

## עבודת 2: תמורה, צופן אניגמה, קריפטו-אנליזה וצופן RSA

### אופן כתיבת תשובה לשאלות

- 1) יש להראות פתרון מלא. הסבירו היטב את מהלך הפתרון.
- 2) יש לנמק היטב כל שלב של פתרון. תשובה ללא הסבר ולא נימוק, אפילו נכון, לא תתקבל.
- 3) יש לרשום ליד כל תשובה את מספר של השאלה שעלייה אתם עונים.

### מועד הגשה

- 1) הגשה היא עד סוף יום ההגשה, ככלומר עד השעה 23:59 באותו היום. אל תחכו לרגע האחרון. תכנו אתzmanכם בהתאם. הגיעו לפני.
- 2) אישור במועד ההגשה יגרור הורדה של ציון, 5 נק' לכל יום אישור או חלק ממנו. בכל מקרה לא יהיה ניתן להגיש מעבר ל-2 ימי אישור ממועד ההגשה דלעיל.

### אופן הגשה

- 1) קראו היטב את השאלות. עליהם לענות על כל השאלות בעבודה זו.
- 2) הגשת העבודה תהיה דרך אתר הקורס במודול בלבד בלבד. הגשת העבודה היא **ביחידים או בזוגות**.
- 3) כיצד הגיעו?
  - א) יש לסרוק או להמיר את העבודה לקובץ pdf ולהגיש אותו (סרייקה לא ברורה או מוטשטשת לא תיבדק).
  - ב) • במידה שאת.ה מגיש.ה פתרונות בלבד אז בשם הקובץ שיוגש למערכת ההגשה יהיה מספר ת"ז ושם של המגיש ושם של העבודה. לדוגמה: עבודה-2-ירמיהו-ת-ז-pdf.123456789-.
  - במידה שאת.ה מגישים פתרונות כזוג או בשם הקובץ שיוגש למערכת ההגשה יהיו מספרי ת"ז ושמות של המגישים ושם של העבודה. לדוגמה: עבודה-2-ירמיהו-ת-ז-123456789-113114115-גל-pdf.113114115-.
- 4) בקובץ המוגש יש להוסיף את התיעוד הבא בעמוד הראשון (בעברית או באנגלית, לבחירתכם). יש לשנות את השם שלכם ואת תעודה הזהות לטעות הזהות שלכם. ובמקום סולומית יש לכתוב את מספר העבודה.  
 Assignment: #  
 Author1: Israel Israeli, ID: 01234567  
 Author2: Dave David, ID: 8910111213
- 5) לאחר שהעליתם את הקבצים שלכם למודול, הורידו אותם מהמודול למחשב שלכם וודאו כי הקבצים תקינים וכי העליתם את הקבצים הנכונים והמלאים. לאחר תום מועד ההגשה לא יתקבלו ערורים על כך שהעליתם קבצים לא תקינים או שהעליתם בטעות קבצים אחרים / לא נכוןים.

### שאלות

- 1) שאלות בנוגע העבודה יש לשאול בפורום באתר המודל של הקורס או בשעות קבלה של המתרגל/ת האחראי/ת בלבד. אין לשלו שאלות במיל לא למתרגל האחראי ולא למתרגלים/מרצים אחרים.
- 2) ניתן לשאול שאלות הבקרה ומיקוד על המשימות שבעבודה במידה ומשימה מסוימת לא ברורה. לא ניתן לשאול על הפתרונות שלכם. לדוגמה, לא ניתן לשאול האם הפתרון שלי נכון, לא ניתן לשאול למה הפתרון לא עובד, וכדומה.

**שונות**

- 1) השאלות בעבודה זו הינם שות משקל. ככלומר, משקל כל שאלה הוא 100 חלקים מס' השאלות בעבודה.
- 2) בשאלת מרובת סעיפים, הסעיפים הם שווים משקל. ככלומר משקל כל סעיף הוא משקל השאלה כולה חלק מס' הסעיפים השאלה.

בצלחה!

## עבודת 2: תמורה, 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 המשותנה

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

מצאו את הטקסט המקורי.

### שאלה 3 (9 נקודות)

הטבלה הבאה מראה מילימ אופייניות מהודעות מוצפנות מאותו יום.

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

**a)** הוכיחו כי התמורות המתאימות של צופן אניגמה הן:

$$\Delta_4 \Delta_1 = (\text{JNVU}) (\text{ZRTE}) (\text{GCXKS} \text{YMPI}) (\text{ALHOFWDQ} \text{B}) ,$$

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

$$\Delta_6 \Delta_3 = (\text{MOS}) (\text{CNK}) (\text{BXZW}) (\text{TGAP}) (\text{FLIYJV}) (\text{QHDREU}) .$$

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

MWORVZ

חשבו את הטקסט המקורי.

**שאלה 4 (9 נקודות)**

הtekst הבא הוכפן 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 בкриיפטו-אנליזה כדי למצוא את הטקסט המקורי.

**שאלה 5 (9 נקודות)**תהי  $\Sigma \rightarrow \Sigma$ :  $\pi$  תמורה מעל אלפבית  $\Sigma$ . הוכחו או הפריכו ע"י דוגמה נגדית את הטענות הבאות:

- (a) אם  $\pi$  מחרור באורך  $k$ izi  $\pi^k = \text{id}$ .
- (b) אם  $\pi$  מחרור באורך  $k$ izi  $k$  הוא השלם הקטן ביותר עבורו  $\pi^k = \text{id}$ .

**שאלה 6 (9 נקודות)**תהי  $\Sigma$  אלפבית בעל  $n$  אותיות. כלומר  $n = |\Sigma|$ . נסמן ב-  $S_n$  הקבוצה של כל התמורות האפשרות מעל  $\Sigma$  הוכחו את הטענה הבאה:  
אם קיימת Tamura  $\alpha \in S_n$  כך שלכל  $\beta \in S_n$  מתקיים:

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

$$\alpha = \text{id}.$$

**שאלה 7 (9 נקודות)**

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

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

ההצפנה של הודעה היא

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

- (a) הוכחו כי המפתח הציבורי הוא  $(a, p, q) = (323, 73, 31)$ .
- (b) חשבו את הטקסט המקורי שאليس שלחה.

**שאלה 8 (9 נקודות)**

פתרו את המערכת משוואות הבאה בעזרת המשפט השאריות הסיני:

$$x \equiv 12 \pmod{25}$$

$$x \equiv 9 \pmod{26}$$

$$x \equiv 23 \pmod{27} .$$

**שאלה 9 (9 נקודות)**

פתרו את המערכת משוואות הבאה:

$$13x \equiv 4 \pmod{99}$$

$$15x \equiv 56 \pmod{101} .$$

רמז: השתמשו באלגוריתם המוכלל של אוקליד ולאחר כך המשפט השאריות הסיני.

**שאלה 10 (9 נקודות)**בוב בונה מפתח ציבורי ומפתח סודי של צופן RSA עם הפרמטרים  $b = 31$ ,  $q = 41$ ,  $p = 37$ .(א) חשבו את  $n$ ,  $\phi(n)$  ו-  $a$ .(ב) אליס מצפינה את הטקסט הגלוי `bccc`. מהי הטקסט מוצפן שהוא שולחת לבוב?(ג) הוכחו שהפענוח של הטקסט מוצפן שמצאתם בסעיף ב' נותן `bccc`.

רמז:

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

**שאלה 11 (9 נקודות)**

נתון הטקסט גלי

`thefutureisgood`

והtekst מוצפן שלו

`FOPBVFWDFCCGMAT`

הtekst הוצפן עם צופן היל. מצאו את המפתח.

**פתרונות** **שאלה 1**

הטקסט הוצפן ע"י צופן זהה 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 מפענה של צופן אניגמה מוגדרים באופן הבא. נתון תמורה משקפת המשתנה (נתונה בשאלת)

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

לכל מילה  $x$  של טקסט גלי, לכל  $n \leq i \leq 1$  הכלל מצפין הוא:

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

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

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

כאשר  $\Delta_i$  היא התמורה המורכבת

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

כאשר

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

נתון הטקסט מוצפן:

BXNKJLGZ .

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

לפייך הטקסט גליי הוא: . GOODLUCK .

### **שאלה 3** בהינתן מילה משוכפלת

$$xyz \ xyz$$

הtekst המוצפן המתקיים ע"י צופן אניגמה הוא נקרא מילה אופיינית, אשר כתוב בבייטוי 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 ריבסקי 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 קיבל:

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

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

התמורות של כל האותיות:

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

$x$	$\Delta_4\Delta_1(x)$
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:

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

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

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

$x$	$\Delta_5\Delta_2(x)$
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:

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

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

התמורות של כל האותיות:

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

$x$	$\Delta_6\Delta_3(x)$
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 בשאלת א' 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 בשאלת א' נשאר רק לחשב את  $a$  לפי הנוסחה  $\phi(n)$  הוא הפונקציה אוילר:  $a = b^{-1} \pmod{\phi(n)}$

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

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

---

**Algorithm 1** האלגוריתם לאייר 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:  $t_n$                                       $\triangleright t_n = B^{-1} \pmod{A}$ 
18: end if

```

---

נשים  $A = 23940, B = 47$ . נתחל 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:

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

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

$$a = 323.$$

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

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

בסעיף הקודם קיבלנו את הפרמטרים  $\phi(n) = 2160, n = 2263, q = 31, p = 73, b = 107$  ו $\chi(q) = 31, p = 73, b = 107$  ו $b^{-1} \pmod{n} = 323$ . כעת נkeh את הטקסט מוצפן  $y = 343$  והמפתח הסודי  $a = 323$  על פי הכלל מפענה  $x = y^a \pmod{n}$ .

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

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

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

$$y_2 = M_2^{-1} \pmod{m_2} = 31^{-1} \pmod{73} \text{ ו } y_1 = M_1^{-1} \pmod{m_1} = 73^{-1} \pmod{31}$$

נחשב את הפירוק אוקלידי של  $73$  ו-  $31$  בעזרת האלגוריתם המוכל של אוקלידי, ומהפירוק אוקלידי 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

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

$$\begin{aligned} y &= a_1 M_1 y_1 + a_2 M_2 y_2 \\ &= 10(31)(33) + 8(73)(17) \pmod{2263} \\ &= 4223186 \pmod{24257} \\ &= 2054. \end{aligned}$$

לכן הטקסט המקורי הוא  
 $x = 2054 \rightarrow \text{cafe}$ .

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

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

כasher

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

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 פיתון שנמצא באתר המודל נחשב את ההופכים

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

הפתרון (מודול  $M$ ) 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 המכולל של אוקליידס באופן הבא.

נסמן:  $a = 99, b = 13$ 

אתחול:

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

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

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

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

לכן

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



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

$$\text{נסמן: } a = 101, b = 15$$

אתחל:

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

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

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

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

לכז

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

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

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

cut נפתר את המערכת

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

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

בעזרת המשפט השARINGOT 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)

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

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

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

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

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

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

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

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

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

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

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

**(ב)** אליס שולחת את ההודעה  $x^b \bmod n = 1228^{31} \bmod 1517$ . כדי לחשב זה משתמש 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 הtekסט מוצפן הינו  $y = 699$

$$\text{לכן } y = 699 \quad \text{ג}$$

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

לכן

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

(ניתן לחשב זה לפי  $(33^7 \times 33^4 \times 33^2 \times 33^1)$ )

בנוסח

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

לכן

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

(ניתן לחשב זה לפה 2

לכן עליינו לפתור את המערכת

$$x = x_1 \mod p = 7 \mod 37$$

$$x = x_2 \mod q = 39 \mod 41$$

בעזרת המשפט השאריות הסיני. נסמן

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

כעת נחשב  $y_2 = M_2^{-1} \mod m_2 = 37^{-1} \mod 41 = -1$  ו-  $y_1 = M_1^{-1} \mod m_1 = 41^{-1} \mod 37 = 28$ 

.10.

לכן

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

**שאלה 11**

יש בדיק 15 תווים בטקסט מוצפן ובtekst גלי. לכן הסדר הכי קטן של המטריצה של המפתח הוא 3. נבדוק אם קיים מפתח  $k \in \mathbb{Z}_{26}^{3 \times 3}$  אשר באמצעות הטקסט מוצפן מתקבל מהtekst גלי.

$x \in P$	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

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

לכן ה-3 אותיות הראשונות של הטקסט מוצפן ( $y_1 \ y_2 \ y_3$ ) מתקבלות מההצפנה של ה-3 אותיות הראשונות של tekst גלי, על פי הכלל מצפין של צופן היל'ק:

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

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

$$(y_3 \ y_4 \ y_5) = (x_3 \ x_4 \ x_5)k \text{ mod } 26 ,$$

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

$$(y_7 \ y_8 \ y_9) = (x_7 \ x_8 \ x_9)k \text{ mod } 26 .$$

אפשר לרשום את השלוש משוואות האלו כמשוואת 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 במטריצה 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

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

**נתיב**  $x_1 = 19, x_2 = 7, x_3 = 4, x_4 = 5, x_5 = 20, x_6 = 19, x_7 = 20, x_8 = 17, x_9 = 4$   
**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. תחילת נמצאת הדטרמיננטה:

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

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

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

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

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

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

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

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

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

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

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

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

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

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