תרגילים 3: צפנים בסיסיים

שאלה 1

נתון הטקסט מוצפן

IAFDXFUUWLFEIALLCRZ

אשר מוצפן על ידי צופן אפיני עם המפתח $a = 5, b = 17$. מצאו את הטקסט גלוי.

שאלה 2

נתון הטקסט מוצפן

HVFDDP

אשר מוצפן על ידי צופן היל עם המפתח

$$k = \begin{pmatrix} 13 & 5 & 6 \\ 2 & 1 & 7 \\ 9 & 7 & 13 \end{pmatrix} .$$

מצאו את הטקסט גלוי.

שאלה 3

נתון הטקסט מוצפן

IAFDXFUUWLFEIALLCRZ

אשר מוצפן על ידי צופן אפיני עם המפתח $a = 5, b = 17$. מצאו את הטקסט גלוי.

שאלה 4

נתונה התמורה

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

פענחו את הטקסט מצפון

CEDOBAERKGNI

שאלה 5

נתון הטקסט מוצפן

IAFDXFUUWLFEIALLCRZ

אשר מוצפן על ידי צופן אפיני עם המפתח $a = 5, b = 17$. מצאו את הטקסט גלוי.

שאלה 6

נתון את הטקסט מוצפן

ZFSXUHIYWU

אשר מוצפן על ידי צופן ויז'נר עם המפתח GREEN. מצאו את הטקסט גלוי.

שאלה 7

נתונה התמורה

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

פענחו את הטקסט מצפון

CEDOBAERKGNI

שאלה 8

נתון הטקסט מוצפן

IAFDXFUUWLFEIALLCRZ

אשר מוצפן על ידי צופן אפיני עם המפתח $a = 5, b = 17$. מצאו את הטקסט גלוי.

שאלה 9

נתון הטקסט מוצפן

HVFDDP

אשר מוצפן על ידי צופן היל עם המפתח

$$k = \begin{pmatrix} 13 & 5 & 6 \\ 2 & 1 & 7 \\ 9 & 7 & 13 \end{pmatrix} .$$

מצאו את הטקסט גלוי.

שאלה 10

נתונה התמורה

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

פענחו את הטקסט מצפון

CEDOBAERKGNI

שאלה 11

נתון את הטקסט מוצפן

ZFSXUHIYWU

אשר מוצפן על ידי צופן ויז'נר עם המפתח GREEN. מצאו את הטקסט גלוי.

שאלה 12 נניח כי $k = (13, 8)$ הוא מפתח של צופן האפיני מעל החוג $\mathbb{Z}_{31}$.

א) מצאו את האיברים a', b' בכלל מפענח

$$d_k(y) = a'y + b'$$

כאשר $a', b' \in \mathbb{Z}_{31}$.

ב) הוכיחו כי $d_k\left(e_k(x)\right) = x$ לכל $x \in \mathbb{Z}_{31}$.

שאלה 13 הטקסט מוצפן הבא מוצפן על ידי צופן הזזה (צופן קיסר).

VWDUZDUV

מצאו את המפתח של הצופן ומצאו את הטקסט גלוי (רמז: חיפוש ממצה).

שאלה 14 נתונה התמורה הבאה:

$$\pi = \begin{pmatrix} 4 & 1 & 6 & 2 & 7 & 3 & 8 & 5 \end{pmatrix}$$

א) מצאו את התמורה ההופכית.

ב) פענחו את הטקסט מוצפן הבא

TGEEMNELNNTDROEOAAHDOETCSHAEIRLM

שאלה 15 נתון המפתח

$$k = \begin{pmatrix} 1 & 3 & 0 \\ 0 & 0 & 1 \\ 3 & 0 & 1 \end{pmatrix}$$

של הצופן היל. לכל טקסט מוצפן למטה מתון את הטקסט גלוי

א) VAZMJR

ב) NDIMZZEMV

שאלה 16

נתון הטקסט מוצפן

FPHOEMJSUPSZZYJ

אשר מוצפן על ידי צופן היל עם המפתח

$$k = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 11 & 9 & 8 \end{pmatrix} .$$

מצאו את הטקסט גלוי.

שאלה 17

נתונה התמורה

x	1	2	3	4	5	6	7	8
$\pi(x)$	4	1	6	2	7	3	8	5

א) מצאו את $\pi^{-1}(x)$.

ב) פענחו את הטקסט מצפון

SQIUOENTMFHREOFTLIXNAAME

שאלה 18

נתון את הטקסט מוצפן

YGSOYNGSUUTOYZNKHKYZIURRKMKOTOYXGKR

אשר מוצפן על ידי צופן קיסר. מצאו את המפתח ואת הטקסט גלוי.

שאלה 19 נניח כי $K = (5, 21)$ הוא מפתח של צופן האפיני מעל החוג $\mathbb{Z}_{29}$.

א) מצאו את האיברים a', b' בכלל מפענח

$$d_K(y) = a'y + b'$$

כאשר $a', b' \in \mathbb{Z}_{29}$.

ב) הוכיחו כי $d_K\left(e_K(x)\right) = x$ לכל $x \in \mathbb{Z}_{29}$.

פתרונות

שאלה 1 הכלל מפענח הוא

$$d_k(y) = a^{-1}(y-b) \mod 26$$

$a^{-1} \mod 26 = 5^{-1} \mod 26 = 21$. לכן

$$d_k(y) = 21(y-17) \mod 26 = 21y - 357 \mod 26 .$$

$357\%26 = 357 - 26\left\lfloor \frac{357}{26} \right\rfloor = 357 - 26(13) = 19$ לכן $(-357)\%26 = 26 - (357\%26) = 26 - 19 = 7$ לכן
$-289 \mod 26 = 7$. מכאן

$$d_k(y) = 21y + 7 .$$

$y \in C$	I	A	F	D	X	F	U	U	W	L	F	E	I	A	L	L	C	R	Z
$y \in \mathbb{Z}_{26}$	8	0	5	3	23	5	20	20	22	11	5	4	8	0	11	11	2	17	25
$x \in \mathbb{Z}_{26}$	19	7	8	18	22	8	11	11	1	4	8	13	19	7	4	4	23	0	12
$x \in P$	t	h	i	s	w	i	l	l	b	e	i	n	t	h	e	e	x	a	m

שאלה 2

$y \in C$	H	V	F	D	D	P
$y \in \mathbb{Z}_{26}$	7	21	5	3	3	15

דטרמיננטה של k היא $|k| = 7 \mod 26 = 7$.
$\gcd(7, 26) = 1$ לכן המטריצה הפיכה ב- $\mathbb{Z}_{26}$.

$$\begin{pmatrix} 13 & 5 & 6 \\ 2 & 1 & 7 \\ 9 & 7 & 13 \end{pmatrix} \Rightarrow C_{11} = (-1)^{1+1}\begin{vmatrix} 1 & 7 \\ 7 & 13 \end{vmatrix} \mod 26 = -36 \mod 26 = 16 .$$

$$\begin{pmatrix} 13 & 5 & 6 \\ 2 & 1 & 7 \\ 9 & 7 & 13 \end{pmatrix} \Rightarrow C_{12} = (-1)^{1+2}\begin{vmatrix} 2 & 7 \\ 9 & 13 \end{vmatrix} \mod 26 = 37 \mod 26 = 11 .$$

$$\begin{pmatrix} 13 & 5 & 6 \\ 2 & 1 & 7 \\ 9 & 7 & 13 \end{pmatrix} \Rightarrow C_{13} = (-1)^{1+3}\begin{vmatrix} 2 & 1 \\ 9 & 7 \end{vmatrix} \mod 26 = 5 \mod 26 = 5 .$$

$$\begin{pmatrix} 13 & 5 & 6 \\ 2 & 1 & 7 \\ 9 & 7 & 13 \end{pmatrix} \Rightarrow C_{21} = (-1)^{2+1}\begin{vmatrix} 5 & 6 \\ 7 & 13 \end{vmatrix} \mod 26 = -23 \mod 26 = 3 .$$

$$\begin{pmatrix} 13 & 5 & 6 \\ 2 & 1 & 7 \\ 9 & 7 & 13 \end{pmatrix} \quad \Rightarrow \quad C_{22} = (-1)^{2+2} \begin{vmatrix} 13 & 6 \\ 9 & 13 \end{vmatrix} \mod 26 = 115 \mod 26 = 11 \ .$$

$$\begin{pmatrix} 13 & 5 & 6 \\ 2 & 1 & 7 \\ 9 & 7 & 13 \end{pmatrix} \quad \Rightarrow \quad C_{23} = (-1)^{2+3} \begin{vmatrix} 13 & 5 \\ 9 & 7 \end{vmatrix} \mod 26 = -46 \mod 26 = 6 \ .$$

$$\begin{pmatrix} 13 & 5 & 6 \\ 2 & 1 & 7 \\ 9 & 7 & 13 \end{pmatrix} \quad \Rightarrow \quad C_{31} = (-1)^{3+1} \begin{vmatrix} 5 & 6 \\ 1 & 7 \end{vmatrix} \mod 26 = 29 \mod 26 = 3 \ .$$

$$\begin{pmatrix} 13 & 5 & 6 \\ 2 & 1 & 7 \\ 9 & 7 & 13 \end{pmatrix} \quad \Rightarrow \quad C_{32} = (-1)^{3+2} \begin{vmatrix} 13 & 6 \\ 2 & 7 \end{vmatrix} \mod 26 = -79 \mod 26 = 25 \ .$$

$$\begin{pmatrix} 13 & 5 & 6 \\ 2 & 1 & 7 \\ 9 & 7 & 13 \end{pmatrix} \quad \Rightarrow \quad C_{33} = (-1)^{3+3} \begin{vmatrix} 13 & 5 \\ 2 & 1 \end{vmatrix} \mod 26 = 3 \mod 26 = 3 \ .$$

$$C = \begin{pmatrix} C_{11} & C_{12} & C_{13} \\ C_{21} & C_{22} & C_{23} \\ C_{31} & C_{32} & C_{33} \end{pmatrix} = \begin{pmatrix} 16 & 11 & 5 \\ 3 & 11 & 6 \\ 3 & 25 & 3 \end{pmatrix} \ .$$

$$\text{adj}(A) = C^t = \begin{pmatrix} 16 & 3 & 3 \\ 11 & 11 & 25 \\ 5 & 6 & 3 \end{pmatrix} \ .$$

$$k^{-1} \mod 26 = |k|^{-1}\text{adj}(k) \ .$$

$$|k|^{-1} \mod 26 = 7^{-1} \mod 26 = 15 \ .$$

$$k^{-1} = 15 \begin{pmatrix} 16 & 3 & 3 \\ 11 & 11 & 25 \\ 5 & 6 & 3 \end{pmatrix} = \begin{pmatrix} 240 & 45 & 45 \\ 165 & 165 & 375 \\ 75 & 90 & 45 \end{pmatrix} \mod 26 = \begin{pmatrix} 6 & 19 & 19 \\ 9 & 9 & 11 \\ 23 & 12 & 19 \end{pmatrix}$$

$$(7, 21, 5) \cdot k^{-1} = (346, 382, 459) \mod 26 = (8, 18, 17)$$

$$(3, 3, 15) \cdot k^{-1} = (390, 264, 375) \mod 26 = (0, 4, 11)$$

$y \in C$	H	V	F	D	D	P
$y \in \mathbb{Z}_{26}$	7	21	5	3	3	15
$x \in \mathbb{Z}_{26}$	8	18	17	0	4	11
$x \in C$	i	s	r	a	e	l

שאלה 3 הכלל מפענח הוא

$$d_k(y) = a^{-1}(y-b) \mod 26$$

$a^{-1} \mod 26 = 5^{-1} \mod 26 = 21$. לכן

$$d_k(y) = 21(y-17) \mod 26 = 21y - 357 \mod 26 .$$

$357\%26 = 357 - 26\left\lfloor \frac{357}{26} \right\rfloor = 357 - 26(13) = 19$ לכן $(-357)\%26 = 26 - (357\%26) = 26 - 19 = 7$ לכן
$-289 \mod 26 = 7$. מכאן

$$d_k(y) = 21y + 7 .$$

$y \in C$	I	A	F	D	X	F	U	U	W	L	F	E	I	A	L	L	C	R	Z
$y \in \mathbb{Z}_{26}$	8	0	5	3	23	5	20	20	22	11	5	4	8	0	11	11	2	17	25
$x \in \mathbb{Z}_{26}$	19	7	8	18	22	8	11	11	1	4	8	13	19	7	4	4	23	0	12
$x \in P$	t	h	i	s	w	i	l	l	b	e	i	n	t	h	e	e	x	a	m

שאלה 4

x	1	2	3	4
$\pi^{-1}(x)$	1	4	3	2

$y \in C$	C	E	D	O	B	A	E	R	K	G	N	I
$y \in \mathbb{Z}_{26}$	2	4	3	14	1	0	4	17	10	6	13	8
$x \in \mathbb{Z}_{26}$	2	14	3	4	1	17	4	0	10	8	13	6
$x \in P$	c	o	d	e	b	r	e	a	k	i	n	g

שאלה 5 הכלל מפענח הוא

$$d_k(y) = a^{-1}(y-b) \mod 26$$

$a^{-1} \mod 26 = 5^{-1} \mod 26 = 21$. לכן

$$d_k(y) = 21(y-17) \mod 26 = 21y - 357 \mod 26 .$$

$357\%26 = 357 - 26\left\lfloor \frac{357}{26} \right\rfloor = 357 - 26(13) = 19$ לכן $(-357)\%26 = 26 - (357\%26) = 26 - 19 = 7$ לכן
$-289 \mod 26 = 7$. מכאן

$$d_k(y) = 21y + 7 .$$

$y \in C$	I	A	F	D	X	F	U	U	W	L	F	E	I	A	L	L	C	R	Z
$y \in \mathbb{Z}_{26}$	8	0	5	3	23	5	20	20	22	11	5	4	8	0	11	11	2	17	25
$x \in \mathbb{Z}_{26}$	19	7	8	18	22	8	11	11	1	4	8	13	19	7	4	4	23	0	12
$x \in P$	t	h	i	s	w	i	l	l	b	e	i	n	t	h	e	e	x	a	m

שאלה 6

$$d_k(y_1y_2y_3y_4y_5) = (x_1 - 6, x_2 - 17, x_3 - 4, x_4 - 4, x_5 - 13) \mod 26 .$$

$y \in C$	Z	F	S	X	U	H	I	Y	W	U
$y \in \mathbb{Z}_{26}$	25	5	18	23	20	7	8	24	22	20
$d_k(y)$	19	14	14	19	7	1	17	20	18	7
$x \in P$	t	o	o	t	h	b	r	u	s	h

שאלה 7

x	1	2	3	4
$\pi^{-1}(x)$	1	4	3	2

$y \in C$	C	E	D	O	B	A	E	R	K	G	N	I
$y \in \mathbb{Z}_{26}$	2	4	3	14	1	0	4	17	10	6	13	8
$x \in \mathbb{Z}_{26}$	2	14	3	4	1	17	4	0	10	8	13	6
$x \in P$	c	o	d	e	b	r	e	a	k	i	n	g

שאלה 8

הכלל מפענח הוא

$$d_k(y) = a^{-1}(y-b) \mod 26$$

$a^{-1} \mod 26 = 5^{-1} \mod 26 = 21$. לכן

$$d_k(y) = 21(y-17) \mod 26 = 21y - 357 \mod 26 \ .$$

$357\%26 = 357 - 26\left\lfloor \frac{357}{26} \right\rfloor = 357 - 26(13) = 19$ לכן $(-357)\%26 = 26 - (357\%26) = 26 - 19 = 7$ לכן
$-289 \mod 26 = 7$. מכאן

$$d_k(y) = 21y + 7 \ .$$

$y \in C$	I	A	F	D	X	F	U	U	W	L	F	E	I	A	L	L	C	R	Z
$y \in \mathbb{Z}_{26}$	8	0	5	3	23	5	20	20	22	11	5	4	8	0	11	11	2	17	25
$x \in \mathbb{Z}_{26}$	19	7	8	18	22	8	11	11	1	4	8	13	19	7	4	4	23	0	12
$x \in P$	t	h	i	s	w	i	l	l	b	e	i	n	t	h	e	e	x	a	m

שאלה 9

$y \in C$	H	V	F	D	D	P
$y \in \mathbb{Z}_{26}$	7	21	5	3	3	15

דטרמיננטה של k היא $|k| = 7 \mod 26 = 7$.
$\gcd(7,26) = 1$ לכן המטריצה הפיכה ב- $\mathbb{Z}_{26}$.

$$\begin{pmatrix} \cancel{13} & \cancel{5} & \cancel{6} \\ 2 & 1 & 7 \\ 9 & 7 & 13 \end{pmatrix} \quad \Rightarrow \quad C_{11} = (-1)^{1+1}\begin{vmatrix} 1 & 7 \\ 7 & 13 \end{vmatrix} \mod 26 = -36 \mod 26 = 16 \ .$$

$$\begin{pmatrix} 13 & 5 & 6 \\ 2 & 1 & 7 \\ 9 & 7 & 13 \end{pmatrix} \quad \Rightarrow \quad C_{12} = (-1)^{1+2} \begin{vmatrix} 2 & 7 \\ 9 & 13 \end{vmatrix} \mod 26 = 37 \mod 26 = 11 \ .$$

$$\begin{pmatrix} 13 & 5 & 6 \\ 2 & 1 & 7 \\ 9 & 7 & 13 \end{pmatrix} \quad \Rightarrow \quad C_{13} = (-1)^{1+3} \begin{vmatrix} 2 & 1 \\ 9 & 7 \end{vmatrix} \mod 26 = 5 \mod 26 = 5 \ .$$

$$\begin{pmatrix} 13 & 5 & 6 \\ 2 & 1 & 7 \\ 9 & 7 & 13 \end{pmatrix} \quad \Rightarrow \quad C_{21} = (-1)^{2+1} \begin{vmatrix} 5 & 6 \\ 7 & 13 \end{vmatrix} \mod 26 = -23 \mod 26 = 3 \ .$$

$$\begin{pmatrix} 13 & 5 & 6 \\ 2 & 1 & 7 \\ 9 & 7 & 13 \end{pmatrix} \quad \Rightarrow \quad C_{22} = (-1)^{2+2} \begin{vmatrix} 13 & 6 \\ 9 & 13 \end{vmatrix} \mod 26 = 115 \mod 26 = 11 \ .$$

$$\begin{pmatrix} 13 & 5 & 6 \\ 2 & 1 & 7 \\ 9 & 7 & 13 \end{pmatrix} \quad \Rightarrow \quad C_{23} = (-1)^{2+3} \begin{vmatrix} 13 & 5 \\ 9 & 7 \end{vmatrix} \mod 26 = -46 \mod 26 = 6 \ .$$

$$\begin{pmatrix} 13 & 5 & 6 \\ 2 & 1 & 7 \\ 9 & 7 & 13 \end{pmatrix} \quad \Rightarrow \quad C_{31} = (-1)^{3+1} \begin{vmatrix} 5 & 6 \\ 1 & 7 \end{vmatrix} \mod 26 = 29 \mod 26 = 3 \ .$$

$$\begin{pmatrix} 13 & 5 & 6 \\ 2 & 1 & 7 \\ 9 & 7 & 13 \end{pmatrix} \quad \Rightarrow \quad C_{32} = (-1)^{3+2} \begin{vmatrix} 13 & 6 \\ 2 & 7 \end{vmatrix} \mod 26 = -79 \mod 26 = 25 \ .$$

$$\begin{pmatrix} 13 & 5 & 6 \\ 2 & 1 & 7 \\ 9 & 7 & 13 \end{pmatrix} \quad \Rightarrow \quad C_{33} = (-1)^{3+3} \begin{vmatrix} 13 & 5 \\ 2 & 1 \end{vmatrix} \mod 26 = 3 \mod 26 = 3 \ .$$

$$C = \begin{pmatrix} C_{11} & C_{12} & C_{13} \\ C_{21} & C_{22} & C_{23} \\ C_{31} & C_{32} & C_{33} \end{pmatrix} = \begin{pmatrix} 16 & 11 & 5 \\ 3 & 11 & 6 \\ 3 & 25 & 3 \end{pmatrix} \ .$$

$$\text{adj}(A) = C^t = \begin{pmatrix} 16 & 3 & 3 \\ 11 & 11 & 25 \\ 5 & 6 & 3 \end{pmatrix} \ .$$

$$k^{-1} \mod 26 = |k|^{-1}\text{adj}(k) \ .$$

$$|k|^{-1} \mod 26 = 7^{-1} \mod 26 = 15 \ .$$

$$k^{-1} = 15 \begin{pmatrix} 16 & 3 & 3 \\ 11 & 11 & 25 \\ 5 & 6 & 3 \end{pmatrix} = \begin{pmatrix} 240 & 45 & 45 \\ 165 & 165 & 375 \\ 75 & 90 & 45 \end{pmatrix} \mod 26 = \begin{pmatrix} 6 & 19 & 19 \\ 9 & 9 & 11 \\ 23 & 12 & 19 \end{pmatrix}$$

$$(7,21,5)\cdot k^{-1} = (346,382,459) \mod 26 = (8,18,17)$$

$$(3,3,15)\cdot k^{-1} = (390,264,375) \mod 26 = (0,4,11)$$

y $\in C$	H	V	F	D	D	P
$y \in \mathbb{Z}_{26}$	7	21	5	3	3	15
$x \in \mathbb{Z}_{26}$	8	18	17	0	4	11
x $\in C$	i	s	r	a	e	l

שאלה 10

x	1	2	3	4
$\pi^{-1}(x)$	1	4	3	2

y $\in C$	C	E	D	O	B	A	E	R	K	G	N	I
$y \in \mathbb{Z}_{26}$	2	4	3	14	1	0	4	17	10	6	13	8
$x \in \mathbb{Z}_{26}$	2	14	3	4	1	17	4	0	10	8	13	6
x $\in P$	c	o	d	e	b	r	e	a	k	i	n	g

שאלה 11

$$d_k\left(y_1y_2y_3y_4y_5\right) = (x_1-6, x_2-17, x_3-4, x_4-4, x_5-13) \mod 26\ .$$

y $\in C$	Z	F	S	X	U	H	I	Y	W	U
$y \in \mathbb{Z}_{26}$	25	5	18	23	20	7	8	24	22	20
$d_k(y)$	19	14	14	19	7	1	17	20	18	7
x $\in P$	t	o	o	t	h	b	r	u	s	h

שאלה 13

y $\in C$	V	W	D	U	Z	D	U	V
$y \in C$	21	22	3	20	25	3	20	21
$x = y - 0 \in P$	21	22	3	20	25	3	20	21
x $\in P$	v	w	d	u	z	d	u	v
$x = y - 1 \in P$	20	21	2	19	24	2	19	20
x $\in P$	u	v	c	t	y	c	t	u
$x = y - 2 \in P$	19	20	1	18	23	1	18	19
x $\in P$	t	u	b	s	x	b	s	t
$x = y - 3 \in P$	18	19	0	17	22	0	17	18
x $\in P$	s	t	a	r	w	a	r	s

המפתח הוא 3 והטקסט גלוי הוא

starwars

שאלה 14

y $\in C$	T	G	E	E	M	N	E	L	N	N	T	D	R	O	E	O
$y \in \mathbb{Z}_{26}$	19	6	4	4	12	13	4	11	13	13	19	3	17	14	4	14

y $\in C$	A	A	H	D	O	E	T	C	S	H	A	E	I	R	L	M
$y \in \mathbb{Z}_{26}$	0	0	7	3	14	4	19	2	18	7	0	4	8	17	11	12

נפרק את האותיות לתת-קבוצות מאורך $m = 8$ (לפי האורך של התמורה).
נפעיל את התמורה ההופכית:

y $\in C$	T	G	E	E	M	N	E	L	N	N	T	D	R	O	E	O
$y \in \mathbb{Z}_{26}$	19	6	4	4	12	13	4	11	13	13	19	3	17	14	4	14

y $\in C$	A	A	H	D	O	E	T	C	S	H	A	E	I	R	L	M
$y \in \mathbb{Z}_{26}$	0	0	7	3	14	4	19	2	18	7	0	4	8	17	11	12

i	1	2	3	4	5	6	7	8
$\pi^{-1}(i)$	2	4	6	1	8	3	5	7

y $\in C$	T	G	E	E	M	N	E	L	N	N	T	D	R	O	E	O
$y \in \mathbb{Z}_{26}$	19	6	4	4	12	13	4	11	13	13	19	3	17	14	4	14
$x = \pi^{-1}(y)$	6	4	13	19	11	4	12	4	13	3	14	13	14	19	17	4

y $\in C$	A	A	H	D	O	E	T	C	S	H	A	E	I	R	L	M
$y \in \mathbb{Z}_{26}$	0	0	7	3	14	4	19	2	18	7	0	4	8	17	11	12
$x = \pi^{-1}(y)$	0	3	4	0	2	7	14	19	7	4	17	18	12	0	8	11

y $\in C$	T	G	E	E	M	N	E	L	N	N	T	D	R	O	E	O
$y \in \mathbb{Z}_{26}$	19	6	4	4	12	13	4	11	13	13	19	3	17	14	4	14
$x = \pi^{-1}(y)$	6	4	13	19	11	4	12	4	13	3	14	13	14	19	17	4
x $\in P$	g	e	n	t	l	e	m	e	n	d	o	n	o	t	r	e

y $\in C$	A	A	H	D	O	E	T	C	S	H	A	E	I	R	L	M
$y \in \mathbb{Z}_{26}$	0	0	7	3	14	4	19	2	18	7	0	4	8	17	11	12
$x = \pi^{-1}(y)$	0	3	4	0	2	7	14	19	7	4	17	18	12	0	8	11
x $\in P$	a	d	e	a	c	h	o	t	h	e	r	s	m	a	i	l

gentlemandonotreadeachothersmail

שאלה 15

$$|k| = 1 \cdot \begin{vmatrix} 0 & 1 \\ 0 & 1 \end{vmatrix} - 3 \begin{vmatrix} 0 & 1 \\ 3 & 1 \end{vmatrix} + 0 \begin{vmatrix} 0 & 0 \\ 3 & 0 \end{vmatrix} = 9 \ .$$

$\gcd(9, 26) = 1$ לכן המטריצה הפיכה ב- $\mathbb{Z}_{26}$.

$$\begin{pmatrix} 1 & 3 & 0 \\ 0 & 0 & 1 \\ 3 & 0 & 1 \end{pmatrix} \quad \Rightarrow \quad C_{11} = (-1)^{1+1} \begin{vmatrix} 0 & 1 \\ 0 & 1 \end{vmatrix} = 0 \ .$$

$$\begin{pmatrix} 1 & 3 & 0 \\ 0 & 0 & 1 \\ 3 & 0 & 1 \end{pmatrix} \quad \Rightarrow \quad C_{12} = (-1)^{1+2} \begin{vmatrix} 0 & 1 \\ 3 & 1 \end{vmatrix} = 3 \ .$$

$$\begin{pmatrix} 1 & 3 & 0 \\ 0 & 0 & 1 \\ 3 & 0 & 1 \end{pmatrix} \quad \Rightarrow \quad C_{13} = (-1)^{1+3} \begin{vmatrix} 0 & 0 \\ 3 & 0 \end{vmatrix} = 0 \ .$$

$$\begin{pmatrix} 1 & 3 & 0 \\ 0 & 0 & 1 \\ 3 & 0 & 1 \end{pmatrix} \quad \Rightarrow \quad C_{21} = (-1)^{2+1} \begin{vmatrix} 3 & 0 \\ 0 & 1 \end{vmatrix} = -3 \ .$$

$$\begin{pmatrix} 1 & 3 & 0 \\ 0 & 0 & 1 \\ 3 & 0 & 1 \end{pmatrix} \quad \Rightarrow \quad C_{22} = (-1)^{2+2} \begin{vmatrix} 1 & 0 \\ 3 & 1 \end{vmatrix} = 1 \ .$$

$$\begin{pmatrix} 1 & 3 & 0 \\ 0 & 0 & 1 \\ 3 & 0 & 1 \end{pmatrix} \quad \Rightarrow \quad C_{23} = (-1)^{2+3} \begin{vmatrix} 1 & 3 \\ 3 & 0 \end{vmatrix} = 9 \ .$$

$$\begin{pmatrix} 1 & 3 & 0 \\ 0 & 0 & 1 \\ 3 & 0 & 1 \end{pmatrix} \quad \Rightarrow \quad C_{31} = (-1)^{3+1} \begin{vmatrix} 3 & 0 \\ 0 & 1 \end{vmatrix} = 3 \ .$$

$$\begin{pmatrix} 1 & 3 & 0 \\ 0 & 0 & 1 \\ 3 & 0 & 1 \end{pmatrix} \quad \Rightarrow \quad C_{32} = (-1)^{3+2} \begin{vmatrix} 1 & 0 \\ 0 & 1 \end{vmatrix} = -1 \ .$$

$$\begin{pmatrix} 1 & 3 & 0 \\ 0 & 0 & 1 \\ 3 & 0 & 1 \end{pmatrix} \quad \Rightarrow \quad C_{33} = (-1)^{3+3} \begin{vmatrix} 1 & 3 \\ 0 & 0 \end{vmatrix} = 0 \ .$$

$$C = \begin{pmatrix} C_{11} & C_{12} & C_{13} \\ C_{21} & C_{22} & C_{23} \\ C_{31} & C_{32} & C_{33} \end{pmatrix} = \begin{pmatrix} 0 & 3 & 0 \\ -3 & 1 & 9 \\ 3 & -1 & 0 \end{pmatrix}$$

$$\text{adj}(A) = C^t = \begin{pmatrix} 0 & -3 & 3 \\ 3 & 1 & -1 \\ 0 & 9 & 0 \end{pmatrix} \mod 26 = \begin{pmatrix} 0 & 23 & 3 \\ 3 & 1 & 25 \\ 0 & 9 & 0 \end{pmatrix} \in \mathbb{Z}_{26}^{3\times 3} \ .$$

$$A^{-1} = |A|^{-1}\text{adj}(A) \ .$$

$$|A|^{-1} = 9^{-1} = 3 \in \mathbb{Z}_{26}$$

לפיכך

$$\begin{aligned} A^{-1} =& |A|^{-1}\text{adj}(A) \\ =& 3 \cdot \begin{pmatrix} 0 & 23 & 3 \\ 3 & 1 & 25 \\ 0 & 9 & 0 \end{pmatrix} \mod 26 \\ =& \begin{pmatrix} 0 & 69 & 9 \\ 9 & 3 & 75 \\ 0 & 27 & 0 \end{pmatrix} \mod 26 \\ =& \begin{pmatrix} 0 & 17 & 9 \\ 9 & 3 & 23 \\ 0 & 1 & 0 \end{pmatrix} \end{aligned}$$

א) <u>שלב 1:</u>

נעביר את האותיות של הטקסט גלוי לערכים של $\mathbb{Z}_{26}$:

y $\in C$	V	A	Z	M	J	R
$y \in \mathbb{Z}_{26}$	21	0	25	12	9	17

<u>שלב 2:</u>

נפרק את הטבלה של התווים של הטקסט מוצפן יחד עם הערכים המתאימים של $\mathbb{Z}_{26}$ לתת-קבוצות של $m = 3$ תווים:

y $\in C$	V	A	Z	M	J	R
$y \in \mathbb{Z}_{26}$	21	0	25	12	9	17

<u>שלב 3:</u>

עבור כל תת-קבוצה המתקבל נחשב

$$\begin{aligned} \begin{pmatrix} x_1 & x_2 & x_3 \end{pmatrix} &= \begin{pmatrix} y_1 & y_2 & y_3 \end{pmatrix} k^{-1} \mod 26 \\ &= \begin{pmatrix} y_1 & y_2 & y_3 \end{pmatrix} \begin{pmatrix} 0 & 17 & 9 \\ 9 & 3 & 23 \\ 0 & 1 & 0 \end{pmatrix} \mod 26 \end{aligned}$$

עבור התת-קבוצה הראשונה נקבל

$$\begin{aligned}\begin{pmatrix}x_1 & x_2 & x_3\end{pmatrix} &= \begin{pmatrix}21 & 0 & 25\end{pmatrix}\begin{pmatrix}0 & 17 & 9\\ 9 & 3 & 23\\ 0 & 1 & 0\end{pmatrix} \mod 26\\ &= \begin{pmatrix}0 & 382 & 189\end{pmatrix} \mod 26\\ &= \begin{pmatrix}0 & 18 & 7\end{pmatrix}\end{aligned}$$

עבור התת-קבוצה השנייה נקבל

$$\begin{aligned}\begin{pmatrix}x_1 & x_2 & x_3\end{pmatrix} &= \begin{pmatrix}12 & 9 & 17\end{pmatrix}\begin{pmatrix}0 & 17 & 9\\ 9 & 3 & 23\\ 0 & 1 & 0\end{pmatrix} \mod 26\\ &= \begin{pmatrix}81 & 248 & 315\end{pmatrix} \mod 26\\ &= \begin{pmatrix}3 & 14 & 3\end{pmatrix}\end{aligned}$$

$y \in C$	V	A	Z	M	J	R
$y \in \mathbb{Z}_{26}$	21	0	25	12	9	17
$x \in \mathbb{Z}_{26}$	0	18	7	3	14	3

<u>שלב 5:</u>

נעבור את הערכים $y \in \mathbb{Z}_{26}$ לאותיות של הטקסט מוצפן:

$y \in C$	V	A	Z	M	J	R
$y \in \mathbb{Z}_{26}$	21	0	25	12	9	17
$x \in \mathbb{Z}_{26}$	0	18	7	3	14	3
$x \in \mathbb{Z}_{26}$	a	s	h	d	o	d

הטקסט גלוי המתקבל הוא

ashdod

ב) <u>שלב 1:</u>

נעביר את האותיות של הטקסט גלוי לערכים של $\mathbb{Z}_{26}$:

$y \in C$	N	D	I	M	Z	Z	E	M	V
$y \in \mathbb{Z}_{26}$	13	3	8	12	25	25	4	12	21

<u>שלב 2:</u>

נפרק את הטבלה של התווים של הטקסט מוצפן יחד עם הערכים המתאימים של $\mathbb{Z}_{26}$ לתת-קבוצות של $m = 3$ תווים:

$y \in C$	N	D	I	M	Z	Z	E	M	V
$y \in \mathbb{Z}_{26}$	13	3	8	12	25	25	4	12	21

שלב 3:

עבור כל תת-קבוצה המתקבל נחשב

$$\begin{aligned}\begin{pmatrix}x_1 & x_2 & x_3\end{pmatrix} &= \begin{pmatrix}y_1 & y_2 & y_3\end{pmatrix} k^{-1} \mod 26\\ &= \begin{pmatrix}y_1 & y_2 & y_3\end{pmatrix}\begin{pmatrix}0 & 17 & 9\\ 9 & 3 & 23\\ 0 & 1 & 0\end{pmatrix} \mod 26\end{aligned}$$

עבור התת-קבוצה הראשונה נקבל

$$\begin{aligned}\begin{pmatrix}x_1 & x_2 & x_3\end{pmatrix} &= \begin{pmatrix}13 & 3 & 8\end{pmatrix}\begin{pmatrix}0 & 17 & 9\\ 9 & 3 & 23\\ 0 & 1 & 0\end{pmatrix} \mod 26\\ &= \begin{pmatrix}27 & 238 & 186\end{pmatrix} \mod 26\\ &= \begin{pmatrix}1 & 4 & 4\end{pmatrix}\end{aligned}$$

עבור התת-קבוצה השנייה נקבל

$$\begin{aligned}\begin{pmatrix}x_1 & x_2 & x_3\end{pmatrix} &= \begin{pmatrix}12 & 25 & 25\end{pmatrix}\begin{pmatrix}0 & 17 & 9\\ 9 & 3 & 23\\ 0 & 1 & 0\end{pmatrix} \mod 26\\ &= \begin{pmatrix}225 & 304 & 683\end{pmatrix} \mod 26\\ &= \begin{pmatrix}17 & 18 & 7\end{pmatrix}\end{aligned}$$

עבור התת-קבוצה השלישית נקבל

$$\begin{aligned}\begin{pmatrix}x_1 & x_2 & x_3\end{pmatrix} &= \begin{pmatrix}4 & 12 & 21\end{pmatrix}\begin{pmatrix}0 & 17 & 9\\ 9 & 3 & 23\\ 0 & 1 & 0\end{pmatrix} \mod 26\\ &= \begin{pmatrix}108 & 125 & 312\end{pmatrix} \mod 26\\ &= \begin{pmatrix}4 & 21 & 0\end{pmatrix}\end{aligned}$$

$\mathtt{y} \in C$	N	D	I	M	Z	Z	E	M	V
$y \in \mathbb{Z}_{26}$	13	3	8	12	25	25	4	12	21
$x \in \mathbb{Z}_{26}$	1	4	4	17	18	7	4	21	0

שלב 5:

נעבור את הערכים $y \in \mathbb{Z}_{26}$ לאותיות של הטקטס מוצפן:

$\mathtt{y} \in C$	N	D	I	M	Z	Z	E	M	V
$y \in \mathbb{Z}_{26}$	13	3	8	12	25	25	4	12	21
$x \in \mathbb{Z}_{26}$	1	4	4	17	18	7	4	21	0
$\mathtt{x} \in P$	b	e	e	r	s	h	e	v	a

הטקטס גלוי המתקבל הוא

beersheva

שאלה 16

$y \in C$	F	P	H	O	E	M	J	S	U	P	S	Z	Z	Y	J
$y \in \mathbb{Z}_{26}$	5	15	7	14	4	12	9	18	20	15	18	25	25	24	9

דטרמיננטה של k היא $|k| = -3 \mod 26 = 23$.
$\gcd(23, 26) = 1$ לכן המטריצה הפיכה ב- $\mathbb{Z}_{26}$.

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 11 & 9 & 8 \end{pmatrix} \Rightarrow C_{11} = (-1)^{1+1} \begin{vmatrix} 5 & 6 \\ 9 & 8 \end{vmatrix} \mod 26 = -14 \mod 26 = 12 .$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 11 & 9 & 8 \end{pmatrix} \Rightarrow C_{12} = (-1)^{1+2} \begin{vmatrix} 4 & 6 \\ 11 & 8 \end{vmatrix} \mod 26 = 24 \mod 26 = 8 .$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 11 & 9 & 8 \end{pmatrix} \Rightarrow C_{13} = (-1)^{1+3} \begin{vmatrix} 4 & 5 \\ 11 & 9 \end{vmatrix} \mod 26 = -19 \mod 26 = 7 .$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 11 & 9 & 8 \end{pmatrix} \Rightarrow C_{21} = (-1)^{2+1} \begin{vmatrix} 2 & 3 \\ 9 & 8 \end{vmatrix} = 11 .$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 11 & 9 & 8 \end{pmatrix} \Rightarrow C_{22} = (-1)^{2+2} \begin{vmatrix} 1 & 3 \\ 11 & 8 \end{vmatrix} \mod 26 = -25 \mod 26 = 1 .$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 11 & 9 & 8 \end{pmatrix} \Rightarrow C_{23} = (-1)^{2+3} \begin{vmatrix} 1 & 2 \\ 11 & 9 \end{vmatrix} = 13 .$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 11 & 9 & 8 \end{pmatrix} \Rightarrow C_{31} = (-1)^{3+1} \begin{vmatrix} 2 & 3 \\ 5 & 6 \end{vmatrix} \mod 26 = -3 \mod 26 = 23 .$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 11 & 9 & 8 \end{pmatrix} \Rightarrow C_{32} = (-1)^{3+2} \begin{vmatrix} 1 & 3 \\ 4 & 6 \end{vmatrix} = 6 .$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 11 & 9 & 8 \end{pmatrix} \Rightarrow C_{33} = (-1)^{3+3} \begin{vmatrix} 1 & 2 \\ 4 & 5 \end{vmatrix} \mod 26 = -3 \mod 26 = 23 .$$

$$C = \begin{pmatrix} C_{11} & C_{12} & C_{13} \\ C_{21} & C_{22} & C_{23} \\ C_{31} & C_{32} & C_{33} \end{pmatrix} = \begin{pmatrix} -14 & 34 & -19 \\ 11 & -25 & 13 \\ -3 & 6 & -3 \end{pmatrix} \mod 26 = \begin{pmatrix} 12 & 8 & 7 \\ 11 & 1 & 13 \\ 23 & 6 & 23 \end{pmatrix} .$$

$$\text{adj}(A) = C^t = \begin{pmatrix} 16 & 3 & 18 \\ 9 & 9 & 1 \\ 21 & 5 & 20 \end{pmatrix} \in \mathbb{Z}_{26}^{3\times 3} \ .$$

$$k^{-1} = |k|^{-1}\text{adj}(k) \ .$$

$$|k|^{-1} = 23^{-1} = 17 \in \mathbb{Z}_{26}$$

$$k^{-1} = 17 \begin{pmatrix} 16 & 3 & 18 \\ 9 & 9 & 1 \\ 21 & 5 & 20 \end{pmatrix} = \begin{pmatrix} 204 & 187 & 391 \\ 136 & 17 & 102 \\ 119 & 221 & 391 \end{pmatrix} = \begin{pmatrix} 22 & 5 & 1 \\ 6 & 17 & 24 \\ 15 & 13 & 1 \end{pmatrix}$$

$$(5,15,7)\cdot k^{-1} = (19,7,8) \ , \qquad (14,4,12)\cdot k^{-1} = (18,8,18) \ , \qquad (9,18,20)\cdot k^{-1} = (8,13,19) \ ,$$

$$(15,18,25)\cdot k^{-1} = (7,4,4) \ , \qquad (25,24,9)\cdot k^{-1} = (23,0,12) \ .$$

$y \in C$	F	P	H	O	E	M	J	S	U	P	S	Z	Z	Y	J
$y \in \mathbb{Z}_{26}$	5	15	7	14	4	12	9	18	20	15	18	25	25	24	9
$x \in \mathbb{Z}_{26}$	19	7	8	18	8	18	8	13	19	7	4	4	23	0	12
$x \in P$	t	h	i	s	i	s	i	n	t	h	e	e	x	a	m

שאלה 17

א)

x	1	2	3	4	5	6	7	8
$\pi^{-1}(x)$	2	4	6	1	8	3	5	7

$y \in C$	S	Q	I	U	O	E	N	T	M	F	H	R	E	O	F	T
$y \in \mathbb{Z}_{26}$	18	16	8	20	14	4	13	19	12	5	7	17	4	14	5	19

$y \in C$	L	I	X	N	A	A	M	E
$y \in \mathbb{Z}_{26}$	11	8	23	13	0	0	12	4

$y \in C$	S	Q	I	U	O	E	N	T	M	F	H	R	E	O	F	T
$y \in \mathbb{Z}_{26}$	18	16	8	20	14	4	13	19	12	5	7	17	4	14	5	19
$x \in \mathbb{Z}_{26}$	16	20	4	18	19	8	14	13	5	17	14	12	19	7	4	5
$x \in P$	q	u	e	s	t	i	o	n	f	r	o	m	t	h	e	f

$y \in C$	L	I	X	N	A	A	M	E
$y \in \mathbb{Z}_{26}$	11	8	23	13	0	0	12	4
$x \in \mathbb{Z}_{26}$	8	13	0	11	4	23	0	12
$x \in P$	i	n	a	l	e	x	a	m

שאלה 18

$y \in C$	Y	G	S	O	Y	N	G	S	U	U	T	O	Y	Z	N	K	H	K	Y	Z
$y \in \mathbb{Z}_{26}$	24	6	18	14	24	13	6	18	20	20	19	14	24	25	13	10	7	10	24	25
$d_6(y)$	18	0	12	8	18	7	0	12	14	14	13	8	18	19	7	4	1	4	18	19
$x \in P$	s	a	m	i	s	h	a	m	o	o	n	i	s	t	h	e	b	e	s	t

$y \in C$	I	U	R	R	K	M	K	O	T	O	Y	X	G	K	R
$y \in \mathbb{Z}_{26}$	8	20	17	17	10	12	10	14	19	14	24	23	6	10	17
$d_6(y)$	2	14	11	11	4	6	4	8	13	8	18	17	0	4	11
$x \in P$	c	o	l	l	e	g	e	i	n	i	s	r	a	e	l

שאלה 19

א) נתון המפתח $a = 5, b = 21$ בכלל מצפין $e_k(x) = ax + b$. אז הכלל מפענח הינו

$$d_k(y) = a^{-1}(y - b) = 5^{-1}(y - 21) \ .$$

ב- $\mathbb{Z}_{29}$, $5^{-1} = 6$ מכיוון ש- $5 \cdot 6 \mod 29 = 30 \mod 29 = 1$. לפיכך

$$d_k(y) = 6(y-21) = 6y-126 \mod 29 = 6y-4\cdot 29-10 \mod 29 = 6y-10 \mod 29 = 6y+19 \ .$$

לפיכך $a' = 6, b' = 19$.

ב)

$$d_k\left(e_k(x)\right) = 6\left(5x + 21\right)+19 \mod 29 = 30x+126+19 \mod 29 = 1\cdot x+145 \mod 29 = x+5\cdot 29 \mod 29 = x \ .$$