

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 $d \in D$:

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

כך ש-

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

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 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 אזי 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

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

-1

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

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

3.1 דוגמה

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 הרצף 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

הטקסט 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 $d_0 = 0, d_1 = 1, d_2 = 2 \dots$ בתור.

$y \in C$	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

דוגמה 3.3

נתון הטקסט מוצפן הבא:

QRQXFJANH XD

מצאו את הטקסט גלוי

פתרון:

ננסה לפענח את הטקסט מוצפן בעזרת הצופן הזזה עם המפתחות d_0, d_1, \dots 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 $k = 9$.

משפט 3.1 צופן הזהה ניתן לפענוח

צופן הזהה ניתן לפענוח. כלומר, אם $e_k(x) = x + k \bmod 26$ ו- $d_k(x) = x - k \bmod 26$ אזי

$$d_k(e_k(x)) = x \bmod 26 .$$

הוכחה:

$$\begin{aligned}
 d_k(e_k(x)) &= (e_k(x) - k) \bmod 26 \\
 &= ((x + k) \bmod 26 - k) \bmod 26 .
 \end{aligned}$$

נציב $q = \left\lfloor \frac{x + k}{26} \right\rfloor$ נקבל $(x + k) \bmod 26 = x + k - 26q$ כאשר q הוא מספר שלם, ונקבל

$$\begin{aligned}
 d_k(e_k(x)) &= (x + k - 26q - k) \bmod 26 \\
 &= (x - 26q) \bmod 26
 \end{aligned}$$

מכיוון ש- q הוא מספר שלם אזי $(x - 26q) \bmod 26 \equiv x \bmod 26$ לכן לפי משפט :

$$d_k(e_k(x)) = (x - 26q) \bmod 26 = x \bmod 26 .$$

3.3 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)

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

יש פתרון יחיד ל- x .

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

משפט 3.2

ליחס שקילות

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

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

הוכחה:

כיוון \Leftarrow

נניח ש- $\gcd(a, 26) = 1$. לכן לפי משפט בזו קיימים שלמים x, y כך ש- $xa + y(26) = 1$. נעביר אגפים ונקבל:
 $xa \equiv 1 \pmod{26}$ ולכן $xa = 1 - y(26)$.

כיוון \Rightarrow

נניח ש- $ax \equiv 1 \pmod{26}$. אזי קיים שלם q עבורו $ax = q(26) + 1$. נעביר אגפים ונקבל: $ax + (-q)(26) = 1$.
לכן קיימים שלמים x ו- $y = -q$ כך ש: $ax + y(26) = 1$. לכן לפי משפט בזו, $\gcd(a, 26) = 1$.

דוגמה 3.4

בדקו אם הפונקציה

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

כלל מצפין תקין, כלומר בדקו אם קיים כלל מפענח.

פתרון:

$\gcd(4, 26) = 2$, אז הפונקציה $e(x) = 4x + 7 \pmod{26}$ 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- $x + 13$:

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

בעוד

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

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

הגדרה 3.3 צופן האפיני

יהי $P = C = \mathbb{Z}_{26}$ ויהי

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

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

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

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

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

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 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):

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

הפרמטר b מקבל כל איבר של \mathbb{Z}_{26} .

לפיכך לצופן האפיני יש $12 \times 26 = 312$ מפתחות אפשריות.

דוגמה 3.5

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

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

(2) כלל המפענח 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 מפענח המתקבל מקיים $d_k(e_k(x)) = x$

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

דוגמה 3.6

בעזרת הצופן של דוגמה 3.5:

(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 הוואתיות של hot לערכים של \mathbb{Z}_{26} :

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

נפעיל את הכלל מצפין על הערכים x :

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

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

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

מכאן 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 מפענח הוא

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

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

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

נפעיל את הכלל מפענח על הערכים y :

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

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

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

$y \in C$	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 גלוי המתקבל הוא

hot

כנדרש.

דוגמה 3.7

נתון הטקסט מוצפן

ACSE

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

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 הוואטיות 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

3.4 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 פוליאלפביתי: אין מצפינים כל אות בנפרד, אלא בלוקים, או קבוצות של כמה אותיות באורך קבוע m .

הגדרה 3.4 צופן ויז'נר (Vigenere Cipher)

יהי m מספר שלם חיובי.

נגדיר $P = C = K = \mathbb{Z}_{26}^m$.

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

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

ונגדיר כלל מפענח

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

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

3.8 דוגמה

נתון הטקסט גלוי

string

והמפתח $k =$ AND

(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) בב्लוק 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 בב्लוק הראשון נקבל

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

בב्लוק 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 שלישייה (y_1, y_2, y_3) בב्लוק 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 בב्लוק הראשון נקבל

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

בב्लוק 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.



3.9 דוגמה

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:

שלב 1:

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

שלב 2:

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

שלב 3:

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

שלב 3:

על כל ששיה $(x_1, x_2, x_3, x_4, x_5, x_6)$ בבלוק אחד, נפעיל את כלל המצפין

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

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

שלב 4:

נעבור את הערכים $y \in \mathbb{Z}_{26}$ לאותיות 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

הטקסט מוצפן המתקבל הוא

VPXZGIA XIVWPUBTTMJPWIZITWZT

3.5 צופן היל

הגדרה 3.5 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 נצצעות ב- \mathbb{Z}_{26} .

הגדרה 3.6 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 3.7 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 3.3 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 3.10

נתון רצף טקסט גלוי

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} :

$x \in P$	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:

$x \in P$	j	u	1	y
$x \in \mathbb{Z}_{26}$	9	20	11	24

שלב 3:

עבור כל תת-קבוצה 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-קבוצה הראשונה נקבל

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

עבור התת-קבוצה השנייה נקבל

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

$x \in P$	j	u	1	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 הטקסט מוצפן:

$x \in P$	j	u	1	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

הטקסט מוצפן המתקבל הוא

DELW

דוגמה 3.11

נתון רצף טקסט 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} .

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

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

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

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

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

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

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

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

לפיכך

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

שלב 1:

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

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

שלב 2:

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

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

שלב 3:

עבור כל תת-קבוצה 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 התת-קבוצה 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 התת-קבוצה 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:

נעבור 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

הטקסט גלוי המתקבל הוא

july

דוגמה 3.12

נתון רצף טקסט מוצפן

ונתון המפתח

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

של צופן היל. מצאו את הטקסט גלוי.

פתרון:שלב 0:נחשב את ההופכית k^{-1} :

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

לפיכך

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

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

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

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

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

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

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 גלוי 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 הטבלה של התווים של הטקסט מוצפן יחד עם הערכים המתאימים של \mathbb{Z}_{26} לתת-קבוצות של $m = 3$ 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 המתקבל 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 נקבל

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

עבור התת-קבוצה השנייה נקבל

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

עבור התת-קבוצה השלישית 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:

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