\ =&10(31)(33)+8(73)(17) \bmod 2263\\ =&4223186 \bmod 24257\\ =&2054\ .\end{aligned}$$

לכן הטקסט הגולי הוא

$$x=2054\to \texttt{cafe}\ .$$

שאלה 8 נפתור מערכת זו באמצעות משפט השאריות הסיני. נסמן

$$\begin{aligned}x\equiv&a_1 \bmod m_1\\ x\equiv&a_2 \bmod m_2\\ x\equiv&a_3 \bmod m_3\ .\end{aligned}$$

כאשר

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

נחשב

$$M = m_1m_2m_3 = 17550 \ , \quad M_1 = \frac{M}{m_1} = 702 \ , \quad M_2 = \frac{M}{m_2} = 675 \ , \quad M_3 = \frac{M}{m_3} = 650 \ .$$

באמצעות הקוד פייתון שנמצא באתר המודל נחשב את ההופכיים

$$\begin{aligned} y_1 =& M_1^{-1} \bmod m_1 = 702^{-1} \bmod 25 = 13 \ , \\ y_2 =& M_2^{-1} \bmod m_2 = 675^{-1} \bmod 26 = 25 \ , \\ y_3 =& M_3^{-1} \bmod m_3 = 650^{-1} \bmod 27 = 14 \ . \end{aligned}$$

הפתרון (מודולר M) הוא

$$\begin{aligned} x =& a_1M_1y_1 + a_2M_2y_2 + a_3M_3y_3 \bmod M \\ =& (12)(702)(13) + (9)(675)(25) + (23)(650)(14) \bmod 17550 \\ =& 470687 \bmod 17550 \\ =& 14387 \ . \end{aligned}$$

שאלה 9 ראשית נחשב את ההופכי המודולרי של 13 ביחס ל- 99 בעזרת האלגוריתם המכולל של אוקלידס באופן הבא.

נסמן: $a = 99, b = 13$.

אתחול:

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

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:

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

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

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

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

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

כעת נפתור את המערכת

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

בעזרת המשפט השאריות הסיני.

נסמן

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

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

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

שאלה 10

א) המפתח הציבורי הוא (b,n).
$b = 31$ נתון לנו.

$$n = pq = (37)(41) = 1517\ .$$

לכן המתח הציבורי הוא: $(b,n) = (31, 1517)$.

המפתח הסודי הוא: (a,p,q).
$p = 37$ ו- $q = 41$ נתון בשאלה. הפרמטר a נתון לפי הנוסחה:

$$a \equiv b^{-1} \pmod{\phi(n)}\ ,$$

כאשר $\phi(n)$ היא הפונקצית אוילר. מכיוון ש- $n = pq$ ו- p,q הם מספרים ראשוניים, אז:

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

לכן:

$$a \equiv b^{-1} \pmod{\phi(n)} \equiv 31^{-1} \pmod{1440}\ .$$

אנחנו נחשב את a באמצעות האלגוריתם המוכלל של אוקלידס באופן הבא. נסמן $A = 1440, B = 31$.

$$r_0 = A = 1440\ , \qquad r_1 = B = 31\ ,$$
$$s_0 = 1\ , \qquad s_1 = 0\ ,$$
$$t_0 = 0\ , \qquad t_1 = 1\ .$$

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 $i = 5$:	$t_6 = -418 - 2 \cdot (511) = -1440$	$s_6 = 9 - 2 \cdot (-11) = 31$	$r_6 = 2 - 2 \cdot 1 = 0$	$q_5 = 2$

לכן:

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

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

מכאן

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

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

ב) כעת נחשב את הטקסט המוצפן של הטקסט הגלוי $x=\texttt{cbbi}$. הערכים של האותיות של המילה הן (בלי להתחשב בספרות הפרדה):

$$x=\texttt{cbbi}\to 1228\ .$$

הטקסט מוצפן ניתן ע"י הכלל מצפין:

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

נשתמש בשיטת ריבועים:
הייצוג בינארי של B הוא:

$$b=b_4b_3b_2b_1b_0=11111\ .$$

Algorithm 2 האלגוריתם לשיטת הריבועים

```
Input: Integers x, b_0, ..., b_k, n .
i ← 1
z_0 ← x
while i ≤ k do
    z_i ← z_{i-1}^2 mod n
end while
i ← 1
y ← x
while i ≤ k do
    if b_i = 1 then
        y ← z_i y mod n
    end if
end while
return: y                                   ▷ y = x^b mod n
```

שלב 1) בדוגמה שלנו החזקה היא

$$b=31=16+8+4+2+1=1\left(2^4\right)+1\left(2^3\right)+1\left(2^2\right)+1\left(2^1\right)+1\left(2^0\right)\ .$$

אזי הייצוג בינארי של b הוא

$$b=b_4b_3b_2b_1b_0=11111\ .$$

שלב 2) נאתחל: $z_0 = x = 1228$.

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

שלב 3) נאתחל: $y = x = 1228$.

$b_1 = 1$	$y = z_1 y \bmod n = (86)(1228) \bmod 1517 = 935$
$b_2 = 1$	$y = z_2 y \bmod n = (1328)(935) \bmod 1517 = 774$
$b_3 = 1$	$y = z_3 y \bmod n = (830)(774) \bmod 1517 = 729$
$b_4 = 1$	$y = z_4 y \bmod n = (182)(729) \bmod 1517 = 699$

לכן השתובה סופיל להטקסט מוצפן הוא:

$$y = 699 \to \mathtt{GJJ}.$$

ג) כעת בהינתן הטקסט מוצפן $y = 699$ נחשב את הטקסט הגלוי עם הכלל מפענח

$$x = y^a \bmod n\ .$$

בעזרת בהאלגוריתם הבא:

$$\begin{aligned} x_1 &= \left[(y \bmod p)^{a \bmod (p-1)} \right] \bmod p\ , \\ x_2 &= \left[(y \bmod q)^{a \bmod (q-1)} \right] \bmod q\ . \end{aligned}$$

ואז פוטרים את המערכת הבאה בעזרת המשפט השאריות הסיני:

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

ראשית נחשב את x_1:

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

לכן

$$x_1 = (y \bmod p)^{a \bmod (p-1)} \bmod p = 33^7 \bmod 37 = 7\ .$$

עכשיו נחשב את x_2:

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

לכן

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

לבסוף השתובה סופית מתקבלת מהפתרון של המערכת הבאה:

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

אנחנו נפתור את המערכת הזו בעזרת המשפט השאריות הסיני.
נסמן: $a_1 = 7$, $m_1 = 37$, $a_2 = 39$, $m_2 = 41$.

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

בשלב הבא אנחנו נחשב $y_1 = M_1^{-1} \bmod m_1 = 41^{-1} \bmod 37$.
נתון לנו את הרמז: $(-9)(41) + (10)(37) = 1$. לפיכך $41^{-1} \equiv -9 \pmod{37} = 28$. לכן:

$$y_1 = M_1^{-1} \bmod m_1 = 41^{-1} \bmod 37 = 28 \ .$$

באופן דומה אנחנו נחשב $y_2 = M_2^{-1} \bmod m_2 = 37^{-1} \bmod 41$.
לפי הרמז $(-9)(41) + (10)(37) = 1 \Leftarrow 37^{-1} \equiv 10 \pmod{41}$. לכן:

$$y_2 = M_2^{-1} \bmod m_2 = 37^{-1} \bmod 41 = 10 \ .$$

לכן

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

כנדרש.

שאלה 11

יש בדיוק 15 תווים בטקסט מוצפן ובטקסט גלוי. לכן הסדר הכי קטן של המטריצה של המפתח הוא 3. נבדוק אם קיים מפתח $k \in \mathbb{Z}_{26}^{3\times3}$ אשר באמצעותו הטקסט מוצפן מתקבל מהטקסט גלוי.

x $\in P$	t	h	e	f	u	t	u	r	e	i	s	g	o	o	d
$x \in \mathbb{Z}_{26}$	19	7	4	5	20	19	20	17	4	8	18	6	14	14	3
y $\in C$	F	O	P	B	V	F	W	D	F	C	C	G	M	A	T
$y \in \mathbb{Z}_{26}$	5	14	15	1	21	5	22	3	5	2	2	6	12	0	19

אם המפתח k הוא מטריצה של סדר 3×3 אז הכלל מצפין יהיה

$$e_k(x_1, x_2, x_3) = (x_1 \ x_2 \ x_3) k \bmod 26 \ .$$

לכן ה-3 אותיות הראשונות של הטקסט מוצפן $(y_1 \ y_2 \ y_3)$ מתקבלות מההצפנה של ה-3 אותיות הראשונות של טקסט גלוי, על פי הכלל מצפין של צופן היל כך:

$$(y_1 \ y_2 \ y_3) = (x_1 \ x_2 \ x_3) k \bmod 26 \ .$$

באותה מידה הקבוצה השנייה של 3 אותיות של טקסט מוצפן $(y_4\ y_5\ y_6)$ מתקבלת מההצפנה של הקבוצה השנייה של 3 אותיות של הטקסט הגלוי:

$$(y_3\ y_4\ y_5) = (x_3\ x_4\ x_5)k \bmod 26 \ ,$$

והקבוצה השלישית של 3 אותיות של הטקסט מוצפן $(y_7\ y_8\ y_9)$ מתקבלת מההצפנה של הקבוצה השלישית של 3 אותיות של הטקסט הגלוי:

$$(y_7\ y_8\ y_9) = (x_7\ x_8\ x_9)k \bmod 26 \ .$$

אפשר לרשום את השלוש משוואות האלו כמשוואה מטריציאלית:

$$\begin{pmatrix} y_1 & y_2 & y_3 \\ y_4 & y_5 & y_6 \\ y_7 & y_8 & y_9 \end{pmatrix} = \begin{pmatrix} x_1 & x_2 & x_3 \\ x_4 & x_5 & x_6 \\ x_7 & x_8 & x_9 \end{pmatrix} k \ .$$

כדי לבודד את k נכפיל בהמטריצה ההופכית של $\begin{pmatrix} x_1 & x_2 & x_3 \\ x_4 & x_5 & x_6 \\ x_7 & x_8 & x_9 \end{pmatrix}$ מצד שמאל ונקבל את הביטוי

$$\begin{pmatrix} x_1 & x_2 & x_3 \\ x_4 & x_5 & x_6 \\ x_7 & x_8 & x_9 \end{pmatrix}^{-1} \begin{pmatrix} y_1 & y_2 & y_3 \\ y_4 & y_5 & y_6 \\ y_7 & y_8 & y_9 \end{pmatrix} = k \ .$$

נציב $x_1 = 19, x_2 = 7, x_3 = 4, x_4 = 5, x_5 = 20, x_6 = 19, x_7 = 20, x_8 = 17, x_9 = 4$
ונציב $y_1 = 5, y_2 = 14, y_3 = 15, y_4 = 1, y_5 = 21, y_6 = 5, y_7 = 22, y_8 = 3, y_9 = 5$:

$$k = \begin{pmatrix} 19 & 7 & 4 \\ 5 & 20 & 19 \\ 20 & 17 & 4 \end{pmatrix}^{-1} \begin{pmatrix} 5 & 14 & 15 \\ 1 & 21 & 5 \\ 22 & 3 & 5 \end{pmatrix} \ .$$

נחשב את המטריצה ההופכית של $X = \begin{pmatrix} 19 & 7 & 4 \\ 5 & 20 & 19 \\ 20 & 17 & 4 \end{pmatrix}$ בעזרת נוסחת קריימר:

$$X^{-1} = |X|^{-1} C^t$$

כאשר C המטריצה של קופקטורים. תחילה נמצא את הדטרמיננטה:

$$|X| = -3357 \bmod 26 = 23 \ , \qquad |X|^{-1} \bmod 26 = 23^{-1} \bmod 26 = 17 \ .$$

$$\begin{pmatrix} 19 & 7 & 4 \\ 5 & 20 & 19 \\ 20 & 17 & 4 \end{pmatrix} \quad \Rightarrow \quad C_{11} = (-1)^{1+1} \begin{vmatrix} 20 & 19 \\ 17 & 4 \end{vmatrix} \bmod 26 = -243 \bmod 26 = 17 \ .$$

$$\begin{pmatrix} 19 & 7 & 4 \\ 5 & 20 & 19 \\ 20 & 17 & 4 \end{pmatrix} \quad \Rightarrow \quad C_{12} = (-1)^{1+2} \begin{vmatrix} 5 & 19 \\ 20 & 4 \end{vmatrix} \bmod 26 = 360 \bmod 26 = 22 \ .$$

$$\begin{pmatrix} 19 & 7 & 4 \\ 5 & 20 & 19 \\ 20 & 17 & 4 \end{pmatrix} \qquad \Rightarrow \qquad C_{13} = (-1)^{1+3} \begin{vmatrix} 5 & 20 \\ 20 & 17 \end{vmatrix} \bmod 26 = -315 \bmod 26 = 23 \ .$$

$$\begin{pmatrix} 19 & 7 & 4 \\ 5 & 20 & 19 \\ 20 & 17 & 4 \end{pmatrix} \qquad \Rightarrow \qquad C_{21} = (-1)^{2+1} \begin{vmatrix} 7 & 4 \\ 17 & 4 \end{vmatrix} \bmod 26 = 40 \bmod 26 = 14 \ .$$

$$\begin{pmatrix} 19 & 7 & 4 \\ 5 & 20 & 19 \\ 20 & 17 & 4 \end{pmatrix} \qquad \Rightarrow \qquad C_{22} = (-1)^{2+2} \begin{vmatrix} 19 & 4 \\ 20 & 4 \end{vmatrix} \bmod 26 = -4 \bmod 26 = 22 \ .$$

$$\begin{pmatrix} 19 & 7 & 4 \\ 5 & 20 & 19 \\ 20 & 17 & 4 \end{pmatrix} \qquad \Rightarrow \qquad C_{23} = (-1)^{2+3} \begin{vmatrix} 19 & 7 \\ 20 & 17 \end{vmatrix} \quad \bmod 26 = -183 \bmod 26 = 25 \ .$$

$$\begin{pmatrix} 19 & 7 & 4 \\ 5 & 20 & 19 \\ 20 & 17 & 4 \end{pmatrix} \qquad \Rightarrow \qquad C_{31} = (-1)^{3+1} \begin{vmatrix} 7 & 4 \\ 20 & 19 \end{vmatrix} \bmod 26 = 53 \bmod 26 = 1 \ .$$

$$\begin{pmatrix} 19 & 7 & 4 \\ 5 & 20 & 19 \\ 20 & 17 & 4 \end{pmatrix} \qquad \Rightarrow \qquad C_{32} = (-1)^{3+2} \begin{vmatrix} 19 & 4 \\ 5 & 19 \end{vmatrix} \bmod 26 = -341 \bmod 26 = 23 \ .$$

$$\begin{pmatrix} 19 & 7 & 4 \\ 5 & 20 & 19 \\ 20 & 17 & 4 \end{pmatrix} \qquad \Rightarrow \qquad C_{33} = (-1)^{3+3} \begin{vmatrix} 19 & 7 \\ 5 & 20 \end{vmatrix} \bmod 26 = 345 \bmod 26 = 7 \ .$$

$$C = \begin{pmatrix} C_{11} & C_{12} & C_{13} \\ C_{21} & C_{22} & C_{23} \\ C_{31} & C_{32} & C_{33} \end{pmatrix} = \begin{pmatrix} 17 & 22 & 23 \\ 14 & 22 & 25 \\ 1 & 23 & 7 \end{pmatrix} \ .$$

$$\mathrm{adj}(X) = C^t = \begin{pmatrix} 17 & 14 & 1 \\ 22 & 22 & 23 \\ 23 & 25 & 7 \end{pmatrix} \ .$$

$$X^{-1} = |X|^{-1}\mathrm{adj}(X) = 17 \begin{pmatrix} 17 & 14 & 1 \\ 22 & 22 & 23 \\ 23 & 25 & 7 \end{pmatrix} \bmod 26 = \begin{pmatrix} 289 & 238 & 17 \\ 374 & 374 & 391 \\ 391 & 425 & 119 \end{pmatrix} \bmod 26 = \begin{pmatrix} 3 & 4 & 17 \\ 10 & 10 & 1 \\ 1 & 9 & 15 \end{pmatrix}$$

$$
\begin{aligned}
k =& X^{-1}Y \bmod 26 \\
=& \begin{pmatrix} 3 & 4 & 17 \\ 10 & 10 & 1 \\ 1 & 9 & 15 \end{pmatrix} \begin{pmatrix} 5 & 14 & 15 \\ 1 & 21 & 5 \\ 22 & 3 & 5 \end{pmatrix} \bmod 26 \\
=& \begin{pmatrix} 393 & 177 & 150 \\ 82 & 353 & 205 \\ 344 & 248 & 135 \end{pmatrix} \bmod 26 \\
=& \begin{pmatrix} 3 & 21 & 20 \\ 4 & 15 & 23 \\ 6 & 14 & 5 \end{pmatrix} \ .
\end{aligned}
$$