

## 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 שאתם מגישים פתרונות לבד אז בשם הקובץ שיוגש למערכת ההגשה יהיה מספר ת"ז ושם של המגיש ושם של העבודה. לדוגמה: עבודה-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: עבודה-ירמיהו-תז-123456789-גל-113114115.pdf

(4) בקובץ המוגש יש להוסיף את התיעוד הבא בעמוד הראשון (בעברית או באנגלית, לבחירתכם). יש לשנות את השם 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

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

מצאו את הטקסט הגלוי.

### שאלה 3 (9 נקודות)

הטבלה הבאה מראה מילים אופייניות מהודעות מוצפנות מאותו יום.

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

(א) הוכיחו כי התמורות המתאימות של צופן אניגמה הן:

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

(ב) נניח כי התמורות  $\Delta_6 \Delta_3, \Delta_5 \Delta_2, \Delta_4 \Delta_1$  הן בסדר ריבסקי. 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 XHVFFFA ZY CUZX CFOO TF UDR ADYC KDSPFC CD ULMF KHY

היעזרו בקריפטו-אנליזה כדי למצוא את הטקסט הגלוי.

#### שאלה 5 (9 נקודות)

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

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

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

#### שאלה 6 (9 נקודות)

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

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

אז  $\alpha = \text{id}$ .

#### שאלה 7 (9 נקודות)

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

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

ההצפנה של ההודעה היא

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

(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:

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

### שאלה 9 (9 נקודות)

פתרו את המערכת משוואות הבאה:

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

רמז: השתמשו באלגוריתם המוכלל של אוקליד ואחר כך המשפט השאריות 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:

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

### שאלה 11 (9 נקודות)

נתון הטקסט גלוי

thefutureisgood

והטקסט מוצפן שלו

FOPBVFWDFFCCGMAT

הטקסט הוצפן עם צופן היל. מצאו את המפתח.

## פתרונות

## שאלה 1

הטקסט הוצפן ע"י צופן הזה 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)

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

לכל מילה  $x_1 x_2 \dots x_n$  של טקסט גלוי, לכל  $1 \leq i \leq n$  הכלל מצפין הוא:

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

ולכל מילה  $y_1 y_2 \dots y_n$  של טקסט מוצפן, לכל  $1 \leq i \leq n$  הכלל מפענח הוא:

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

כאשר  $\Delta_i$  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

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

נתון הטקסט מוצפן:

BXNKJLGZ .

$$\underline{y_1 = B} \quad (1)$$

$$\begin{array}{ccccccccccccccc} B & \xrightarrow{\pi} & B & \xrightarrow{\sigma_1} & C & \xrightarrow{\alpha_3} & F & \xrightarrow{\sigma_{-1}} & E & \xrightarrow{\alpha_2} & S & \xrightarrow{\alpha_1} & S & \xrightarrow{\rho} & F \\ & \xrightarrow{\alpha_1^{-1}} & D & \xrightarrow{\alpha_2^{-1}} & C & \xrightarrow{\sigma_1} & D & \xrightarrow{\alpha_3^{-1}} & B & \xrightarrow{\sigma_{-1}} & A & \xrightarrow{\pi} & \textcolor{blue}{G} \end{array}$$

$$\underline{x_2 = X} \quad (2)$$

$$\begin{array}{ccccccccccccccc} X & \xrightarrow{\pi} & I & \xrightarrow{\sigma_2} & K & \xrightarrow{\alpha_3} & X & \xrightarrow{\sigma_{-2}} & V & \xrightarrow{\alpha_2} & Y & \xrightarrow{\alpha_1} & C & \xrightarrow{\rho} & U \\ & \xrightarrow{\alpha_1^{-1}} & R & \xrightarrow{\alpha_2^{-1}} & G & \xrightarrow{\sigma_2} & I & \xrightarrow{\alpha_3^{-1}} & Q & \xrightarrow{\sigma_{-2}} & O & \xrightarrow{\pi} & \textcolor{blue}{O} \end{array}$$

$$\underline{x_3 = N} \quad (3)$$

$$\begin{array}{ccccccccccccccc} N & \xrightarrow{\pi} & N & \xrightarrow{\sigma_3} & Q & \xrightarrow{\alpha_3} & I & \xrightarrow{\sigma_{-3}} & F & \xrightarrow{\alpha_2} & I & \xrightarrow{\alpha_1} & V & \xrightarrow{\rho} & W \\ & \xrightarrow{\alpha_1^{-1}} & N & \xrightarrow{\alpha_2^{-1}} & T & \xrightarrow{\sigma_3} & W & \xrightarrow{\alpha_3^{-1}} & R & \xrightarrow{\sigma_{-3}} & O & \xrightarrow{\pi} & \textcolor{blue}{O} \end{array}$$

$$\underline{x_4 = K} \quad (4)$$

$$\begin{array}{ccccccccccccccc} K & \xrightarrow{\pi} & K & \xrightarrow{\sigma_4} & O & \xrightarrow{\alpha_3} & Y & \xrightarrow{\sigma_{-4}} & U & \xrightarrow{\alpha_2} & P & \xrightarrow{\alpha_1} & H & \xrightarrow{\rho} & D \\ & \xrightarrow{\alpha_1^{-1}} & G & \xrightarrow{\alpha_2^{-1}} & R & \xrightarrow{\sigma_4} & V & \xrightarrow{\alpha_3^{-1}} & L & \xrightarrow{\sigma_{-4}} & H & \xrightarrow{\pi} & \textcolor{blue}{D} \end{array}$$

$$\underline{x_5 = J} \quad (5)$$

$$\begin{array}{ccccccccccccccc} J & \xrightarrow{\pi} & J & \xrightarrow{\sigma_5} & O & \xrightarrow{\alpha_3} & Y & \xrightarrow{\sigma_{-5}} & T & \xrightarrow{\alpha_2} & N & \xrightarrow{\alpha_1} & W & \xrightarrow{\rho} & V \\ & \xrightarrow{\alpha_1^{-1}} & I & \xrightarrow{\alpha_2^{-1}} & F & \xrightarrow{\sigma_5} & K & \xrightarrow{\alpha_3^{-1}} & U & \xrightarrow{\sigma_{-5}} & P & \xrightarrow{\pi} & \textcolor{blue}{L} \end{array}$$

$$\underline{x_6 = L} \quad (6)$$

$$\begin{array}{ccccccccccccccc} L & \xrightarrow{\pi} & P & \xrightarrow{\sigma_6} & V & \xrightarrow{\alpha_3} & M & \xrightarrow{\sigma_{-6}} & G & \xrightarrow{\alpha_2} & R & \xrightarrow{\alpha_1} & U & \xrightarrow{\rho} & C \\ & \xrightarrow{\alpha_1^{-1}} & Y & \xrightarrow{\alpha_2^{-1}} & V & \xrightarrow{\sigma_6} & B & \xrightarrow{\alpha_3^{-1}} & A & \xrightarrow{\sigma_{-6}} & U & \xrightarrow{\pi} & \textcolor{blue}{U} \end{array}$$

$$\underline{x_7 = G} \quad (7)$$

$$\begin{array}{ccccccccccccccc} G & \xrightarrow{\pi} & A & \xrightarrow{\sigma_7} & H & \xrightarrow{\alpha_3} & P & \xrightarrow{\sigma_{-7}} & I & \xrightarrow{\alpha_2} & X & \xrightarrow{\alpha_1} & R & \xrightarrow{\rho} & B \\ & \xrightarrow{\alpha_1^{-1}} & W & \xrightarrow{\alpha_2^{-1}} & M & \xrightarrow{\sigma_7} & T & \xrightarrow{\alpha_3^{-1}} & J & \xrightarrow{\sigma_{-7}} & C & \xrightarrow{\pi} & \textcolor{blue}{C} \end{array}$$

$$\underline{x_8 = Z} \quad (8)$$

$$\begin{array}{ccccccccccccccc} Z & \xrightarrow{\pi} & Z & \xrightarrow{\sigma_8} & H & \xrightarrow{\alpha_3} & P & \xrightarrow{\sigma_{-8}} & H & \xrightarrow{\alpha_2} & U & \xrightarrow{\alpha_1} & A & \xrightarrow{\rho} & Y \\ \xrightarrow{\alpha_1^{-1}} & O & \xrightarrow{\alpha_2^{-1}} & Y & \xrightarrow{\sigma_8} & G & \xrightarrow{\alpha_3^{-1}} & S & \xrightarrow{\sigma_{-8}} & K & \xrightarrow{\pi} & \textcolor{blue}{K} \end{array}$$

לפיכך הטקסט גלוי הוא: GOODLUCK .

**שאלה 3** בהינתן מילה משוכפלת

$$xyz \ xyz$$

הטקסט המוצפן המתקבל ע"י צופן אנגימה 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:

$$\sigma_4 = \Delta_4 \Delta_1 (\sigma_1) ,$$

$$\sigma_5 = \Delta_5 \Delta_2 (\sigma_2) ,$$

$$\sigma_6 = \Delta_6 \Delta_3 (\sigma_3) .$$

לדוגמה, לפי המילה האופיינית הראשונה ברשימה נקבל:

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

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



## התמורות של כל האותיות:

$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \text{WWODFS}$	$\Rightarrow \sigma_1 = W, \sigma_4 = D \Rightarrow \Delta_4\Delta_1(W) = D.$
$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \text{DLVQMF}$	$\Rightarrow \sigma_1 = D, \sigma_4 = Q \Rightarrow \Delta_4\Delta_1(D) = Q.$
$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \text{PEQITH}$	$\Rightarrow \sigma_1 = P, \sigma_4 = I \Rightarrow \Delta_4\Delta_1(P) = I.$
$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \text{NQTVCJ}$	$\Rightarrow \sigma_1 = N, \sigma_4 = V \Rightarrow \Delta_4\Delta_1(N) = V.$
$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \text{SGMTXO}$	$\Rightarrow \sigma_1 = S, \sigma_4 = T \Rightarrow \Delta_4\Delta_1(S) = T.$
$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \text{YASEQM}$	$\Rightarrow \sigma_1 = Y, \sigma_4 = E \Rightarrow \Delta_4\Delta_1(Y) = E.$
$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \text{VBRULE}$	$\Rightarrow \sigma_1 = V, \sigma_4 = U \Rightarrow \Delta_4\Delta_1(V) = U.$
$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \text{XONKHK}$	$\Rightarrow \sigma_1 = X, \sigma_4 = K \Rightarrow \Delta_4\Delta_1(X) = K.$
$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \text{MHGPOA}$	$\Rightarrow \sigma_1 = M, \sigma_4 = P \Rightarrow \Delta_4\Delta_1(M) = P.$
$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \text{EIVZBF}$	$\Rightarrow \sigma_1 = E, \sigma_4 = Z \Rightarrow \Delta_4\Delta_1(E) = Z.$
$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \text{JZKNIC}$	$\Rightarrow \sigma_1 = J, \sigma_4 = N \Rightarrow \Delta_4\Delta_1(J) = N.$
$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \text{GYACDP}$	$\Rightarrow \sigma_1 = G, \sigma_4 = C \Rightarrow \Delta_4\Delta_1(G) = C.$
$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \text{UNBJWX}$	$\Rightarrow \sigma_1 = U, \sigma_4 = J \Rightarrow \Delta_4\Delta_1(U) = J.$
$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \text{TDDMJR}$	$\Rightarrow \sigma_1 = T, \sigma_4 = M \Rightarrow \Delta_4\Delta_1(T) = M.$
$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \text{OQYFCJ}$	$\Rightarrow \sigma_1 = O, \sigma_4 = F \Rightarrow \Delta_4\Delta_1(O) = F.$
$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \text{FSZWUW}$	$\Rightarrow \sigma_1 = F, \sigma_4 = W \Rightarrow \Delta_4\Delta_1(F) = W.$
$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \text{KTESYU}$	$\Rightarrow \sigma_1 = K, \sigma_4 = S \Rightarrow \Delta_4\Delta_1(K) = S.$
$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \text{LVIHPT}$	$\Rightarrow \sigma_1 = L, \sigma_4 = H \Rightarrow \Delta_4\Delta_1(L) = H.$
$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \text{QXCBGN}$	$\Rightarrow \sigma_1 = Q, \sigma_4 = B \Rightarrow \Delta_4\Delta_1(Q) = B.$
$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \text{JBPPLY}$	$\Rightarrow \sigma_1 = J, \sigma_4 = N \Rightarrow \Delta_4\Delta_1(J) = N.$
$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \text{AMJLZV}$	$\Rightarrow \sigma_1 = A, \sigma_4 = L \Rightarrow \Delta_4\Delta_1(A) = L.$
$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \text{ZCFRSL}$	$\Rightarrow \sigma_1 = Z, \sigma_4 = R \Rightarrow \Delta_4\Delta_1(Z) = R.$
$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \text{HPHORD}$	$\Rightarrow \sigma_1 = H, \sigma_4 = O \Rightarrow \Delta_4\Delta_1(H) = O.$
$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \text{CFWXVB}$	$\Rightarrow \sigma_1 = C, \sigma_4 = X \Rightarrow \Delta_4\Delta_1(C) = X.$
$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \text{IRLGNI}$	$\Rightarrow \sigma_1 = I, \sigma_4 = G \Rightarrow \Delta_4\Delta_1(I) = G.$
$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \text{BJXAEZ}$	$\Rightarrow \sigma_1 = B, \sigma_4 = A \Rightarrow \Delta_4\Delta_1(B) = A.$
$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \text{RUUYKQ}$	$\Rightarrow \sigma_1 = R, \sigma_4 = Y \Rightarrow \Delta_4\Delta_1(R) = Y.$

$x$	$\Delta_4\Delta_1(x)$
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	Y

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

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

לדוגמה, לפי המילה האופיינית הראשונה ברשימה נקבל:

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

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

$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \text{WWODFS}$	$\Rightarrow \sigma_2 = W, \sigma_5 = F$	$\Rightarrow \Delta_5\Delta_2(W) = F.$
$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \text{DLVQMF}$	$\Rightarrow \sigma_2 = L, \sigma_5 = M$	$\Rightarrow \Delta_5\Delta_2(L) = M.$
$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \text{PEQITH}$	$\Rightarrow \sigma_2 = E, \sigma_5 = T$	$\Rightarrow \Delta_5\Delta_2(E) = T.$
$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \text{NQTVCJ}$	$\Rightarrow \sigma_2 = Q, \sigma_5 = C$	$\Rightarrow \Delta_5\Delta_2(Q) = C.$
$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \text{SGMTXO}$	$\Rightarrow \sigma_2 = G, \sigma_5 = X$	$\Rightarrow \Delta_5\Delta_2(G) = X.$
$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \text{YASEQM}$	$\Rightarrow \sigma_2 = A, \sigma_5 = Q$	$\Rightarrow \Delta_5\Delta_2(A) = Q.$
$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \text{VBRULE}$	$\Rightarrow \sigma_2 = B, \sigma_5 = L$	$\Rightarrow \Delta_5\Delta_2(B) = L.$
$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \text{XONKHK}$	$\Rightarrow \sigma_2 = O, \sigma_5 = H$	$\Rightarrow \Delta_5\Delta_2(O) = H.$
$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \text{MHGPOA}$	$\Rightarrow \sigma_2 = H, \sigma_5 = O$	$\Rightarrow \Delta_5\Delta_2(H) = O.$
$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \text{EIVZBF}$	$\Rightarrow \sigma_2 = I, \sigma_5 = B$	$\Rightarrow \Delta_5\Delta_2(I) = B.$
$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \text{JZKNIC}$	$\Rightarrow \sigma_2 = Z, \sigma_5 = I$	$\Rightarrow \Delta_5\Delta_2(Z) = I.$
$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \text{GYACDP}$	$\Rightarrow \sigma_2 = Y, \sigma_5 = D$	$\Rightarrow \Delta_5\Delta_2(Y) = D.$
$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \text{UNBJWX}$	$\Rightarrow \sigma_2 = N, \sigma_5 = W$	$\Rightarrow \Delta_5\Delta_2(N) = W.$
$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \text{TDDMJR}$	$\Rightarrow \sigma_2 = D, \sigma_5 = J$	$\Rightarrow \Delta_5\Delta_2(D) = J.$
$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \text{OQYFCJ}$	$\Rightarrow \sigma_2 = Q, \sigma_5 = C$	$\Rightarrow \Delta_5\Delta_2(Q) = C.$
$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \text{FSZWUW}$	$\Rightarrow \sigma_2 = S, \sigma_5 = U$	$\Rightarrow \Delta_5\Delta_2(S) = U.$
$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \text{KTESYU}$	$\Rightarrow \sigma_2 = T, \sigma_5 = Y$	$\Rightarrow \Delta_5\Delta_2(T) = Y.$
$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \text{LVIHPT}$	$\Rightarrow \sigma_2 = V, \sigma_5 = P$	$\Rightarrow \Delta_5\Delta_2(V) = P.$
$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \text{QXC BGN}$	$\Rightarrow \sigma_2 = X, \sigma_5 = G$	$\Rightarrow \Delta_5\Delta_2(X) = G.$
$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \text{JBP NLY}$	$\Rightarrow \sigma_2 = B, \sigma_5 = L$	$\Rightarrow \Delta_5\Delta_2(B) = L.$
$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \text{AMJLZV}$	$\Rightarrow \sigma_2 = M, \sigma_5 = Z$	$\Rightarrow \Delta_5\Delta_2(M) = Z.$
$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \text{ZCFRSL}$	$\Rightarrow \sigma_2 = C, \sigma_5 = S$	$\Rightarrow \Delta_5\Delta_2(C) = S.$
$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \text{HPHORD}$	$\Rightarrow \sigma_2 = P, \sigma_5 = R$	$\Rightarrow \Delta_5\Delta_2(P) = R.$
$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \text{CFWXVB}$	$\Rightarrow \sigma_2 = F, \sigma_5 = V$	$\Rightarrow \Delta_5\Delta_2(F) = V.$
$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \text{IRLGNI}$	$\Rightarrow \sigma_2 = R, \sigma_5 = N$	$\Rightarrow \Delta_5\Delta_2(R) = N.$
$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \text{BJXAEZ}$	$\Rightarrow \sigma_2 = J, \sigma_5 = E$	$\Rightarrow \Delta_5\Delta_2(J) = E.$
$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \text{RUUYKQ}$	$\Rightarrow \sigma_2 = U, \sigma_5 = K$	$\Rightarrow \Delta_5\Delta_2(U) = K.$

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

$x$	$\Delta_5\Delta_2(x)$
G	X
H	O
I	B
J	E
K	
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	Y
U	K
V	P
W	F
X	G

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

לדוגמה, לפי המילה האופיינית הראשונה ברשימה נקבל:

$$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \text{WWODES} \Rightarrow \sigma_3 = W, \sigma_6 = F \Rightarrow \Delta_6\Delta_3(W) = F.$$

ז"א התמורה  $\Delta_6\Delta_3$  על האות W פולטת F. בעזרת השיטה הזו על כל המילים האופייניות ברשימה נקבל את

## התמורות של כל האותיות:

$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \text{WWODFS}$	$\Rightarrow \sigma_3 = \text{W}, \sigma_6 = \text{F}$	$\Rightarrow \Delta_6\Delta_3(\text{W}) = \text{F}$
$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \text{DLVQMF}$	$\Rightarrow \sigma_3 = \text{L}, \sigma_6 = \text{M}$	$\Rightarrow \Delta_6\Delta_3(\text{L}) = \text{M}$
$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \text{PEQITH}$	$\Rightarrow \sigma_3 = \text{E}, \sigma_6 = \text{T}$	$\Rightarrow \Delta_6\Delta_3(\text{E}) = \text{T}$
$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \text{NQTVCJ}$	$\Rightarrow \sigma_3 = \text{Q}, \sigma_6 = \text{C}$	$\Rightarrow \Delta_6\Delta_3(\text{Q}) = \text{C}$
$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \text{SGMTXO}$	$\Rightarrow \sigma_3 = \text{G}, \sigma_6 = \text{X}$	$\Rightarrow \Delta_6\Delta_3(\text{G}) = \text{X}$
$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \text{YASEQM}$	$\Rightarrow \sigma_3 = \text{A}, \sigma_6 = \text{Q}$	$\Rightarrow \Delta_6\Delta_3(\text{A}) = \text{Q}$
$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \text{VBRULE}$	$\Rightarrow \sigma_3 = \text{B}, \sigma_6 = \text{L}$	$\Rightarrow \Delta_6\Delta_3(\text{B}) = \text{L}$
$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \text{XONKHK}$	$\Rightarrow \sigma_3 = \text{O}, \sigma_6 = \text{H}$	$\Rightarrow \Delta_6\Delta_3(\text{O}) = \text{H}$
$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \text{MHGPOA}$	$\Rightarrow \sigma_3 = \text{H}, \sigma_6 = \text{O}$	$\Rightarrow \Delta_6\Delta_3(\text{H}) = \text{O}$
$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \text{EIVZBF}$	$\Rightarrow \sigma_3 = \text{I}, \sigma_6 = \text{B}$	$\Rightarrow \Delta_6\Delta_3(\text{I}) = \text{B}$
$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \text{JZKNIC}$	$\Rightarrow \sigma_3 = \text{Z}, \sigma_6 = \text{I}$	$\Rightarrow \Delta_6\Delta_3(\text{Z}) = \text{I}$
$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \text{GYACDP}$	$\Rightarrow \sigma_3 = \text{Y}, \sigma_6 = \text{D}$	$\Rightarrow \Delta_6\Delta_3(\text{Y}) = \text{D}$
$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \text{UNBJWX}$	$\Rightarrow \sigma_3 = \text{N}, \sigma_6 = \text{W}$	$\Rightarrow \Delta_6\Delta_3(\text{N}) = \text{W}$
$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \text{TDDMJR}$	$\Rightarrow \sigma_3 = \text{D}, \sigma_6 = \text{J}$	$\Rightarrow \Delta_6\Delta_3(\text{D}) = \text{J}$
$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \text{OQYFCJ}$	$\Rightarrow \sigma_3 = \text{Q}, \sigma_6 = \text{C}$	$\Rightarrow \Delta_6\Delta_3(\text{Q}) = \text{C}$
$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \text{FSZWUW}$	$\Rightarrow \sigma_3 = \text{S}, \sigma_6 = \text{U}$	$\Rightarrow \Delta_6\Delta_3(\text{S}) = \text{U}$
$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \text{KTESYU}$	$\Rightarrow \sigma_3 = \text{T}, \sigma_6 = \text{Y}$	$\Rightarrow \Delta_6\Delta_3(\text{T}) = \text{Y}$
$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \text{LVIHPT}$	$\Rightarrow \sigma_3 = \text{V}, \sigma_6 = \text{P}$	$\Rightarrow \Delta_6\Delta_3(\text{V}) = \text{P}$
$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \text{QXCBGN}$	$\Rightarrow \sigma_3 = \text{X}, \sigma_6 = \text{G}$	$\Rightarrow \Delta_6\Delta_3(\text{X}) = \text{G}$
$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \text{JBPPLY}$	$\Rightarrow \sigma_3 = \text{B}, \sigma_6 = \text{L}$	$\Rightarrow \Delta_6\Delta_3(\text{B}) = \text{L}$
$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \text{AMJLZV}$	$\Rightarrow \sigma_3 = \text{M}, \sigma_6 = \text{Z}$	$\Rightarrow \Delta_6\Delta_3(\text{M}) = \text{Z}$
$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \text{ZCFRSL}$	$\Rightarrow \sigma_3 = \text{C}, \sigma_6 = \text{S}$	$\Rightarrow \Delta_6\Delta_3(\text{C}) = \text{S}$
$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \text{HPHORD}$	$\Rightarrow \sigma_3 = \text{P}, \sigma_6 = \text{R}$	$\Rightarrow \Delta_6\Delta_3(\text{P}) = \text{R}$
$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \text{CFWXVB}$	$\Rightarrow \sigma_3 = \text{F}, \sigma_6 = \text{V}$	$\Rightarrow \Delta_6\Delta_3(\text{F}) = \text{V}$
$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \text{IRLGNI}$	$\Rightarrow \sigma_3 = \text{R}, \sigma_6 = \text{N}$	$\Rightarrow \Delta_6\Delta_3(\text{R}) = \text{N}$
$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \text{BJXAEZ}$	$\Rightarrow \sigma_3 = \text{J}, \sigma_6 = \text{E}$	$\Rightarrow \Delta_6\Delta_3(\text{J}) = \text{E}$
$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \text{RUUYKQ}$	$\Rightarrow \sigma_3 = \text{U}, \sigma_6 = \text{K}$	$\Rightarrow \Delta_6\Delta_3(\text{U}) = \text{K}$

$x$	$\Delta_6\Delta_3(x)$
A	Q
B	L
C	S
D	J
E	T
F	V

$x$	$\Delta_6\Delta_3(x)$
G	X
H	O
I	B
J	E
K	
L	M

$x$	$\Delta_6\Delta_3(x)$
M	Z
N	W
O	H
P	R
Q	C
R	N

$x$	$\Delta_6\Delta_3(x)$
S	U
T	Y
U	K
V	P
W	F
X	G

$x$	$\Delta_6\Delta_3(x)$
Y	D
Z	I

#### שאלה 4

#### שאלה 5

#### שאלה 6

#### שאלה 7

סעיף 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 הפונקציה 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

---

1: **Input:** Integers  $A, B$ .

2:  $r_0 \leftarrow A$

3:  $r_1 \leftarrow B$

4:  $t_0 \leftarrow 0$

5:  $t_1 \leftarrow 1$

6:  $n \leftarrow 1$

7: **while**  $r_n \neq 0$  **do**

8:      $q_n \leftarrow \left\lfloor \frac{r_{n-1}}{r_n} \right\rfloor$

9:      $r_{n+1} \leftarrow r_{n-1} - q_n r_n$

10:     $t_{n+1} \leftarrow t_{n-1} - q_n t_n$

11:     $n \leftarrow n + 1$

12: **end while**

13:  $n \leftarrow n - 1$

14: **if**  $r_n \neq 1$  **then**

15:      $B$  has no inverse modulo  $A$

16: **else**

17:     **return:**  $t_n$

18: **end if**

---

$$\triangleright t_n = B^{-1} \pmod{A}$$

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

$$\begin{aligned} r_0 &= A = 2160, & r_1 &= B = 107, \\ t_0 &= 0, & t_1 &= 1. \end{aligned}$$

אזי האיטרציות של האלגוריתם הם כמפורט למטה:

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

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

$$a = 323.$$

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

$$y = \text{DED} \rightarrow 343.$$

בסעיף הקודם קיבלנו את הפרמטרים  $p = 73, b = 107, q = 31$  וחישבנו  $n = 2263, \phi(n) = 2160$  והוכחנו כי  $a = b^{-1} \pmod{n} = 323$ . 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  $x = y^a \pmod{n}$ .

$$y \pmod{p} = 343 \pmod{73} = 51, \quad a \pmod{(p-1)} = 323 \pmod{70} = 43.$$

לכן

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

$$y \pmod{q} = 343 \pmod{31} = 2, \quad a \pmod{(q-1)} = 323 \pmod{30} = 23.$$

לכן

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

התשובה הסופית ניתנת ע"י הפתרון למערכת הבאה:

$$x = x_1 \pmod{p} = 10 \pmod{73}$$

$$x = x_2 \pmod{q} = 8 \pmod{31}$$

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

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

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, ומהפריק אוקלידס נמצא את האיברים ההופכיים המודולריים באופן הבא. נסמן:  $A = 73, B = 31$ .

$$\begin{aligned} r_0 &= A = 73, & r_1 &= B = 31, \\ s_0 &= 1, & s_1 &= 0, \\ t_0 &= 0, & t_1 &= 1. \end{aligned}$$

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

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

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

לכן

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

לכן

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

$$\begin{aligned} y &= a_1 M_1 y_1 + a_2 M_2 y_2 \\ &= 10(31)(33) + 8(73)(17) \bmod 2263 \\ &= 4223186 \bmod 2263 \\ &= 2054. \end{aligned}$$

לכן הטקסט הגולי הוא

$$x = 2054 \rightarrow \text{cafe} .$$

**שאלה 8** נפתור מערכת זו באמצעות משפט השאריות הסיני. נסמן

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

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

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

באמצעות הקוד פייתון שנמצא באתר המודל נחשב את ההופכיים

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

הפתרון (מודולר  $M$ ) הוא

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

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

נסמן:  $a = 99, b = 13$ .

אתחול:

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



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

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

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

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.

$$a = 101, b = 15.$$

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 $k = 5$ :

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

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

לכן

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

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

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

כעת נפתור את המערכת

$$x \equiv 46 \pmod{99} ,$$

$$x \equiv 98 \pmod{101} ,$$

בעזרת המשפט השאריות הסיני.

נסמן

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

$$y_1 = M_1^{-1} \pmod{m_1} = 101^{-1} \pmod{99} = 50 , \quad y_2 = M_2^{-1} \pmod{m_2} = 99^{-1} \pmod{101} = 50 .$$

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

**שאלה 10**

(א)

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

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

$$a = 31^{-1} \pmod{1440} . \text{ נשתמש באלגוריתם של אוקליד:}$$

**שיטה 1**

$$r_0 = \phi(n) = 1440 , \quad r_1 = b = 31 ,$$

$$s_0 = 1 , \quad s_1 = 0 ,$$

$$t_0 = 0 , \quad t_1 = 1 .$$

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

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

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

מכאן

$$31^{-1} = 511 \bmod 1440.$$

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

(ב) אליס שולחת את ההודעה  $x^b \bmod n = 1228^{31} \bmod 1517$  כדי לחשב זה נשתמש בשיטת ריבועים:  
 $31 = 16 + 8 + 4 + 2 + 1$

$$\begin{aligned} (1228)^2 \bmod 1517 &= 86 \bmod 1517 \\ (1228)^4 \bmod 1517 &= (86)^2 \bmod 1517 = 1328 \bmod 1517 \\ (1228)^8 \bmod 1517 &= (1328)^2 \bmod 1517 = 830 \bmod 1517 \\ (1228)^{16} \bmod 1517 &= (830)^2 \bmod 1517 = 182 \bmod 1517 \end{aligned}$$

לכן

$$\begin{aligned} 1228^{31} \bmod 1517 &= (1228)^{16} \times (1228)^8 \times (1228)^4 \times (1228)^2 \times 1228 \bmod 1517 \\ &= 182 \times 830 \times 1328 \times 86 \times 1228 \bmod 1517 \\ &= 699 \bmod 1517. \end{aligned}$$

לכן הטקסט מוצפן הינו  $y = 699$ .

(ג)  $y = 699$

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

לכן

$$\begin{aligned} x_1 &= (y \bmod p)^{a \bmod (p-1)} \bmod p = 33^7 \bmod 37 = 7. \\ &(\text{ניתן לחשב זה לפי } 33^7 \times 33^4 \times 33^2 \times 33^1) \end{aligned}$$

בנוסף

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

לכן

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

(ניתן לחשב זה לפי  $2^{31} \times 2^{16} \times 2^8 \times 2^4 \times 2^2 \times 2$ )

לכן עלינו לפתור את המערכת

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

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

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

$$y_2 = M_2^{-1} \bmod m_2 = 37^{-1} \bmod 41 = 10, \quad y_1 = M_1^{-1} \bmod m_1 = 41^{-1} \bmod 37 = 28$$

לכן

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

## שאלה 11

יש בדיוק 15 תווים בטקסט מוצפן ובטקסט גלוי. לכן הסדר הכי קטן של המטריצה של המפתח הוא 3. נבדוק אם קיים מפתח  $k \in \mathbb{Z}_{26}^{3 \times 3}$  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  $3 \times 3$  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 לבדוד 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:

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

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

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

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

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

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

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

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

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

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

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

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

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

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