שיעור 3
הצפנים הבסיסיים

3.1 מושג של קריפטו-מערכת

אליס ובוב, לתקשר מעל גבי ערוץ תקשורת בלתי אמין (נאמר קו טלסון או דואר אלקרוני), ומבקשים ליהנות מסודיות. כלומר , הם מעוניינים ש שום גורם עוין, אוסקר, שעלול לצותת לשיחתם , לא יוכל להבין את תוכנה.

לשם כך משתמשים אליס ובוב בצופן (cryptosystem). אליס ובוב מסכימים ביניהם מראש על שיטה מסויימת להצפנה ועל מפתח, (key) שהוא ערך מספרי (או כמה ערכים מספריים). כעת , נניח שאליס מעוניינת לשלוח לבוב הודעה מסוימת. היא מצפינה encrypt את ההודעה בשיטה שהיא ובוב בחרו בה תוך כדי שימוש במפתח שהם קבעו. לאחר ההצפנה, ההודעה שינתה את צורתה. להודעה המקורית אנו קוראים טקסט גלוי (plaintext) ואילו ההודעה לאחר ההצפנה נקראת טקסט מוצפן (ciphertext). אליס שולחת את הטקסט המוצפן לבוב. בוב מפענח (decrypt) אותו ומשחזר את הטקסט הגלוי , המקורי. אוסקר, המצותת לערוץ , איננו יודע את ערכו של המפתח שנעשה בו שימוש (למרות ש י יתכן בהחלט ואף סביר להניח שהוא י ודע מהו הצופן ש השתמשו בו אליס ובוב).

הגדרה 3.1 צופן

צופן, (או לעתים קריפטו-מערכת) מוצג באמצעות קבוצה (P, C, K, E, D), כאשר:

1. E מסמן קבוצה של טקסט גלוי plaintext,
2. C מסמן קבוצה של טקסט מוצפן ciphertext,
3. K מסמן את מרחב המפתח keyspace,
4. לכל $k \in K$ יש שתי פונקציות: כלל מצפין $e \in E$ וכלל מפענח $d \in D$:

$$e : P \to C \ , \qquad d : C \to P \ ,$$

כך ש-

$$d\left(e\left(x\right)\right) = x$$

לכל איבר של מרחב הטקסט גלוי $x \in P$.

נניח כי ההודעה הנשלחה על ידי אליס לבוב היא הרצף האותיות

$$X = x_1 x_2 \cdots x_n$$

עבור $n \geq 1$ טבעי, כאשר כל אות הוא אות של טקסט גלוי $x_i \in P$, $1 \leq i \leq n$. כל x_i מוצפן באמצעות הכלל הצפנה e_k אשר נקבעת מראש על על ידי המפתח k הנבחר. ז"א אליס מחשבת

$$y_i = e_k(x_i)$$

$1 \leq i \leq n$ ומקבלת את רצף אותיות מוצפנות

$$Y = y_1 y_2 \cdots y_n \ .$$

הרצף הזה נשלח מעל גבי הערוץ. כאשר בוב מקבל את Y הוא מפענח אותו באמצעות הפונקציה d_k וכך הוא מקבל הרצף אותיות של טקסט גלוי המקורי

$$X = x_1 x_2 \cdots x_n \ .$$

פונקציה הצפנה e_k חד-חד ערכית. אחרת לא יהיה אפשרי לפענח את הרצף אותיות מוצפנות. הרי אם e_k לא חד-חד ערכית אז יכול להיות מצב ש-

$$y = e_k(x_1) = e_k(x_2)$$

כאשר $x_1 \neq x_2$ ואז לבוב לא יכול לדעת אם y ההפענחה של x_1 או x_2.

3.2 צופן ההזזה

הגדרה 3.2 צופן ההזזה

יהיו $P = C = K = \mathbb{Z}_{26}$. עבור $0 \leq k \leq 25$ נגדיר

$$e_k(x) = (x + k) \ \% \ 26 \ , \qquad x \in \mathbb{Z}_{26}$$

ו-

$$d_k(y) = (y - k) \ \% \ 26 \ , \qquad y \in \mathbb{Z}_{26} \ .$$

צופן ההזזה מוגדר מעל $\mathbb{Z}_{26}$ בגלל שיש 26 אותיות באלפבית.

במטרה להשתמש בצופן ההזזה כדי להצפין טקסט גלוי, קודם כל נגדיר התאמה בין אותיות של האלפבית ומספרים של $\mathbb{Z}_{26}$:

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

דוגמה 3.1

נתון טקסט גלוי

`shamoon`

נניח כי המפתח בשביל צופן הזזה הוא $k = 11$. מצאו את הטקסט מוצפן.

פתרון:

שלב 1) נמיר את הטקסט גלוי לרצף מספרים לפי הסדר של האלפבית:

x $\in P$	s	h	a	m	o	o	n
$x \in \mathbb{Z}_{26}$	18	7	0	12	14	14	13

שלב 2) נוסיף 11 לכל ערך ולעבור את הערך המתקבל לאיבר ב- $\mathbb{Z}_{26}$:

x $\in P$	s	h	a	m	o	o	n
$x \in \mathbb{Z}_{26}$	18	7	0	12	14	14	13
$y \in \mathbb{Z}_{26}$	3	18	11	23	25	25	24

שלב 3) נעבור את הרצץ מספרים לטקסט מוצפן:

$\mathtt{x} \in P$	s	h	a	m	o	o	n
$x \in \mathbb{Z}_{26}$	18	7	0	12	14	14	13
$y \in \mathbb{Z}_{26}$	3	18	11	23	25	25	24
$\mathtt{y} \in C$	D	S	L	X	Z	Z	Y

הטקטס מוצפן המתקבל הוא

DSLXZZY

■

דוגמה 3.2

נתון הטקסט מוצפן על ידי צופן קיסר (צופן הזזה):

UJCNQO

מצאו את הטקסט גלוי.

פתרון:
ננסה לפענח את הטקסט מוצפן בעזרת הצופן הזזה עם המפתחות $d_0 = 0, d_1 = 1, d_2 = 2 \ldots$ בתור.

$\mathtt{y} \in C$	U	J	C	N	Q	O
$y \in \mathbb{Z}_{26}$	20	9	2	13	16	14
$y - d_1 \in \mathbb{Z}_{26}$	19	8	1	12	15	13
$\mathtt{x} \in P$	t	i	b	m	p	n
$y - d_2 \in \mathbb{Z}_{26}$	18	7	0	11	14	12
$\mathtt{x} \in P$	s	h	a	l	o	m

■

דוגמה 3.3

נתון הטקסט מוצפן הבא:

QRQXFJANHXD

מצאו את הטסטק גלוי

פתרון:
ננסה לפענח את הטקסט מוצפן בעזרת הצופן הזזה עם המפתחות $d_0, d_1, \ldots$ בתור.

d_0 qrqxfjanhxd

d_1 pqpweizmgwc

d_2 opovdhylfvb

d_3 nonucgxkeua

d_4 mnmtbfwjdtz

d_5 lmlsaevicsy

d_6 klkrzduhbrx

d_7 jkjqyctgaqw

d_8 ijipxbsfzpv

d_9 hihowareyou

בשלב זה מצאנו את הטקסט גלוי:

hihowareyou .

המפתח הוא $k = 9$. ■

3.3 צופן ההחלפה

הגדרה 3.3 (substitution cypher) צופן ההחלפה

בצופן ההחלפה, $P = C = \mathbb{Z}_{26}$.

K מורכב מכל ההחלפות האפשריות של ה- 26 סמלים $0, 1, 2, \ldots, 25$.

עבור כל החלפה $\pi \in K$ נגדיר כלל מצפין

$$e_\pi(x) = \pi(x)$$

ונגדיר כלל מפענח

$$d_\pi(x) = \pi^{-1}(x) \ ,$$

כאשר π^{-1} ההחלפה ההופכית של π.

קיימות $26! = 4.032914611266056355 84 \times 10^{26}$ החלפות אפשרויות.

דוגמה 3.4

הצופן החלפה π נתון ע"י הטבלה

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
Z	T	B	A	H	P	O	G	X	Q	W	Y	N	S	F	L	R	C	V	M	U	E	K	J	D	I

בפרט,

$$e_\pi(\mathtt{a}) = \mathtt{Z}\ , \qquad e_\pi(\mathtt{b}) = \mathtt{T}\ , \ldots$$

וכן הלאה. הכלל המפענח הוא ההחלפה ההופכית, π^{-1} אשר נתונה באמצעות הטבלה

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
d	c	r	y	v	o	h	e	z	x	w	p	t	m	g	f	j	q	n	b	u	s	k	i	l	a

בפרט, ו-

$$d_\pi(\mathtt{A}) = \mathtt{d}\ , \qquad d_\pi(\mathtt{B}) = \mathtt{c}\ , \ldots$$

וכן הלאה.
נתון הטקסט מוצפן

GHYYF

מצאו את הטקטס גלוי.

פתרון:

$$d_\pi(\mathtt{G}) = \mathtt{h}\ , \quad d_\pi(\mathtt{H}) = \mathtt{e}\ , \quad d_\pi(\mathtt{Y}) = \mathtt{l}\ , \quad d_\pi(\mathtt{F}) = \mathtt{o}\ .$$

לכן הטקסט גלוי הינו

hello .

■

דוגמה 3.5

למטה יש דוגמה של צופן החלפה. ההחלפה עצמה, π נתונה ע"י הטבלה

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
X	N	Y	A	H	P	O	G	Z	Q	W	B	T	S	F	L	R	C	V	M	U	E	K	J	D	I

בפרט,

$$e_\pi(\mathtt{a}) = \mathtt{X}\ , \qquad e_\pi(\mathtt{b}) = \mathtt{N}\ ,$$

וכן הלאה. הכלל המפענח הוא ההחלפה ההופכית, π^{-1} אשר נתונה באמצעות הטבלה

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
d	l	r	y	v	o	h	e	z	x	w	p	t	b	g	f	j	q	n	m	u	s	k	a	c	i

בפרט,

$$d_\pi(\mathtt{A}) = \mathtt{d}\ , \qquad d_\pi(\mathtt{B}) = \mathtt{l}\ ,$$

וכן הלאה.

דוגמה 3.6

נתון הטקסט מוצפן הבא:

MGZVYZLGHCMHJMYXSSFMNHAHYCDLMHA

והכלל מפענח של דוגמה 3.5. מצאו את הטקסט גלוי.

פתרון:
כלל מפענח :

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
d	l	r	y	v	o	h	e	z	x	w	p	t	b	g	f	j	q	n	m	u	s	k	a	c	i

ז"א

$$
\begin{aligned}
d_\pi(\mathtt{M}) &= \mathtt{t}\ ,\\
d_\pi(\mathtt{G}) &= \mathtt{h}\ ,\\
d_\pi(\mathtt{Z}) &= \mathtt{i}\ ,\\
d_\pi(\mathtt{V}) &= \mathtt{s}\ ,\\
d_\pi(\mathtt{Y}) &= \mathtt{c}\ ,\\
d_\pi(\mathtt{L}) &= \mathtt{p}\ ,\\
d_\pi(\mathtt{H}) &= \mathtt{e}\ ,\\
d_\pi(\mathtt{C}) &= \mathtt{r}\ ,\\
d_\pi(\mathtt{M}) &= \mathtt{t}\ ,\\
d_\pi(\mathtt{J}) &= \mathtt{x}\ ,\\
d_\pi(\mathtt{Y}) &= \mathtt{c}\ ,\\
d_\pi(\mathtt{X}) &= \mathtt{a}\ ,\\
d_\pi(\mathtt{S}) &= \mathtt{n}\ ,\\
d_\pi(\mathtt{S}) &= \mathtt{n}\ ,\\
d_\pi(\mathtt{F}) &= \mathtt{o}\ ,\\
d_\pi(\mathtt{M}) &= \mathtt{t}\ ,\\
d_\pi(\mathtt{N}) &= \mathtt{b}\ ,\\
d_\pi(\mathtt{H}) &= \mathtt{e}\ ,\\
d_\pi(\mathtt{A}) &= \mathtt{d}\ ,\\
d_\pi(\mathtt{H}) &= \mathtt{e}\ ,\\
d_\pi(\mathtt{Y}) &= \mathtt{c}\ ,\\
d_\pi(\mathtt{C}) &= \mathtt{r}\ ,\\
d_\pi(\mathtt{D}) &= \mathtt{y}\ ,\\
d_\pi(\mathtt{L}) &= \mathtt{p}\ ,\\
d_\pi(\mathtt{M}) &= \mathtt{t}\ ,\\
d_\pi(\mathtt{H}) &= \mathtt{e}\ ,\\
d_\pi(\mathtt{A}) &= \mathtt{d}\ ,
\end{aligned}
$$

קיבלנו את הטקסט גלוי

thisciphertextcannotbedecrypted

■

3.4 צופן האפיני

באופן כללי, בצופן האפיני הכלל מצפין נתון ע"י הפונקציה מצורה

$$e(x) = (ax + b) \ \% \ 26 \ .$$

עבור $a, b \in \mathbb{Z}_{26}$. פונקציה מסוג זה נקראת **פונקציה אפינית**.

כדי שפענוח יהיה אפשרי נדרוש כי הפונקציה הזאת חד-חד-ערכית. במילים אחרות, נדרוש כי לביטוי (יחס שקילות)

$$ax + b \equiv y \mod 26$$

יש פתרון יחיד ל-x.

למטה נוכיח כי אכן יש פתרון יחיד אם ורק אם $\gcd(a, 26) = 1$.

משפט 3.1

ליחס שקילות

$$ax + b \equiv y \mod 26$$

יש פתרון יחיד בשביל x אם ורק אם $\gcd(a, 26) = 1$.

הוכחה: (ראו גם הוכחה למשפט 2.9).

נניח כי יש פתרון יחיד. נוכיח דרך השלילה כי ו- $\gcd(a, 26) = 1$.

נניח כי $\gcd(a, 26) = d > 1$.

אם $x_1 = a^{-1}y$ פתרון ל- $ax \equiv y \mod 26$, אז גם $x_1 + \frac{26}{d}$ פתרון הסבר:

$$ax_1 + \frac{a26}{d} = ax_1 + k26 \equiv ax_1 \mod 26 \ ,$$

כאשר $k = \frac{a}{d}$. שלם.

בפרט, מכיוון ש- $d > 1$ אז $x_1 + \frac{26}{d} \not\equiv x_1 \mod 26$, ז"א קיימים שני פתרונות שונים, בסתירה לכך שהפתרון יחיד.

נניח כי $\gcd(a, 26) = 1$. נוכיח בשלילה כי הפתרון יחיד.
נניח כי קיים שני פתרונות שונים: $x_1 \not\equiv x_2 \mod 26$.

ז"א

$$ax_1 \equiv y \mod 26 \ , \qquad ax_2 \equiv y \mod 26 \ .$$

לכן

$$ax_1 \equiv ax_2 \mod 26 \ .$$

לכן

$$26 \mid ax_1 - ax_2 \ .$$

$\gcd(a, 26) = 1$ לפיכך

$$26 \mid x_1 - x_2 \ ,$$

ז"א

$$x_1 \equiv x_2 \mod 26 ,$$

בסתירה לכך ש- $x_1 \not\equiv x_2 \mod 26$.

■

דוגמה 3.7

בדקו אם הפונקציה

$$e(x) = 4x + 7 \mod 26$$

כלל מצפין תקין, כלומר בדקו אם קיים כלל מפענח.

פתרון:
$\gcd(4, 26) = 2$, אז הפונקציה $e(x) = 4x + 7 \mod 26$ אינה כלל מצפין תקין, בגלל שהיא לא חד-חד ערכית ולכן לא יכולה להיות כלל מצפין.

למשל, הפונקציה הזאת מחזירה הערכים הבאים בשביל x ו- $x + 13$:

$$e(x) = 4x + 7 \mod 26$$

בעוד

$$\begin{aligned} e(x + 13) =& 4(x + 13) + 7 \mod 26 \\ =& 4x + 52 + 7 \mod 26 \\ =& 4x + 2 \cdot 26 + 7 \mod 26 \\ =& 4x + 7 \mod 26 \end{aligned}$$

ז"א $e(x)$ מצפין את x ו- $x + 13$ לאותו אות מוצפן. ■

הגדרה 3.4 צופן האפיני

יהי $P = C = \mathbb{Z}_{26}$ ויהי

$$K = \left\{ a, b \in \mathbb{Z}_{26} \middle| \gcd(a, 26) = 1 \right\} .$$

עבור $k = (a, b) \in K$ ועבור $x \in \mathbb{Z}_{26}$ נגדיר כלל המצפין

$$e_k(x) = (ax + b) \mod 26 ,$$

ועבור $y \in \mathbb{Z}_{26}$ נגדיר כלל המענח

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

כלל 3.1

הפירוק לראשוניים של 26 הינו

$$26 = 2^1 13^2 .$$

לכן האיברים $a \in \mathbb{Z}_{26}$ עבורם $\gcd(a, 26) = 1$ הם

$$a = 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25 .$$

ז"א יש בדיוק 12 ערכים של a עבורם $\gcd(a, 26) = 1$.

המספר איברים ב- $\mathbb{Z}_{26}$ עבורם $\gcd(a,26)=1$ נובע מנוסחת אוילר (הגדרה 2.4):

$$\phi(26)=\left(2^1-2^0\right)\left(13^1-13^0\right)=12\ .$$

הפרמטר b מקבל כל איבר של $\mathbb{Z}_{26}$.
לפיכך לצופן האפיני יש $12\times 26=312$ מפתחות אפשריות.

דוגמה 3.8

נתון כלל מצפין של צופן אפיני בעל המפתח $k=(7,3)$ ($a=7, b=3$).

1) רשמו את כלל המצפין.

2) רשמו את כלל המפענח.

3) בדקו כי התנאי

מתקיים.

פתרון:

1) כלל המצפין הוא

$$e_k(x)=7x+3 \mod 26\ ,$$

2) כלל המפענח הוא

$$\begin{aligned} d_k(y) =& 7^{-1}(y-3) \mod 26\\ =& 15(y-3) \mod 26\\ =& 15y-45 \mod 26\\ =& 15y-19\\ =& 15y+7\ . \end{aligned}$$

3) נבדוק כי הכלל מפענח המתקבל מקיים $d_k\left(e_k(x)\right)=x$:

$$\begin{aligned} d_k\left(e_k(x)\right) =& d_k\left(7x+3\right) \mod 26\\ =& 15(7x+3)+7 \mod 26\\ =& 105x+45+7 \mod 26\\ =& 104x+x+52 \mod 26\\ =& 4\times 26x+x+52 \mod 26\\ =& x\ . \end{aligned}$$

■

דוגמה 3.9

בעזרת הצופן של דוגמה 3.8:

1) מצאו את הטקסט מוצפן של הטקסט גלוי

`hot` .

2) בדקו שהפעולה של הכלל מפענח על הטקסט מוצפן מחזיר את טקסט גלוי

`hot` .

פתרון:

סעיף 1) נעביר את הואתיות של `hot` לערכים של $\mathbb{Z}_{26}$:

$\texttt{x} \in P$	h	o	t
$x \in \mathbb{Z}_{26}$	7	14	19

נפעיל את הכלל מצפין על הערכים x:

$$\begin{aligned} e_k(7) =& 7 \times 7 + 3 \mod 26 \\ =& 52 \mod 26 \\ =& 2 \times 26 \mod 26 \\ =& 0 \ . \end{aligned}$$

$$\begin{aligned} e_k(14) =& 7 \times 14 + 3 \mod 26 \\ =& 101 \mod 26 \\ =& 3 \times 26 + 23 \mod 26 \\ =& 23 \ . \end{aligned}$$

$$\begin{aligned} e_k(19) =& 7 \times 19 + 3 \mod 26 \\ =& 136 \mod 26 \\ =& 5 \times 26 + 6 \mod 26 \\ =& 6 \ . \end{aligned}$$

מכאן נקבל

$\texttt{x} \in P$	h	o	t
$x \in \mathbb{Z}_{26}$	7	14	19
$y \in \mathbb{Z}_{26}$	0	23	6
$\texttt{y} \in C$	A	X	G

לכן הטקסט מוצפן המתקבל הוא

`AXG`

סעיף 2) הכלל מפענח הוא

$$d_k(y) = 15y + 7 \ .$$

נעביר את הואתיות של `AXG` לערכים של $\mathbb{Z}_{26}$:

$\texttt{y} \in P$	A	X	G
$y \in \mathbb{Z}_{26}$	1	23	6

נפעיל את הכלל מפענח על הערכים y:

$$\begin{aligned} d_k(1) =& 15 \times 1 + 7 \mod 26 \\ =& 22 \mod 26 \\ =& 22 \ . \end{aligned}$$

$$\begin{aligned} d_k(23) =& 15 \times 23 + 7 \mod 26 \\ =& 352 \mod 26 \\ =& 338 + 14 \mod 26 \\ =& 13 \times 26 + 14 \mod 26 \\ =& 14 \ . \end{aligned}$$

$$\begin{aligned} d_k(6) =& 15 \times 6 + 7 \mod 26 \\ =& 97 \mod 26 \\ =& 3 \times 26 + 19 \mod 26 \\ =& 19 \ . \end{aligned}$$

$\mathtt{y} \in C$	A	X	G
$y \in \mathbb{Z}_{26}$	1	23	6
$x \in \mathbb{Z}_{26}$	22	14	19
$\mathtt{x} \in P$	h	o	t

לכן הטקסט גלוי המתקבל הוא

hot

כנדרש.

■

דוגמה 3.10

נתון הטקסט מוצפן

ACSE

והמפתח $(23, 2)$ של צופן אפיני. מצאו את הטקסט גלוי.

פתרון:

$$\begin{aligned} d_k(y) =& 23^{-1}(y - 2) \mod 26 \\ =& 17(y - 2) = \qquad 17y - 34 \mod 26 \\ =& 17y - 26 - 8 \mod 26 \\ =& 17y - 8 \mod 26 \\ =& 17y + 18 \ . \end{aligned}$$

נעביר את הואתיות של ACSE לערכים של $\mathbb{Z}_{26}$:

$\mathtt{y} \in C$	A	C	S	E
$y \in \mathbb{Z}_{26}$	0	2	18	4

$$\begin{aligned} d_k(0) =& 18 \mod 26 \\ =& 18 \ . \end{aligned}$$

$$\begin{aligned} d_k(2) =& 17 \times 2 + 18 \mod 26 \\ =& 52 \mod 26 \\ =& 0 \ . \end{aligned}$$

$$\begin{aligned} d_k(18) =& 17 \times 18 + 18 \mod 26 \\ =& 324 \mod 26 \\ =& 12 \times 26 + 12 \mod 26 \\ =& 12 \ . \end{aligned}$$

$$\begin{aligned} d_k(4) =& 17 \times 4 + 18 \mod 26 \\ =& 86 \mod 26 \\ =& 3 \times 26 + 8 \mod 26 \\ =& 8 \ . \end{aligned}$$

$y \in C$	A	C	S	E
$y \in \mathbb{Z}_{26}$	0	2	18	4
$x \in \mathbb{Z}_{26}$	18	0	12	8
$x \in P$	s	a	m	i

■

3.5 צופן ויז'נר

צופן ההזזה וצופן ההחלפה דוגמאות של צופן מונואלפביתי: כל תו אלפביתי ב- P נתאים לתו אלפביתי יחיד ב- C. צופן ויז'נר הוא צופן פוליאלפיביתי: אין מצפינים כל אות בנפרד, אלא בלוקים, או קבוצות של כמה אותיות באורך קבוע m.

הגדרה 3.5 צופן ויז'נר (Vigenere Cipher)

יהי m מספר שלם חיובי.
נגדיר $P = C = K = \mathbb{Z}_{26}^m$.
עבור מפתח $k = (k_1, k_2, \ldots, k_m)$ נגדיר כלל מצפין

$$e_k(x_1, x_2, \ldots, x_m) = (x_1 + k_1, x_2 + k_2, x_3 + k_3, \ldots, x_m + k_m)$$

ונגדיר כלל מפענח

$$d_k(y_1, y_2, \ldots, y_m) = (y_1 - k_1, y_2 - k_2, y_3 - k_3, \ldots, y_m - k_m) \ ,$$

כאשר כל הפעולות נבצעות ב- $\mathbb{Z}_{26}$.

דוגמה 3.11

נתון הטקסט גלוי

string

והמפתח AND $= k$.

1) מצאו את הכלל מצפין והכלל מפענח.

2) מצאו את הטקסט מצפון.

3) בדקו כי הכלל מפענח מחזיר את הטקסט גלוי.

פתרון:

1) והמפתח הוא

AND.

הערכים המתאימים ב- $\mathbb{Z}_{26}$ הינם

$$k = (0, 13, 3) \ .$$

לכן $m = 3$.

הכלל מצפין הוא

$$e_k(x_1, x_2, x_3) = (x_1, x_2 + 13, x_3 + 3) \ ,$$

והכלל מפענח הוא

$$d_k(y_1, y_2, y_3) = (y_1, y_2 - 13, y_3 - 3) \ .$$

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

x $\in P$	s	t	r	i	n	g
$x \in \mathbb{Z}_{26}$	18	19	17	8	13	6

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

x $\in P$	s	t	r	i	n	g
$x \in \mathbb{Z}_{26}$	18	19	17	8	13	6

בכל תת-קבוצה, נתאים לכל תו ערך של המפתח $k = (0, 13, 3)$:

x $\in P$	s	t	r	i	n	g
$x \in \mathbb{Z}_{26}$	18	19	17	8	13	6
$k_i \in k$	0	13	3	0	13	3

על כל שלישיה (x_1, x_2, x_3) בבלוק אחד, נפעיל את כלל המצפין

$$e_k\left(x_1, x_2, x_3\right) = (x_1 + k_1, x_2 + k_2, x_3 + k_3) \mod 26 \ .$$

לדוגמה בבלוק הראשון נקבל

$$\begin{aligned} e_k(18, 19, 17) =& (18 + 0, 19 + 13, 17 + 3) \mod 26 \\ =& (18, 32, 20) \mod 26 \\ =& (18, 6, 20) \ . \end{aligned}$$

בבלוק השני נקבל

$$\begin{aligned} e_k(8, 13, 6) =& (8 + 0, 13 + 13, 6 + 3) \mod 26 \\ =& (8, 26, 9) \mod 26 \\ =& (8, 0, 9) \ . \end{aligned}$$

$x \in P$	s	t	r	i	n	g
$x \in \mathbb{Z}_{26}$	18	19	17	8	13	6
$k_i \in k$	0	13	3	0	13	3
$x \in \mathbb{Z}_{26}$	18	6	20	8	0	9

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

$x \in P$	s	t	r	i	n	g
$x \in \mathbb{Z}_{26}$	18	19	17	8	13	6
$k_i \in k$	0	13	3	0	13	3
$y \in \mathbb{Z}_{26}$	18	6	20	8	0	9
$y \in C$	S	G	U	I	A	J

הטקסט מוצפן המתקבל הוא

SGUIAJ .

3) נעביר את האותיות של הטקסט מוצפן לערכים של $\mathbb{Z}_{26}$:

$y \in C$	S	G	U	I	A	J
$y \in \mathbb{Z}_{26}$	18	6	20	8	0	9

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

$y \in C$	S	G	U	I	A	J
$y \in \mathbb{Z}_{26}$	18	6	20	8	0	9

בכל תת-קבוצה, נתאים לכל תו ערך של המפתח $k = (0, 13, 3)$:

$x \in P$	S	G	U	I	A	J
$y \in \mathbb{Z}_{26}$	18	6	20	8	0	9
$k_i \in k$	0	13	3	0	13	3

על כל שלישיה (y_1, y_2, y_3) בבלוק אחד, נפעיל את כלל המצפין

$$d_k(y_1, y_2, y_3) = (y_1 - k_1, y_2 - k_2, y_3 - k_3) \mod 26 .$$

לדוגמה בבלוק הראשון נקבל

$$\begin{aligned} d_k(18, 6, 20) &= (18, -7, 17) \mod 26 \\ &= (18, 19, 17) . \end{aligned}$$

בבלוק השני נקבל

$$\begin{aligned} d_k(8, 0, 9) &= (8 + 0, -13, 6) \mod 26 \\ &= (8, 13, 6) . \end{aligned}$$

$y \in C$	s	t	r	i	n	g
$y \in \mathbb{Z}_{26}$	18	6	20	8	0	9
$k_i \in k$	0	13	3	0	13	3
$x \in \mathbb{Z}_{26}$	18	19	17	8	13	6

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

y $\in C$	S	G	U	I	A	J
$y \in \mathbb{Z}_{26}$	18	6	20	8	0	9
$k_i \in k$	0	13	3	0	13	3
$x \in \mathbb{Z}_{26}$	18	19	17	8	13	6
x $\in P$	s	t	r	i	n	g

הטקסט גלוי המתקבל הוא

string .

■

דוגמה 3.12

נניח כי $m = 6$ והמפתח הוא

CIPHER.

הערכים המתאימים ב- $\mathbb{Z}_{26}$ הינם

$k = (2, 8, 15, 7, 4, 17)$.

נתון הטקסט גלוי

thiscryptosystemisnotsecure.

מצאו את הטקסט מוצפן.

פתרון:

<u>שלב 1:</u>

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

x $\in P$	t	h	i	s	c	r	y	p	t	o	s	y	s	t	e	m	i	s
$x \in \mathbb{Z}_{26}$	19	7	8	18	2	17	24	15	19	14	18	24	18	19	4	12	8	18

x $\in P$	n	o	t	s	e	c	u	r	e
$x \in \mathbb{Z}_{26}$	13	14	19	18	4	2	20	17	4

<u>שלב 2:</u>

נפרק את הטבלה של התווים של הטקסט גלוי יחד עם הערכים המתאימים של $\mathbb{Z}_{26}$ לתת-קבוצות של $m = 6$ תווים:

x $\in P$	t	h	i	s	c	r	y	p	t	o	s	y	s	t	e	m	i	s
$x \in \mathbb{Z}_{26}$	19	7	8	18	2	17	24	15	19	14	18	24	18	19	4	12	8	18

x $\in P$	n	o	t	s	e	c	u	r	e
$x \in \mathbb{Z}_{26}$	13	14	19	18	4	2	20	17	4

<u>שלב 3:</u>

בכל תת-קבוצה, נתאים לכל תו ערך של המפתח $k = (2, 8, 15, 7, 4, 17)$:

$x \in P$	t	h	i	s	c	r	y	p	t	o	s	y	s	t	e	m	i	s
$x \in \mathbb{Z}_{26}$	19	7	8	18	2	17	24	15	19	14	18	24	18	19	4	12	8	18
$k_i \in k$	2	8	15	7	4	17	2	8	15	7	4	17	2	8	15	7	4	17

$x \in P$	n	o	t	s	e	c	u	r	e
$x \in \mathbb{Z}_{26}$	13	14	19	18	4	2	20	17	4
$k_i \in k$	2	8	15	7	4	17	2	8	15

<u>שלב 3:</u>

על כל ששיה $(x_1, x_2, x_3, x_4, x_5, x_5)$ בבלוק אחד, נפעיל את כלל המצפין

$$e_k\left(x_1, x_2, x_3, x_4, x_5, x_6\right) = (x_1 + k_1, x_2 + k_2, x_3 + k_3, x_4 + k_4, x_5 + k_5, x_6 + k_6) \mod 26 \ .$$

לדוגמה בבלוק הראשון נקבל

$$\begin{aligned} e_k(19, 7, 8, 18, 2, 17) =& (19 + 2, 7 + 8, 8 + 15, 18 + 7, 2 + 4, 17 + 17) \mod 26 \\ =& (21, 15, 23, 25, 6, 34) \mod 26 \\ =& (21, 15, 23, 25, 6, 8) \ . \end{aligned}$$

$x \in P$	t	h	i	s	c	r	y	p	t	o	s	y	s	t	e	m	i	s
$x \in \mathbb{Z}_{26}$	19	7	8	18	2	17	24	15	19	14	18	24	18	19	4	12	8	18
$k_i \in k$	2	8	15	7	4	17	2	8	15	7	4	17	2	8	15	7	4	17
$y \in \mathbb{Z}_{26}$	21	15	23	25	6	8	0	23	34	21	22	15	20	1	19	19	12	9

$x \in P$	n	o	t	s	e	c	u	r	e
$x \in \mathbb{Z}_{26}$	13	14	19	18	4	2	20	17	4
$k_i \in k$	2	8	15	7	4	17	2	8	15
$y \in \mathbb{Z}_{26}$	15	22	8	25	8	19	22	25	19

<u>שלב 4:</u>

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

$x \in P$	t	h	i	s	c	r	y	p	t	o	s	y	s	t	e	m	i	s
$x \in \mathbb{Z}_{26}$	19	7	8	18	2	17	24	15	19	14	18	24	18	19	4	12	8	18
$k_i \in k$	2	8	15	7	4	17	2	8	15	7	4	17	2	8	15	7	4	17
$y \in \mathbb{Z}_{26}$	21	15	23	25	6	8	0	23	8	21	22	15	20	1	19	19	12	9
$y \in \mathbb{C}$	V	P	X	Z	G	I	A	X	I	V	W	P	U	B	T	T	M	J

$x \in P$	n	o	t	s	e	c	u	r	e
$x \in \mathbb{Z}_{26}$	13	14	19	18	4	2	20	17	4
$k_i \in k$	2	8	15	7	4	17	2	8	15
$y \in \mathbb{Z}_{26}$	15	22	8	25	8	19	22	25	19
$y \in \mathbb{C}$	P	W	I	Z	I	T	W	Z	T

הטקטס מוצפן המתקבל הוא

VPXZGIAXIVWPUBTTMJPWIZITWZT

■

3.6 צופן היל

הגדרה 3.6 צופן היל

נניח כי $m \geq 2$ מספר שלם.
יהי $P = C = \mathbb{Z}_{26}^m$ ויהי

$$k = \mathbb{Z}_{26}^{m \times m}$$

מטריצה בחוג $\mathbb{Z}_{26}$ מסדר $m \times m$.
עבור מפתח $k \in K$ נגדיר כלל מצפין

$$e_k(x) = x \cdot k \ ,$$

ונגדיר כלל מפענח

$$d_k(y) = y \cdot k^{-1} \ ,$$

כאשר כל פעולות נצעות ב- $\mathbb{Z}_{26}$.

הגדרה 3.7 המטריצה של קופקטורים

תהי $A \in \mathbb{R}^{n \times n}$.

הקופקטור ה- (i,j) של A מוגדר להיות הדטרמיננטה של המטריצה המתקבלת מ-A ע"י מחיקת שורה i ועמודה j, כפול $(-1)^{i+j}$.

המטריצה של קופקטורים של המטריצה A מוגדרת

$$C = \begin{pmatrix} C_{11} & \cdots & C_{1n} \\ \vdots & \ddots & \vdots \\ C_{n1} & \cdots & C_{nn} \end{pmatrix}$$

כאשר C_{ij} הקופקטור ה- (i,j) של A.

הגדרה 3.8 המטריצה המצורפת

תהי $A \in \mathbb{R}^{n \times n}$. המטריצה המצורפת של A היא מטריצה מסדר $n \times n$ שמסומנת $\text{adj}(A)$ ומוגדרת

$$\text{adj}(A) = C^t$$

כאשר C המטריצה של קופקטורים של A.

משפט 3.2 נוסחת קיילי המילטון

נניח כי $A \in \mathbb{R}^{n \times n}$ מטריצה ריבועית. אם A הפיכה, כלומר אם $|A| \neq 0$ אז המטריצה ההופכית נתונה ע"י נוסחת קיילי המילטון:

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

כאשר $\text{adj}(A)$ המטריצה המצורפת של A.

דוגמה 3.13

נתון רצף טקטסת גלוי

$$\texttt{july}$$

ונתון המפתח

$$k = \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}$$

של צופן היל. מצאו את הטקסט מוצפן.

פתרון:

שלב 1:

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

$\texttt{x} \in P$	j	u	l	y
$x \in \mathbb{Z}_{26}$	9	20	11	24

שלב 2:

נפרק את הטבלה של התווים של הטקסט גלוי יחד עם הערכים המתאימים של $\mathbb{Z}_{26}$ לתת-קבוצות של $m = 2$ תווים:

$\texttt{x} \in P$	j	u	l	y
$x \in \mathbb{Z}_{26}$	9	20	11	24

שלב 3:

עבור כל תת-קבוצה המתקבל נחשב

$$\begin{aligned} \begin{pmatrix} y_1 & y_2 \end{pmatrix} &= \begin{pmatrix} x_1 & x_2 \end{pmatrix} k \mod 26 \\ &= \begin{pmatrix} x_1 & x_2 \end{pmatrix} \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix} \mod 26 \end{aligned}$$

עבור התת-קבוצה הראשונה נקבל

$$\begin{aligned} \begin{pmatrix} y_1 & y_2 \end{pmatrix} &= \begin{pmatrix} 9 & 20 \end{pmatrix} \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix} \mod 26 \\ &= \begin{pmatrix} 99+60 & 72+140 \end{pmatrix} \mod 26 \\ &= \begin{pmatrix} 159 & 212 \end{pmatrix} \mod 26 \\ &= \begin{pmatrix} 3 & 4 \end{pmatrix} \end{aligned}$$

עבור התת-קבוצה השנייה נקבל

$$\begin{aligned} \begin{pmatrix} y_1 & y_2 \end{pmatrix} &= \begin{pmatrix} 11 & 24 \end{pmatrix} \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix} \mod 26 \\ &= \begin{pmatrix} 121+72 & 88+168 \end{pmatrix} \mod 26 \\ &= \begin{pmatrix} 193 & 256 \end{pmatrix} \mod 26 \\ &= \begin{pmatrix} 11 & 22 \end{pmatrix} \end{aligned}$$

$x \in P$	j	u	l	y
$x \in \mathbb{Z}_{26}$	9	20	11	24
$x \cdot k \in \mathbb{Z}_{26}$	3	4	11	22

שלב 4:

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

$x \in P$	j	u	l	y
$x \in \mathbb{Z}_{26}$	9	20	11	24
$x \cdot k \in \mathbb{Z}_{26}$	3	4	11	22
$y \in C$	D	E	L	W

הטקטס מוצפן המתקבל הוא

DELW

■

דוגמה 3.14

נתון רצף טקטסת מוצפן

DELW

ונתון המפתח

$$k = \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}$$

של צופן היל. מצאו את הטקסט גלוי.

פתרון:

שלב 0:

נחשב את ההופכית k^{-1}:

$$|k| = 11 \cdot 7 - 8 \cdot 3 \mod 26 = 77 - 24 \mod 26 = 53 \mod 26 = 1 \ .$$

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

$$\begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix} \Rightarrow C_{11} = (-1)^{1+1}(7) = 7 \ .$$

$$\begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix} \Rightarrow C_{12} = (-1)^{2+1}(3) = -3 \ .$$

$$\begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix} \Rightarrow C_{21} = (-1)^{1+2}(8) = -8 \ .$$

$$\begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix} \Rightarrow C_{22} = (-1)^{2+2}(11) = 11 \ .$$

$$C = \begin{pmatrix} C_{11} & C_{12} \\ C_{21} & C_{22} \end{pmatrix} = \begin{pmatrix} 7 & -3 \\ -8 & 11 \end{pmatrix}$$

$$\text{adj}(A) = C^t = \begin{pmatrix} 7 & -8 \\ -3 & 11 \end{pmatrix} \mod 26 = \begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix} \in \mathbb{Z}_{26}^{2\times 2} .$$

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

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

לפיכך

$$A^{-1} = |A|^{-1}\text{adj}(A) = 1 \cdot \begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix}$$

<u>שלב 1:</u>

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

$\mathtt{y} \in C$	D	E	L	W
$y \in \mathbb{Z}_{26}$	3	4	11	22

<u>שלב 2:</u>

נפרק את הטבלה של התווים של הטקסט מוצפן יחד עם הערכים המתאימים של $\mathbb{Z}_{26}$ לתת-קבוצות של $m = 2$ תווים:

$\mathtt{y} \in C$	D	E	L	W
$y \in \mathbb{Z}_{26}$	3	4	11	22

<u>שלב 3:</u>

עבור כל תת-קבוצה המתקבל נחשב

$$\begin{aligned} \begin{pmatrix} x_1 & x_2 \end{pmatrix} &= \begin{pmatrix} y_1 & y_2 \end{pmatrix} k^{-1} \mod 26 \\ &= \begin{pmatrix} y_1 & y_2 \end{pmatrix} \begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix} \mod 26 \end{aligned}$$

עבור התת-קבוצה הראשונה נקבל

$$\begin{aligned} \begin{pmatrix} x_1 & x_2 \end{pmatrix} &= \begin{pmatrix} 3 & 4 \end{pmatrix} \begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix} \mod 26 \\ &= \begin{pmatrix} 21+92 & 54+44 \end{pmatrix} \mod 26 \\ &= \begin{pmatrix} 113 & 98 \end{pmatrix} \mod 26 \\ &= \begin{pmatrix} 9 & 20 \end{pmatrix} \end{aligned}$$

עבור התת-קבוצה השנייה נקבל

$$\begin{aligned} \begin{pmatrix} x_1 & x_2 \end{pmatrix} &= \begin{pmatrix} 11 & 22 \end{pmatrix} \begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix} \mod 26 \\ &= \begin{pmatrix} 77+468 & 198+242 \end{pmatrix} \mod 26 \\ &= \begin{pmatrix} 583 & 440 \end{pmatrix} \mod 26 \\ &= \begin{pmatrix} 11 & 24 \end{pmatrix} \end{aligned}$$

$\mathtt{y} \in C$	D	E	L	W
$y \in \mathbb{Z}_{26}$	3	4	11	22
$y \cdot k^{-1} \in \mathbb{Z}_{26}$	9	20	11	24

<u>שלב 5:</u>

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

$\mathtt{y} \in C$	D	E	L	W
$y \in \mathbb{Z}_{26}$	3	4	11	22
$y \cdot k^{-1} \in \mathbb{Z}_{26}$	9	20	11	24
$\mathtt{x} \in P$	j	u	l	y

הטקסט גלוי המתקבל הוא

july

■

דוגמה 3.15

נתון רצף טקסטת מוצפן

PGRFGGCSY

ונתון המפתח

$$k = \begin{pmatrix} 3 & 2 & 5 \\ 5 & 10 & 8 \\ 6 & 11 & 13 \end{pmatrix}$$

של צופן היל. מצאו את הטקסט גלוי.

פתרון:

<u>שלב 0:</u>

נחשב את ההופכית k^{-1}:

$$\begin{aligned} |k| =& 3 \cdot (13 \cdot 10 - 11 \cdot 8) - 2 \cdot (5 \cdot 13 - 8 \cdot 6) + 5 \cdot (5 \cdot 11 - 6 \cdot 10) \mod 26 \\ =& 3 \cdot 42 - 2 \cdot 17 + 5 \cdot (-5) \mod 26 \\ =& 126 - 34 - 25 \mod 26 \\ =& 67 \mod 26 \\ =& 15 \ . \end{aligned}$$

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

$$\begin{pmatrix} 3 & 2 & 5 \\ 5 & 10 & 8 \\ 6 & 11 & 13 \end{pmatrix} \quad \Rightarrow \quad C_{11} = (-1)^{1+1} \begin{vmatrix} 10 & 8 \\ 11 & 13 \end{vmatrix} = 42 \mod 26 = 16 \ .$$

$$\begin{pmatrix} 3 & 2 & 5 \\ 5 & 10 & 8 \\ 6 & 11 & 13 \end{pmatrix} \quad \Rightarrow \quad C_{12} = (-1)^{1+2} \begin{vmatrix} 5 & 8 \\ 6 & 13 \end{vmatrix} = -17 \mod 26 = 9 \ .$$

$$\begin{pmatrix} 3 & 2 & 5 \\ 5 & 10 & 8 \\ 6 & 11 & 13 \end{pmatrix} \Rightarrow C_{13} = (-1)^{1+3} \begin{vmatrix} 5 & 10 \\ 6 & 11 \end{vmatrix} = -5 \mod 26 = 21 .$$

$$\begin{pmatrix} 3 & 2 & 5 \\ 5 & 10 & 8 \\ 6 & 11 & 13 \end{pmatrix} \Rightarrow C_{21} = (-1)^{2+1} \begin{vmatrix} 2 & 5 \\ 11 & 13 \end{vmatrix} = -29 \mod 26 = 23 .$$

$$\begin{pmatrix} 3 & 2 & 5 \\ 5 & 10 & 8 \\ 6 & 11 & 13 \end{pmatrix} \Rightarrow C_{22} = (-1)^{2+2} \begin{vmatrix} 3 & 5 \\ 6 & 13 \end{vmatrix} = 9 .$$

$$\begin{pmatrix} 3 & 2 & 5 \\ 5 & 10 & 8 \\ 6 & 11 & 13 \end{pmatrix} \Rightarrow C_{23} = (-1)^{2+3} \begin{vmatrix} 3 & 2 \\ 6 & 11 \end{vmatrix} = -21 \mod 26 = 5 .$$

$$\begin{pmatrix} 3 & 2 & 5 \\ 5 & 10 & 8 \\ 6 & 11 & 13 \end{pmatrix} \Rightarrow C_{31} = (-1)^{3+1} \begin{vmatrix} 2 & 5 \\ 10 & 8 \end{vmatrix} = -34 \mod 26 = 18 .$$

$$\begin{pmatrix} 3 & 2 & 5 \\ 5 & 10 & 8 \\ 6 & 11 & 13 \end{pmatrix} \Rightarrow C_{32} = (-1)^{3+2} \begin{vmatrix} 3 & 5 \\ 5 & 8 \end{vmatrix} = 1 .$$

$$\begin{pmatrix} 3 & 2 & 5 \\ 5 & 10 & 8 \\ 6 & 11 & 13 \end{pmatrix} \Rightarrow C_{33} = (-1)^{3+3} \begin{vmatrix} 3 & 2 \\ 5 & 10 \end{vmatrix} = 20 .$$

$$C = \begin{pmatrix} C_{11} & C_{12} & C_{13} \\ C_{21} & C_{22} & C_{23} \\ C_{31} & C_{32} & C_{33} \end{pmatrix} = \begin{pmatrix} 16 & 9 & 21 \\ 3 & 9 & 5 \\ 18 & 1 & 20 \end{pmatrix}$$

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

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

$$|k|^{-1} = 15^{-1} = 7 \in \mathbb{Z}_{26}$$

לפיכך

$$\begin{aligned} k^{-1} &= |k|^{-1}\text{adj}(k) \\ &= 7 \cdot \begin{pmatrix} 16 & 3 & 18 \\ 9 & 9 & 1 \\ 21 & 5 & 20 \end{pmatrix} \mod 26 \\ &= \begin{pmatrix} 112 & 21 & 126 \\ 63 & 63 & 7 \\ 147 & 35 & 140 \end{pmatrix} \mod 26 \end{aligned}$$

$$112 \texttt{ \% } 26 = 112 - 26 \cdot \left\lfloor \frac{112}{26} \right\rfloor = 8 .$$

$$63 \texttt{ \% } 26 = 63 - 26 \cdot \left\lfloor \frac{63}{26} \right\rfloor = 11 .$$

$$147 \ \% \ 26 = 147 - 26 \cdot \left\lfloor \frac{147}{26} \right\rfloor = 17 \ .$$

$$35 \ \% \ 26 = 35 - 26 \cdot \left\lfloor \frac{35}{26} \right\rfloor = 9 \ .$$

$$140 \ \% \ 26 = 140 - 26 \cdot \left\lfloor \frac{140}{26} \right\rfloor = 10 \ .$$

לפיכך

$$k^{-1} = \begin{pmatrix} 8 & 21 & 22 \\ 11 & 11 & 7 \\ 17 & 9 & 10 \end{pmatrix} \in \mathbb{Z}_{26}^{3\times 3} \ .$$

<u>שלב 1:</u>

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

$\mathtt{y} \in C$	P	G	R	F	G	G	C	S	Y
$y \in \mathbb{Z}_{26}$	15	6	17	5	6	6	2	18	24

<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:

$\mathtt{y} \in C$	P	G	R	F	G	G	C	S	Y
$y \in \mathbb{Z}_{26}$	15	6	17	5	6	6	2	18	24

<u>שלב 3:</u>

עבור כל תת-קבוצה המתקבל נחשב

$$\begin{aligned} \begin{pmatrix} x_1 & x_2 & x_3 \end{pmatrix} &= \begin{pmatrix} y_1 & y_2 & y_3 \end{pmatrix} k^{-1} \mod 26 \\ &= \begin{pmatrix} y_1 & y_2 & y_3 \end{pmatrix} \begin{pmatrix} 8 & 21 & 22 \\ 11 & 11 & 7 \\ 17 & 9 & 10 \end{pmatrix} \mod 26 \end{aligned}$$

עבור התת-קבוצה הראשונה נקבל

$$\begin{aligned} \begin{pmatrix} x_1 & x_2 & x_3 \end{pmatrix} &= \begin{pmatrix} 15 & 6 & 17 \end{pmatrix} \begin{pmatrix} 8 & 21 & 22 \\ 11 & 11 & 7 \\ 17 & 9 & 10 \end{pmatrix} \mod 26 \\ &= \begin{pmatrix} 475 & 534 & 542 \end{pmatrix} \mod 26 \\ &= \begin{pmatrix} 7 & 14 & 22 \end{pmatrix} \end{aligned}$$

עבור התת-קבוצה השנייה נקבל

$$\begin{aligned} \begin{pmatrix} x_1 & x_2 & x_3 \end{pmatrix} &= \begin{pmatrix} 5 & 6 & 6 \end{pmatrix} \begin{pmatrix} 8 & 21 & 22 \\ 11 & 11 & 7 \\ 17 & 9 & 10 \end{pmatrix} \mod 26 \\ &= \begin{pmatrix} 208 & 225 & 212 \end{pmatrix} \mod 26 \\ &= \begin{pmatrix} 0 & 17 & 4 \end{pmatrix} \end{aligned}$$

עבור התת-קבוצה השלישי נקבל

$$\begin{aligned}(x_1 \quad x_2 \quad x_3) &= (2 \quad 18 \quad 24)\begin{pmatrix} 8 & 21 & 22 \\ 11 & 11 & 7 \\ 17 & 9 & 10 \end{pmatrix} \mod 26 \\ &= (622 \quad 456 \quad 410) \mod 26 \\ &= (24 \quad 14 \quad 20)\end{aligned}$$

$y \in C$	P	G	R	F	G	G	C	S	Y
$y \in \mathbb{Z}_{26}$	15	6	17	5	6	6	2	18	24
$y \cdot k^{-1} \in \mathbb{Z}_{26}$	7	14	22	0	17	4	24	14	20

<u>שלב 5:</u>

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

$y \in C$	P	G	R	F	G	G	C	S	Y
$y \in \mathbb{Z}_{26}$	15	6	17	5	6	6	2	18	24
$y \cdot k^{-1} \in \mathbb{Z}_{26}$	7	14	22	0	17	4	24	14	20
$x \in P$	h	o	w	a	r	e	y	o	u

הטקסט גלוי המתקבל הוא

howareyou

■

3.7 צופן התמורה

הגדרה 3.9 תופן התמורה (permutation cipher)

נניח כי m מספר שלים חיובי.
יהי $P = C = \mathbb{Z}_{26}^m$ ויהי K להיות הקבוצה של כל התמורות האפשריות של $\{1, \ldots, m\}$.
עבור מפתח $\pi \in K$ (עבור תמרוה של K) נגדיר כלל מצפין

$$e_\pi(x_1, \ldots, x_m) = (x_{\pi(1)}, \ldots, x_{\pi(m)})$$

ונגדיר כלל מפענח

$$d_\pi(y_1, \ldots, y_m) = (y_{\pi^{-1}(1)}, \ldots, y_{\pi^{-1}(m)}) \ ,$$

כאשר π^{-1} התמורה ההופכית של π.

דוגמה 3.16

נתון התמורה הבאה:

x	1	2	3
$\pi(x)$	2	3	1

ונתון את הטקסט גלוי

flower

1) מצאו את הטקסט מוצפן.

2) מצאו את הטקסט גלוי באמצעות לפענח את הטקטס מצפון מסעיף הקודם עם התמורה ההופכית.

פתרון:

סעיף 1) <u>שלב 1:</u>

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

$\mathtt{x} \in P$	f	l	o	w	e	r
$x \in \mathbb{Z}_{26}$	5	11	14	22	4	17

<u>שלב 2:</u>

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

$\mathtt{x} \in P$	f	l	o	w	e	r
$x \in \mathbb{Z}_{26}$	5	11	14	22	4	17

<u>שלב 3:</u>

עבור כל תת-קבוצה המתקבל נפעיל את התמרוה π:

$$(5 \quad 11 \quad 14) \xrightarrow{\pi} (11 \quad 14 \quad 5)$$

$$(22 \quad 4 \quad 17) \xrightarrow{\pi} (4 \quad 17 \quad 22)$$

$\mathtt{x} \in P$	f	l	o	w	e	r
$x \in \mathbb{Z}_{26}$	5	11	14	22	4	17
$\pi(x) \in \mathbb{Z}_{26}$	11	14	5	4	17	22

<u>שלב 4:</u>

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

$\mathtt{x} \in P$	f	l	o	w	e	r
$x \in \mathbb{Z}_{26}$	5	11	14	22	4	17
$\pi(x) \in \mathbb{Z}_{26}$	11	14	5	4	17	22
$\mathtt{y} \in C$	L	O	F	E	R	W

לכן הטקסט מוצפן הוא

LOFERW

סעיף 2)

<u>שלב 1:</u>

נתחיל עם הטקסט מוצפן

LOFERW

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

$\mathtt{y} \in C$	L	O	F	E	R	W
$y \in \mathbb{Z}_{26}$	11	14	5	4	17	22

<u>שלב 2:</u>

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

$\mathtt{y} \in C$	L	O	F	E	R	W
$y \in \mathbb{Z}_{26}$	11	14	5	4	17	22

<u>שלב 3:</u>

עבור כל תת-קבוצה המתקבל נפעיל את התמרוה ההופכית: π^{-1}:

x	1	2	3
$\pi(x)$	3	1	2

$$\begin{pmatrix} 11 & 14 & 5 \end{pmatrix} \xrightarrow{\pi} \begin{pmatrix} 5 & 11 & 14 \end{pmatrix}$$

$$\begin{pmatrix} 4 & 17 & 22 \end{pmatrix} \xrightarrow{\pi} \begin{pmatrix} 22 & 4 & 17 \end{pmatrix}$$

$\mathtt{y} \in C$	L	O	F	E	R	W
$y \in \mathbb{Z}_{26}$	11	14	5	4	17	22
$x = \pi^{-1}(y)$	5	11	14	22	4	17

<u>שלב 4:</u>

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

$\mathtt{y} \in C$	L	O	F	E	R	W
$y \in \mathbb{Z}_{26}$	11	14	5	4	17	22
$x = \pi^{-1}(y)$	5	11	14	22	4	17
$\mathtt{x} \in C$	f	l	o	w	e	r

לכן הטקסט מוצפן הוא

LOFERW

■

3.8 צפני זרם

עד כה דיברנו על צפנים המבוססים על מפתח k אילו הטקסט מוצפן y מתקבל על ידי הכלל מצפין

$$\mathrm{y} = y_1 y_2 \cdots = e_k(x_1)e_k(x_2)\cdots \ .$$

צפנים מסוג זה נקראים צפני בלוק.

כעת נדבר על צפני זרם. להתחיל נגדיר **צופן זרם סינכרוני** .

הגדרה 3.10 צופן זרם סינכרוני

צופן זרם סינכרוני (synchronized stream cipher) מוצג באמצעות קבוצה (P, C, K, L, E, D) יחד עם פונקציה g כאשר:

1. E מסמן קבוצה של טקסטים גלויים אפשריים (plaintexts),
2. C מסמן קבוצה של טקסטים מוצפנים אפשריים (ciphertexts),
3. K מסמן קבוצה של המפתחות אפשריים (keyspace),
4. L מסמן את האלפיבית של המפתח הפנימי (key-stream alphabet).
5. g מסמן את ה **מחולל הפנימי** (keystream generator). g מקבלת מפתח k ומחזירה רצף אותיות אינסופי $z_1 z_2 \cdots$ כאשר $z_i \in L$ לכל $i \geq 1$.
6. לכל $z \in L$ יש כלל מצפין $e_z \in E$ וכלל מפענח $d_z \in D$:

$$e_z : P \to C \ , \qquad d_z : C \to P \ ,$$

כך ש-

$$d_z\left(e_z\left(x\right)\right) = x$$

לכל איבר של מרחב הטקסט גלוי $x \in P$.

הגדרה 3.11 צופן אוטו מפתח (Autokey cipher)

נניח כי $P = C = K = L = \mathbb{Z}_{26}$.
נגדיר מפתח הפנימי

$$g: \qquad z_1 = k \ , \qquad z_i = x_{i-1} \ \forall i \geq 2 \ .$$

לכל $z \in \mathbb{Z}_{26}$ נגדיר כלל מצפין

$$e_z(x) = (x + z) \mod 26$$

לכל $x \in \mathbb{Z}_{26}$ ונגדיר כלל מפענח

$$d_z(y) = (y - z) \mod 26$$

לכל $y \in \mathbb{Z}_{26}$.

דוגמה 3.17 (צופן אוטו-מפתח)

נתון צופן אוטו-מפתח עם מפתח $k = 8$.

1. מצאו את הטקסט מוצפן של המילה

rendezvous .

2) פענחו את הטקטס מוצפן המתקבל וודאו שקיבלתם את הטקטסט הגלוי.

פתרון:

סעיף 1) נרשום את האותיות של הטקטסט גלוי ב- $\mathbb{Z}_{26}$:

x $\in P$	r	e	n	d	e	z	v	o	u	s
$x \in \mathbb{Z}_{26}$	17	4	13	3	4	25	21	14	20	18

המפתח הפנימי הוא

$x_i \in \mathbb{Z}_{26}$	17	4	13	3	4	25	21	14	20	18
$z_i \in \mathbb{Z}_{26}$	8	17	4	13	3	4	25	21	14	20

על פי המפתח הפנימי נפעיל את הכלל מצפין

$$e_z(x_i) = x_i + z_i \mod 26$$

על הטקטס גלוי ונחשב את ה- x_i של הטקסט מצפון באמצעות הכלל מצפין:

$$\begin{aligned}
y_1 =& e_8(17) &&= (8+17) \mod 26 = 25\ ,\\
y_2 =& e_{17}(4) &&= (17+4) \mod 26 = 21\ ,\\
y_3 =& e_4(13) &&= (4+13) \mod 26 = 17\ ,\\
y_4 =& e_{13}(3) &&= (13+3) \mod 26 = 16\ ,\\
y_5 =& e_3(4) &&= (3+4) \mod 26 = 7\ ,\\
y_6 =& e_4(25) &&= (4+25) \mod 26 = 3\ ,\\
y_7 =& e_{25}(21) &&= (25+21) \mod 26 = 20\ ,\\
y_8 =& e_{21}(14) &&= (21+14) \mod 26 = 9\ ,\\
y_9 =& e_{14}(20) &&= (14+20) \mod 26 = 8\ ,\\
y_{10} =& e_{20}(18) &&= (20+18) \mod 26 = 12\ .
\end{aligned}$$

x $\in P$	r	e	n	d	e	z	v	o	u	s
$x_i \in \mathbb{Z}_{26}$	17	4	13	3	4	25	21	14	20	18
$z_i \in \mathbb{Z}_{26}$	8	17	4	13	3	4	25	21	14	20
$y_i = e_{z_i}(x_i)$	25	21	17	16	7	3	20	9	8	12

נמיר את האיברים y_i של $\mathbb{Z}_{26}$ לתווים של הטקסט מוצפן:

x $\in P$	r	e	n	d	e	z	v	o	u	s
$x_i \in \mathbb{Z}_{26}$	17	4	13	3	4	25	21	14	20	18
$z_i \in \mathbb{Z}_{26}$	8	17	4	13	3	4	25	21	14	20
$y_i = e_{z_i}(x_i)$	25	21	17	16	7	3	20	9	8	12
y $\in C$	Z	V	R	Q	H	D	U	J	I	M

סעיף 2) נתחיל עם הטקטס מוצפן:

ZVRQHDUJIM

y $\in C$	Z	V	R	Q	H	D	U	J	I	M
$y_i = \mathbb{Z}_{26}$	25	21	17	16	7	3	20	9	8	12

נחשב את ה- x_i של הטקסט גלוי באמצעות הכלל מפענח:

$$\begin{aligned}
x_1 =& d_8(25) &&= (25-8) \mod 26 = 17\ ,\\
x_2 =& d_{17}(21) &&= (21-17) \mod 26 = 4\ ,\\
x_3 =& d_4(17) &&= (17-4) \mod 26 = 13\ ,\\
x_4 =& d_{13}(16) &&= (16-13) \mod 26 = 3\ ,\\
x_5 =& d_3(7) &&= (7-3) \mod 26 = 4\ ,\\
x_6 =& d_4(3) &&= (3-4) \mod 26 = 25\ ,\\
x_7 =& d_{25}(20) &&= (20-25) \mod 26 = 21\ ,\\
x_8 =& d_{21}(9) &&= (9-21) \mod 26 = 14\ ,\\
x_9 =& d_{14}(8) &&= (8-14) \mod 26 = 20\ ,\\
x_{10} =& d_{20}(12) &&= (12-20) \mod 26 = 18\ .
\end{aligned}$$

y $\in C$	Z	V	R	Q	H	D	U	J	I	M
$y_i = \mathbb{Z}_{26}$	25	21	17	16	7	3	20	9	8	12
$x_i = d_{z_i}(y_i)$	17	4	13	3	4	25	21	14	20	18

לבסוף נעבור מאיברים של $\mathbb{Z}_{26}$ דתווים של טקטסט גלוי:

y $\in C$	Z	V	R	Q	H	D	U	J	I	M
$y_i = \mathbb{Z}_{26}$	25	21	17	16	7	3	20	9	8	12
$x_i = d_{z_i}(y_i)$	17	4	13	3	4	25	21	14	20	18
x	r	e	n	d	e	z	v	o	u	s

■

3.9 צופן חד פעמי

הגדרה 3.12 צופן חד פעמי

יהי n שלם ויהי $X = Y = K = (\mathbb{Z}_2)^n$. לכל $k \in (\mathbb{Z}_2)^n$ נגדיר כלל מצפין

$$e_k(x) = (x_1 + k_1, \ldots, x_n + k_n) \mod 2\ ,$$

ונגדיר כלל מפענח

$$\begin{aligned}
d_k(y) &= (y_1 - k_1, \ldots, y_n - k_n) \mod 2\\
&= (y_1 + k_1, \ldots, y_n + k_n) \mod 2\ .
\end{aligned}$$

דוגמה 3.18

נתון הקבוצת מפתחות $K = \{0,1,1,0,0\}$ של צופן חד-פעמי ונתון הטקסט גלוי $x = 1110100010$.

1) מצאו את הטקסט מוצפן.

2) וודאו כי הכלל מפענח מחזירה הטקסט גלוי המקורי.

פתרון:

1)

$$\begin{aligned} e_k(x) =& \{1+0\ ,\ 1+1\ ,\ 1+1\ ,\ 0+0\ ,\ 1+1\ ,\ 0+0\ ,\ 0+1\ ,\ 0+1\ ,\ 1+0\ ,\ 0+1\} \mod 2 \\ =& \{1,0,0,0,0,0,1,1,1,1\}\ . \end{aligned}$$

2)

$$\begin{aligned} d_k(y) =& \{1+0\ ,\ 0+1\ ,\ 0+1\ ,\ 0+0\ ,\ 0+1\ ,\ 0+0\ ,\ 1+1\ ,\ 1+1\ ,\ 1+0\ ,\ 1+1\} \mod 2 \\ =& \{1,1,1,0,1,0,0,0,1,0\}\ . \end{aligned}$$

■

נשים לב כי בצופן חד-פעמי

$$|X| = |Y| = |K| = \mathbb{Z}_2^n$$

לפיכך לפי משפט שאנון לצופן חד-פעמי יש סודיות מושלמת.