

שיעור 3

הצפנים הבסיסיים

1.3. מושג של קריפטו-מערכת

אליס וbob, לתקשר מעל גבי עורך תקשורת בלתי אמין (נאמר קו טלפון או דואר אלקטרוני), ומבקשים להנחות מסוימות. כמובן, הם מעריכים שום גורם עיוון, אוסקר, עשוי לזכות לשיחתם, לא יכול להבין את תוכנה.

שם כך משתמשים אליס וbob בצופן (cryptosystem). אליס וbob מסכימים ביניהם מראש על שיטה מסוימת להצפנה ועל מפתח, (key) שהוא ערך מסוימי (או כמה ערכים מסוימים).עת, נניח שאليس מעריכים מועוניית לשЛОח לבוב הודעה מסוימת. היא מצפינה את הודעה בשיטה שהיא וbob בחרו בה תוך כדי שימוש במפתח שהם קבעו. לאחר ההצפנה, הודעה שניתנה את צורתה. להזעה המקורית אלו קוראים טקסט גלי (plaintext) ואילו הודעה לאחר ההצפנה נקראת טקסט מוצפן (ciphertext). אליס שולחת את הטקסט המוצפן לבוב. bob מפענחת אותו ומשחרר את הטקסט המקורי. אוסקר, המצותת לעורך, איננו ידע את ערכו של המפתח שנעשה בו שימוש (למרות ש, יתכן בהחלט ואף סביר להניח שהוא, ידוע מהו הצפן שהשתמשו בו אליס וbob).

הגדרה 3.1 צופן

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

(1) E מסמן קבוצה של טקסט גלי, 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 מצפן $e \in E$ וכלל מפענה $d \in D$:

$$e : P \rightarrow C , \quad d : C \rightarrow P ,$$

כך ש-

$$d(e(x)) = x$$

לכל איבר של מרחב הטקסט גלי P

נניח כי הודעה הנשלחה על ידי אליס לבוב היא הרץ האותיות

$$X = x_1 x_2 \cdots x_n$$

עבור $1 \leq n$ טבעי, אשר כל אות הוא אחת של טקסט גלי $x_i \in P$, $i \leq n$. כל x_i מוצפן באמצעות הכלל הצפנה e_k אשר נקבעת מראש על ידי המפתח k הנבחר. "אليس מחשבת

$$y_i = e_k(x_i)$$

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

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

הרץ זה נשלח מעל גבי העורך. כאשר bob מקבל את Y הוא מפענחת אותו באמצעות הפונקציה d_k וכך הוא מקבל הרץ אותיות של טקסט גלי 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 $x_2 \neq x_1$ ואז לבוב לא יוכל לדעת אם y הפענחה של x_1 או x_2 .

3.2 צופן ההזהה

הגדרה 3.2 צופן ההזהה

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

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

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

-1

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

במטרה להשתמש בצופן ההזהה כדי להצפין טקסט גלי, קודם כל נגידר 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 גלי

shamoon

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

פתרונות:

שלב 1) נמיר את הטקסט גלי 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 המתקין 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) נעביר את הרצץ מספרים לטקסט מוצפן:

$x \in P$	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
$y \in C$	D	S	L	X	Z	Z	Y

текסט מוצפן המתקבל הוא
DSLXZZY



3.2 דוגמה

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

UJCNQO

מצאו את הטקסט גלי.

פתרונות:

נססה לפענח את הטקסט מוצפן בעזרת הצופן הזה עם המפתחות $d_0 = 0, d_1 = 1, d_2 = 2, \dots$ בטור.

$y \in C$	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
$x \in P$	t	i	b	m	p	n
$y - d_2 \in \mathbb{Z}_{26}$	18	7	0	11	14	12
$x \in P$	s	h	a	l	o	m



3.3 דוגמה

נתון הטקסט מוצפן הבא:

QRQXFJANHXD

מצאו את הטסט גלי

פתרונות:

נססה לפענח את הטקסט מוצפן בעזרת הצופן הזה עם המפתחות d_0, d_1, \dots בטור.

d_0 qrqxfjanhx
 d_1 pqeweizmgwc
 d_2 opovdhylfvb
 d_3 nonucgxkeua
 d_4 mnmtbfwjdtz
 d_5 lmlsaevicsy
 d_6 klkrzduhbrx
 d_7 jkjqyctgaqw
 d_8 ijipxbssfzp
 d_9 hihowareyou

בשלב זה מצאנו את הטקסט גלי:

hihowareyou .

המפתח הוא $.k = 9$.

3.3 צופן החלפה

הגדרה 3.3 צופן החלפה (substitution cypher)

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

K מורכב מכל החלפות האפשריות של ה- 26 סמלים $0, 1, 2, \dots, 25$

עבור כל החלפה $K \in \pi$ נגידר כלל מצפן

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

ונגידר כלל מפענה

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

כאשר π^{-1} החלפה ההופכית של π .

קיימות $26! = 4.03291461126605635584 \times 10^{26}$ החלפות אפשריות.

3.4 דוגמה

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,

$$e_{\pi}(a) = Z, \quad e_{\pi}(b) = T, \dots$$

וכן הלאה. הכלל המופיע הוא החלפה ההופכית,⁻¹ π 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-

$$d_{\pi}(A) = d, \quad d_{\pi}(B) = c, \dots$$

וכן הלאה.

נתון הטקסט מוצפן

GHYYF

מצאו את הטקסט גליוי.

פתרונות:

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

לכן הטקסט גליוי הינו

hello.

**3.5 דוגמה**

למטה יש דוגמה של צופן החלפה. החלפה 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,

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

וכן הלאה. הכלל המופיע הוא החלפה ההופכית,⁻¹ π 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,

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

וכן הלאה.

3.6 דוגמה

נתון הטקסט מוצפן הבא:

MGZVYZLGHCMHJMYXSSFMNHAHYCDLMHA

והכלל מפענה של דוגמה 3.5. מצאו את הטקסט גלי.

פתרונות:

כלל מפענה :

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

א"ז

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

קיבלו את הטקסט גלי

this ciphertext cannot be decrypted



3.4 צופן האפייני

באופן כללי, בצופן האפייני הכלל מצפין נתון ע"י הפונקציה מצורפת

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

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

כדי שפענוח יהיה אפשרי נדרש כי הפונקציה הזאת חד-חד-ערכית. במקרים אחרים, נדרש כי לביטוי (יחס שיקילות)

$$ax + b \equiv y \pmod{26}$$

יש פתרון ייחיד ל- x .

למקרה נוכחה כי אכן יש פתרון ייחיד אם ורק אם $\gcd(a, 26) = 1$.

משפט 3.1

לייחס שיקילות

$$ax + b \equiv y \pmod{26}$$

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

הוכחה: (ראו גם הוכחה למשפט 2.7).

נניח כי יש פתרון ייחיד. נוכחה דרך השילילה כי $-1 = \gcd(a, 26)$.

נניח כי $1 > \gcd(a, 26) = d$.

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

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

כאשר $k = \frac{a}{d}$. שלם.

בפרט, מכיוון ש- $1 > d$, אז $x_1 + \frac{26}{d} \not\equiv x_1 \pmod{26}$.

נניח כי $1 = \gcd(a, 26)$. נוכחה בשילילה כי הפתרון ייחיד.

נניח כי קיימים שני פתרונות שונים: $x_1 \not\equiv x_2 \pmod{26}$.

ז"א

$$ax_1 \equiv y \pmod{26}, \quad ax_2 \equiv y \pmod{26}.$$

לכן

$$ax_1 \equiv ax_2 \pmod{26}.$$

לכן

$$26 \mid ax_1 - ax_2.$$

$\gcd(a, 26) = 1$ לפיכך

$$26 \mid x_1 - x_2,$$

$$x_1 \equiv x_2 \pmod{26},$$

בסתירה לכך ש- $x_1 \not\equiv x_2 \pmod{26}$.

3.7 דוגמה

בדקו אם הפונקציה

$$e(x) = 4x + 7 \pmod{26}$$

כלל מצפין תקין, כלומר בדקו אם קיים כלל מפענה.

פתרון:

לפי הטענה, הפונקציה $e(x) = 4x + 7 \pmod{26}$ אינה כלל מצפין תקין, בגלל שהוא לא חד-חד ערכית ולכן לא יכולה להיות כלל מצפין.

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

$$e(x) = 4x + 7 \pmod{26}$$

ובודך

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

ז"א מצפין את x ו- $x+13$ לאותו אותו מופען.

הגדרה 3.4 צופן האפיני

יהי $P = C = \mathbb{Z}_{26}$ ויהי

$$K = \{a, b \in \mathbb{Z}_{26} \mid \gcd(a, 26) = 1\}.$$

עבור $k = (a, b) \in K$ נגידיר כלל המצפין

$$e_k(x) = (ax + b) \pmod{26},$$

ועבור $y \in \mathbb{Z}_{26}$ נגידיר כלל המעננה

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

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 לבדוק 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):

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

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

3.8 דוגמה

נתון כלל מצפן של צופן אפיני בעל המפתח (a, b) .

- 1) רשמו את כלל המצפן.
- 2) רשמו את כלל המפענה.
- 3) בדקו כי התנאי

מתקיים.

פתרונות:

1) כלל המצפן הוא

$$e_k(x) = 7x + 3 \pmod{26},$$

2) כלל המפענה הוא

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

3) נבדוק כי הכלל מפענה המתivalent מקיים x

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



3.9 דוגמה

בעזרת הצופן של דוגמה 3.8

- 1) מצאו את הטקסט מוצפן של הטקסט גליי

hot.

(2) בדקו שהפעולה של הכלל מפענча על הטקסט מוצפן מהזיר את טקסט גליי

hot .

פתרון:

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

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

נפעיל את הכלל מוצפן על הערכים x :

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

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

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

مكان נקבל

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

לכן הטקסט מוצפן המתקבל הוא
AXG

סעיף 2) הכלל מפענча הוא
 $d_k(y) = 15y + 7$.

נעביר את הواتיות של AXG לערכים של \mathbb{Z}_{26} :

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

נפעיל את הכלל מפענה על הערכים y :

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

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

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

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

לכן הטקסט גליי המתקבל הוא
 hot
 כנדרש.



3.10 דוגמה

נתון הטקסט מוצפן

ACSE

והמפתח $(23, 2)$ של צופן אפייני. מצאו את הטקסט גליי.

פתרון:

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

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

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

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

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

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

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

$y \in C$	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'נֶר

צופן ההזהה וצופן החלפה דוגמאות של צופן מונואלפיבטי: כל TWO אלפביתיים ב- P נתאים לטו אלפביתי יחיד ב- C . צופן ויז'נֶר הוא צופן פוליאלפיבטי: אין מצפינים כל אות בנפרד, אלא בלוקים, או קבוצות של כמה אותיות באורך קבוע m .

הגדרה 3.5 צופן ויז'נֶר (Vigenere Cipher)

יהי m מספר שלם חיובי.

נגדיר $P = C = K = \mathbb{Z}_{26}^m$

עבור מפתח $k = (k_1, k_2, \dots, k_m)$ נגדיר כלל מצפן

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

ונגדיר כלל מפענה

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

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

דוגמה 3.11

נתון הטקסט גלי

string

$.k = \text{ AND }$ והמפתח

1) מצאו את הכלל מצפין והכלל מפענה.

2) מצאו את הטקסט מצפון.

3) בדקו כי הכלל מפענה מוחזר את הטקסט גליי.

פתרונות:

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 מפענה הוא

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

2) נעביר את האותיות של הטקסט גליי 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 גליי יחד עם הערך המתאים של \mathbb{Z}_{26} למת-קובוצות של 3 תווים:

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

בכל מת-קובוצה, נתאים לכל TWO ערך של המפתח

$x \in P$	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 שלישייה (x_1, x_2, x_3) בבלוק אחד, נפעיל את כלל המצפין

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

לדוגמה בבלוק הראשון נקבל

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

בלוק 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

הtekסט מוצפן המתכבר 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 הטליה של התווים של הטקסט גלוי יחד עם הערכים המתאימים של \mathbb{Z}_{26} לחת-קבוצות של 3 תווים:

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

בכל חת-קבוצה, נתאים לכל TWO 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 שלייה (y_1, y_2, y_3) בבלוק אחד, נפעיל את כלל המיפוי

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

לדוגמה בבלוק הראשון קיבל

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

בלוק השני קיבל

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

$y \in C$	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

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

$y \in C$	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

הtekst גלי 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 גלי

thiscryptosystemisnotsecure.

מצאו את הטקסט מוצפן.

פתרון:
שלב 1:

נעביר את האותיות של הטקסט גלי 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

שלב 2:

נפרק את הפעלה של התווים של הטקסט גלי יחד עם הערכים המתאימים של \mathbb{Z}_{26} לחת-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

שלב 3:

בכל חת-קבוצה, נתאים לכל TWO ערך של המפתח :

$x \in P$	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

שלב 3:על כל ששייה $(x_1, x_2, x_3, x_4, x_5, x_6)$ בבלוק אחד, נפעיל את כלל המכפין

$$e_k(x_1, x_2, x_3, x_4, x_5, x_6) = (x_1 + k_1, x_2 + k_2, x_3 + k_3, x_4 + k_4, x_5 + k_5, x_6 + k_6) \pmod{26}.$$

לדוגמא בבלוק הראשון קיבל

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

$x \in P$	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

שלב 4:

מעבר את הערכים של אותיות של הטקסט 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

הтекסט מוצפן המתקבל הוא

VPXZGIAIXIVWPUBTMJPWIZITWZT



3.6 צופן היל

הגדרה 3.6 צופן היל

נניח כי $2 \leq m$ 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 מפענה

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

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

הגדרה 3.7 המטריצה של קופקטורים

תהי $A \in \mathbb{R}^{n \times n}$.

הkopקטור ה- (i, j) של A מוגדר להיות הדטרמיננטה של המטריצה המותקבלת 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 $|A| \neq 0$ 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 טקסט גליי

July

ונתנו המפתח

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

של צופן היל. מצאו את הטקסט מוצפן.

פתרונות:
שלב 1:

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

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

שלב 2:נפרק את הטלחה של התווים של הטקסט גליי יחד עם הערכים המתאים של \mathbb{Z}_{26} לחת-קבוצות של $m = 2$ תווים:

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

שלב 3:

עבור כל תת-קובוצה המתקבל נחשב

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

עבור התת-קובוצה הראשונה קיבל

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

עבור התת-קובוצה השנייה קיבל

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

$x \in P$	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:נעביר את הערכים $y \in \mathbb{Z}_{26}$ לאותיות של הטקסט 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

הтекסט מוצפן המתקבל הוא

DELW

■

דוגמה 3.14

נתון רצף טקסט מוצפן

DELW

ונתון המפתח

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

של צופן היל. מצאו את הטקסט גלי.

פתרון:שלב 0:נחשב את החופכית k^{-1} :

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

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

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

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

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

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

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

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

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

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

לפיכך

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

שלב 1:נעביר את האותיות של הטקסט גלי לערכים של \mathbb{Z}_{26} :

$$\begin{array}{c|c|c|c|c} y \in C & D & E & L & W \\ \hline y \in \mathbb{Z}_{26} & 3 & 4 & 11 & 22 \end{array}$$

שלב 2:נפרק את הטלבה של התווים של הטקסט מוצפן יחד עם הערכים המתאימים של \mathbb{Z}_{26} למת-קבוצות של 2 תווים:

$$\begin{array}{c|c|c||c|c} y \in C & D & E & L & W \\ \hline y \in \mathbb{Z}_{26} & 3 & 4 & 11 & 22 \end{array}$$

שלב 3:

עבור כל מת-קובוצה המתקבל נחשב

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

עבור המת-קובוצה הראשונה נקבל

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

עבור המת-קובוצה השנייה נקבל

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

$y \in C$	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

שלב 5:נעביר את הערכים $y \in \mathbb{Z}_{26}$ לאותיות של הטקסט מוצפן:

$y \in C$	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
$x \in P$	j	u	l	y

הtekst גלי המתקבל הוא

july

**3.15 דוגמה**

נתון רצף טקסט מוצפן

PGRFGGCSY

ונתנו המפתח

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

של צופן היל. מצאו את הטקסט גלי.

פתרונות:שלב 0:נחשב את ההופכית $:k^{-1}$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

לפי

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

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

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

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

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

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

לפיכך

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

שלב 1:

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

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

שלב 2:

נפרק את הטלבה של התווים של הטקסט מוצפן יחד עם הערכים המתאימים של \mathbb{Z}_{26} לחת-קבוצות של 3 תווים:

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

שלב 3:

עבור כל תת-קבוצה המתאפשר נחשב

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

עבור התת-קבוצה הראשונה קיבל

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

עבור התת-קבוצה השנייה קיבל

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

עבור התת-קבוצה השלישי נקבל

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

$y \in C$	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

שלב 5:

נעביר 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

הтекסט גלי המתקבל הוא

howareyou

3.7 צופן התמורה

הגדרה 3.9 צופן התמורה (permutation cipher)

נניח כי m מספר שלמים חיובי. יהיו $P = C = \mathbb{Z}_{26}^m$ ויהי K Subset של כל התמורות האפשריות של $\{1, \dots, m\}$. עבור מפתח $\pi \in K$ (עבור תמורה של K) נגידר כלל מצפין

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

ונגידר כלל מפענה

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

כאשר π^{-1} התמורה ההפוכה של π .

דוגמה 3.16

נתון התמורה הבאה:

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

ונתנו את הטקסט גלי

flower

- 1) מצאו את הטקסט מוצפן.
- 2) מצאו את הטקסט גליי באמצעות פענח את הטקסט מוצפן מסעיף הקודם עם התמורה ההופכית.

פתרונות:

סעיף 1) שלב 1:

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

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

שלב 2:

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

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

שלב 3:

עבור כל תת-קבוצה המתקבל נפעיל את התמורה π :

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

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

$x \in P$	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

שלב 4:

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

$x \in P$	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
$y \in C$	L	O	F	E	R	W

לכן הטקסט מוצפן הוא

סעיף 2שלב 1:

נתחיל עם הטקסט מוצפן

LOFERW

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

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

שלב 2:נפרק את הטרבלת התווים של הטקסט גליי יחד עם הערכים המותאימים של \mathbb{Z}_{26} למת-קבוצות של $3 = m$ תווים:

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

שלב 3:עבור כל מת-קבוצה המתקבל נפעיל את התמורה ההופכית: π^{-1} :

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

$$(11 \ 14 \ 5) \xrightarrow{\pi^{-1}} (5 \ 11 \ 14)$$

$$(4 \ 17 \ 22) \xrightarrow{\pi^{-1}} (22 \ 4 \ 17)$$

$y \in C$	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

שלב 4:נעבור את הערכים $y \in \mathbb{Z}_{26}$ לאותיות של הטקסט גליי:

$y \in C$	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
$x \in C$	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 כך מתקבל על ידי הכלל מצפין

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

צפנים מסוג זה נקראים צפני בлок.

כעת נדבר על צפני זרם. להתחילה 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 גלוים אפשריים (plaintexts),
- (2) C מסמן קבוצה של טקסטים מוצפנים אפשריים (ciphertexts),
- (3) K מסמן קבוצה של המפתחות אפשריים (keyspace),
- (4) L מסמן את האלפבית של המפתח הפנימי (key-stream alphabet).
- (5) g מסמן את ה **מחולל הפנימי** (keystream generator). g מקבלת מפתח k ומחזירה רצף אותיות אינסופי $\dots z_1 z_2 \dots$ כאשר $z_i \in L$ לכל $i \geq 1$.
- (6) לכל $z \in L$ יש כלל מצפין $E_z \in E$ וכלל מפענה $d_z \in D$:

$$e_z : P \rightarrow C , \quad d_z : C \rightarrow P ,$$

כך ש-

$$d_z(e_z(x)) = x$$

לכל איבר של מרחב הטקסט גלי P

הגדרה 3.11 צופן אוטו מפתח (Autokey cipher)

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

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

$$\text{לכל } z \in \mathbb{Z}_{26} \text{ נגדיר כלל מצפין} \\ e_z(x) = (x + z) \mod 26$$

$$\text{לכל } x \in \mathbb{Z}_{26} \text{ ונגידר כלל מפענה} \\ d_z(y) = (y - z) \mod 26$$

לכל $y \in \mathbb{Z}_{26}$

דוגמה 3.17 (צופן אוטו-מפתח)

נתוון צופן אוטו-מפתח עם מפתח 8 .

1) מצאו את הטקסט מוצפן של המילה
rendezvous .

(2) פענו את הטקסט מוצפן המתקבל וודאו שקיבלתם את הטקסט המקורי.

פתרון:

סעיף 1) נרשום את האותיות של הטקסט המקורי ב- \mathbb{Z}_{26} :

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

המפתח הפנימי הוא

x _i ∈ \mathbb{Z}_{26}	17	4	13	3	4	25	21	14	20	18
z _i ∈ \mathbb{Z}_{26}	8	17	4	13	3	4	25	21	14	20

על פי המפתח הפנימי נפעיל את הכלל מצפין

$$e_z(x_i) = x_i + z_i \pmod{26}$$

על הטקסט המקורי ונחשב את ה- y_i של הטקסט מצפון באמצעות הכלל מצפין:

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

x ∈ P	r	e	n	d	e	z	v	o	u	s
x _i ∈ \mathbb{Z}_{26}	17	4	13	3	4	25	21	14	20	18
z _i ∈ \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 הטקסט מוצפן:

x ∈ P	r	e	n	d	e	z	v	o	u	s
x _i ∈ \mathbb{Z}_{26}	17	4	13	3	4	25	21	14	20	18
z _i ∈ \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 ∈ C	Z	V	R	Q	H	D	U	J	I	M

סעיף 2) נתחיל עם הטקסט 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 גליי באמצעות הכלל מפענה:

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

$y \in C$	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} לאותים של טקסט גליי:

$y \in C$	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 $k \in (\mathbb{Z}_2)^n$ נגידר כלל מצפין

$$e_k(x) = (x_1 + k_1, \dots, x_n + k_n) \bmod 2,$$

ונגידר כלל מפענה

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

דוגמיה 3.18

נתון הקבוצה מפתחות $K = \{0, 1, 1, 0, 0\}$ של צופן חד-פעמי ונთון הטקסט גליי $x = 1110100010$.

(1) מצאו את הטקסט מוצפן.

(2) וודאו כי הכלל מפענח מחזירה הטקסט גליי המקורי.

פתרונות:

(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 שאנו לצופן חד-פעמי יש סודיות מושלמת.