

## שיעור 5

### קריפטו-אליזה

#### **1.5. סוגים של התקפת סייבר**

נניח שאليس שולחת הודעה מוצפנת לבוב. יש גורם עיון, אוסקר, שמנסה לצותת לשיחתם. אנחנו מניחים כי אוסקר מודע לקריפטו-מערכת (הצופן) שבאמצעותה אליס הצפינה את הודעה. ההנחה הזאת נקראת עקרון קירשוף Kerchoff's principle.

המטרה בהרכבת צופן היא שהצופן מספיק בטוח כך שאוסקר לא יוכל לפענה אפילו אם הוא ידוע את הסוג של הצופן בשימוש.

ישנו 4 סוגי התקפת סייבר.

**1) התקפת טקסט מוצפן בלבד.**

למתקיף (אוסקר) יש מהרוזת של טקסט מוצפן ע' .

**2) התקפת טקסט גליי ידוע**

למתקיף יש מהרוזת של טקסט גליי × יחד עם הטקסט מוצפן המתאים ע' .

**3) התקפת טקסט גליי נבחר**

למתקיף היכולת להשיג טקסטים גלייים × של טקסטים מוצפניהם ע' כלשהם חופשי בחירתו, שהוצפנו באמצעות הקריפטו-מערכת המותקפה.

**4) התקפת טקסט מוצפן נבחר**

למתקיף היכולת להשיג טקסטים מוצפניהם ע' של טקסטים גלייים × כלשהם חופשי בחירתו, שהוצפנו באמצעות הקריפטו-מערכת המותקפה.

החלק הבא מתעסק עם התקפת טקסט מוצפן.

#### **5.2 קבוצות אותיות הנפוצים ביותר בтекסט גליי**

התקפת טקסט מוצפן בלבד מבוססת על ההתדיינות של אותיות בקיטסט גליי בשפה אנגלית.

### כלל 5.1 פונקציית הסתברות של האותיות של האלפיבית

אות	הסתברות	אות	הסתברות
a	0.082	n	0.067
b	0.015	o	0.075
c	0.028	p	0.019
d	0.043	q	0.001
e	0.127	r	0.06
f	0.022	s	0.063
g	0.02	t	0.091
h	0.061	u	0.028
i	0.07	v	0.01
j	0.002	w	0.023
k	0.008	x	0.001
l	0.04	y	0.02
m	0.024	z	0.001

Piper Becker ו- Sdroo צדרו את האותיות לחמש קבוצות שונות, לפי הסדר גודל של התדריות של האותיות בטקסט גליי.

### כלל 5.2 קבוצות תדריות של אותיות בטקסט גליי

	אות	הסתברות
1.	e	$p = 0.127$
2.	t, a, o, i, n, s, h, r	$0.06 \lesssim p \lesssim 0.09$
3.	d, l	$p \approx 0.04$
4.	c, u, m, w, f, g, y, p, b	$0.015 \lesssim p \lesssim 0.028$
5.	v, k, j, x, q, z	$p < 0.01$

### כלל 5.3 זוגות אותיות הנפוצים ביותר בטקסט גליי

השלושים זוגות אותיות הנפוצים ביותר בטקסט גליי רשומים בטבלה למטה:

th	he	in	er	an	re	ed	on	es	st
en	at	to	nt	ha	nd	ou	ea	ng	as
or	ti	is	et	it	ar	te	se	hi	of

#### כלל 5.4 קבוצות שלושת אותיות הנפוצים ביותר בטקסט גלי

ה12 שלשות של אותיות הנפוצים ביותר בטקסט גלי רשומים בטבלה למטה:

the	ing	and	her	ere	ent
tha	nth	was	eth	for	dth

### 5.3 קריפטו-אנליזה של צופן האפיני

זו דוגמה של התקפת טקסט מוצפן בלבד.

#### דוגמה 5.1

נניח כי אליס שלחה הודעה מוצפנת לבוב ואוסקר השיג את ההודעה. הטקסט מוצפן הוא

KARSRROHVUKARPFSZFERXERFKREKAFSKARSRROHVUKARURTVEKARVSR

-aoskar יודע כי אליס הצינה את ההודעה באמצעות צופן איפיני אבל הוא לא יודע את המפתח. כתת הוא מנסה לפענה אותה. מצאו את הטקסט גלי.

**פתרון:**

**שלב 1)** נרשום את התדריות של האותיות המופיעות בטקסט מוצפן:

A	6	N	0
B	0	O	2
C	0	P	1
D	0	Q	0
E	4	R	14
F	4	S	5
G	0	T	1
H	2	U	3
I	0	V	4
J	0	W	0
K	7	X	1
L	0	Y	0
M	0	Z	1

**שלב 2)** נרשום את האותיות הנפוצות ביותר:

- R מופיעה 14 פעמים.
- K מופיעה 7 פעמים.
- A מופיעה 6 פעמים.
- S מופיעה 5 פעמים.
- E, F, V מופיעות 4 פעמים.
- U מופיעה 3 פעמים.

**שלב 3)** ננסה למצוא את המפתח  $(a, b) \in \mathbb{Z}_{26}$  של הכלל מצפן של הצופן אפייני

$$e_k(x) = ax + b ,$$

לכל  $x \in \mathbb{Z}_{26}$  על ידי התאמת אותיות hei נפוצות.

$$e \xrightarrow{e_k} R , \quad t \xrightarrow{e_k} K .$$

$$\begin{aligned} e_k(4) &= 17 \\ e_k(19) &= 10 . \end{aligned}$$

$$\begin{aligned} &\bullet \text{ נציב } e_k = ax + b \text{ ונקבל} \\ 4a + b &= 17 , \\ 19a + b &= 10 . \end{aligned}$$

כעת נפתרו את המערכת מעל  $\mathbb{Z}_{26}$ :

$$\left( \begin{array}{cc|c} 4 & 1 & 17 \\ 19 & 1 & 10 \end{array} \right) \xrightarrow{R_2 \rightarrow R_2 - R_1} \left( \begin{array}{cc|c} 4 & 1 & 17 \\ 15 & 0 & -7 \end{array} \right) = \left( \begin{array}{cc|c} 4 & 1 & 17 \\ 15 & 0 & 19 \end{array} \right)$$

$$\xrightarrow{R_2 \rightarrow 15^{-1}R_2 = 7R_2} \left( \begin{array}{cc|c} 4 & 1 & 17 \\ 1 & 0 & 133 \end{array} \right) = \left( \begin{array}{cc|c} 4 & 1 & 17 \\ 1 & 0 & 3 \end{array} \right)$$

$$\xrightarrow{R_1 \rightarrow R_1 - 4R_2} \left( \begin{array}{cc|c} 0 & 1 & 5 \\ 1 & 0 & 3 \end{array} \right)$$

$$a = 3, b = 5$$

$k = (3, 5)$  אז המפתח  $\text{gcd}(a, 26) = 1$

- נבנה את הכלל מפענה עם המפתח המתקיים:

$$\begin{aligned} d_k(y) &= a^{-1}(y - b) \pmod{26} \\ &= 3^{-1}(y - 5) \\ &= 9(y - 5) \pmod{26} \\ &= 9y - 45 \pmod{26} \\ &= 9y + 7. \end{aligned}$$

**שלב 4)** ננסה לפענה את הטקסט מצפן עם הכלל מפענה

$y \in C$	K	A	R	S	R	R	O	H	V	U	K	A	R	P	F	S	Z	F	E	R
$y \in \mathbb{Z}_{26}$	10	0	17	18	17	17	14	7	21	20	10	0	17	15	5	18	25	5	4	17
$x = d_k(y) \in \mathbb{Z}_{26}$	19	7	4	13	4	4	3	18	14	5	19	7	4	12	0	13	24	0	17	4
$x \in P$	t	h	e	n	e	e	d	s	o	t	t	h	e	m	a	n	y	a	r	e

$y \in C$	X	E	R	F	K	R	E	K	A	F	S	K	A	R	S	R	R	O	H
$y \in \mathbb{Z}_{26}$	23	4	17	5	10	17	4	10	0	5	18	10	0	17	18	17	17	14	7
$x = d_k(y) \in \mathbb{Z}_{26}$	6	17	4	0	19	4	17	19	7	0	13	19	7	4	13	4	4	3	18
$x \in P$	g	r	e	a	t	e	r	t	h	a	n	t	h	e	n	e	e	d	s

$y \in C$	V	U	K	A	R	U	R	T	V	E	K	A	R	V	S	R
$y \in \mathbb{Z}_{26}$	21	20	10	0	17	20	17	19	21	4	10	0	17	21	18	17
$x = d_k(y) \in \mathbb{Z}_{26}$	14	5	19	7	4	5	4	22	14	17	19	7	4	14	13	4
$x \in P$	o	f	t	h	e	f	e	w	o	r	t	h	e	o	n	e



## דוגמה 5.2

נניח כי אליס שלחה הודעה מוצפנת לבוב ואוסקר השיג את ההודעה. הטקסט מוצפן הוא

FMXVEDKAPHFERBNDKRXRSREFMORUDSDKDVSHVUFEDKAPRKDLYEVLRHHRH

אוסקר ידוע כי אליס השתמשה בצופן איפיני אבל אינו יודע את המפתח. כתע הוא מנסה לפענה אותה. מצאו את הטקסט גלי.

**פתרון:**

**שלב 1)** נרשום את התדריות של האותיות המופיעות בטקסט מוצפן:

A	2	N	1
B	1	O	1
C	0	P	2
D	7	Q	0
E	5	R	8
F	4	S	3
G	0	T	0
H	5	U	2
I	0	V	4
J	0	W	0
K	5	X	2
L	2	Y	1
M	2	Z	0

**שלב 2)** נרשום את האותיות הנפוצות ביותר:

- R מופיעה 8 פעמים.
- D מופיעה 7 פעמים.
- E, H, K מופיעות 5 פעמים.
- F, V מופיעה 4 פעמים.

**שלב 3)** ננסה למצוא את המפתח  $(a, b) \in \mathbb{Z}_{26}$  של הכלל מצפן של הצופן אפיני

$$e_k(x) = ax + b ,$$

לכל  $x \in \mathbb{Z}_{26}$  על ידי התאמת אותיות הכי נפוצים.

$$e \xrightarrow{e_k} R , \quad t \xrightarrow{e_k} D .$$

• נניח כי

$$\begin{aligned} e_k(4) &= 17 \\ e_k(19) &= 3 . \end{aligned}$$

• נציב  $b$  ונקבל

$$\begin{aligned} 4a + b &= 17 , \\ 19a + b &= 3 . \end{aligned}$$

כעת נפתרו את המערכת מעל :

$$\left( \begin{array}{cc|c} 4 & 1 & 17 \\ 19 & 1 & 3 \end{array} \right) \xrightarrow{R_2 \rightarrow R_2 - R_1} \left( \begin{array}{cc|c} 4 & 1 & 17 \\ 15 & 0 & -14 \end{array} \right) = \left( \begin{array}{cc|c} 4 & 1 & 17 \\ 15 & 0 & 12 \end{array} \right) \xrightarrow{R_2 \rightarrow 15^{-1}R_2 = 7R_2} \left( \begin{array}{cc|c} 4 & 1 & 17 \\ 1 & 0 & 84 \end{array} \right) = \left( \begin{array}{cc|c} 4 & 1 & 17 \\ 1 & 0 & 6 \end{array} \right)$$

$$\xrightarrow{R_1 \rightarrow R_1 - 4R_2} \left( \begin{array}{cc|c} 0 & 1 & -7 \\ 1 & 0 & 6 \end{array} \right) = \left( \begin{array}{cc|c} 0 & 1 & 19 \\ 1 & 0 & 6 \end{array} \right)$$

.gcd( $a, 26$ ) = 2 ≠ 1 המפתח הזה לא תקין בغالל ש-

• עכשו נחזיר וננסה

$$e \xrightarrow{e_k} R , \quad t \xrightarrow{e_k} E .$$

• נ"א

$$\begin{aligned} e_k(4) &= 17 \\ e_k(19) &= 4 . \end{aligned}$$

• נציג  $e_k = ax + b$  ונקבל

$$\begin{aligned} 4a + b &= 17, \\ 19a + b &= 4. \end{aligned}$$

כעת נפתח את המערכת מעל  $\mathbb{Z}_{26}$

$$\left( \begin{array}{cc|c} 4 & 1 & 17 \\ 19 & 1 & 4 \end{array} \right) \xrightarrow{R_2 \rightarrow R_2 - R_1} \left( \begin{array}{cc|c} 4 & 1 & 17 \\ 15 & 0 & -13 \end{array} \right) = \left( \begin{array}{cc|c} 4 & 1 & 17 \\ 15 & 0 & 13 \end{array} \right) \xrightarrow{R_2 \rightarrow 15^{-1}R_2 = 7R_2} \left( \begin{array}{cc|c} 4 & 1 & 17 \\ 1 & 0 & 91 \end{array} \right) = \left( \begin{array}{cc|c} 4 & 1 & 17 \\ 1 & 0 & 13 \end{array} \right)$$

$$\xrightarrow{R_1 \rightarrow R_1 - 4R_2} \left( \begin{array}{cc|c} 0 & 1 & -35 \\ 1 & 0 & 13 \end{array} \right) = \left( \begin{array}{cc|c} 0 & 1 & 17 \\ 1 & 0 & 13 \end{array} \right)$$

.gcd( $a, 26$ ) = 2 ≠ 1 המפתח זהה גם לא תקין בغالל ש-

עכשו נחזור וננסה

$$e \xrightarrow{e_k} R, \quad t \xrightarrow{e_k} H.$$

א"ז •

$$e_k(4) = 17$$

$$e_k(19) = 7.$$

• נציג  $e_k = ax + b$  ונקבל

$$\begin{aligned} 4a + b &= 17, \\ 19a + b &= 7. \end{aligned}$$

כעת נפתח את המערכת מעל  $\mathbb{Z}_{26}$

$$\left( \begin{array}{cc|c} 4 & 1 & 17 \\ 19 & 1 & 7 \end{array} \right) \xrightarrow{R_2 \rightarrow R_2 - R_1} \left( \begin{array}{cc|c} 4 & 1 & 17 \\ 15 & 0 & -10 \end{array} \right) = \left( \begin{array}{cc|c} 4 & 1 & 17 \\ 15 & 0 & 16 \end{array} \right) \xrightarrow{R_2 \rightarrow 15^{-1}R_2 = 7R_2} \left( \begin{array}{cc|c} 4 & 1 & 17 \\ 1 & 0 & 112 \end{array} \right) = \left( \begin{array}{cc|c} 4 & 1 & 17 \\ 1 & 0 & 8 \end{array} \right)$$

$$\xrightarrow{R_1 \rightarrow R_1 - 4R_2} \left( \begin{array}{cc|c} 0 & 1 & -15 \\ 1 & 0 & 8 \end{array} \right) = \left( \begin{array}{cc|c} 0 & 1 & 11 \\ 1 & 0 & 13 \end{array} \right)$$

.gcd( $a, 26$ ) = 2 ≠ 1 המפתח זהה גם לא תקין בغالל ש-

עכשו נחזור וננסה

$$e \xrightarrow{e_k} R, \quad t \xrightarrow{e_k} K.$$

א"ז •

$$e_k(4) = 17$$

$$e_k(19) = 10.$$

• נציג  $e_k = ax + b$  ונקבל

$$\begin{aligned} 4a + b &= 17, \\ 19a + b &= 10. \end{aligned}$$

כעת נפתח את המערכת מעל  $\mathbb{Z}_{26}$

$$\left( \begin{array}{cc|c} 4 & 1 & 17 \\ 19 & 1 & 10 \end{array} \right) \xrightarrow{R_2 \rightarrow R_2 - R_1} \left( \begin{array}{cc|c} 4 & 1 & 17 \\ 15 & 0 & -7 \end{array} \right) = \left( \begin{array}{cc|c} 4 & 1 & 17 \\ 15 & 0 & 19 \end{array} \right) \xrightarrow{R_2 \rightarrow 15^{-1}R_2 = 7R_2} \left( \begin{array}{cc|c} 4 & 1 & 17 \\ 1 & 0 & 133 \end{array} \right) = \left( \begin{array}{cc|c} 4 & 1 & 17 \\ 1 & 0 & 3 \end{array} \right)$$

$$\xrightarrow{R_1 \rightarrow R_1 - 4R_2} \left( \begin{array}{cc|c} 0 & 1 & 5 \\ 1 & 0 & 3 \end{array} \right)$$

$a = 3, b = 5$  א"ז

$k = (3, 5)$  אז המפתח gcd( $a, 26$ ) = 1

- נבנה את הכלל מפענה עם המפתח המתובל:

$$\begin{aligned}
 d_k(y) &= a^{-1}(y - b) \pmod{26} \\
 &= 3^{-1}(y - 5) \\
 &= 9(y - 5) \pmod{26} \\
 &= 9y - 45 \pmod{26} \\
 &= 9y + 7 .
 \end{aligned}$$

**שלב 4)** ננסה לפענה את הטקסט מצפונו עם הכלל מפענה

$y \in C$	F	M	X	V	E	D	K	A	P	H	F	E	R	B	N	D	K	R	X	R
$y \in \mathbb{Z}_{26}$	5	12	23	21	4	3	10	0	15	7	5	4	17	1	13	3	10	17	23	17
$x = d_k(y) \in \mathbb{Z}_{26}$	0	11	6	14	17	8	19	7	12	18	0	17	4	16	20	8	19	4	6	4
$x \in P$	a	l	g	o	r	i	t	h	m	s	a	r	e	q	u	i	t	e	g	e

$y \in C$	S	R	E	F	M	O	R	U	D	S	D	K	D	V	S	H	V	U	F	E
$y \in \mathbb{Z}_{26}$	18	17	4	5	12	14	17	20	3	18	3	10	3	21	18	7	21	20	5	4
$x = d_k(y) \in \mathbb{Z}_{26}$	13	4	17	0	11	3	4	5	8	13	8	19	8	14	13	18	14	5	0	17
$x \in P$	n	e	r	a	l	d	e	f	i	n	i	t	i	o	n	s	o	f	a	r

$y \in C$	D	K	A	P	R	K	D	L	Y	E	V	L	R	H	H	R	H
$y \in \mathbb{Z}_{26}$	3	10	0	15	17	10	3	11	24	4	21	11	17	7	7	17	7
$x = d_k(y) \in \mathbb{Z}_{26}$	8	19	7	12	4	19	8	2	15	17	14	2	4	18	18	4	18
$x \in P$	i	t	h	m	e	t	i	c	p	r	o	c	e	s	s	e	s



## 5.4 קרייפטו-אליזה של צופן היל

זו דוגמה של התקפת טקסט גליי ידוע.

### משפט 5.1

נניח שלמתקיף יש מחרוזת טקסט גליי  $x$  ומחרוזת טקסט מוצפן שלו. נניח כי המתקיף יודע כי הטקסט הוצפן באמצעות צופן היל עם מפתח של סדר  $m$ .

נניח שיש למתקיף לפחות  $m$  טקסטים גליים וטקסטים מוצפנים. של הטקסט גליי:

$$x_j = (x_{1j}, x_{2j}, \dots, x_{mj})$$

-1

$$y_j = (y_{1j}, y_{2j}, \dots, y_{mj})$$

$j \leq 1 \text{ עד ש-}$

$$y_j = e_k(x_j) .$$

נגידר שתי מטריצות

$$X = (x_{ij}) , \quad Y = (y_{ij}) .$$

אם  $X$  הפיכה אז

$$Y = XK \Leftrightarrow K = X^{-1}Y.$$

כאשר  $K \in \mathbb{Z}_{26}^{m \times m}$  המפתח של הצופן היל.**דוגמה 5.3**

נתון הטקסט גלי

friday

אשר הוצפן באמצעות צופן היל עם מפתח של סדר  $2 = m$ . נניח כי הטקסט מוצפן הינו

PQCFKU

מצאו את המפתח של הצופן.

**פתרון:**

$$(f, r) \xrightarrow{e_k} (P, Q), \quad (i, d) \xrightarrow{e_k} (C, F), \quad (a, y) \xrightarrow{e_k} (K, U)$$

א"א

$$e_k(5, 17) = (15, 16), \quad e_k(8, 3) = (2, 5), \quad e_k(0, 24) = (10, 20).$$

נkeh את שני טקסטים גלויים וטקסיום מוצפנים המתאימים נגדיר את המטריצות

$$X = \begin{pmatrix} 5 & 17 \\ 8 & 3 \end{pmatrix}, \quad Y = \begin{pmatrix} 15 & 16 \\ 2 & 5 \end{pmatrix}.$$

א"ז

$$K = X^{-1}Y.$$

נחשב את ההופכית  $X^{-1}$  באמצעות נוסחת קיילי

$$\begin{aligned} |X| &= 15 - 136 \mod 26 \\ &= -121 \mod 26 \\ &= -4(26) - 17 \mod 26 \\ &= -17 \mod 26 \\ &= 9 \mod 26. \end{aligned}$$

לכן

$$|K|^{-1} \mod 26 = 9^{-1} \mod 26 = 3.$$

המטריצה הקופקטורים של  $X$  היא  $C = \begin{pmatrix} C_{11} & C_{12} \\ C_{21} & C_{22} \end{pmatrix}$  כאשר

$$C_{11} = 3, \quad C_{12} = -8, \quad C_{21} = -17, \quad C_{22} = 5.$$

לכן

$$C = \begin{pmatrix} 3 & -8 \\ -17 & 5 \end{pmatrix} \Rightarrow \text{adj}(X) = C^t = \begin{pmatrix} 3 & -17 \\ -8 & 5 \end{pmatrix} \mod 26 = \begin{pmatrix} 3 & 9 \\ 18 & 5 \end{pmatrix}.$$

לבסוף נקבל

$$X^{-1} = 3 \begin{pmatrix} 3 & 9 \\ 18 & 5 \end{pmatrix} = \begin{pmatrix} 9 & 27 \\ 54 & 15 \end{pmatrix} \mod 26 = \begin{pmatrix} 9 & 1 \\ 2 & 15 \end{pmatrix}.$$

$$\begin{aligned}
 K &= \begin{pmatrix} 9 & 1 \\ 2 & 15 \end{pmatrix} \begin{pmatrix} 15 & 16 \\ 2 & 5 \end{pmatrix} \mod 26 \\
 &= \begin{pmatrix} 137 & 149 \\ 60 & 107 \end{pmatrix} \mod 26 \\
 &= \begin{pmatrix} 7 & 19 \\ 8 & 3 \end{pmatrix}.
 \end{aligned}$$

לפיכך

**דוגמה 5.4**

נתון הטקסט גלי

theresnoplacealikehome

אשר הוצפן באמצעות צופן היל עם מפתח של סדר  $3 = m$ . נניח כי הטקסט מוצפן הינו

FHVTUTGQVRWPSCPSSFGGAMG

מצאו את המפתח של הצופן.

**פתרון:**

$$(t, h, e) \xrightarrow{e_k} (F, H, V), \quad (r, e, s) \xrightarrow{e_k} (T, U, T), \quad (n, o, p) \xrightarrow{e_k} (G, Q, V)$$

ואז

$$e_k(19, 7, 4) = (5, 7, 21), \quad e_k(17, 4, 18) = (19, 20, 19), \quad e_k(13, 14, 15) = (6, 16, 21).$$

נkeh את שני טקסטים גליים וtekstois מוצפנים המתאימים נגדיר את המטריצות

$$X = \begin{pmatrix} 19 & 7 & 4 \\ 17 & 4 & 18 \\ 13 & 14 & 15 \end{pmatrix}, \quad Y = \begin{pmatrix} 5 & 7 & 21 \\ 19 & 20 & 19 \\ 6 & 16 & 21 \end{pmatrix}.$$

ואז

$$K = X^{-1}Y.$$

נחשב את ההופכית  $X^{-1}$  באמצעות נוסחת קיילי

$$\begin{aligned}
 |X| &= 15 - 136 \mod 26 \\
 &= -3051 \mod 26 \\
 &= 17.
 \end{aligned}$$

לכן

$$|K|^{-1} \mod 26 = 17^{-1} \mod 26 = 23.$$

המטריצת הקופקטורים של  $X$  היא

$$C = \begin{pmatrix} -192 & -21 & 186 \\ -49 & 233 & -175 \\ 110 & -274 & -43 \end{pmatrix} \mod 26 = \begin{pmatrix} 16 & 5 & 4 \\ 3 & 25 & 7 \\ 6 & 12 & 9 \end{pmatrix}$$

לכן

$$\text{adj}(X) = C^t = \begin{pmatrix} 16 & 3 & 6 \\ 5 & 25 & 12 \\ 4 & 7 & 9 \end{pmatrix}.$$

לבסוף נקבל

$$X^{-1} = 23 \begin{pmatrix} 16 & 3 & 6 \\ 5 & 25 & 12 \\ 4 & 7 & 9 \end{pmatrix} = \begin{pmatrix} 368 & 69 & 138 \\ 115 & 575 & 276 \\ 92 & 161 & 207 \end{pmatrix} \pmod{26} = \begin{pmatrix} 4 & 17 & 8 \\ 11 & 3 & 16 \\ 14 & 5 & 25 \end{pmatrix}.$$

לפיכך

$$\begin{aligned} K &= X^{-1} \cdot Y \pmod{26} \\ &= \begin{pmatrix} 4 & 17 & 8 \\ 11 & 3 & 16 \\ 14 & 5 & 25 \end{pmatrix} \cdot \begin{pmatrix} 5 & 7 & 21 \\ 19 & 20 & 19 \\ 6 & 16 & 21 \end{pmatrix} \pmod{26} \\ &= \begin{pmatrix} 391 & 496 & 575 \\ 208 & 393 & 624 \\ 315 & 598 & 914 \end{pmatrix} \pmod{26} \\ &= \begin{pmatrix} 1 & 2 & 3 \\ 0 & 3 & 0 \\ 3 & 0 & 4 \end{pmatrix}. \end{aligned}$$



## 5.5 מודד צירוף המקרים

### הגדרה 5.1 מודד צירוף המקרים $I_c$

נתון מחרוזת של טקסט גליי  $x_1x_2 \cdots x_n$  של אורך  $n$ .

**המודד צירוף המקרים** של  $x$  מסומן ( $x$ )  $I_c$  ומוגדר להיות ההסתברות ששתי אותיות הנבחרת באקראי מותוק  $x$  יהיו זהות.

### משפט 5.2 נוסחה לחישוב המודד צירוף המקרים

נתון מחרוזת של טקסט גליי  $x_1x_2 \cdots x_n$  של אורך  $n$ .  
יהי  $f_k$  מספר הפעמים שהאות מס'  $k$  באלפיבית מופיעה במחרוזת  $x$ . למשל,  $f_0$  מסמן את מסטר הפעמים שהאות a מופיעה,  $f_1$  מסמן את מסטר הפעמים שהאות b מופיעה, וכן הלא.

מספר הדרכים לבחור שתי אותיות מותוק  $n$  אותיות של  $x$  ללא החזרה ניתן על ידי

$$\binom{n}{2}.$$

לכן לכל  $0 \leq k \leq 25$  יש  $\binom{f_k}{2}$  דרכים לבחור שתי אותיות  $k$  מותוק  $x$ .

המדד צירוף המקרים של הטקסט גלי  $x$  נתון על ידי הנוסחה

$$I_c(x) = \frac{\sum_{k=0}^{25} \binom{f_k}{2}}{\binom{n}{2}} = \frac{\sum_{k=0}^{25} f_k(f_k - 1)}{n(n-1)} .$$

### משפט 5.3 מדד צירוף המקרים בטקסט גלי

נניח כי  $x = x_1x_2 \dots x_n$  הוא טקסט של  $n$  אותיות.  
נסמן ב-  $p_0, p_1, \dots, p_{25}$  ההסתברויות של האותיות כמפורט למטה:

אות	$p_i$
a	0.082
b	0.015
c	0.028
d	0.043
e	0.127
f	0.022

אות	$p_i$
g	0.02
h	0.061
i	0.07
j	0.002
k	0.008
l	0.04

אות	$p_i$
m	0.024
n	0.067
o	0.075
p	0.019
q	0.001
r	0.06

אות	$p_i$
s	0.063
t	0.091
u	0.028
v	0.01
w	0.023
x	0.001
y	0.02
z	0.001

המדד צירוף המקרים מצופה להיות

$$I_c(x) \approx \sum_{k=0}^{25} p_k^2 = 0.065 .$$

## 5.6 קרייפטו-אליזה של צופן ויז'נר - מבחן פרידמן

### דוגמה 5.5

נתון הטקסט מוצפן

MOKSMNXBIUCMQXGCAXOFXMUWLNRNSFMIQBHNCFCGDTAHANTTIJNIERGCHURYHOGGSWTMP  
 CCOYISKOGXLQAFMVXNFEDAEMHQTNAAQXUDIXXRSILCIZKGWEFLAWGUJAOAUPLXRQTGATPS  
 MKLQSWRGTXJNPXEUNSYIACRGWLQEIMDUBQQGAEEYULEEWXDLIIDUHQFXWEAZJTUOFXWKS  
 MTNAAFXTTMFPMUWLNRNSFMOTIJJTUSFPRMRVBLMQXXRURKCAZGWCWAAGADECGDMMCZJVQS  
 NNRTISADILALHOEFWOFTGBSUFDHMZWNKWAPNUJALAZGWCOKSMXRMRQXNQMFHOGVGAGMR  
 AIAFMGWCMRQXUMJXXRPXGCAWILOQAFGZJNOIQXUMVWZUUXWAISLLVIEXWABARVHOGEJNWAV  
 LQMAWCOYISUIHIK

שהוחצפן באמצעות צופן ויז'נר עם מפתח של אורך 5. מצאו את המפתח ואת הטקסט גלי.

**פתרונות:**

**שלב 1: נפרק את הטקסט לעמודות של 3 אותיות**

$\underline{y}_1$	M	N	C	C	X	N	M	N	D	N	N	C	H	W	C	K	Q	X	A	T	X	X	C	W	W	O	X	A	K	R	...
$\underline{y}_2$	O	X	M	A	M	R	I	C	T	T	I	H	O	T	O	O	A	N	E	N	U	R	I	E	G	A	R	T	L	G	...
$\underline{y}_3$	K	B	Q	X	U	N	Q	F	A	T	E	U	G	M	Y	G	F	F	M	A	D	S	Z	F	U	U	Q	P	Q	T	...
$\underline{y}_4$	S	I	X	O	W	S	B	C	H	I	R	R	G	P	I	X	M	E	H	A	I	I	K	L	J	P	T	S	S	X	...
$\underline{y}_5$	M	U	G	F	L	F	H	G	A	J	G	Y	S	C	S	L	V	D	Q	Q	X	L	G	A	A	L	G	M	W	J	...

**שלב 2:-Calculating the average length of each row**

יהיו  $f_i$  התדריות של האותיות במחזור  $\underline{y}_i$  ונניח כי האורך של  $\underline{y}_i$  הוא  $n$ . אזי הפונקציות הסתבות של האותיות ב- $\underline{y}_i$  הן

$$\frac{f_0}{n}, \dots, \frac{f_{25}}{n}.$$

כל רצף אותיות  $\underline{y}_i$  מתקיים על ידי הזהה קבועה של  $k_i$  מקומות של הטקסט גלי. לפי זה, הפונקציות הסבתרות של האותיות המזוזות,

$$\frac{f_{k_i}}{n}, \dots, \frac{f_{25+k_i}}{n},$$

תהיי קרובות להסתברויות  $p_0, \dots, p_{25}$  של אותיות בטקסט גלי. בcut נגדר את הממד המשותף

$$M_g(\underline{y}_i) = \sum_{i=0}^{25} \frac{p_i f_{i+g}}{n}.$$

לכל  $g = k_i$  אם  $0 \leq g \leq 25$

$$M_g(\underline{y}_i) \approx \sum_{i=0}^{25} p_i^2 = 0.065.$$

על פי זה נבדוק את הממד המשותף לכל  $\underline{y}_i$  ולכל  $0 \leq g \leq 25$

$\underline{y}_1$

a	0.0336437	b	0.0285977	c	0.0381264	d	0.0335977
e	0.0374943	f	0.0414023	g	0.0374138	h	0.034046
i	0.0388046	j	0.0647931	k	0.0382184	l	0.0352414
m	0.0347586	n	0.0328391	o	0.0302759	p	0.0468161
q	0.0384253	r	0.0272184	s	0.0344828	t	0.0484253
u	0.0454598	v	0.0395747	w	0.0457011	x	0.0391839
y	0.0390345	z	0.0374253				

$\underline{y}_2$

a	0.0602644	b	0.0361839	c	0.0321264	d	0.0373333
e	0.0423333	f	0.0316092	g	0.0397816	h	0.0383333
i	0.0391954	j	0.0425057	k	0.0407586	l	0.0352759
m	0.037	n	0.0468046	o	0.0396092	p	0.0426207
q	0.0327931	r	0.0309655	s	0.0317816	t	0.0412529
u	0.0371609	v	0.0383218	w	0.0422989	x	0.0324828
y	0.0340575	z	0.0381494				

 $\underline{Y}_3$ 

a	0.0396092	b	0.046931	c	0.0417011	d	0.0312299
e	0.0352069	f	0.0387701	g	0.0417816	h	0.0348161
i	0.0475402	j	0.0337356	k	0.0285977	l	0.030977
m	0.0625517	n	0.0407816	o	0.0315977	p	0.029931
q	0.0469885	r	0.0332989	s	0.0376782	t	0.042977
u	0.041954	v	0.0300115	w	0.036069	x	0.0395287
y	0.039931	z	0.0368046				

 $\underline{Y}_4$ 

a	0.0459655	b	0.0364483	c	0.0323908	d	0.0362184
e	0.0632644	f	0.0395747	g	0.0334598	h	0.0316092
i	0.0438276	j	0.0342414	k	0.0386437	l	0.0336092
m	0.0323333	n	0.0371379	o	0.045092	p	0.0466207
q	0.0363448	r	0.0403678	s	0.0388851	t	0.0392874
u	0.035954	v	0.0374253	w	0.0336207	x	0.0362069
y	0.0372529	z	0.0352184				

 $\underline{Y}_5$ 

a	0.0288046	b	0.0362529	c	0.0446322	d	0.0437586
e	0.037069	f	0.0421839	g	0.0347931	h	0.0410805
i	0.0387126	j	0.036977	k	0.0274253	l	0.0331839
m	0.0445172	n	0.0405172	o	0.0408391	p	0.0345977
q	0.0306897	r	0.0342759	s	0.064046	t	0.0436322
u	0.0348161	v	0.0311494	w	0.0374368	x	0.0362414
y	0.0438046	z	0.0395632				

ונסה לפענח את הטקסט מוצפן עם המפתח

JAMES

ונקבל את התשובה

doyouexpectmetotalknomisterbondiexpectyoutodie therereisnothingyoucant talk  
tomeaboutthatidontalreadyknowyoureforgottenethingififailtoreportdou  
bleoeightreplacesmeitrustthewillbemoresuccessfulwellheknowswhatiknowyou  
knownothingmisterbondoperationgrandslamforinstancetwoordsyoumayhaveov  
erheardwhichcannotpossiblyhaveany significa nceto youor anyonein yourorgani  
zationcanyouaffordtotakethatchanceyouarequiterightmisterbondyouarewort  
hmoretomealive

עם רוחים וסימני פיסוק:

Do you expect me to talk? No, Mister Bond, I expect you to die. There is nothing you can talk to me about that I don't already know. You're forgetting one thing: if I fail to report, Double-O Eight replaces me. I trust he will be more successful. Well, he knows what I know. You know nothing, Mister Bond. Operation Grand Slam, for instance. Two words you may have overheard, which cannot possibly have any significance to you or anyone in your organization. Can you afford to take that chance? You are quite right, Mister Bond. You are worth more to me alive.

```
1 def letterToZ26(a):
2     if a.isalpha():
3         if a.isupper():
4             return ord(a) - 65
5         if a.islower():
6             return ord(a) - 97
7
8 def Z26ToUpperLetter(a):
9     return chr(a+65)
10
11 def Z26ToLowerLetter(a):
12     return chr(a+97)
13
14 probabilities = [0.082, 0.015, 0.028, 0.043, 0.127, 0.022, 0.02, 0.061, 0.07, 0.002,
15     0.008, 0.04, 0.024, 0.067, 0.075, 0.019, 0.001, 0.06, 0.063, 0.091, 0.028, 0.01,
16     0.023, 0.001, 0.02, 0.001]
17
18 alphabetLower = ['a', 'b', 'c', 'd', 'e', 'f', 'g', 'h', 'i', 'j', 'k', 'l', 'm', 'n', 'o', 'p', 'q',
19     'r', 's', 't', 'u', 'v', 'w', 'x', 'y', 'z']
20 alphabetUpper = ['A', 'B', 'C', 'D', 'E', 'F', 'G', 'H', 'I', 'J', 'K', 'L', 'M', 'N', 'O', 'P', 'Q',
21     'R', 'S', 'T', 'U', 'V', 'W', 'X', 'Y', 'Z']
22
23 cipherText = "
24     MOKSMNXBIUCMQXGCAXOFXMUWLNRNSFMIQBHNCFCGDTAHANTTIJNIERGCHURYHOGGSWTMPCCOYISKOGXLQAFMVXNFEDAE
25 "
26
27 cipherTextList = list(cipherText)
28
29 y= [None]*5
30 for i in range(0,6):
31     y[i] = cipherTextList[i::5]
```

```
31 print( len(y[0]) == len(y[1]) == len(y[2]) == len(y[3]) == len(y[4]) )  
32  
33 f = [None]*26  
34  
35 n = len(y[0])  
36  
37 My = [None]*5  
38  
39 for k, yi in enumerate(y):  
40     for i,X in enumerate(alphabetUpper):  
41         f[i] = yi.count(X)  
42  
43 A = [None]*26  
44  
45 for g in range(0,26):  
46     Sum = 0;  
47     b = alphabetLower[g]  
48  
49     for i in range(0,26):  
50         a = alphabetLower[i]  
51         Sum += P(a)*f[(i+g) % 26]  
52  
53     Sum = Sum / n  
54  
55     A[g] = [b, Sum]  
56  
57 My[k] = A  
58  
59 keyWord = 'james'  
60  
61 keyZ26 = [letterToZ26(a) for a in list(keyWord)]  
62  
63 Y = [letterToZ26(a) for a in cipherTextList]  
64  
65 X = []  
66  
67 for i,y in enumerate(Y):  
68     x = (y - keyZ26[i%5]) % 26  
69     X.append(x)  
70  
71 plainTextList = [Z26ToLowerLetter(a) for a in X]  
72 plainText = ''.join(plainTextList)
```

