

קריפטוגרפיה

תוכן העניינים

3	1 תורת המספרים
3	הגדרות בסיסיות
10	האלגוריתם של אוקליד
14	משפטים של מספרים ראשוניים
17	משפט השאריות הסיני
19	2 חוגים מתמטיים
19	החוג \mathbb{Z}_m
22	הפיכת מטריצות בחוג \mathbb{Z}_m
25	תמורות
29	3 הצפנים הבסיסיים
29	מושג של קריפטו-מערכת
30	צופן ההזזה
32	צופן ההחלפה
35	צופן האפיני
40	צופן ויז'נר
45	צופן היל
52	צופן התמורה
55	4 הצפנים הבסיסיים (המשך)
55	צפני זרם
58	5 צופן RSA
58	משפט השאריות הסיני
59	משפטים של מספרים ראשוניים
62	אלגוריתם RSA
70	6 קריפטו-אנליזה
70	סוגים של התקפת סייבר
70	קבוצות אותיות הנפוצים ביותר בטקסט גלוי
72	קריפטו-אנליזה של צופן האפיני
77	קריפטו-אנליזה של צופן היל
80	מדד צירוף המקרים
81	קריפטו-אנליזה של צופן ויז'נר - מבחן פרידמן

86	7 סודיות מושלמת
86	סודיות מושלמת
94	תכונות של אנטרופיה
99	צופן מרוכב
100	משפט האנטרופיה לקריפטו-מערכת
104	8 אנטרופיה ומידע
104	המושג של מידע
107	הגדרה של מידע
110	אנטרופיה
112	הצפנת האפמן

שיעור 1

תורת המספרים

1.1 הגדרות בסיסיות

1.1 הגדרה

יהיו a, b מספרים שלמים. אומרים כי b מחלק את a אם קיים מספר שלם q כך ש-

$$a = qb.$$

כלומר $\frac{a}{b}$ שווה למספר שלם q .

הסימון $a \mid b$ אומר כי b מחלק את a .

1.1 דוגמה

א) $3 \mid 6$ בגלל שקיים מספר שלם $q = 2$ כך ש- $6 = 3q$.

ב) $7 \nmid 42$ בגלל שקיים מספר שלם $q = 6$ כך ש- $42 = 7q$.

ג) $5 \nmid 8$ בגלל שלא קיים מספר שלם q כך ש- $8 = 5q$.

1.2 הגדרה יחס שקילות בין a ל- b

נניח כי $a, b \in \mathbb{Z}$ מספרים שלמים ו- m מספר שלם חיובי. היחס

$$a \equiv b \pmod{m}$$

אומר כי m מחלק את ההפרש $a - b$, כלומר $m \mid a - b$.

בנסוח שקול, $a \equiv b \pmod{m}$ אם קיים שלם q כך ש- $a = qm + b$.

לעתים אומרים כי " a שקול ל- b מודולו m ".

1.2 דוגמה

הוכיחו כי

$$5 \equiv 2 \pmod{3} \quad \text{א)}$$

$$43 \equiv 23 \pmod{10} \quad \text{ב)}$$

$$7 \not\equiv 2 \pmod{4} \quad \text{ג)}$$

פתרון:

(א)

$$5 - 2 = 3 = 1 \cdot 3 \Rightarrow 3 \mid 5 - 2 \Rightarrow 5 \equiv 2 \pmod{3}.$$

(ב)

$$43 - 23 = 20 = 2 \cdot 10 \Rightarrow 10 \mid 43 - 23 \Rightarrow 43 \equiv 23 \pmod{10}.$$

$$7 - 2 = 5 \quad (ג)$$

לא קיים שלם q כך ש- $7 - 2 = 4q$ לכן $7 - 2 \nmid 4$

$$7 \not\equiv 2 \pmod{4}.$$

הגדרה 1.3 השארית

נתונים מספרים שלמים $a, b \in \mathbb{Z}$, היחס

$$a \% b$$

מציין את השארית בחלוקת a ב- b .

דוגמה 1.3

$$43 \% 10 = 3.$$

$$13 \% 4 = 1.$$

$$8 \% 2 = 0.$$

$$-10 \% 3 = -1.$$

משפט 1.1 משפט החילוק של אוקלידס

יהיו a, b מספרים שלמים $b \neq 0$. קיימים מספרים שלמים q, r יחידים כך ש-

$$a = qb + r$$

כאשר $0 \leq r < |b|$.

• b נקרא ה מודולו,

• q נקראת המנה

• ואילו r נקרא השארית.

שימו לב: $r = a \% b$.

דוגמה 1.4

עבור המספרים $b = 8, a = 46$ מצאו את הפירוק האוקלידי $a = bq + r$.

פתרון:

עבור $b = 8$ ו- $a = 46$ מתקיים

$$46 = 8 \cdot 5 + 6 \Rightarrow q = 5, r = 6.$$

1.5 דוגמה

עבור $b = 8$ ו- $a = -46$ מתקיים

$$-46 = 8 \cdot (-6) + 2 \Rightarrow q = -6, r = 2.$$

משפט 1.2 נוסחת השארית

נתונים $a, b > 0$ מספר שלמים.

$$(א) \quad a \% b = a - b \left\lfloor \frac{a}{b} \right\rfloor$$

$$(ב) \quad (-a) \% b = b - (a \% b) = b \left\lceil \frac{a}{b} \right\rceil - a$$

הוכחה:

(א) לפי משפט החילוק של אוקלידס 1.1, קיימים שלמים q, r כך ש-

$$a = qb + r \quad (*)1$$

כאשר $0 \leq r < b$ ו- $r = a \% b$. נחלק ב- b ונקבל

$$\frac{a}{b} = q + \frac{r}{b} \quad (*)2$$

נשים לב כי $0 < \frac{r}{b} < 1$, לכן לפי (*)2

$$\left\lfloor \frac{a}{b} \right\rfloor = q.$$

נציב זה ב- (*)1 ונקבל

$$a = \left\lfloor \frac{a}{b} \right\rfloor b + r \Rightarrow r = a - b \left\lfloor \frac{a}{b} \right\rfloor. \quad (*)3$$

(ב) לפי משפט החילוק של אוקלידס 1.1, קיימים שלמים q', r' כך ש-

$$-a = q'b + r'$$

כאשר $r' = (-a) \% b$ מכאן

$$a = -q'b - r' = -q'b - b + b - r' = -(q' + 1)b + (b - r'). \quad (*)4$$

נשים לב כי $b - r' \geq 0$. אבל לפי (*)1 $a = qb + r$ כאשר $r = a \% b$ יחיד. לכן

$$r = b - r' \Rightarrow r' = b - r \stackrel{(*)3}{=} b - a + b \left\lfloor \frac{a}{b} \right\rfloor = b - \left(a - b \left\lfloor \frac{a}{b} \right\rfloor \right) = b - (a \% b). \quad (*)5$$

לכן $r' = (-a) \% b = b - (a \% b)$

הזהות השני מנובע מ- (*)5:

$$r = b - r' \Rightarrow r' = b - r \stackrel{(*)3}{=} b - a + b \left\lfloor \frac{a}{b} \right\rfloor - a + \left\lceil \frac{a}{b} \right\rceil.$$

לכן $r' = (-a) \% b = -a + \left\lceil \frac{a}{b} \right\rceil$

דוגמה 1.6

מצאו את $101 \% 7$.

פתרון:

$$b = 7, a = 101$$

$$101 \% 7 = 101 - 7 \left\lfloor \frac{101}{7} \right\rfloor = 101 - 7(14) = 3 .$$

דוגמה 1.7

מצאו את $-101 \% 7$.

פתרון:

$b = 7, -a = -101$. נשתמש בנוסחה $(-a) \% b = b - (a \% m)$. מדוגמה הקודמת: $(101 \% 7) = 3$ לפיכך

$$(-101) \% 7 = 7 - (101 \% 7) = 7 - 3 = 4 .$$

הגדרה 1.4 המחלק המשותף הגדול ביותר gcd

נתונים שני מספרים שלמים $a, b > 0$. המחלק המשותף הגדול ביותר של a ו- b מסומן $\gcd(a, b)$ (greatest common divisor) ומוגדר להיות המספר שלם הגדול ביותר שמחלק גם a וגם b .

דוגמה 1.8

$$\gcd(2, 6) = 2 ,$$

$$\gcd(3, 6) = 3 ,$$

$$\gcd(24, 5) = 1 ,$$

$$\gcd(20, 10) = 10 ,$$

$$\gcd(14, 12) = 2 ,$$

$$\gcd(8, 12) = 4 .$$

הגדרה 1.5 כפולה משותפת קטנה ביותר

נתונים שני מספרים שלמים $a, b > 0$. הכפולה המשותפת הקטנה ביותר מסומן $\text{lcm}(a, b)$ (lowest common multiple) ומוגדר להיות המספר השלם החיובי הקטן ביותר ש a ו- b מחלקים אותו.

דוגמה 1.9

$$\text{lcm}(6, 21) = 42 ,$$

$$\text{lcm}(3, 6) = 6 ,$$

$$\text{lcm}(24, 5) = 120 ,$$

$$\text{lcm}(20, 10) = 20 ,$$

$$\text{lcm}(14, 12) = 84 ,$$

$$\text{lcm}(8, 12) = 24 .$$

הגדרה 1.6 מספרים זרים

נניח כי $a \geq 1$ ו- $b \geq 2$ מספרים שלמים. אומרים כי a ו- b מספרים זרים אם

$$\gcd(a, b) = 1 .$$

במילים פשוטות, שני מספרים שלמים נקראים מספרים זרים אם המחלק המשותף המקסימלי שלהם הוא 1, כלומר, אין אף מספר גדול מאחת שמחלק את שניהם.

משפט 1.3 משפט הפירוק לראשוניים

המשפט היסודי של האריתמטיקה או משפט הפירוק לראשוניים קובע כי כל מספר טבעי ניתן לרשום כמכפלה יחידה של מספרים ראשוניים. ז"א, יהי $a \in \mathbb{N}$ כל מספר טבעי. אז

$$a = p_1^{e_1} \times p_2^{e_2} \times \cdots \times p_n^{e_n} .$$

כאשר p_1, \dots, p_n מספרים ראשוניים ו- $e_1, \dots, e_n \in \mathbb{N}$, והפירוק הזה יחיד.

דוגמה 1.10

$$60 = 2^2 \times 3^2 \times 5 ,$$

דוגמה 1.11

$$98 = 2^1 \times 7^2 .$$

הגדרה 1.7 פונקציית אוילר

יהי m מספר שלם.

הפונקציית אוילר מסומנת ב- $\phi(m)$ ומוגדרת להיות השלמים שקטנים ממש מ- m וזרים ביחס ל- m .

$$\phi(m) := \{a \in \mathbb{N} \mid \gcd(a, m) = 1, a < m\} .$$

דוגמה 1.12

מכיוון ש- $26 = 2 \times 13$, הערכים של a עבורם $\gcd(a, 26) = 1$ הם
 $\{1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25\}$.

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

$$\phi(26) = 12.$$

משפט 1.4 הפירוק לראשוניים של פונקציית אוילר

נתון מספר טבעי m . נניח כי הפירוק למספרים ראשוניים שלו הוא

$$m = \prod_{i=1}^n p_i^{e_i},$$

כאשר p_i מספרים ראשוניים שונים ו- $e_i > 0$ מספרים שלמים ו- $1 \leq i \leq n$. אז

$$\phi(m) = \prod_{i=1}^n (p_i^{e_i} - p_i^{e_i-1}).$$

דוגמה 1.13

מצאו את $\phi(60)$.

פתרון:

$$60 = 2^2 \times 3^1 \times 5^1 \text{ לכן}$$

$$\phi(60) = (2^2 - 2^1) (3^1 - 3^0) (5^1 - 5^0) = (2)(2)(4) = 16.$$

משפט 1.5 שיטה לחישוב gcd

נתונים השלמים a, b כך שהפירוק לראשוניים שלהם הם:

$$a = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}, \quad b = p_1^{f_1} p_2^{f_2} \dots p_n^{f_n}$$

וללא הגבלה כלליות נניח כי $k \leq n$. אז ה- \gcd נתון על ידי

$$\gcd(a, b) = p_1^{\min(e_1, f_1)} p_2^{\min(e_2, f_2)} \dots p_k^{\min(e_k, f_k)}$$

הוכחה:

דוגמה 1.14

מצאו את $\gcd(19200, 320)$.

פתרון:

$$19200 = 2^8 3^1 5^2, \quad 320 = 2^6 5^1 = 2^6 3^0 5^1.$$

$$\gcd(19200, 320) = 2^{\min(8,6)} 3^{\min(1,0)} 5^{\min(2,1)} = 2^6 3^0 5^1 = 320.$$

דוגמה 1.15

מצאו את $\gcd(154, 36)$.

פתרון:

$$154 = 2^1 7^1 11^1, \quad 36 = 2^2 3^2.$$

ז"א

$$154 = 2^1 3^0 7^1 11^1, \quad 36 = 2^2 3^2 7^0 11^0.$$

$$\gcd(154, 36) = 2^{\min(1,2)} 3^{\min(0,2)} 7^{\min(1,0)} 11^{\min(1,0)} = 2^1 3^0 7^0 11^0 = 2.$$

משפט 1.6 שיטה לחישוב lcm

נתונים השלמים a, b כך שהפירוק לראשוניים שלהם הם:

$$a = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}, \quad b = p_1^{f_1} p_2^{f_2} \dots p_n^{f_n}$$

וללא הגבלה כלליות נניח כי $k \leq n$. אז ה- lcm נתון על ידי

$$\text{lcm}(a, b) = p_1^{\max(e_1, f_1)} p_2^{\max(e_2, f_2)} \dots p_k^{\max(e_k, f_k)}$$

הוכחה:

משפט 1.7

$$\gcd(a, b) \text{ lcm}(a, b) = ab.$$

הוכחה:

$$\min(a, b) + \max(a, b) = a + b.$$

1.2 האלגוריתם של אוקליד

משפט 1.8 האלגוריתם של אוקליד

יהיו a, b משפרים שלמים חיוביים ($a, b \in \mathbb{Z}, a > 0, b > 0$). קיים אלגוריתם אשר נותן את $d = \gcd(a, b)$. האלגוריתם הינו מתואר להלן. נגדיר

$$r_0 = a, \quad r_1 = b.$$

לפי משפט החילוק 1.1 קיימים שלמים q_1 ו- $0 \leq r_2 < |b|$ עבורם $a = bq_1 + r_2$ כלומר

$$r_0 = r_1q_1 + r_2.$$

באותה מידה, לפי משפט החילוק קיימים שלמים q_2 ו- $0 \leq r_3 < |r_2|$ עבורם

$$r_1 = r_2q_2 + r_3.$$

התהליך ממשיך עד שנקבל $r_{n+1} = 0$ בשלב ה- n -ית.

$$0 \leq r_2 < |b| \quad a = bq_1 + r_2 \quad \text{שלב } k=1$$

$$0 \leq r_3 < |r_2| \quad b = r_2q_2 + r_3 \quad \text{שלב } k=2$$

$$0 \leq r_4 < |r_3| \quad r_2 = r_3q_3 + r_4 \quad \text{שלב } k=3$$

\vdots

$$0 \leq r_n < |r_{n-1}| \quad r_{n-2} = r_{n-1}q_{n-1} + r_n \quad \text{שלב } k=n-1$$

$$r_{n+1} = 0 \quad r_{n-1} = r_nq_n \quad \text{שלב } k=n$$

התהליך מסתיים בשלב ה- n -ית אם $r_{n+1} = 0$ ואז

$$r_n = \gcd(a, b).$$

דוגמה 1.16

מצאו את ה- $\gcd(1071, 462)$.

פתרון:

$$a = 1071, b = 462$$

נגדיר $r_0 = a = 1071$ ו- $r_1 = b = 462$.

נבצע את האלגוריתם $r_{k-1} = q_k r_k + r_{k+1}$ עד השלב ה- n -ית שבו $r_{n+1} = 0$.

שלב		q_k	r_{k+1}
$k=1$	$1071 = 2 \cdot 462 + 147$	$q_1 = 2$	$r_2 = 147$
$k=2$	$462 = 3 \cdot 147 + 21$	$q_2 = 3$	$r_3 = 21$
$k=3$	$147 = 7 \cdot 21 + 0$	$q_3 = 7$	$r_4 = 0$

לפיכך $\gcd(1071, 462) = r_3 = 21$.

דוגמה 1.17

מצאו את $\gcd(26, 11)$.

פתרון:

$$a = 26, b = 11$$

נגדיר $r_0 = a = 26$ ו- $r_1 = b = 11$.

נבצע את האלגוריתם $r_{k-1} = q_k r_k + r_{k+1}$ עד השלב ה- n -ית שבו $r_{n+1} = 0$.

שלב		q_k	r_{k+1}
$k = 1$	$26 = 2 \cdot 11 + 4$	$q_1 = 2$	$r_2 = 4$
$k = 2$	$11 = 2 \cdot 4 + 3$	$q_2 = 2$	$r_3 = 3$
$k = 3$	$4 = 1 \cdot 3 + 1$	$q_3 = 1$	$r_4 = 1$
$k = 4$	$3 = 3 \cdot 1 + 0$	$q_4 = 3$	$r_5 = 0$

לכן $\gcd(26, 11) = r_4 = 1$.

משפט 1.9 משפט בזו (Bezout's identity)

יהיו a, b שלמים ויהי $d = \gcd(a, b)$. קיימים שלמים s, t כך שניתן לרשום ה- $\gcd(a, b)$ כצירוף לינארי של a ו- b :

$$sa + tb = d.$$

משפט 1.10 האלגוריתם של אוקליד המוכלל (שיטה 1)

יהיו a, b שלמים חיוביים. קיים אלגוריתם אשר נותן שלמים s, t עבורם

$$d = sa + tb$$

כאשר $d = \gcd(a, b)$, כמפורט להלן.

מגדירים את הפרמטרים ההתחלתיים:

$$\begin{aligned} r_0 &= a, & r_1 &= b, \\ s_0 &= 1, & s_1 &= 0, \\ t_0 &= 0, & t_1 &= 1. \end{aligned}$$

אז מבצעים את השלבים הבאים:

$(0 \leq r_2 < r_1)$	$t_2 = t_0 - q_1 t_1$	$s_2 = s_0 - q_1 s_1$	$r_2 = r_0 - q_1 r_1$	שלב 1:
$(0 \leq r_3 < r_2)$	$t_3 = t_1 - q_2 t_2$	$s_3 = s_1 - q_2 s_2$	$r_3 = r_1 - q_2 r_2$	שלב 2:
				\vdots
$(0 \leq r_{k+1} < r_k)$	$t_{k+1} = t_{k-1} - q_k t_k$	$s_{k+1} = s_{k-1} - q_k s_k$	$r_{k+1} = r_{k-1} - q_k r_k$	שלב k:
				\vdots
$(0 \leq r_n < r_{n-1})$	$t_n = t_{n-2} - q_{n-1} t_{n-1}$	$s_n = s_{n-2} - q_{n-1} s_{n-1}$	$r_n = r_{n-2} - q_{n-1} r_{n-1}$	שלב n-1:
			$r_{n+1} = 0$	שלב n:

$$d = \gcd(a, b) = r_n, \quad s = s_n, \quad t = t_n.$$

דוגמה 1.18 (אלגוריתם איוקליד המוכלל)

מצאו את $d = \gcd(240, 46)$ ומצאו שלמים s, t עבורם $d = 240s + 46t$.

פתרון:

פתרון לדוגמה 1.18 עם השיטה במשפט 1.10 של האלגוריתם איוקליד המוכלל

$$a = 240, b = 46$$

$$\begin{aligned} r_0 &= a = 240, & r_1 &= b = 46, \\ s_0 &= 1, & s_1 &= 0, \\ t_0 &= 0, & t_1 &= 1. \end{aligned}$$

$q_1 = 5$	$t_2 = 0 - 5 \cdot 1 = -5$	$s_2 = 1 - 5 \cdot 0 = 1$	$r_2 = 240 - 5 \cdot 46 = 10$	שלב k=1:
$q_2 = 4$	$t_3 = 1 - 4 \cdot (-5) = 21$	$s_3 = 0 - 4 \cdot 1 = -4$	$r_3 = 46 - 4 \cdot 10 = 6$	שלב k=2:
$q_3 = 1$	$t_4 = -5 - 1 \cdot (21) = -26$	$s_4 = 1 - 1 \cdot (-4) = 5$	$r_4 = 10 - 1 \cdot 6 = 4$	שלב k=3:
$q_4 = 1$	$t_5 = 21 - 1 \cdot (-26) = 47$	$s_5 = -4 - 1 \cdot 5 = -9$	$r_5 = 6 - 1 \cdot 4 = 2$	שלב k=4:
$q_5 = 2$	$t_6 = -26 - 2 \cdot (47) = -120$	$s_6 = 5 - 2 \cdot (-9) = 23$	$r_6 = 4 - 2 \cdot 2 = 0$	שלב k=5:

$$\gcd(a, b) = r_5 = 2, \quad s = s_5 = -9, \quad t = t_5 = 47.$$

$$ta + sb = -9(240) + 47(46) = 2.$$

יש שיטה נוספת למציאת המקדמים s, t במשפט בזו. נתאר אותה על ידי הדוגמה הקודמת.

פתרון לדוגמה 1.18 עם השיטה השניה של האלגוריתם איוקליד המוכלל

לשיטה הזאת יש 2 שלבים. בשלב הראשון מבצעים האלגוריתם של אוקליד במשפט 1.8.

$$\boxed{240} = 5 \cdot \boxed{46} + \boxed{10} \quad (*0)$$

$$\boxed{46} = 4 \cdot \boxed{10} + \boxed{6} \quad (*1)$$

$$\boxed{10} = 1 \cdot \boxed{6} + \boxed{4} \quad (*2)$$

$$\boxed{6} = 1 \cdot \boxed{4} + \boxed{2} \quad (*3)$$

$$\boxed{4} = 2 \cdot \boxed{2} + 0 \quad (*4)$$

$$d = \gcd(240, 46) = 2 \text{ לכן}$$

בשלב השני רושמים 2 כצירוף לינארי של 240 ו-46 באמצעות המשוואות למעלה:

$$\boxed{2} = \boxed{6} - 1 \cdot \boxed{4} \quad \text{לפי } (*3)$$

$$= \boxed{6} - 1 \cdot (\boxed{10} - 1 \cdot \boxed{6}) \quad \text{לפי } (*2)$$

$$= 2 \cdot \boxed{6} - 1 \cdot \boxed{10}$$

$$= 2 \cdot (\boxed{46} - 4 \cdot \boxed{10}) - 1 \cdot \boxed{10} \quad \text{לפי } (*1)$$

$$= 2 \cdot \boxed{46} - 9 \cdot \boxed{10}$$

$$= 2 \cdot \boxed{46} - 9 \cdot (\boxed{240} - 5 \cdot \boxed{46}) \quad \text{לפי } (*0)$$

$$= 47 \cdot \boxed{46} - 9 \cdot \boxed{240}.$$

דוגמה 1.19 (אלגוריתם איוקליד המוכלל)

מצאו את $d = \gcd(326, 78)$ ומצאו שלמים s, t עבורם $d = 326s + 78t$.

פתרון:

פתרון לדוגמה 1.19 עם השיטה במשפט 1.10 של האלגוריתם איוקליד המוכלל

$$a = 326, b = 78$$

$$r_0 = a = 326, \quad r_1 = b = 78,$$

$$s_0 = 1, \quad s_1 = 0,$$

$$t_0 = 0, \quad t_1 = 1.$$

$q_1 = 4$	$t_2 = 0 - 4 \cdot 1 = -4$	$s_2 = 1 - 4 \cdot 0 = 1$	$r_2 = 326 - 4 \cdot 78 = 14$	שלב $k = 1$
$q_2 = 5$	$t_3 = 1 - 5 \cdot (-4) = 21$	$s_3 = 0 - 5 \cdot 1 = -5$	$r_3 = 78 - 5 \cdot 14 = 8$	שלב $k = 2$
$q_3 = 1$	$t_4 = -4 - 1 \cdot (21) = -25$	$s_4 = 1 - 1 \cdot (-5) = 6$	$r_4 = 14 - 1 \cdot 8 = 6$	שלב $k = 3$
$q_4 = 1$	$t_5 = 21 - 1 \cdot (-25) = 46$	$s_5 = -5 - 1 \cdot 6 = -11$	$r_5 = 8 - 1 \cdot 6 = 2$	שלב $k = 4$
$q_5 = 3$			$r_6 = 6 - 3 \cdot 2 = 0$	שלב $k = 5$

$$\gcd(a, b) = r_5 = 2, \quad s = s_5 = -11, \quad t = t_5 = 46.$$

$$sa + tb = -11(326) + 46(78) = 2.$$

יש שיטה נוספת למציאת המקדמים s, t במשפט בזו. נתאר אותה על ידי הדוגמה הקודמת.

פתרון לדוגמה 1.19 עם השיטה השניה של האלגוריתם איוקליד המוכלל

לשיטה הזאת יש 2 שלבים. בשלב הראשון מבצעים האלגוריתם של אוקליד במשפט 1.8.

$$\boxed{326} = 4 \cdot \boxed{78} + \boxed{14} \quad (*)0$$

$$\boxed{78} = 5 \cdot \boxed{14} + \boxed{8} \quad (*)1$$

$$\boxed{14} = 1 \cdot \boxed{8} + \boxed{6} \quad (*)2$$

$$\boxed{8} = 1 \cdot \boxed{6} + \boxed{2} \quad (*)3$$

$$\boxed{4} = 3 \cdot \boxed{2} + 0 \quad (*)4$$

$$d = \gcd(326, 78) = 2 \quad \text{לכן}$$

בשלב השני רושמים 2 כצירוף לינארי של 326 ו-78 באמצעות המשוואות למעלה:

$$\boxed{2} = \boxed{8} - 1 \cdot \boxed{6} \quad \text{לפי } (*)3$$

$$= \boxed{8} - 1 \cdot (\boxed{14} - 1 \cdot \boxed{8}) \quad \text{לפי } (*)2$$

$$= 2 \cdot \boxed{8} - 1 \cdot \boxed{14}$$

$$= 2 \cdot (\boxed{78} - 5 \cdot \boxed{14}) - 1 \cdot \boxed{14} \quad \text{לפי } (*)1$$

$$= 2 \cdot \boxed{78} - 11 \cdot \boxed{14}$$

$$= 2 \cdot \boxed{78} - 11 \cdot (\boxed{326} - 4 \cdot \boxed{78}) \quad \text{לפי } (*)0$$

$$= 46 \cdot \boxed{78} - 11 \cdot \boxed{326}.$$

1.3 משפטים של מספרים ראשוניים

משפט 1.11 קיימים אינסוף מספרים ראשוניים

קיימים אינסוף מספרים ראשוניים.

הוכחה: נוכיח הטענה דרך השלילה.

נניח כי $\{p_1, \dots, p_n\}$ הוא הקבוצה של כל הראשוניים שקיימים וקבוצה זו נוצרת סופי.

נגדיר השלם $M = (p_1 \cdot p_2 \cdot \dots \cdot p_n) + 1$.

לפי משפט הפירוק לראשוניים (ראו משפט 1.3 למעלה או משפט 5.3 למטה) M הוא מספר ראשוני או שווה למכפלה של ראשוניים.

M לא מספר ראשוני בגלל ש- $M > p_i$ לכל $1 \leq i \leq n$.
גם לא קיים מספק ראשוני p_i אשר מחלק את M . הרי

$$M \% p_i = 1 \Rightarrow p_i \nmid M .$$

הגענו לסתירה של המשפט הפירוק לראשוניים, לכן קיימים אינסוף מספרים ראשוניים.

משפט 1.12 משפט הפירוק לראשוניים

(ראו משפט 1.3) לכל מספר שלם n קיימים שלמים e_i וראשוניים p_i כך ש-

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$

הוכחה: אינדוקציה.

משפט 1.13 נוסחה לפונקצית אוילר

(ראו משפט 1.4) לכל מספר שלם n בעל פירוק לראשוניים

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$

פונקציית אוילר ניתנת על ידי

$$\phi(n) = \prod_{i=1}^k (p_i^{e_i} - p_i^{e_i-1}) = (p_1^{e_1} - p_1^{e_1-1}) (p_2^{e_2} - p_2^{e_2-1}) \cdots (p_k^{e_k} - p_k^{e_k-1})$$

דוגמה 1.20

חשבו את $\phi(24)$

פתרון:

$$24 = 2^3 3^1 .$$

לכן

$$\phi(24) = (2^3 - 2^2)(3^1 - 3^0) = (8 - 4)(3 - 1) = 8 .$$

■

משפט 1.14

אם p מספר ראשוני אז

$$\phi(p) = p - 1 .$$

■

הוכחה: תרגיל בית.

משפט 1.15

אם p מספר ראשוני אז

$$\phi(p^n) = p^n - p^{n-1} .$$

הוכחה: תרגיל בית.

משפט 1.16

אם s, t שלמים זרים (כלומר $\gcd(s, t) = 1$) אז

$$\phi(s \cdot t) = \phi(s) \cdot \phi(t) .$$

הוכחה: תרגיל בית.

משפט 1.17

אם p ו- q מספרים ראשוניים שונים אז

$$\phi(p \cdot q) = (p - 1)(q - 1) .$$

הוכחה: תרגיל בית.

משפט 1.18 המשפט הקטן של פרמה

אם p מספר ראשוני ו- $a \in \mathbb{Z}_p$ אז התנאים הבאים מתקיימים:

$$1. \quad a^p \equiv a \pmod{p}$$

$$2. \quad a^{p-1} \equiv 1 \pmod{p}$$

$$3. \quad a^{-1} \equiv a^{p-2} \pmod{p}$$

הוכחה:

טענה 1. נוכיח באינדוקציה.

בסיס:

עבור $a = 0$ הטענה $0^p \equiv 0 \pmod{p}$ מתקיימת.

מעבר:

נניח כי הטענה מתקיימת עבור a .

$$(a + 1)^p = a^p + pa^{p-1} + \frac{p(p-1)}{2}a^{p-2} + \dots + pa + 1 \equiv a^p + 1 \pmod{p}$$

ההנחת האינדוקציה אומרת ש- $a^p \equiv a \pmod{p}$ לכן

$$(a + 1)^p \pmod{p} \equiv a^p + 1 \pmod{p} \equiv (a + 1) \pmod{p}$$

כנדרש.

טענה 2. $\gcd(a, p) = 1$ לפיכך קיים איבר הופכי $a^{-1} \in \mathbb{Z}_p$. נכפיל ב- a^{-1} אשר הוכחנו בסעיף הקודם:

$$a^{-1}a^p \equiv a^{-1} \cdot a \pmod{p} \Rightarrow a^{p-1} \equiv 1 \pmod{p} .$$

טענה 3.

$$a^{p-1} \equiv 1 \pmod{p} \Leftrightarrow 1 \equiv a^{p-1} \pmod{p} \Rightarrow a^{-1} \equiv a^{p-2} \pmod{p} .$$

משפט 1.19 משפט אוילר

אם a, n שלמים ו- $\gcd(a, n) = 1$ אז

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

משפט 1.20

אם a, n שלמים ו- $\gcd(a, n) = 1$ אז

$$a^{-1} \equiv a^{\phi(n)-1} \pmod{n}.$$

דוגמה 1.21

חשבו את האיבר ההופכי ל-5 ב- \mathbb{Z}_{11} .

פתרון:

לפי משפט פרמט 5.9:

$$5^{-1} = 5^{11-2} \pmod{11} = 5^9 \pmod{11}.$$

לפי הנוסחת לשארית 1.2:

$$5^9 \% 11 = 5^9 - 11 \left\lfloor \frac{5^9}{11} \right\rfloor = 9$$

לכן $5^{-1} \in \mathbb{Z}_{11} = 9$.



1.4 משפט השאריות הסיני

משפט 1.21 משפט השאריות הסיני

יהיו m_1, m_2, \dots, m_r שלמים אשר זרים בזוגות ויהיו a_1, a_2, \dots, a_r שלמים. למערכת של יחסים שקילות

$$x = a_1 \pmod{m_1},$$

$$x = a_2 \pmod{m_2},$$

$$\vdots$$

$$x = a_r \pmod{m_r},$$

קיים פתרון יחיד מודולו $M = m_1 m_2 \dots m_r$ שניתן על ידי

$$x = \sum_{i=1}^r a_i M_i y_i \pmod{M}$$

כאשר $M_i = \frac{M}{m_i}$ ו- $y_i = M_i^{-1} \pmod{m_i}$ לכל $1 \leq i \leq r$.

דוגמה 1.22

היעזרו במשפט השאריות הסיני כדי לפתור את המערכת

$$x = 22 \pmod{101},$$

$$x = 104 \pmod{113}.$$

פתרון:

$$a_1 = 22, \quad a_2 = 104, \quad m_1 = 101, \quad m_2 = 113.$$

$$M = m_1 m_2 = 11413, \quad M_1 = \frac{M}{m_1} = 113, \quad M_2 = \frac{M}{m_2} = 101.$$

בעזרת הקוד-פיתון modularinverse.py

$$y_1 = M_1^{-1} \bmod m_1 = 113^{-1} \bmod 101 = 59$$

$$x = 22 \cdot \left(\frac{101 \cdot 113}{101} \right).$$

-1

$$y_2 = M_2^{-1} \bmod m_2 = 101^{-1} \bmod 113 = 47$$

$$\begin{aligned} x &= a_1 M_1 y_1 + a_2 M_2 y_2 \bmod M \\ &= 22 \cdot 113 \cdot 59 + 104 \cdot 111 \cdot 47 \bmod 11413 \\ &= 640362 \bmod 11413 \\ &= 1234. \end{aligned}$$



שיעור 2

חוגים מתמטיים

2.1 החוג \mathbb{Z}_m

הגדרה 2.1 החוג \mathbb{Z}_m

החוג \mathbb{Z}_m מוגדר להיות הקבוצה של מספרים שלמים

$$\mathbb{Z}_m = \{0, 1, \dots, m-1\}$$

יחד עם הפעולות \oplus ו- \odot המוגדרות כך:

לכל $a, b \in \mathbb{Z}_m$,

$$a \oplus b = (a + b) \% m, \quad a \odot b = ab \% m.$$

במילים אחרות, \mathbb{Z}_m היא קבוצת השארית בחלוקה ב- m .

מכאן ואילך נסמן חיבור וכפל ב- \mathbb{Z}_m עם הסימנים הרגילים $+$ ו- \times או \cdot .

2.1 דוגמה

חשבו את 11×13 ב- \mathbb{Z}_{16} .

פתרון:

$11 \times 13 = 143$. נמצא את השארית בחלוקה ב- 16:

$$(11 \times 13) \% 16 = 143 \% 16 = 15.$$

לפיכך $11 \times 13 = 15$ ב- \mathbb{Z}_{16} .

משפט 2.1 תכונות של החוג \mathbb{Z}_m

לכל $a, b, c \in \mathbb{Z}_m$ התנאים הבאים מתקיימים.

1. סגירה תחת חיבור:

$$a + b \in \mathbb{Z}_m.$$

2. חוק החילוף לחיבור:

$$a + b = b + a.$$

3. חוק הקיבוץ לחיבור:

$$(a + b) + c = a + (b + c).$$

4. קיום איבר הניטרלי ביחס לחיבור:

$$a + 0 = 0 + a = a.$$

5. האיבר הנגדי של a הוא $m - a$, ז"א $-a = m - a$. הסבר:

$$a + (m - a) = (m - a) + a = m = 0$$

ב- \mathbb{Z}_m .

6. סגירה תחת כפל:

$$ab \in \mathbb{Z}_m .$$

7. חוק החילוף לכפל:

$$ab = ba .$$

8. חוק הקיבוץ לכפל:

$$(ab)c = a(bc) .$$

9. קיום איבר הניטרלי ביחס לכפל:

$$a \times 1 = 1 \times a = a .$$

10. חוק הפילוג:

$$(a + b)c = (ac) + (bc) .$$

תכונות 1, 3-5 אומרות כי \mathbb{Z}_m הינו "חבורה מתמטית".

יחד עם תכונה 2, \mathbb{Z}_m הוא חבורה אֶבֶלית.

כל התכונות 1-10 אומרות כי \mathbb{Z}_m הוא חוג מתמטי.

הגדרה 2.2 איבר ההופכי ב- \mathbb{Z}_m

יהי $a \in \mathbb{Z}_m$. האיבר ההופכי של a מסומן ב- a^{-1} ומקיים את התנאי

$$a^{-1}a \equiv 1 \pmod{m} \quad \text{וגם} \quad aa^{-1} \equiv 1 \pmod{m} .$$

משפט 2.2

נתון היחס שקילות

$$ax \equiv y \pmod{m} .$$

יש פתרון יחיד $x \in \mathbb{Z}_m$ לכל $y \in \mathbb{Z}_m$ אם ורק אם $\gcd(a, m) = 1$.

הוכחה:

ללא הגבלת כלליות נניח כי $a > m$.

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

כלומר, נניח כי יש פתרון יחיד אך $\gcd(a, m) = d > 1$.

יהי $x_1 = a^{-1}y$ פתרון ל- $ax \equiv y \pmod{m}$.

נשים לב ש- $ax_1 + \frac{am}{d} = ax_1 + km \equiv ax_1 \pmod{m}$, כאשר $k = \frac{a}{d}$ שלם.

ז"א גם $x_1 + \frac{m}{d}$ פתרון.

זאת בסתירה לכך שהפתרון יחיד.

נניח כי $\gcd(a, m) = 1$. נוכיח בשלילה כי הפתרון יחיד.

נניח כי $\gcd(a, m) = 1$ וקיימים שני פתרונות שונים: $x_1 \not\equiv x_2 \pmod{m}$.

ז"א

$ax_1 \equiv y \pmod{m}$, וגם $ax_2 \equiv y \pmod{m}$.

לכן

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

לכן

$m \mid ax_1 - ax_2$.

$\gcd(a, m) = 1$ לפיכך

$m \mid x_1 - x_2$,

ז"א

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

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



מסקנה 2.1

יהי $a \in \mathbb{Z}_m$. קיים איבר הופכי $a^{-1} \in \mathbb{Z}_m$ אשר לפי הגדרתו 2.2 מקיים את התנאי

$aa^{-1} \equiv 1 \pmod{m}$,

אם ורק אם $\gcd(a, m) = 1$.



הוכחה: משפט 2.2.

דוגמה 2.2

הוכיחו שקיים איבר הופכי ל- 11 ב- \mathbb{Z}_{26} ואם כן מצאו אותו.

פתרון:

קיים איבר הופכי של a ב- \mathbb{Z}_m אם ורק אם $\gcd(a, m) = 1$. לכן נבדוק את ה- $\gcd(26, 11)$ באמצעות האלגוריתם של אוקליד המוכלל. יהיו $a = 26, b = 11$.

$r_0 = a = 26$, $r_1 = b = 11$,
 $s_0 = 1$, $s_1 = 0$,
 $t_0 = 0$, $t_1 = 1$.

$q_1 = 2$	$t_2 = 0 - 2 \cdot 1 = -2$	$s_2 = 1 - 2 \cdot 0 = 1$	$r_2 = 26 - 2 \cdot 11 = 4$	שלב $i = 1$
$q_2 = 2$	$t_3 = 1 - 2 \cdot (-2) = 5$	$s_3 = 0 - 2 \cdot 1 = -2$	$r_3 = 11 - 2 \cdot 4 = 3$	שלב $i = 2$
$q_3 = 1$	$t_4 = -2 - 1 \cdot (5) = -7$	$s_4 = 1 - 1 \cdot (-2) = 3$	$r_4 = 4 - 1 \cdot 3 = 1$	שלב $i = 3$
$q_4 = 3$	$t_5 = 5 - 3 \cdot (-7) = 28$	$s_5 = -2 - 3 \cdot (3) = -11$	$r_5 = 3 - 3 \cdot 1 = 0$	שלב $i = 4$

$$\gcd(a, b) = r_4 = 1, \quad x = s_4 = 3, \quad y = t_4 = -7.$$

$$ax + by = 3(26) - 7(11) = 1.$$

מכאן אנחנו רואים כי $\gcd(26, 11) = 1$ ולכן לפי משפט 2.2 ההופכי של 11 קיים ב- \mathbb{Z}_{26} . מחשבים את האיבר ההופכי לפי השיטה הבאה:

$$-7(11) = 1 - 9(26) \Rightarrow -7(11) = 1 \pmod{26} \Rightarrow 19(11) = 1 \pmod{26} \Rightarrow 11^{-1} = 19 \pmod{26}.$$

■

כלל 2.1

האיברים של \mathbb{Z}_{26} שעבורם קיימים איברים הופכיים הינם

1^{-1}	3^{-1}	5^{-1}	7^{-1}	9^{-1}	11^{-1}	15^{-1}	17^{-1}	19^{-1}	21^{-1}	23^{-1}	25^{-1}
1	9	21	15	3	19	7	23	11	5	17	25

הגדרה 2.3 פונקציית אוילר $\phi(m)$

נתון החוג \mathbb{Z}_m כאשר $m \geq 2$ מספר טבעי. $\phi(m)$ תוגדר להיות הפונקציה הנותנת את מספר איברים ב- \mathbb{Z}_m אשר זרים ל- m .

(שימו לב להגדרה הזאת זהה להגדרה 1.7).

מסקנה 2.2 מספר איברים הפיכים ב- \mathbb{Z}_m

מספר האיברים של החוג \mathbb{Z}_m שעבורם קיימים איברים הופכיים שווה ל- $\phi(m)$.

הוכחה: $a \in \mathbb{Z}_m$ שווה למספר איברים $\phi(m)$

עבורם $\gcd(a, m) = 1$, ולפי משפט 2.1 אותם האיברים הם האיברים ההפיכים של \mathbb{Z}_m .

■

2.2 הפיכת מטריצות בחוג \mathbb{Z}_m

הגדרה 2.4 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 2.5 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 2.3 נוסחת למטריצה ההופכית

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 2.3

מצאו את ההופכית של

$$A = \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix} \in \mathbb{Z}_{26}^{2 \times 2} .$$

פתרון:

$$|A| = 11 \cdot 7 - 8 \cdot 3 = 53 = 1 \pmod{26} .$$

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

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

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

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

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

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

$$\text{adj}(A) = C^t = \begin{pmatrix} 7 & -8 \\ -3 & 11 \end{pmatrix}$$

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

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

לפיכך

$$A^{-1} = |A|^{-1} \text{adj}(A) = 1 \cdot \begin{pmatrix} 7 & -8 \\ -3 & 11 \end{pmatrix} = \begin{pmatrix} 7 & 22 \\ 23 & 11 \end{pmatrix} \in \mathbb{Z}_{26}^{2 \times 2}.$$

■

2.4 דוגמה

מצאו את ההופכית של

$$A = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 5 & 0 \\ 2 & 0 & 3 \end{pmatrix} \in \mathbb{Z}_{26}^{3 \times 3}.$$

פתרון:

$$|A| = 1 \cdot \begin{vmatrix} 5 & 0 \\ 0 & 3 \end{vmatrix} + 0 \begin{vmatrix} 0 & 0 \\ 2 & 3 \end{vmatrix} + 1 \begin{vmatrix} 0 & 5 \\ 2 & 0 \end{vmatrix} = 1 \cdot 15 + 1 \cdot (-10) = 5.$$

 $\gcd(15, 26) = 1$ לכן המטריצה הפיכה ב- \mathbb{Z}_{26} .

$$\begin{pmatrix} \cancel{1} & 0 & \cancel{1} \\ 0 & 5 & 0 \\ 2 & 0 & 3 \end{pmatrix} \Rightarrow C_{11} = (-1)^{1+1} \begin{vmatrix} 5 & 0 \\ 0 & 3 \end{vmatrix} = 15.$$

$$\begin{pmatrix} \cancel{1} & \cancel{0} & \cancel{1} \\ 0 & 5 & 0 \\ 2 & 0 & 3 \end{pmatrix} \Rightarrow C_{12} = (-1)^{1+2} \begin{vmatrix} 0 & 0 \\ 2 & 3 \end{vmatrix} = 0.$$

$$\begin{pmatrix} \cancel{1} & 0 & \cancel{1} \\ 0 & 5 & \cancel{0} \\ 2 & 0 & 3 \end{pmatrix} \Rightarrow C_{13} = (-1)^{1+3} \begin{vmatrix} 0 & 5 \\ 2 & 0 \end{vmatrix} = -10.$$

$$\begin{pmatrix} \cancel{1} & 0 & 1 \\ \cancel{0} & 5 & \cancel{0} \\ 2 & 0 & 3 \end{pmatrix} \Rightarrow C_{21} = (-1)^{2+1} \begin{vmatrix} 0 & 1 \\ 0 & 3 \end{vmatrix} = 0.$$

$$\begin{pmatrix} 1 & \cancel{0} & 1 \\ 0 & \cancel{5} & \cancel{0} \\ 2 & 0 & 3 \end{pmatrix} \Rightarrow C_{22} = (-1)^{2+2} \begin{vmatrix} 1 & 1 \\ 2 & 3 \end{vmatrix} = 1.$$

$$\begin{pmatrix} 1 & 0 & \cancel{1} \\ \cancel{0} & 5 & \cancel{0} \\ 2 & 0 & 3 \end{pmatrix} \Rightarrow C_{23} = (-1)^{2+3} \begin{vmatrix} 1 & 0 \\ 2 & 0 \end{vmatrix} = 0.$$

$$\begin{pmatrix} \cancel{1} & 0 & 1 \\ 0 & 5 & 0 \\ \cancel{2} & \cancel{0} & \cancel{3} \end{pmatrix} \Rightarrow C_{31} = (-1)^{3+1} \begin{vmatrix} 0 & 1 \\ 5 & 0 \end{vmatrix} = -5.$$

$$\begin{pmatrix} 1 & \cancel{0} & 1 \\ 0 & 5 & 0 \\ \cancel{2} & \cancel{0} & \cancel{3} \end{pmatrix} \Rightarrow C_{32} = (-1)^{3+2} \begin{vmatrix} 1 & 1 \\ 0 & 0 \end{vmatrix} = 0.$$

$$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 5 & 0 \\ 2 & 0 & 3 \end{pmatrix} \Rightarrow C_{33} = (-1)^{3+3} \begin{vmatrix} 1 & 0 \\ 0 & 5 \end{vmatrix} = 5.$$

$$C = \begin{pmatrix} C_{11} & C_{12} & C_{13} \\ C_{21} & C_{22} & C_{23} \\ C_{31} & C_{32} & C_{33} \end{pmatrix} = \begin{pmatrix} 15 & 0 & -10 \\ 0 & 1 & 0 \\ -5 & 0 & 5 \end{pmatrix}$$

$$\text{adj}(A) = C^t = \begin{pmatrix} 15 & 0 & -5 \\ 0 & 1 & 0 \\ -10 & 0 & 5 \end{pmatrix} = \begin{pmatrix} 15 & 0 & 21 \\ 0 & 1 & 0 \\ 16 & 0 & 5 \end{pmatrix} \in \mathbb{Z}_{26}^{3 \times 3}.$$

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

$$|A|^{-1} = 5^{-1} = 21 \in \mathbb{Z}_{26}$$

לפיכך

$$A^{-1} = |A|^{-1} \text{adj}(A) = 21 \cdot \begin{pmatrix} 15 & 0 & 21 \\ 0 & 1 & 0 \\ 16 & 0 & 5 \end{pmatrix} = \begin{pmatrix} 315 & 0 & 441 \\ 0 & 21 & 0 \\ 336 & 0 & 105 \end{pmatrix} \in \mathbb{Z}_{26}^{3 \times 3}.$$

$$315 \% 26 = 315 - 26 \cdot \left\lfloor \frac{315}{26} \right\rfloor = -23 \equiv 3 \pmod{26} \Rightarrow 315 \equiv 3 \pmod{26}.$$

$$441 \% 26 = 441 - 26 \cdot \left\lfloor \frac{441}{26} \right\rfloor = 25 \Rightarrow 441 \equiv 25 \pmod{26}.$$

$$336 \% 26 = 336 - 26 \cdot \left\lfloor \frac{336}{26} \right\rfloor = 24 \Rightarrow 336 \equiv 24 \pmod{26}.$$

$$105 \% 26 = 105 - 26 \cdot \left\lfloor \frac{105}{26} \right\rfloor = 1 \Rightarrow 105 \equiv 1 \pmod{26}.$$

לפיכך

$$A^{-1} = \begin{pmatrix} 3 & 0 & 25 \\ 0 & 21 & 0 \\ 24 & 0 & 1 \end{pmatrix} \in \mathbb{Z}_{26}^{3 \times 3}.$$

בדיקה:

$$A \cdot A^{-1} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 5 & 0 \\ 2 & 0 & 3 \end{pmatrix} \begin{pmatrix} 3 & 0 & 25 \\ 0 & 21 & 0 \\ 24 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 27 & 0 & 26 \\ 0 & 105 & 0 \\ 78 & 0 & 53 \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \pmod{26}.$$

2.3 תמורות

הגדרה 2.6 תמורה

נתונה קבוצה מסודרת נוצר סופית $X = \{x_1, x_2, \dots, x_n\}$ ללא חזרות. תמורה היא פונקציה חד-חד-ערכית ועל $\pi: X \rightarrow X$ שמקבלת X ומחזירה הקבוצה X ומשנה את הסדר של האיברים.

דוגמה 2.5

- תמורות של הקבוצה (a, b) :

$$\pi_1(a, b) = (a, b), \quad \pi_2(a, b) = (b, a).$$

הראשון הוא מקרה פרטי של תמורה, אשר הוא פונקצית הזהות. קיימים $2!$ תמורות. תמורות.

- תמורות של הקבוצה (a, b, c) :

$$\begin{aligned} \pi_1(a, b, c) &= (a, b, c), & \pi_2(a, b, c) &= (c, a, b), & \pi_3(a, b, c) &= (b, c, a), \\ \pi_4(a, b, c) &= (b, a, c), & \pi_5(a, b, c) &= (a, c, b), & \pi_6(a, b, c) &= (c, b, a). \end{aligned}$$

קיימים $3!$ תמורות.

- תמורות של הקבוצה $(\alpha, \beta, \gamma, \delta)$:

$$\pi_1(\alpha, \beta, \gamma, \delta) = (\delta, \alpha, \gamma, \beta), \dots$$

קיימים $4!$

- תמורות של הקבוצה $(\alpha, \beta, \gamma, \delta)$:

$$\pi_1(\alpha, \beta, \gamma, \delta) = (\delta, \alpha, \gamma, \beta), \quad \pi_2(\alpha, \beta, \gamma, \delta) = (\beta, \gamma, \delta, \alpha), \dots$$

קיימים $4!$ תמורות.

משפט 2.4

יהי X קבוצה מסודרת נוצר סופית ללא חזרות של אורך n . קיימות $n!$ תמורות.

הוכחה: תרגיל בית.

הגדרה 2.7 סימון אינדקס של תמורה

יהי $X = (x_1, x_2, \dots, x_n)$ ויהי $\pi : X \rightarrow X$ תמורה. נניח שאחרי ביצוע של התמורה π על X , האיבר שהיה במיקום ה- i עכשיו במיקום ה- j ($1 \leq i, j \leq n$). אז אנחנו כותבים

$$\pi(i) = j.$$

הביטוי הזה נקרא **סימון אינדקס**.

דוגמה 2.6

(א) נתונה התמורה

$$\pi(a, b) = (b, a).$$

בסימון אינדקס,

$$\pi(1) = 2, \quad \pi(2) = 1.$$

(ב) נתונה התמורה

$$\pi(a, b, c) = (b, c, a).$$

בסימון אינדקס,

$$\pi(1) = 3, \quad \pi(2) = 1, \quad \pi(3) = 2.$$

ג) נתונה התמורה

$$\pi(\alpha, \beta, \gamma, \delta) = (\beta, \gamma, \delta, \alpha).$$

בסימון אינדקס,

$$\pi(1) = 4, \quad \pi(2) = 1, \quad \pi(3) = 2, \quad \pi(4) = 3.$$

הגדרה 2.8 הצגת שתי-שורות והצגת שורת-אחת

יהי $X = (x_1, x_2, \dots, x_n)$ ויהי $\pi : X \rightarrow X$ תמורה שמוגדרת

$$\pi(X) = (x_{\pi(1)}, x_{\pi(2)}, \dots, x_{\pi(n)}).$$

• ההצגה שתי-שורות של התמורה הזאת הינה

$$\pi = \begin{pmatrix} 1 & 2 & \dots & i & \dots & n \\ \pi(1) & \pi(2) & \dots & \pi(i) & \dots & \pi(n) \end{pmatrix}$$

• ההצגה שורת-אחת של התמורה הזאת הינה

$$\pi = (\pi(1) \ \pi(2) \ \dots \ \pi(i) \ \dots \ \pi(n))$$

דוגמה 2.7

א) נתונה התמורה

$$\pi(a, b) = (b, a).$$

בסימון אינדקס:

$$\pi(1) = 2, \quad \pi(2) = 1.$$

$$\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}.$$

$$(2 \ 1).$$

הצגת שתי-שורות:

הצגת שורה-אחת:

ב) נתונה התמורה

$$\pi(a, b, c) = (b, c, a).$$

בסימון אינדקס:

$$\pi(1) = 3, \quad \pi(2) = 1, \quad \pi(3) = 2.$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

$$(3 \ 1 \ 2).$$

הצגת שתי-שורות:

הצגת שורה-אחת:

ג) נתונה התמורה

$$\pi(\alpha, \beta, \gamma, \delta) = (\beta, \gamma, \delta, \alpha).$$

בסימון אינדקס:

$$\pi(1) = 4, \quad \pi(2) = 1, \quad \pi(3) = 2, \quad \pi(4) = 3.$$

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

$$(4 \ 1 \ 2 \ 3).$$

הצגת שתי-שורות:

הצגת שורה-אחת:

דוגמה 2.8 הרכבה של תמורות

תהיינה $\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ ו- $\beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$. חשבו את $\alpha \circ \beta$ ו- $\beta \circ \alpha$.

פתרון:

$$\alpha \circ \beta = \begin{pmatrix} 1 & 2 & 3 \\ \alpha(\beta(1)) & \alpha(\beta(2)) & \alpha(\beta(3)) \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ \alpha(2) & \alpha(1) & \alpha(3) \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$\beta \circ \alpha = \begin{pmatrix} 1 & 2 & 3 \\ \beta(\alpha(1)) & \beta(\alpha(2)) & \beta(\alpha(3)) \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ \beta(2) & \beta(3) & \beta(1) \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

■

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

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

-1

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

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:

QRQXFJANHXD

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 $k = 9$.

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 $0, 1, 2, \dots, 25$.

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 $26! = 4.03291461126605635584 \times 10^{26}$ 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 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-

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

וכן הלאה.
נתון הטקסט מוצפן

GHYYF

מצאו את הטקסט גלוי.

פתרון:

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

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,

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

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,

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

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

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

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)

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

יש פתרון יחיד ל- x .

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

משפט 3.1

ליחס שקילות

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

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

הוכחה: (ראו גם הוכחה למשפט 2.2).

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- $ax \equiv y \pmod{26}$, אז גם $x_1 + \frac{26}{d}$ פתרון הסבר:

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

כאשר $k = \frac{a}{d}$. שלם.

בפרט, מכיוון ש- $d > 1$ אז $x_1 + \frac{26}{d} \not\equiv x_1 \pmod{26}$, 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: $x_1 \not\equiv x_2 \pmod{26}$.

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

$$26 \mid x_1 - x_2 ,$$

ז"א

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

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

דוגמה 3.7

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 מוצפן.

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 $k = (a, b) \in K$ 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 2.3):

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

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

דוגמה 3.8

נתון כלל מצפין של צופן אפייני 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 3.9

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 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 :

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

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

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

מכאן נקבל

$x \in P$	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 3.10

נתון הטקסט מוצפן

ACSE

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

פתרון:

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

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

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

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

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

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

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

$y \in C$	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 פוליאלפביתי: 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 $k = (k_1, k_2, \dots, k_m)$ 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} .

דוגמה 3.11

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 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

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

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 שלישייה (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:

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 $(x_1, x_2, x_3, x_4, x_5, x_6)$ בבולק 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 בבולק 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

3.6 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 נצצעות 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 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	l	y
$x \in \mathbb{Z}_{26}$	9	20	11	24

שלב 3:

עבור כל תת-קבוצה המתקבל נחשב

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

עבור התת-קבוצה הראשונה נקבל

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

עבור התת-קבוצה השנייה נקבל

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

$x \in P$	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 3.14

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} .

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

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

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

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

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

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

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

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

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 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

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

עבור התת-קבוצה הראשונה נקבל

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

עבור התת-קבוצה השנייה נקבל

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

$y \in C$	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 3.15

נתון רצף טקסט 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:

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} .

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

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

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

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

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

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

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

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

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

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

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

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

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

לפיכך

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

$$= 7 \cdot \begin{pmatrix} 16 & 3 & 18 \\ 9 & 9 & 1 \\ 21 & 5 & 20 \end{pmatrix} \pmod{26}$$

$$= \begin{pmatrix} 112 & 21 & 126 \\ 63 & 63 & 7 \\ 147 & 35 & 140 \end{pmatrix} \pmod{26}$$

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

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

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

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

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

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

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

עבור התת-קבוצה הראשונה נקבל

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

עבור התת-קבוצה השנייה נקבל

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

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:

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 $\{1, \dots, m\}$. עבור מפתח $\pi \in K$ (עבור תמורה של K) נגדיר כלל מצפין

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

ונגדיר כלל מפענח

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

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 הטקסט מצפון מסעיף הקודם עם התמורה ההופכית.

פתרון:

סעיף (1) שלב 1:

נעביר את האותיות של הטקסט גלוי 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 הטבלה של התווים של הטקסט גלוי 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 2)

שלב 1:

נתחיל עם הטקסט מוצפן

LOFERW

ונעביר את האותיות של הטקסט גלוי 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 הטבלה של התווים של הטקסט גלוי יחד עם הערכים המתאימים של \mathbb{Z}_{26} לתת-קבוצות של $m = 3$ 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 תת-קבוצה המתקבל נפעיל את התמרוה ההופכית: π^{-1} :

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

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

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

$y \in C$	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 גלוי:

$y \in C$	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

שיעור 4

הצפנים הבסיסיים (המשך)

4.1 צפני זרם

עד כה דיברנו על צפנים המבוססים על מפתח k אילו הטקסט מוצפן y 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 בלוק.

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

הגדרה 4.1 צופן זרם סינכרוני

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

(1) E מסמן קבוצה של טקסטים גלויים (plaintexts),

(2) C מסמן קבוצה של טקסטים מוצפנים (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 $d_z \in D$:

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

כך ש-

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

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

הגדרה 4.2 צופן אוטו מפתח (Autokey cipher)

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

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

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 4.1 (צופן אוטו-מפתח)

נתון צופן אוטו-מפתח עם מפתח $k = 8$.

(1) מצאו את הטקסט מוצפן של המילה

rendezvous .

(2) פענחו את הטקסט מוצפן המתקבל וודאו שקיבלתם את הטקסט הגלוי.

פתרון:

סעיף 1) נרשום את האותיות של הטקסט 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 הטקסט 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 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 גלוי באמצעות הכלל מפענח:

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

$y \in C$	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} דתווים של טקסט 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



שיעור 5

צופן RSA

5.1 משפט השאריות הסיני

משפט 5.1 משפט השאריות הסיני

יהיו m_1, m_2, \dots, m_r שלמים אשר זרים בזוגות ויהיו a_1, a_2, \dots, a_r שלמים. למערכת של יחסים שקילות

$$x = a_1 \pmod{m_1},$$

$$x = a_2 \pmod{m_2},$$

$$\vdots$$

$$x = a_r \pmod{m_r},$$

קיים פתרון יחיד מודולו $M = m_1 m_2 \cdots m_r$ שניתן על ידי

$$x = \sum_{i=1}^r a_i M_i y_i \pmod{M}$$

כאשר $M_i = \frac{M}{m_i}$ ו- $y_i = M_i^{-1} \pmod{m_i}$ לכל $1 \leq i \leq r$.

דוגמה 5.1

היעזרו במשפט השאריות הסיני כדי לפתור את המערכת

$$x = 22 \pmod{101},$$

$$x = 104 \pmod{113}.$$

פתרון:

$$a_1 = 22, \quad a_2 = 104, \quad m_1 = 101, \quad m_2 = 113.$$

$$M = m_1 m_2 = 11413, \quad M_1 = \frac{M}{m_1} = 113, \quad M_2 = \frac{M}{m_2} = 101.$$

$$y_1 = M_1^{-1} \pmod{m_1} = 113^{-1} \pmod{101}, \quad y_2 = M_2^{-1} \pmod{m_2} = 101^{-1} \pmod{113}.$$

כדי לחשב את האיברים ההופכיים נשתמש בהאלגוריתם המוכלל של אוקליד.

נסמן $a = 113, b = 101$.

$$r_0 = a = 113, \quad r_1 = b = 101,$$

$$s_0 = 1, \quad s_1 = 0,$$

$$t_0 = 0, \quad t_1 = 1.$$

$q_1 = 1$	$t_2 = 0 - 1 \cdot 1 = -1$	$s_2 = 1 - 1 \cdot 0 = 1$	$r_2 = 113 - 1 \cdot 101 = 12$	שלב $k = 1$
$q_2 = 4$	$t_3 = 1 - 8 \cdot (-1) = 9$	$s_3 = 0 - 8 \cdot 1 = -8$	$r_3 = 101 - 8 \cdot 12 = 5$	שלב $k = 2$
$q_3 = 2$	$t_4 = -1 - 2 \cdot (9) = -19$	$s_4 = 1 - 2 \cdot (-8) = 17$	$r_4 = 12 - 2 \cdot 5 = 2$	שלב $k = 3$
$q_4 = 2$	$t_5 = 9 - 2 \cdot (-19) = 47$	$s_5 = -8 - 2 \cdot 17 = -42$	$r_5 = 5 - 2 \cdot 2 = 1$	שלב $k = 4$
$q_5 = 2$	$t_6 = -19 - 2 \cdot (47) = -113$	$s_6 = 17 - 2 \cdot (-42) = 101$	$r_6 = 2 - 2 \cdot 1 = 0$	שלב $k = 5$

$$\gcd(a, b) = r_5 = 1, \quad s = s_5 = -42, \quad t = t_5 = 47.$$

$$ta + sb = -42(113) + 47(101) = 1.$$

מכאן

$$101^{-1} \equiv 47 \pmod{113}$$

ו-

$$113^{-1} \equiv -42 \pmod{101} = 59 \pmod{101}$$

לכן

$$y_1 = M_1^{-1} \pmod{m_1} = 113^{-1} \pmod{101} = 59$$

ו-

$$y_2 = M_2^{-1} \pmod{m_2} = 101^{-1} \pmod{113} = 47$$

$$\begin{aligned} x &= a_1 M_1 y_1 + a_2 M_2 y_2 \pmod{M} \\ &= 22 \cdot 113 \cdot 59 + 104 \cdot 111 \cdot 47 \pmod{11413} \\ &= 640362 \pmod{11413} \\ &= 1234. \end{aligned}$$

■

5.2 משפטים של מספרים ראשוניים

משפט 5.2 קיימים אינסוף מספרים ראשוניים

קיימים אינסוף מספרים ראשוניים.

הוכחה: נוכיח הטענה דרך השלילה.

נניח כי $\{p_1, \dots, p_n\}$ הוא הקבוצה של כל הראשוניים שקיימים וקבוצה זו נוצרת סופי.

נגדיר השלם $M = (p_1 \cdot p_2 \cdot \dots \cdot p_n) + 1$.

לפי משפט הפירוק לראשוניים (ראו משפט 1.3 למעלה או משפט 5.3 למטה) M הוא מספר ראשוני או שווה למכפלה של ראשוניים.

M לא מספר ראשוני בגלל ש- $M > p_i$ לכל $1 \leq i \leq n$.

גם לא קיים מספק ראשוני p_i אשר מחלק את M . הרי

$$M \% p_i = 1 \Rightarrow p_i \nmid M.$$

■ הגענו לסתירה של המשפט הפירוק לראשוניים, לכן קיימים אינסוף מספרים ראשוניים.

משפט 5.3 משפט הפירוק לראשוניים

(ראו משפט 1.3) לכל מספר שלם n קיימים שלמים e_i וראשוניים p_i כך ש-

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$

■ **הוכחה:** אינדוקציה.

משפט 5.4

אם a, b שלמים זרים (כלומר $\gcd(a, b) = 1$) אז

$$\phi(m \cdot n) = \phi(m) \cdot \phi(n) .$$

■ **הוכחה:** (להעשרה בלבד)

משפט 5.5

אם p מספר ראשוני אז

$$\phi(p^n) = p^n - p^{n-1} .$$

■ **הוכחה:** נתבונן על $\gcd(p^n, m)$ כאשר m שלם ו- p ראשוני.

האפשרויות היחידות של המחלק המשותף הגדול ביותר $\gcd(p^n, m)$ הן $1, p, p^2, \dots, p^n$. בסה"כ יש p^n אפשרויות.

$\gcd(p^n, m) > 1$ רק אם $m \in \{p, 2p, 3p, \dots, p^{n-1}p\}$, כלומר רק אם m שווה לכפולה של p .

מכאן קיימים $p^n - p^{n-1}$ שלמים עבורם $\gcd(p^n, m) = 1$.

■

משפט 5.6 נוסחה לפונקצית אוילר

(ראו משפט 1.4) לכל מספר שלם n בעל פירוק לראשוניים

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$

פונקציית אוילר ניתנת על ידי

$$\phi(n) = \prod_{i=1}^k (p_i^{e_i} - p_i^{e_i-1}) = (p_1^{e_1} - p_1^{e_1-1}) (p_2^{e_2} - p_2^{e_2-1}) \cdots (p_k^{e_k} - p_k^{e_k-1})$$

■ **הוכחה:** משפט 5.4 ו- 5.5.

דוגמה 5.2

חשבו את $\phi(24)$

פתרון:

$$24 = 2^3 3^1 .$$

לכן

$$\phi(24) = (2^3 - 2^2)(3^1 - 3^0) = (8 - 4)(3 - 1) = 8 .$$

משפט 5.7

אם p מספר ראשוני אז

$$\phi(p) = p - 1 .$$

הוכחה: משפט 5.4 ו- 5.5.

משפט 5.8

אם p ו- q מספרים ראשוניים שונים אז

$$\phi(p \cdot q) = (p - 1)(q - 1) .$$

הוכחה: תרגיל בית.

משפט 5.9 המשפט הקטן של פרמה

אם p מספר ראשוני ו- $a \in \mathbb{Z}_p$. אז התנאים הבאים מתקיימים:

$$1. \quad a^p \equiv a \pmod{p}$$

$$2. \quad a^{p-1} \equiv 1 \pmod{p}$$

$$3. \quad a^{-1} \equiv a^{p-2} \pmod{p}$$

הוכחה:

טענה 1. נוכיח באינדוקציה.

בסיס:עבור $a = 0$ הטענה $0^p \equiv 0 \pmod{p}$ מתקיימת.מעבר:נניח כי הטענה מתקיימת עבור a .

$$(a + 1)^p = a^p + pa^{p-1} + \frac{p(p-1)}{2}a^{p-2} + \dots + pa + 1 \equiv a^p + 1 \pmod{p}$$

ההנחת האינדוקציה אומרת ש- $a^p \equiv a \pmod p$ לכן

$$(a+1)^p \pmod p \equiv a^p + 1 \pmod p \equiv (a+1) \pmod p$$

כנדרש.

טענה 2. $\gcd(a, p) = 1$ לפיכך קיים איבר הופכי $a^{-1} \in \mathbb{Z}_p$. נכפיל ב- a^{-1} אשר הוכחנו בסעיף הקודם:

$$a^{-1}a^p \equiv a^{-1} \cdot a \pmod p \Rightarrow a^{p-1} \equiv 1 \pmod p .$$

טענה 3.

$$a^{p-1} \equiv 1 \pmod p \Leftrightarrow 1 \equiv a^{p-1} \pmod p \Rightarrow a^{-1} \equiv a^{p-2} \pmod p .$$

■

משפט 5.10 משפט אוילר

אם a, n שלמים ו- $\gcd(a, n) = 1$ אז

$$a^{\phi(n)} \equiv 1 \pmod n .$$

משפט 5.11

אם a, n שלמים ו- $\gcd(a, n) = 1$ אז

$$a^{-1} \equiv a^{\phi(n)-1} \pmod n .$$

דוגמה 5.3

חשבו את האיבר ההופכי ל- 5 ב- \mathbb{Z}_{11} .

פתרון:

לפי משפט פרמט 5.9:

$$5^{-1} = 5^{11-2} \pmod{11} = 5^9 \pmod{11} .$$

לפי הנוסחת לשארית 1.2 :

$$5^9 \% 11 = 5^9 - 11 \left\lfloor \frac{5^9}{11} \right\rfloor = 9$$

לכן $5^{-1} \in \mathbb{Z}_{11} = 9$.

■

5.3 אלגוריתם RSA

צופן RSA הומצא בשנה 1977 על ידי Ron Rivest, Adi Shamir and Len Adleman .

הגדרה 5.1 צופן RSA

יהי $n = pq$ כאשר p, q מספרים ראשוניים שונים. תהי הקבוצת טקסט גלוי $P = \mathbb{Z}_n$, והקבוצת טקסט מוצפן $C = \mathbb{Z}_n$. נגדיר קבוצת המפתחות

$$K = \left\{ (n, p, q, a, b) \mid ab = 1 \pmod{\phi(n)} \right\}$$

לכל $k = (n, p, q, a, b) \in K$, ולכל $x \in P$ ו- $y \in C$ נגדיר כלל מצפין

$$e_k(x) = x^b \mod n,$$

ונגדיר כלל מפענח

$$d_k(x) = y^a \mod n.$$

הערכים של n ו- b הם ערכים ציבוריים בעוד p, q, a ערכים סודיים.

משפט 5.12 קריפטו-מערכת RSA ניתן לפענוח

יהי $n = pq$ מספרים ראשוניים שונים, $a, b \in \mathbb{Z}$ שלמים חיוביים כך ש- $ab = 1 \mod \phi(n)$.

אם $x \in \mathbb{Z}_n$ אז

$$(x^b)^a = x \mod n.$$

הוכחה: נתון כי $ab = 1 \mod \phi(n)$.

לפי משפט 5.8, $\phi(n) = \phi(pq) = (p-1)(q-1)$, $\phi(n)$ ז"א

$$ab = 1 \mod \phi(n) = 1 \mod (p-1)(q-1)$$

לכן קיים $t \in \mathbb{Z}$ כך ש-

$$ab - 1 = t(p-1)(q-1).$$

לכל $z \neq 0 \in \mathbb{Z}$ לפי משפט 5.9, $z^{p-1} = 1 \mod p$ בפרט

$$x^{ab-1} = x^{t(p-1)(q-1)} = (x^{t(q-1)})^{p-1} = y^{p-1}$$

כאשר $y = x^{t(q-1)}$. מכאן $x^{ab-1} = 1 \mod p$

משיקולות של סיימטריה באותה מידה $x^{ab-1} = 1 \mod q$

לכן $x^{ab-1} - 1 = 0 \mod p$ ו- $x^{ab-1} - 1 = 0 \mod q$

מכיוון ש- p ו- q זרים אז

$$x^{ab-1} - 1 = 0 \mod (pq).$$

לפיכך

$$x^{ab-1} = 1 \mod (pq).$$

נכפיל ב- x ונקבל

$$(x^a)^b = x \mod (pq).$$

ז"א הוכחנו כי לכל טקסט גלוי x , אם נצפין אותו ואז אחר כך נפענח את הטקסט מוצפן המתקבל מאלגוריתם RSA, נקבל אותו טקסט גלוי המקורי בחזרה. ■

הגדרה 5.2 אלגוריתם RSA

שלב הרכבת המפתח

נניח שאלים (A) שולחת הודעה לבוב (B) .

[1] יוצר B שני מספרים ראשוניים גדולים שונים, p ו- q בסדר גודל של 100 ספרות דצמליות.

[2] B מחשב $n = pq$ ו- $\phi(n) = (p-1)(q-1)$.

[3] בוחר במספר שלם באופן מקרי $(0 \leq b \leq \phi(n))$ כך ש- $\gcd(b, \phi(n)) = 1$.

[4] מחשב a כך ש- $a = b^{-1} \mod \phi(n)$ בעזרת האלגוריתם של אוקלידס, (ראו כלל 1.10) ולכן $0 \leq a < \phi(n)$.

[5] שומר את המפתח ציבורי (b, n) בכתובת קובץ ציבורי, ושומר על המפתח פנימי (a, p, q) סודי.

בניית מפתח עשוי פעם אחת.

שלב הצפנה

[6] אליס (A) קוראת את המפתח הצפנה (הציבורי) $k = (b, n)$ מכתובת קובץ הציבורי.

[7] בכדי להצפין הודעה x , $(0 \leq x < n)$ אליס (A) מחשבת $y = x^b \mod n$.

[8] A שולחת טקסט מוצפן ל- B .

[9] בכדי לפענח את הטקסט מוצפן y , בוב (B) משמש במפתח הפרטי שלו $k^{-1} = (a, p, q)$ ומחשב $x = y^a \mod n$.

5.4 דוגמה

בוב בונה צופן RSA עם המפתח ציבורי $(b = 47, p = 127, q = 191)$.

(א) חשבו את n , $\phi(n)$ ו- a .

(ב) אליס קוראת את המפתח ציבורי (b, n) ומשתמשת בה כדי להצפין את המסר 2468. מהי הטקסט מוצפן שהיא שולחת לבוב?

(ג) כעת בוב מפענח את הטקסט מוצפן שהוא קיבל מאליס בעזרת המפתח (a, p, q) . בדקו כי הפענוח של הטקסט מוצפן מסעיף ב' זהה לטקסט גלוי אשר אליס שלחה.

פתרון:

סעיף א)

$$n = pq = 191 \times 127 = 24257$$

$$\phi(n) = \phi(pq) = (p-1)(q-1) = 190 \times 126 = 23940$$

$$a = 47^{-1} \mod 23940 \text{ נשתמש באלגוריתם של אוקלידס:}$$

שיטה 1

$$a = 23940, b = 47$$

$$r_0 = a = 23940, \quad r_1 = b = 47,$$

$$s_0 = 1, \quad s_1 = 0,$$

$$t_0 = 0, \quad t_1 = 1.$$

$q_1 = 509$	$t_2 = 0 - 509 \cdot 1 = -509$	$s_2 = 1 - 509 \cdot 0 = 1$	$r_2 = 23940 - 509 \cdot 47 = 17$	שלב $k = 1$:
$q_2 = 2$	$t_3 = 1 - 2 \cdot (-509) = 1019$	$s_3 = 0 - 2 \cdot 1 = -2$	$r_3 = 47 - 2 \cdot 17 = 13$	שלב $k = 2$:
$q_3 = 1$	$t_4 = -509 - 1 \cdot (1019) = -1528$	$s_4 = 1 - 1 \cdot (-2) = 3$	$r_4 = 17 - 1 \cdot 13 = 4$	שלב $k = 3$:
$q_4 = 3$	$t_5 = 1019 - 3 \cdot (-1528) = 5603$	$s_5 = -2 - 3 \cdot (3) = -11$	$r_5 = 13 - 3 \cdot 4 = 1$	שלב $k = 4$:
$q_5 = 4$	$t_6 = -1528 - 4 \cdot (5603) = -23940$	$s_6 = 3 - 4 \cdot (-11) = 47$	$r_6 = 4 - 4 \cdot 1 = 0$	שלב $k = 5$:

$$\gcd(a, b) = r_5 = 1, \quad x = s_5 = -11, \quad y = t_5 = 5603.$$

$$sa + tb = -11(23940) + 5603(47) = 1.$$

מכאן

$$5603(47) = 1 + 11(23940) \Rightarrow 5603(47) = 1 \pmod{23940} \Rightarrow 47^{-1} = 5603 \pmod{23940}.$$

שיטה 2

$$23940 = 509(47) + 17$$

$$47 = 2(17) + 13$$

$$17 = 13 + 4$$

$$13 = 3(4) + 1$$

$$4 = 4(1) + 0.$$

$$1 = 13 - 3(4)$$

$$= 13 - 3(17 - 13)$$

$$= 4(13) - 3(17)$$

$$= 4(47 - 2(17)) - 3(17)$$

$$= 4(47) - 11(17)$$

$$= 4(47) - 11(23940 - 509(47))$$

$$= 5603(47) - 11(23940)$$

$$.a^{-1} = 5603 \text{ לכן}$$

סעיף ב) אליס שולחת את ההודעה $2468^{47} \pmod{24257}$. כדי לחשב זה נשתמש בשיטת ריבועים:

$$.47 = 32 + 8 + 4 + 2 + 1$$

$$(2468)^2 = 2517 \pmod{24257}$$

$$(2468)^4 = (2517)^2 = 4212 \pmod{24257}$$

$$(2468)^8 = (4212)^2 = 9077 \pmod{24257}$$

$$(2468)^{16} = (9077)^2 = 15157 \pmod{24257}$$

$$(2468)^{32} = (15157)^2 = 20859 \pmod{24257}$$

לכן

$$\begin{aligned}
 246847 &= (2468)^{32} \times (2468)^8 \times (2468)^4 \times (2468)^2 \times 2468 \pmod{24257} \\
 &= 20859 \times 9077 \times 4212 \times 2517 \times 2468 \pmod{24257} \\
 &= 10642 \pmod{24257}.
 \end{aligned}$$

לכן הטקסט מוצפן הוא $y = 10642$.סעיף ג) $y = 10642$

$$y \pmod{p} = 10642 \pmod{127} = 101, \quad a \pmod{(p-1)} = 5603 \pmod{126} = 59.$$

לכן

$$\begin{aligned}
 x_1 &= (y \pmod{p})^{a \pmod{(p-1)}} \pmod{p} = 101^{59} \pmod{127} = 55 \\
 &\quad (\text{ניתן לחשב זה לפי } 101^{32} \times 101^{16} \times 101^8 \times 101^2 \times 101)
 \end{aligned}$$

$$\begin{aligned}
 (101)^2 &\equiv 41 \pmod{127} \\
 (101)^4 &\equiv (41)^2 \pmod{127} \equiv 30 \pmod{127} \\
 (101)^8 &\equiv (30)^2 \pmod{127} \equiv 11 \pmod{127} \\
 (101)^{16} &\equiv (11)^2 \pmod{127} \equiv 121 \pmod{127} \\
 (101)^{32} &\equiv (121)^2 \pmod{127} \equiv 36 \pmod{127}
 \end{aligned}$$

לכן

$$101^{59} \pmod{127} = (101)(41)(11)(121)(36) \pmod{127} = 55.$$

$$y \pmod{q} = 10642 \pmod{191} = 137, \quad a \pmod{(p-1)} = 5603 \pmod{190} = 93.$$

לכן

$$\begin{aligned}
 x_2 &= (y \pmod{q})^{a \pmod{(q-1)}} \pmod{q} = 137^{93} \pmod{191} = 176 \\
 &\quad (\text{ניתן לחשב זה לפי } 137^{64} \times 137^{16} \times 137^8 \times 137^4 \times 137)
 \end{aligned}$$

$$\begin{aligned}
 (137)^2 &\equiv 51 \pmod{191} \\
 (137)^4 &\equiv (51)^2 \pmod{191} \equiv 118 \pmod{191} \\
 (137)^8 &\equiv (118)^2 \pmod{191} \equiv 172 \pmod{191} \\
 (137)^{16} &\equiv (172)^2 \pmod{191} \equiv 170 \pmod{191} \\
 (137)^{32} &\equiv (170)^2 \pmod{191} \equiv 59 \pmod{191} \\
 (137)^{64} &\equiv (59)^2 \pmod{191} \equiv 43 \pmod{191}
 \end{aligned}$$

לכן

$$137^{93} \pmod{191} = (137)(118)(172)(170)(43) \pmod{191} = 176.$$

בנוסף

$$y \pmod{q} = 9625 \pmod{127} = 100, \quad a \pmod{(q-1)} = 5603 \pmod{126} = 59.$$

לכן

$$x_2 = (y \pmod{q})^{a \pmod{(q-1)}} \pmod{q} = 100^{59} \pmod{127} = 87$$

לכן עלינו לפתור את המערכת

$$x = x_1 \pmod{p} = 55 \pmod{127}$$

$$x = x_2 \pmod{q} = 176 \pmod{191}$$

בעזרת המשפט השאריות הסיני. נסמן $m_2 = 191, a_2 = 176, m_1 = 127, a_1 = 55$.

$$M = m_1 m_2 = (191)(127) = 24257, \quad M_1 = \frac{M}{m_1} = 191, \quad M_2 = \frac{M}{m_2} = 127.$$

כעת נחשב $y_2 = M_2^{-1} \pmod{m_2} = 127^{-1} \pmod{191}$ ו- $y_1 = M_1^{-1} \pmod{m_1} = 191^{-1} \pmod{127}$.

שיטה 1

$$.a = 191, b = 127$$

$$r_0 = a = 191, \quad r_1 = b = 127,$$

$$s_0 = 1, \quad s_1 = 0,$$

$$t_0 = 0, \quad t_1 = 1.$$

$q_1 = 1$	$t_2 = 0 - 1 \cdot 1 = -1$	$s_2 = 1 - 1 \cdot 0 = 1$	$r_2 = 191 - 1 \cdot 127 = 64$	שלב $k = 1$:
$q_2 = 1$	$t_3 = 1 - 1 \cdot (-1) = 2$	$s_3 = 0 - 1 \cdot 1 = -1$	$r_3 = 127 - 1 \cdot 64 = 63$	שלב $k = 2$:
$q_3 = 1$	$t_4 = -1 - 1 \cdot (2) = -3$	$s_4 = 1 - 1 \cdot (-1) = 2$	$r_4 = 64 - 1 \cdot 63 = 1$	שלב $k = 3$:
$q_4 = 63$	$t_5 = 2 - 63 \cdot (-3) = 191$	$s_5 = -1 - 63 \cdot (2) = -127$	$r_5 = 63 - 63 \cdot 1 = 0$	שלב $k = 4$:

$$\gcd(a, b) = r_4 = 1, \quad s = s_4 = 2, \quad t = t_4 = -3.$$

$$sa + tb = 2(191) - 3(127) = 1.$$

לכן

$$191^{-1} \equiv 2 \pmod{127}$$

$$127^{-1} \equiv (-3) \pmod{191} \equiv 188 \pmod{191}.$$

שיטה 2

נחשב $y_2 = 127^{-1} \pmod{191}$ ו- $y_1 = 191^{-1} \pmod{127}$ בעזרת האלגוריתם של אוקליד:

$$191 = 127 \cdot 1 + 64$$

$$127 = 64 \cdot 1 + 63$$

$$64 = 63 \cdot 1 + 1$$

$$63 = 1 \cdot 63 + 0.$$

$$\gcd(191, 127) = 1 \text{ לכן}$$

$$\begin{aligned}
 1 &= 64 - 63 \cdot 1 \\
 &= 64 - (127 - 64 \cdot 1) \\
 &= 64 \cdot 2 - 127 \cdot 1 \\
 &= (191 - 127 \cdot 1) \cdot 2 - 127 \\
 &= 191 \cdot 2 + 127 \cdot (-3) .
 \end{aligned}$$

לכן

$$\begin{aligned}
 y_1 &= M_1^{-1} \mod m_1 = 127^{-1} \mod 191 \equiv 188 \mod 191 \\
 y_2 &= M_2^{-1} \mod m_2 = 191^{-1} \mod 127 \equiv 2 \mod 127 .
 \end{aligned}$$

נחשב

$$y_1 = M_1^{-1} \mod m_1 = 127^{-1} \mod 191 = 188, \quad y_2 = M_2^{-1} \mod m_2 = 191^{-1} \mod 127 = 2 .$$

לכן

$$\begin{aligned}
 y &= a_1 M_1 y_1 + a_2 M_2 y_2 \\
 &= 55(191)(2) + 176(127)(188) \mod 24257 \\
 &= 4223186 \mod 24257 \\
 &= 2468 .
 \end{aligned}$$

משפט 5.13

יהיו p, q מספרים ראשוניים ויהי $n = pq$. יהי

$$\lambda(n) = \frac{(p-1)(q-1)}{\gcd(p-1, q-1)} .$$

נגדיר צופן חדש אשר זהה ל-RSA אלא $\phi(n)$ הוחלף עם $\lambda(n)$ כך ש- $ab \equiv 1 \mod \lambda(n)$. אזי הקריפטו-מערכת ניתן לפענח.

הוכחה:

(שלב 1) רושמים את הצופן:

$$\left. \begin{aligned} e_k(x) &= x^b \mod n \\ d_k(y) &= y^a \mod n \end{aligned} \right\} \quad n = pq, \quad ab \equiv 1 \mod \lambda(n) .$$

(שלב 2) נתון כי $d = \gcd(p-1, q-1)$. ז"א שקיים p' שלם כך ש-

$$p-1 = p'd \Leftrightarrow \frac{p-1}{d} = p' \Leftrightarrow d = \frac{p-1}{p'} . \quad (\#1)$$

באותה מידה קיים q' שלם כך ש-

$$q-1 = q'd \Leftrightarrow \frac{q-1}{d} = q' \Leftrightarrow d = \frac{q-1}{q'} . \quad (\#2)$$

(שלב 3)

$$\lambda(n) = \frac{(p-1)(q-1)}{\gcd(p-1, q-1)} = \frac{(p-1)(q-1)}{d} .$$

$$\lambda(n) \stackrel{(\#1)}{=} \frac{(p-1)(q-1)}{\left(\frac{p-1}{p'}\right)} = p'(q-1) . \quad \Leftrightarrow \quad d = \frac{p-1}{p'} . \quad (1*)$$

$$\lambda(n) \stackrel{(\#2)}{=} \frac{(p-1)(q-1)}{\left(\frac{q-1}{q'}\right)} = q'(p-1) . \quad \Leftrightarrow \quad d = \frac{p-1}{p'} . \quad (2*)$$

שלב 4 $ab \equiv 1 \pmod{\lambda(n)}$ (נתון) לכן קיים t שלם כך ש-

$$ab = 1 + t\lambda(n) \stackrel{(2*)}{=} 1 + t(p-1)q' .$$

לכן

$$ab - 1 = t(p-1)q' .$$

מכאן

$$x^{ab-1} x^{tq'(p-1)} = y^{p-1} \stackrel{\text{פרמה}}{\equiv} 1 \pmod{p}$$

כאשר $y = x^{tq'}$ והשוויון השני מתקיים בגלל ש- p מספר ראשוני. לפיכך

$$x^{ab-1} \equiv 1 \pmod{p} .$$

שלב 5 $ab \equiv 1 \pmod{\lambda(n)}$ (נתון) לכן קיים t שלם כך ש-

$$ab = 1 + t\lambda(n) \stackrel{(1*)}{=} 1 + t(q-1)p' .$$

לכן

$$ab - 1 = t(q-1)p' .$$

מכאן

$$x^{ab-1} x^{tp'(q-1)} = z^{q-1} \stackrel{\text{פרמה}}{\equiv} 1 \pmod{q}$$

כאשר $z = x^{tp'}$ והשוויון השני מתקיים בגלל ש- q מספר ראשוני. לפיכך

$$x^{ab-1} \equiv 1 \pmod{q} .$$

שלב 6 מכיוון ש- p, q ראשוניים אז

$$\left. \begin{array}{l} x^{ab-1} \equiv 1 \pmod{q} \\ x^{ab-1} \equiv 1 \pmod{p} \end{array} \right\} \Rightarrow x^{ab-1} \equiv 1 \pmod{pq}$$

לפיכך

$$x^{ab-1} \equiv 1 \pmod{n} \Rightarrow (x^b)^a \equiv x \pmod{n}$$

כנדרש.



שיעור 6

קריפטו-אנליזה

6.1 סוגים של התקפת סייבר

נניח שאליס שולחת הודעה מוצפנת לבוב. ויש גורם עוין, אוסקר, שמנסה לצותת לשיחתם. אנחנו מניחים כי אוסקר מודע לקריפטו-מערכת (הצופן) שבאמצעותה אליס הצפינה את ההודעה. ההנחה הזאת נקראת עקרון קירשוף *Kercheoff's principle*.

המטרה בהרכבת צופן היא שהצופן מספיק בטוח כך שאוסקר לא יכול לפענח אפילו אם הוא יודע את הסוג של הצופן בשימוש.

ישנם 4 סוגים של התקפת סייבר.

(1) **התקפת טקסט מוצפן בלבד.**

למתקיף (אוסקר) יש מחרוזת של טקסט מוצפן y .

(2) **התקפת טקסט גלוי ידוע**

למתקיף יש מחרוזת של טקסט גלוי x יחד עם הטקסט מוצפן המתאים y .

(3) **התקפת טקסט גלוי נבחר**

למתקיף היכולת להשיג טקסטים גלויים x של טקסטים מוצפנים y כלשהם חפי בחירתו, שהוצפנו באמצעות הקריפטו-מערכת המותקפה.

(4) **התקפת טקסט מוצפן נבחר**

למתקיף היכולת להשיג טקסטים מוצפנים y של טקסטים גלויים x כלשהם חפי בחירתו, שהוצפנו באמצעות הקריפטו-מערכת המותקפה.

החלק הבא מתעסק עם התקפת טקסט מוצפן.

6.2 קבוצות אותיות הנפוצים ביותר בטקסט גלוי

התקפת טקסט מוצפן בלבד מבוסס על ההתדיקויות של אותיות בקטסט גלוי בשפה אנגלית.

כלל 6.1 פונקצית 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

Becker ו- Piper סדרו את האותיות לחמש קבוצות שונות, לפי הסדר גודל של התדירות של האותיות בטקסט גלוי.

כלל 6.2 קבוצות תדירות של אותיות בטקסט גלוי

	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 6.3 זוגות אותיות הנפוצים ביותר בטקסט גלוי

השלושים זוגות אותיות הנפוצים ביותר בטקסט גלוי 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 6.4 קבוצות שלשת אותיות הנפוצים ביותר בטקסט גלוי

ה-12 שלשות של אותיות הנפוצים ביותר בטקסט גלוי רשומים בטבלה למטה:

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

6.3 קריפטו-אנליזה של צופן האפיני

זו דוגמה של התקפת טקסט מוצפן בלבד.

6.1 דוגמה

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

KARSRROHVUKARPF^SZFERXERFKREKAF^SKARSRROHVUKARURTVEKARVSR

אוסקר יודע כי אליס הצפינה את ההודעה באמצעות צופן איפיני אבל הוא לא יודע את המפתח. כעת הוא מנסה לפענח אותה. מצאו את הטקסט גלוי.

פתרון:

שלב 1 נרשום את התדירויות 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 $k = (a, b)$ של הכלל מצפין של הצופן אפיני

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

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

- נניח כי

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

- ז"א

$$e_k(4) = 17$$

$$e_k(19) = 10 .$$

- נציב $e_k = ax + b$ ונקבל

$$4a + b = 17 ,$$

$$19a + b = 10 .$$

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

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

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

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

$$a = 3, b = 5$$

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

• נבנה את הכלל מפענח עם המפתח המתקבל:

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

שלב 4 ננסה לפענח את הטקסט מצפון עם הכלל מפענח

$y \in C$	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 6.2

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

FMXVEDKAPHFERBNDKRXRSREFMORUDSDKDVSHVUFEDKAPRKDLYEVLRRHHRH

אוסקר יודע כי אליס השתמשה בצופן איפניי אבל אינו יודע את המפתח. כעת הוא מנסה לפענח אותה. מצאו את הטקסט גלוי.

פתרון:

שלב 1 נרשום את התדירויות 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 $k = (a, b)$ של הכלל מצפין של הצופן אפיני

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

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

- נניח כי

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

- ז"א

$$e_k(4) = 17$$

$$e_k(19) = 3.$$

- נציב $e_k = ax + b$ ונקבל

$$4a + b = 17,$$

$$19a + b = 3.$$

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

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

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

ז"א $a = 6, b = 19$ המפתח הזה לא תקין בגלל ש- $\gcd(a, 26) = 2 \neq 1$.

- עכשיו נחזור וננסה

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

- ז"א

$$e_k(4) = 17$$

$$e_k(19) = 4.$$

• נציב $e_k = ax + b$ ונקבל

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

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

$$\begin{aligned} \left(\begin{array}{cc|c} 4 & 1 & 17 \\ 19 & 1 & 4 \end{array} \right) &\xrightarrow{R_2 \rightarrow R_2 - R_1} \left(\begin{array}{cc|c} 4 & 1 & 17 \\ 15 & 0 & -13 \end{array} \right) = \left(\begin{array}{cc|c} 4 & 1 & 17 \\ 15 & 0 & 13 \end{array} \right) \xrightarrow{R_2 \rightarrow 15^{-1}R_2 = 7R_2} \left(\begin{array}{cc|c} 4 & 1 & 17 \\ 1 & 0 & 91 \end{array} \right) = \left(\begin{array}{cc|c} 4 & 1 & 17 \\ 1 & 0 & 13 \end{array} \right) \\ &\xrightarrow{R_1 \rightarrow R_1 - 4R_2} \left(\begin{array}{cc|c} 0 & 1 & -35 \\ 1 & 0 & 13 \end{array} \right) = \left(\begin{array}{cc|c} 0 & 1 & 17 \\ 1 & 0 & 13 \end{array} \right) \end{aligned}$$

ז"א $a = 13, b = 17$ המפתח הזה גם לא תקין בגלל ש- $\gcd(a, 26) = 2 \neq 1$.

עכשיו נחזור וננסה

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

• ז"א

$$\begin{aligned} e_k(4) &= 17 \\ e_k(19) &= 7. \end{aligned}$$

• נציב $e_k = ax + b$ ונקבל

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

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

$$\begin{aligned} \left(\begin{array}{cc|c} 4 & 1 & 17 \\ 19 & 1 & 7 \end{array} \right) &\xrightarrow{R_2 \rightarrow R_2 - R_1} \left(\begin{array}{cc|c} 4 & 1 & 17 \\ 15 & 0 & -10 \end{array} \right) = \left(\begin{array}{cc|c} 4 & 1 & 17 \\ 15 & 0 & 16 \end{array} \right) \xrightarrow{R_2 \rightarrow 15^{-1}R_2 = 7R_2} \left(\begin{array}{cc|c} 4 & 1 & 17 \\ 1 & 0 & 112 \end{array} \right) = \left(\begin{array}{cc|c} 4 & 1 & 17 \\ 1 & 0 & 8 \end{array} \right) \\ &\xrightarrow{R_1 \rightarrow R_1 - 4R_2} \left(\begin{array}{cc|c} 0 & 1 & -15 \\ 1 & 0 & 8 \end{array} \right) = \left(\begin{array}{cc|c} 0 & 1 & 11 \\ 1 & 0 & 13 \end{array} \right) \end{aligned}$$

ז"א $a = 8, b = 11$ המפתח הזה גם לא תקין בגלל ש- $\gcd(a, 26) = 2 \neq 1$.

עכשיו נחזור וננסה

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

• ז"א

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

• נציב $e_k = ax + b$ ונקבל

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

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

$$\begin{aligned} \left(\begin{array}{cc|c} 4 & 1 & 17 \\ 19 & 1 & 10 \end{array} \right) &\xrightarrow{R_2 \rightarrow R_2 - R_1} \left(\begin{array}{cc|c} 4 & 1 & 17 \\ 15 & 0 & -7 \end{array} \right) = \left(\begin{array}{cc|c} 4 & 1 & 17 \\ 15 & 0 & 19 \end{array} \right) \xrightarrow{R_2 \rightarrow 15^{-1}R_2 = 7R_2} \left(\begin{array}{cc|c} 4 & 1 & 17 \\ 1 & 0 & 133 \end{array} \right) = \left(\begin{array}{cc|c} 4 & 1 & 17 \\ 1 & 0 & 3 \end{array} \right) \\ &\xrightarrow{R_1 \rightarrow R_1 - 4R_2} \left(\begin{array}{cc|c} 0 & 1 & 5 \\ 1 & 0 & 3 \end{array} \right) \end{aligned}$$

ז"א $a = 3, b = 5$.

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

• נבנה את הכלל מפענח עם המפתח המתקבל:

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

שלב 4 ננסה לפענח את הטקסט מציפון עם הכלל מפענח

$y \in C$	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

■

6.4 קריפטו-אנליזה של צופן היל

זו דוגמה של התקפת טקסט גלוי ידוע.

משפט 6.1

נניח שלמתקין יש מחרוזת טקסט גלוי x ומחרוזת טקסט מוצפן שלו. נניח כי המתקין יודע כי הטקסט הוצפן באמצעות צופן היל עם מפתח של סדר m .

נניח שיש למתקין לפחות m טקסטים גלויים וטקסטים מוצפנים. של הטקסט גלוי:

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

-1

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

$1 \leq j \leq m$ כך ש-

$$y_j = e_k(x_j).$$

נגדיר שתי מטריצות

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

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 6.3

נתון הטקסט גלוי

friday

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

PQCFKU

מצאו את המפתח של הצופן.

פתרון:

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

ז"א

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

נקח את שני טקסטים גלויים וטקסטים מוצפנים המתאימים נגדיר את המטריצות

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

אזי

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

נחשב את ההופכית X^{-1} באמצעות נוסחת קיילי $X^{-1} = |X|^{-1} \text{adj}(X)$.

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

לכן

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

המטריצת 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

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

לבסוף נקבל

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

לפיכך

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

■

דוגמה 6.4

נתון הטקסט גלוי

theresnoplacelikehome

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

FHVTUTGQVRWPCPSFGGAMG

מצאו את המפתח של הצופן.

פתרון:

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

ז"א

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

נקח את שני טקסטים גלויים וטקסטים מוצפנים המתאימו נגדיר את המטריצות

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

אזי

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

נחשב את ההופכית X^{-1} באמצעות נוסחת קיילי $X^{-1} = |X|^{-1} \text{adj}(X)$.

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

לכן

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

המטריצת הקופקטורים של X היא

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

לכן

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

לבסוף נקבל

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

לפיכך

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

■

6.5 מדד צירוף המקרים

הגדרה 6.1 מדד צירוף המקרים I_c

נתון מחרוזת של טקסט גלוי $x = x_1x_2 \cdots x_n$ של אורך n .

המדד צירוף המקרים של x מסומן $I_c(x)$ ומוגדר להיות ההסתברות ששתי אותיות הנבחרות באקראי מתוך x יהיו זהות.

משפט 6.2 נוסחה לחישוב המדד צירוף המקרים

נתון מחרוזת של טקסט גלוי $x = x_1x_2 \cdots x_n$ של אורך n .
יהי f_k מספר הפעמים שהאות מספר k באלפבית מופיעה במחרוזת x . למשל, f_0 מסמן את מספר הפעמים שהאות a מופיעה, f_1 מסמן את מספר הפעמים שהאות b מופיעה, וכן הלאה.

מספר הדרכים לבחור שתי אותיות מתוך 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 מתוך x .

המדד צירוף המקרים של הטקסט גלוי 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 6.3 מדד צירוף המקרים בטקסט גלוי

נניח כי $x = x_1 x_2 \dots x_n$ 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

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

6.6 קריפטו-אנליזה של צופן ויז'נר - מבחן פרידמן

דוגמה 6.5

נתון הטקסט מוצפן

MOKSMNXBIUCMQXGCAXOFXMUWLNRRNSFMIQBHNCF CGDTAHANTTIJNIERGCHURYHOGGSWTMP
CCOYISKOGXLQAFMVXNFEDAEMHQTNAAQXUDIXXRSILCIZKGWEFLAWGUJAOAUPLXRQTGATPS
MKLQSWRGTXJNPXEUNSYIACRGWLQEIMDUBQQGAEEYULEEWXDLIIDUHQOFXWEAZJTUOFXWKS
MTNAAFXTTMFPMUWLNRRNSFMOBIIJTUSFPRMRVBLMQXXRURKCAZGWCWAAGADECGDMMMCZJVQS
NNRTISADILALHOEFWOF TGBSUF DHMZWNK WAPNUJALAZGWCOKSMXRMRQXNQMFHOGVGAGMR
AIAFMGWC MRQXUMJXXRPXGCAWILQAFGZJNOIQXUMVWZUUXWAISLLVIE XWABARVHOG E JNWAV
LQMAVWCOYISUIHIK

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

פתרון:

שלב 1: נפרק את הטקסט לעמודות של 3 אותיות

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	...
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	...
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	...
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	...
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: נחשב את המדד המשותף של כל שורה

יהיו f_i התדירויות של האותיות במחרוזת Y_i ונניח כי האורך של Y_i הוא n . אזי הפונקציות הסתברות של האותיות ב- Y_i הן

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

כל רצף אותיות Y_i מתקבל על ידי הזזה קבועה של k_i מקומות של הטקסט גלוי. לפי זה, הפונקציות הסתברות של האותיות המוזזות,

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

תהיו קרובות להסתברויות p_0, \dots, p_{25} של אותיות בטקסט גלוי. כעת נגדיר את המדד המשותף

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

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

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

על פי זה נבדוק את המדד המשותף לכל Y_i ולכל $0 \leq g \leq 25$:

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				

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				

Y₃

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				

Y₄

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				

Y₅

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				

ננסה לפענח את הטקסט מוצפן עם המפתח

JAMES

ונקבל את התשובה

doyouexpectmetotalknomisterbondiexpectyoutodiethereisnothingyoucantalk
 tomeaboutthatidontalreadyknowyoureforgettingonethingififailtoreportdou
 bleoeightreplacesmeitrusthewilllbemoresuccessfulwellheknowswhatiknowyou
 knownothingmisterbondoperationgrandslamforinstancetwowordsyoumayhaveov
 erheardwhichcannotpossiblyhaveanysignificancetoyouoranyoneinyourorgani
 zationcanyouaffordtotakethatchanceyouarequiterightmisterbondyouarewort
 hmoretomealives

עם רווחים 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 def P(a):
24     i = alphabetLower.index(a)
25     return probabilities[i]
26
27 cipherText = "
28     MOKSMNXBIUCMQXGCAXOFXMUWLNRRNSFMIQBHNCFGDTAHANTTIJNIERGCHURYHOGGSWTMPCCOYISKOGXLQAFMVXNFEDAE
29     "
30
31 cipherTextList = list(cipherText)
32
33 y= [None]*5
34 for i in range(0,6):
35     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)
```



שיעור 7

סודיות מושלמת

7.1 סודיות מושלמת

נתונה קריפטו-מערכת

$$(X, Y, K, E, D)$$

כאשר X הקבוצה של כל טקסטים גלויים האפשריים, Y הקבוצה של כל טקסטים מוצפנים האפשריים, K הקבוצה של כל המפתחות האפשריים, E הקבוצה של כל כללי מצפין האפשריים ו- D הקבוצה של כל כללי מפענח האפשריים.

אנחנו נתייחס לטקסטים גלויים

$$X = \{x_1, x_2, \dots, x_n\}$$

כמשתנה מקרי (מ"מ) בדיד, אשר ערכו שווה לתוצאה של בחירת טקסט גלוי. כמו כן נתייחס למפתחות

$$K = \{k_1, k_2, \dots, k_m\}$$

כמשתנה מקרי בדיד אשר ערכו שווה למפתח הנבחר.

נסמן את הפונקציית הסתברות של הטקסט גלוי ב-

$$P_X(x_i) = P(X = x_i) .$$

כלומר $P(X = x_i)$ מסמן את ההסתברות לבחור את הטקסט גלוי x מתוך X .
נסמן את הפונקציית הסתברות של המפתחות ב-

$$P_K(k_i) = P(K = k_i) .$$

כלומר $P(K = k_i)$ הוא ההסתברות לבחור את המפתח k_i מתוך K .

הטקסט מוצפן $Y = y$ המתקבל באמצעות הטקסט גלוי $X = x$ הנבחר והמפתח $K = k$ הנבחר הוא גם משתנה מקרי בדיד שמוגדר

$$Y(k) = \{e_k(x) \mid x \in X\} .$$

ז"א $Y(k)$ מייצג את קבוצת כל הטקסטעם המוצפנים האפשריים המתקבלים על ידי המפתח $k \in K$.
לפיכך, ההסתברות ש- $Y = y$ כאשר y מתקבל על ידי להצפין הטקסט גלוי x באמצעות המפתח k היא

$$P(Y = y) = \sum_{k \in K} P(K = k) P(X = d_k(y)) . \quad (7.1)$$

ההסתברות מותנית $P(Y = y \mid X = x)$, כלומר ההסתברות לקבל הטקסט מוצפן y בידיעה כי הטקסט גלוי הוא x , היא בדיוק ההסתברות לבחור מפתח מסוים k אשר באמצעותו מקבלים y על ידי להצפין x עם המפתח זה k .

$$P(Y = y \mid X = x) = \sum_{\substack{k \in K \\ x = d_k(y)}} P(K = k) . \quad (7.2)$$

מכאן, לפי נוסחת בייס, $P(X = x|Y = y) = \frac{P(Y = y|X = x)P(X = x)}{P(Y = y)}$, נציב את משוואת (7.1) ומשוואות (7.2) ונקבל את הביטוי

$$P(X = x|Y = y) = \frac{P(X = x) \sum_{\substack{k \in K \\ x=d_k(y)}} P(K = k)}{\sum_{k \in K} P(K = k)P(X = d_k(y))} . \quad (7.3)$$

דוגמה 7.1

נתונה קבוצת טקסט גלוי $X = \{a, b\}$ עם פונקצית הסתברות

$$P(X = a) = \frac{1}{4} , \quad P(X = b) = \frac{3}{4} ,$$

נתונה קבוצת מפתחות $K = \{k_1, k_2, k_3\}$ עם פונקצית הסתברות

$$P(K = k_1) = \frac{1}{2} , \quad P(K = k_2) = P(K = k_3) = \frac{1}{4} .$$

ונתונה קבוצת טקסט מוצפן

$$Y = \{1, 2, 3, 4\} .$$

נניח כי הכלל מצפין מוגדר כך ש-

$$e_{k_1}(a) = 1 , \quad e_{k_1}(b) = 2 , \quad e_{k_2}(a) = 2 , \quad e_{k_2}(b) = 3 , \quad e_{k_3}(a) = 3 , \quad e_{k_3}(b) = 4 .$$

מצאו את $P(X = x|Y = y)$ לכל $x \in X$ ולכל $y \in Y$.

פתרון:

אפשר לייצג את הקריפטו-מערכת כמטריצת הצפנה:

$X \backslash K$	a	b
k_1	1	2
k_2	2	3
k_3	3	4

נחשב את הפונקציה ההסתברות של Y :

$$\begin{aligned} P(Y = 1) &= P(K = k_1)P(X = d_{k_1}(1)) + P(K = k_2)P(X = d_{k_2}(1)) + P(K = k_3)P(X = d_{k_3}(1)) \\ &= P(K = k_1)P(X = a) + P(K = k_2)P(X = \emptyset) + P(K = k_3)P(X = \emptyset) \\ &= \frac{1}{2} \cdot \frac{1}{4} + 0 + 0 \\ &= \frac{1}{8} . \end{aligned}$$

$$\begin{aligned}
P(Y = 2) &= P(K = k_1)P(X = d_{k_1}(2)) + P(K = k_2)P(X = d_{k_2}(2)) + P(K = k_3)P(X = d_{k_3}(2)) \\
&= P(K = k_1)P(X = b) + P(K = k_2)P(X = a) + P(K = k_3) \cdot P(X = \emptyset) \\
&= \frac{1}{2} \cdot \frac{3}{4} + \frac{1}{4} \cdot \frac{1}{4} \\
&= \frac{7}{16} .
\end{aligned}$$

$$\begin{aligned}
P(Y = 3) &= P(K = k_1)P(X = d_{k_1}(3)) + P(K = k_2)P(X = d_{k_2}(3)) + P(K = k_3)P(X = d_{k_3}(3)) \\
&= P(K = k_1) \cdot P(X = \emptyset) + P(K = k_2)P(X = b) + P(K = k_3) \cdot P(X = a) \\
&= \frac{1}{4} \cdot \frac{3}{4} + \frac{1}{4} \cdot \frac{1}{4} \\
&= \frac{1}{4} .
\end{aligned}$$

$$\begin{aligned}
P(Y = 4) &= P(K = k_1)P(X = d_{k_1}(4)) + P(K = k_2)P(X = d_{k_2}(4)) + P(K = k_3)P(X = d_{k_3}(4)) \\
&= P(K = k_1) \cdot P(X = \emptyset) + P(K = k_2) \cdot P(X = \emptyset) + P(K = k_3) \cdot P(X = b) \\
&= \frac{1}{4} \cdot \frac{3}{4} \\
&= \frac{3}{16} .
\end{aligned}$$

$$\begin{aligned}
P(X = a|Y = 1) &= \frac{P(Y = 1|X = a)P(X = a)}{P(Y = 1)} \\
&= \frac{P(Y = 1|X = a) \left(\frac{1}{4}\right)}{\left(\frac{1}{8}\right)} \\
&= 2 \sum_{\substack{k \in K \\ a = d_k(1)}} P(K = k) \\
&= 2P(K = k_1) \\
&= 1 .
\end{aligned}$$

$$\begin{aligned}
P(X = b|Y = 1) &= \frac{P(Y = 1|X = b)P(X = b)}{P(Y = 1)} \\
&= \frac{P(Y = 1|X = b) \left(\frac{3}{4}\right)}{\left(\frac{1}{8}\right)} \\
&= 6 \sum_{\substack{k \in K \\ b = d_k(1)}} P(K = k) \\
&= 6 \cdot 0 \\
&= 0 .
\end{aligned}$$

$$\begin{aligned}
 P(X = a|Y = 2) &= \frac{P(Y = 2|X = a)P(X = a)}{P(Y = 2)} \\
 &= \frac{P(Y = 2|X = a) \left(\frac{1}{4}\right)}{\left(\frac{7}{16}\right)} \\
 &= \frac{4}{7} \sum_{\substack{k \in K \\ a=d_k(2)}} P(K = k) \\
 &= \frac{4}{7} P(K = k_2) \\
 &= \frac{1}{7} .
 \end{aligned}$$

$$\begin{aligned}
 P(X = b|Y = 2) &= \frac{P(Y = 2|X = b)P(X = b)}{P(Y = 2)} \\
 &= \frac{P(Y = 2|X = b) \left(\frac{3}{4}\right)}{\left(\frac{7}{16}\right)} \\
 &= \frac{12}{7} \sum_{\substack{k \in K \\ b=d_k(2)}} P(K = k) \\
 &= \frac{12}{7} P(K = k_1) \\
 &= \frac{6}{7} .
 \end{aligned}$$

$$\begin{aligned}
 P(X = a|Y = 3) &= \frac{P(Y = 3|X = a)P(X = a)}{P(Y = 3)} \\
 &= \frac{P(Y = 3|X = a) \left(\frac{1}{4}\right)}{\left(\frac{1}{4}\right)} \\
 &= \sum_{\substack{k \in K \\ a=d_k(3)}} P(K = k) \\
 &= P(K = k_3) \\
 &= \frac{1}{4} .
 \end{aligned}$$

$$\begin{aligned}
 P(X = b|Y = 3) &= \frac{P(Y = 3|X = b)P(X = b)}{P(Y = 3)} \\
 &= \frac{P(Y = 3|X = b) \left(\frac{3}{4}\right)}{\left(\frac{1}{4}\right)} \\
 &= 3 \sum_{\substack{k \in K \\ b=d_k(3)}} P(K = k) \\
 &= 3P(K = k_2) \\
 &= \frac{3}{4} .
 \end{aligned}$$

$$\begin{aligned}
 P(X = a|Y = 4) &= \frac{P(Y = 4|X = a)P(X = a)}{P(Y = 4)} \\
 &= \frac{P(Y = 4|X = a) \left(\frac{1}{4}\right)}{\left(\frac{3}{16}\right)} \\
 &= \frac{4}{3} \sum_{\substack{k \in K \\ a=d_k(4)}} P(K = k) \\
 &= \frac{4}{3} \cdot 0 \\
 &= 0 .
 \end{aligned}$$

$$\begin{aligned}
 P(X = b|Y = 4) &= \frac{P(Y = 4|X = b)P(X = b)}{P(Y = 4)} \\
 &= \frac{P(Y = 4|X = b) \left(\frac{3}{4}\right)}{\left(\frac{3}{16}\right)} \\
 &= 4 \sum_{\substack{k \in K \\ b=d_k(4)}} P(K = k) \\
 &= 4P(K = k_3) \\
 &= \frac{1}{4} \\
 &= 1 .
 \end{aligned}$$

■

דוגמה 7.2 (משך של דוגמה 7.1)

$$\begin{aligned}
 H(X) &= -P(X = a) \log_2 P(X = a) - P(X = b) \log_2 P(X = b) \\
 &= -\frac{1}{4} \log_2 \left(\frac{1}{4}\right) - \frac{3}{4} \log_2 \left(\frac{3}{4}\right) \\
 &= -\frac{1}{4} (-2) - \frac{3}{4} (\log_2 3 - \log_2 4) \\
 &= \frac{1}{2} - \frac{3}{4} \log_2 3 + \frac{6}{4} \\
 &= 2 - \frac{3}{4} \log_2 3 \\
 &\approx 0.81 .
 \end{aligned}$$

$$\begin{aligned}
 H(K) &= -P(K = k_1) \log_2 P(K = k_1) - P(K = k_2) \log_2 P(K = k_2) - P(K = k_3) \log_2 P(K = k_3) \\
 &= -\frac{1}{2} \log_2 \left(\frac{1}{2}\right) - \frac{1}{4} \log_2 \left(\frac{1}{4}\right) - \frac{1}{4} \log_2 \left(\frac{1}{4}\right) \\
 &= -\frac{1}{2} (-1) - \frac{1}{4} (-2) - \frac{1}{4} (-2) \\
 &= 1 + \frac{1}{2} + \frac{1}{2} \\
 &= \frac{3}{2} .
 \end{aligned}$$

$$\begin{aligned}
 H(Y) &= -P(Y=1) \log_2 P(Y=1) - P(Y=2) \log_2 P(Y=2) - P(Y=3) \log_2 P(Y=3) \\
 &\quad - P(Y=4) \log_2 P(Y=4) \\
 &= -\frac{1}{8} \log_2 \left(\frac{1}{8}\right) - \frac{7}{16} \log_2 \left(\frac{7}{16}\right) - \frac{1}{4} \log_2 \left(\frac{1}{4}\right) - \frac{3}{16} \log_2 \left(\frac{3}{16}\right) \\
 &= \frac{27}{8} - \frac{7}{16} \log_2 7 - \frac{3}{16} \log_2 3 \\
 &\approx 1.85.
 \end{aligned}$$

הגדרה 7.1 סודיות מושלמת

אומרים כי לקריפטו-מערכת יש סודיות מושלמת אם

$$P(X = x | Y = y) = P(X = x)$$

לכל $y \in Y, x \in X$.

ז"א ההסתברות כי הטקסט גלוי $X = x$, בידיעה כי הטקסט מוצפן $Y = y$ שווה רק להסתברות כי הטקסט גלוי הוא $X = x$ והבחירה של המפתח שבאמצעותו מתקבל הטקסט מוצפן y לא משפיע על ההסתברות כי הטקסט גלוי $X = x$.

משפט 7.1 תנאי לסודיות מושלמת של צופן קיסר

אם לכל מפתח $k \in K$ בצופן קיסר יש הסתברות שווה, כלומר

$$P(K = k) = \frac{1}{26}.$$

אז לצופן קיסר יש סודיות מושלמת.

הוכחה: תחילה נחשב את ההסתברות $P(Y = y)$ באמצעות (7.1). הקבוצת מפתחות בצופן קיסר היא

$$K = \{0, 1, \dots, 25\} = \mathbb{Z}_{26}.$$

לכן

$$P(Y = y) = \sum_{k \in \mathbb{Z}_{26}} P(K = k) P(X = d_k(y)).$$

אם ההסתברות של כל מפתח שווה אז $P(K = k) = \frac{1}{26}$ ולכן

$$P(Y = y) = \frac{1}{26} \sum_{k \in \mathbb{Z}_{26}} P(X = d_k(y)).$$

הכלל מצפין והכלל מפענח של צופן קיסר מוגדרים

$$e_k(x) = x + k \mod 26, \quad d_k(y) = y - k \mod 26.$$

כאשר $k \in \mathbb{Z}_{26}$. לכן $P(X = d_k(y)) = P(X = y - k \mod 26)$. לפיכך

$$P(Y = y) = \frac{1}{26} \sum_{k \in \mathbb{Z}_{26}} P(X = y - k \mod 26).$$

הסכום בצד הימין הוא רק סכום של $P(X = k)$ מעל כל האיברים k ב- \mathbb{Z}_{26} . לכן

$$P(Y = y) = \frac{1}{26} \sum_{k \in \mathbb{Z}_{26}} P(X = k) = \frac{1}{26} \cdot 1 = \frac{1}{26}.$$

כאשר בשוויון השני השתמשנו בתכונת הנרמול של הפונקציה הסתברות של המ"מ X .

מצד שני, לפי (7.2),

$$P(Y = y|X = x) = \sum_{\substack{k \in \mathbb{Z}_{26} \\ x = d_k(y)}} P(K = k)$$

האילוץ על הסכום $x = d_k(y)$ אומר ש-

$$x = k - y \pmod{26} \quad \Rightarrow \quad k = x + y \pmod{26}.$$

לכל $x \in X$ ולכל $y \in Y$ קיים רק מפתח אחד אשר מקיים תנאי זה. ז"א רק איבר אחד של הסכום נשאר ולפיכך

$$P(Y = y|X = x) = \sum_{\substack{k \in \mathbb{Z}_{26} \\ x = d_k(y)}} P(K = k) = P(K = y - x \pmod{26}).$$

אם ההסתברות של כל מפתח שווה, כלומר אם $P_K(k) = \frac{1}{26}$ לכל $k \in K$, אז

$$P(Y = y|X = x) = P(K = y - x \pmod{26}) = \frac{1}{26}.$$

לכן

$$P(Y = y) = \frac{1}{26} = P(Y = y|X = x)$$

ז"א לצופן קיסר יש סודיות מושלמת.

במילים פשוטות צופן קיסר אינו ניתן לפענח בתנאי שמשתמשים במפתח מקרי חדש כל פעם שמצפינים אות אחד של טקסט גלוי.

למה 7.1 תנאי חילופי לסודיות מושלמת

לפי נוסחת בייס אם לקריפטו-מערכת יש סודיות מושלמת אז מתקיים גם

$$P(Y = y|X = x) = P(Y = y). \quad (7.4)$$

למה 7.2

נתונה קריפטו-מערכת בעלת סודיות מושלמת.

אם $P(Y = y) > 0$ אז

(1) קיים לפחות מפתח אחד $k \in K$ כך ש- $e_k(x) = y$

(2) $|K| \geq |Y|$.

(1) לפי 7.4,

$$P(Y = y|X = x) = P(Y = y) > 0 \quad (\#1)$$

נציב (7.2) בצד שמאל ונקבל

$$\sum_{\substack{k \in K \\ x=d_k(y)}} P(K = k) = P(Y = y) > 0 \quad (\#2)$$

ז"א

$$\sum_{\substack{k \in K \\ x=d_k(y)}} P(K = k) > 0 \quad (\#3)$$

לכן קיים לפחות מפתח אחד, k עבורו $x = d_k(y)$.

ז"א קיים לפחות מפתח אחד, k עבורו $y = e_k(x)$.

(2) לפי (#1) ו- (#3), לכל $y \in Y$ קיים לפחות מפתח אחד, k עבורו $y = e_k(x)$, לכן בהכרח

$$|K| \geq |Y|. \quad (\#4)$$

משפט 7.2 משפט שאנון

נתונה קריפטו-מערכת (X, Y, K, E, D) כך ש- $|K| = |X| = |Y|$. למערכת יש סודיות מושלמת אם ורק אם

(1) לכל $x \in X$ ולכל $y \in Y$ קיים מפתח k יחיד עבורו $y = e_k(x)$.

(2) לכל מפתח יש הסתברות שווה, כלומר $P(K = k) = \frac{1}{|K|}$.

הוכחה:

(1) נניח כי $|Y| = |K|$. כלומר

$$|\{e_k(x) | x \in X\}| = |K|.$$

ז"א לא קיימים שני מפתחות $k_1 \neq k_2$ כך ש- $e_{k_1}(x) = y = e_{k_2}(x)$.

לכן לכל $x \in X$ ולכל $y \in Y$ קיים מפתח k יחיד עבורו $e_k(x) = y$.

(2) נסמן אורך של קבוצת מפתחות ב- $n = |K|$. נרשום את הקבוצת טקסטים גלויים כ-

$$X = \{x_i | 1 \leq i \leq n\}.$$

נתון $y \in Y$ קבוע. נמספר את המפתחות כ- k_1, k_2, \dots, k_n כך ש- $e_{k_i}(x_i) = y$. לפי נוסחת בייס,

$$P(X = x_i | Y = y) = \frac{P(Y = y | X = x_i) P(X = x_i)}{P(Y = y)} \\ \stackrel{(7.2)}{=} \frac{P(K = k_i) P(X = x_i)}{P(Y = y)}$$

אם למערכת יש סודיות מושלמת אז $P(X = x_i | Y = y) = P(X = x_i)$ לכן

$$P(X = x_i) = \frac{P(K = k_i)P(X = x_i)}{P(Y = y)} \Rightarrow P(K = k_i) = P(Y = y)$$

לכל $1 \leq i \leq n$. ז"א לכל מפתח יש הסתברות שווה

$$P(K = k_i) = \frac{1}{|K|}.$$

הגדרה 7.2 צופן חד פעמי

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

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

ונגדיר כלל מפענח

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

דוגמה 7.3

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.

7.2 תכונות של אנטרופיה

הגדרה 7.3 פונקציה קעורה

פונקציה ממשית $f(x)$ נקראת **פונקציה קעורה** בתחום I אם

$$f\left(\frac{x_1 + x_2}{2}\right) \geq \frac{f(x_1) + f(x_2)}{2}$$

לכל $x_1, x_2 \in I$

פונקציה ממשית $f(x)$ נקראת **פונקציה קעורה ממש** בתחום I אם

$$f\left(\frac{x_1 + x_2}{2}\right) > \frac{f(x_1) + f(x_2)}{2}$$

לכל $x_1, x_2 \in I$

משפט 7.3 אי-שוויון ינסן

נניח כי f פונקציה רציפה וקעורה ממש בקטע I . נתון מספרים ממשיים $a_i > 0$, $i = 1, \dots, n$ כך ש-
 $\sum_{i=1}^n a_i = 1$ אז

$$\sum_{i=1}^n a_i f(x_i) \leq f\left(\sum_{i=1}^n a_i x_i\right)$$

לכל $x \in I$. אם $x_1 = \dots = x_n$ ורק אם $\sum_{i=1}^n a_i f(x_i) = f\left(\sum_{i=1}^n a_i x_i\right)$

משפט 7.4

יהי

$$X = \{x_1, \dots, x_n\}$$

משתנה מקרי בדיד בעל פונקצית הסתברות

$$P_X(x_1) = p_1, \dots, P_X(x_n) = p_n,$$

אז $0 < p_i \leq 1$ לכל $1 \leq i \leq n$

$$H(X) \leq \log_2 n$$

אם ורק אם

$$p_i = \frac{1}{n}$$

לכל $1 \leq i \leq n$

הוכחה: לפי אי-שוויון ינסן:

$$\begin{aligned} H(X) &= - \sum_{i=1}^n p_i \log_2 p_i \\ &= \sum_{i=1}^n p_i \log_2 \left(\frac{1}{p_i} \right) \\ &\leq \log_2 \left(\sum_{i=1}^n p_i \cdot \frac{1}{p_i} \right) \\ &= \log_2 \left(\sum_{i=1}^n 1 \right) \\ &= \log_2 n . \end{aligned}$$

בנוסף $H(X) = \log_2 n$ אם ורק אם $p_i = \frac{1}{n}$ לכל $1 \leq i \leq n$.

משפט 7.5

יהי $X = \{x_1, \dots, x_m\}$ משתנה מקרי בדיד בעל פונקצית הסתברות

$$P_X(x_1) = p_1, \dots, P_X(x_m) = p_m,$$

ויהי $Y = \{y_1, \dots, y_n\}$ משתנה מקרי בדיד בעל פונקצית הסתברות

$$P_Y(y_1) = q_1, \dots, P_Y(y_n) = q_n,$$

אז $0 < q_i \leq 1$ לכל $1 \leq i \leq n$.

$$H(X, Y) \leq H(X) + H(Y)$$

ו- $H(X, Y) = H(X) + H(Y)$ אם ורק אם X ו- Y בלתי תלויים.

הוכחה: (*להעשרה בלבד)

פונקצית הסתברות של X היא $P_X(x_i) = p_i$ ופונקצית הסתברות של X היא $P_Y(y_i) = q_i$. נגדיר הפונקציות הסתברות של המשתנה מקרי דו-ממדי:

$$r_{ij} = P(X = x_i, Y = y_j) .$$

אז הפונקצית הסתברות שולית של X היא

$$p_i = \sum_{j=1}^n r_{ij}, \quad \forall 1 \leq i \leq m$$

והפונקצית הסתברות שולית של Y היא

$$q_j = \sum_{i=1}^m r_{ij}, \quad \forall 1 \leq j \leq n .$$

מכאן

$$\begin{aligned}
 H(X) + H(Y) &= - \sum_{i=1}^m p_i \log_2 p_i - \sum_{j=1}^n q_j \log_2 q_j \\
 &= - \sum_{i=1}^m \left(\sum_{j=1}^n r_{ij} \right) \log_2 p_i - \sum_{j=1}^n \left(\sum_{i=1}^m r_{ij} \right) \log_2 q_j \\
 &= - \sum_{i=1}^m \sum_{j=1}^n r_{ij} \log_2 p_i - \sum_{j=1}^n \sum_{i=1}^m r_{ij} \log_2 q_j \\
 &= - \sum_{i=1}^m \sum_{j=1}^n r_{ij} (\log_2 p_i + \log_2 q_j) \\
 &= - \sum_{i=1}^m \sum_{j=1}^n r_{ij} \log_2 (p_i q_j) .
 \end{aligned}$$

מצד שני:

$$H(X, Y) = - \sum_{i=1}^m \sum_{j=1}^n r_{ij} \log_2 r_{ij} = \sum_{i=1}^m \sum_{j=1}^n r_{ij} \log_2 \frac{1}{r_{ij}} .$$

לכן

$$\begin{aligned}
 H(X, Y) - H(X) - H(Y) &= \sum_{i=1}^m \sum_{j=1}^n r_{ij} \log_2 \frac{1}{r_{ij}} + \sum_{i=1}^m \sum_{j=1}^n r_{ij} \log_2 (p_i q_j) \\
 &= \sum_{i=1}^m \sum_{j=1}^n r_{ij} \log_2 \left(\frac{p_i q_j}{r_{ij}} \right) \\
 &\leq \log_2 \left(\sum_{i=1}^m \sum_{j=1}^n p_i q_j \right) \quad (\text{אי-שוויון ינסון}) \\
 &= \log_2 1 \\
 &= 0 .
 \end{aligned}$$

לכן

$$H(X, Y) - H(X) - H(Y) \leq 0 \quad \Rightarrow \quad H(X, Y) \leq H(X) + H(Y) .$$

הגדרה 7.4 אנטרופיה מותנית

יהיו X, Y משתנים מקריים בדידים. נגדיר

$$H(X|Y = y) = - \sum_{x \in X} P(X = x|Y = y) \log_2 P(X = x|Y = y) .$$

האנטרופיה מותנית תסומן $H(X|y)$ ותוגדר הממוצע המשוקללת של $H(X|Y = y)$ ביחס להתברויות $P(Y = y)$, כלומר התוחלת של $H(X|Y = y)$:

$$H(X|Y) = - \sum_{y \in Y} \sum_{x \in X} P(Y = y) P(X = x|Y = y) \log_2 P(X = x|Y = y) .$$

האנטרופיה המותנית $H(X|Y)$ מכמתת המידע הממוצע של המ"מ X המועברת אשר לא מוגלה באמצעות Y .

משפט 7.6

$$H(X, Y) = H(Y) + H(X|Y) .$$

הוכחה: (*להעשרה בלבד)

$$\begin{aligned} H(X|Y) &= - \sum_{i=1}^m \sum_{j=1}^n P(Y = y_j) P(X = x_i | Y = y_j) \log_2 P(X = x_i | Y = y_j) \\ &= - \sum_{i=1}^m \sum_{j=1}^n P(X = x_i \cap Y = y_j) \log_2 \frac{P(X = x_i \cap Y = y_j)}{P(Y = y_j)} \\ &= - \sum_{i=1}^m \sum_{j=1}^n r_{ij} \log_2 \frac{r_{ij}}{q_j} . \end{aligned}$$

מצד שני

$$H(Y) = - \sum_{j=1}^n q_j \log_2 q_j = - \sum_{i=1}^m \sum_{j=1}^n r_{ij} \log_2 q_j$$

ו-

$$H(X, Y) = - \sum_{i=1}^m \sum_{j=1}^n r_{ij} \log_2 r_{ij} .$$

לכן

$$\begin{aligned} H(Y) + H(X|Y) &= - \sum_{i=1}^m \sum_{j=1}^n r_{ij} \log_2 \frac{r_{ij}}{q_j} - \sum_{i=1}^m \sum_{j=1}^n r_{ij} \log_2 q_j \\ &= - \sum_{i=1}^m \sum_{j=1}^n r_{ij} \left(\log_2 \frac{r_{ij}}{q_j} + \log_2 q_j \right) \\ &= - \sum_{i=1}^m \sum_{j=1}^n r_{ij} \log_2 \left(\frac{r_{ij}}{q_j} \cdot q_j \right) \\ &= - \sum_{i=1}^m \sum_{j=1}^n r_{ij} \log_2 r_{ij} \\ &= H(X, Y) . \end{aligned}$$

משפט 7.7

$$H(X|Y) \leq H(X)$$

ו- $H(X|Y) = H(X)$ אם ורק אם X ו- Y משתנים מקיים בלתי-תלויים.

הוכחה: (*להעשרה בלבד)

לפי משפט 7.5, $H(X, Y) \leq H(X) + H(Y)$. נציב משפט 7.6 ונקבל

$$H(Y) + H(X|Y) \leq H(X) + H(Y) \quad \Rightarrow \quad H(X|Y) \leq H(X) .$$

בנוסף לפי משפט 7.5, $H(X, Y) = H(X) + H(Y)$ אם ורק אם X, Y משתנים בלתי תלויים, לכן

$$H(X|Y) = H(X)$$

אם ורק אם X, Y משתנים בלתי תלויים.

7.3 צופן מרוכב

הגדרה 7.5 צופן מרוכב

נתון קריפטו-מערכת

$$S_1 = (P, P, K_1, E_1, D_1)$$

וקריפטו-מערכת שניה

$$S_2 = (P, P, K_2, E_2, D_2)$$

הקריפטו-מערכת המורכבת מ- S_1 ו- S_2 מסומנת $S_1 \times S_2$ ומוגדרת להיות הקריפטו-מערכת

$$(P, P, K_1 \times K_2, E, D)$$

מפתח של הקריפטו-מערכת המורכבת $k \in K$,

$$k = (k_1, k_2)$$

כאשר $k_1 \in K_1$ ו- $k_2 \in K_2$. הכלל מצפין של $S_1 \times S_2$ הוא

$$e_{(k_1, k_2)}(x) = e_{k_2}(e_{k_1}(x))$$

והכלל מפענח של $S_1 \times S_2$ הוא

$$d_{(k_1, k_2)}(y) = d_{k_1}(d_{k_2}(y))$$

כלומר, ראשית מצפינים x עם e_{k_1} ואז חוזרים ומצפינים שוב עם e_{k_2} . מבצעים פענוח בסדר הפוך, כלומר

$$\begin{aligned} d_{k_1, k_2}(e_{(k_1, k_2)}(x)) &= d_{k_1, k_2}(e_{k_2}(e_{k_1}(x))) \\ &= d_{k_1}(d_{k_2}(e_{k_2}(e_{k_1}(x)))) \\ &= d_{k_1}((e_{k_1}(x))) \\ &= x. \end{aligned}$$

לכל קריפטו-מערכת יש פונקצית הסתברות של קבוצת מפתחות. נגדיר את הפונקציה הסתברות של המפתח של הצופן המורכב כך:

$$P(k_1, k_2) = P(k_1)P(k_2)$$

ז"א הבחירות של המפתחות k_1 ו- k_2 הם מאורעות בלתי-תלויים.

הגדרה 7.6 צופן הרכבה

יהיו $P = C = \mathbb{Z}_{26}$ ונגדיר קבוצת מפתחות

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

לכל $a \in K$ נגדיר כלל מצפין

$$e_a(x) = ax \pmod{26},$$

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

$$d_a(y) = a^{-1}y \pmod{26},$$

לכל $y \in \mathbb{Z}_{26}$.

7.4 דוגמה

יהי S צופן הזזה עם מפתח $k \in \mathbb{Z}_{26}$ ויהי M צופן מכפלה עם מפתח $a \in \mathbb{Z}_{26}$. הוכיחו כי הקריפטו-מערכת המורכבת $M \times S$ היא צופן איפני.

פתרון:

$$e_{a,k}(x) = e_a(x + k) = ax + ak.$$

מכיוון ש- $\gcd(a, 26) = 1$ לכן $ak \pmod{26} = k$ ולכן

$$e_{a,k}(x) = e_a(x + k) = ax + k.$$

ז"א $e_{a,k}(x)$ זהה לכלל מצפין של צופן אפני. נשאר להוכיח כי הפונקציה הסתברות של המפתח (a, k) של $M \times S$ שווה להסתברות של המפתח של צופן האפני, דהיינו $\frac{1}{312}$: עבור צופן הזזה:

$$P_S(k) = \frac{1}{26}$$

עבור צופן הרכבה:

$$P_M(a) = \frac{1}{12}$$

לכן

$$P_{M \times S} = P_M(a)P_S(k) = \frac{1}{12} \cdot \frac{1}{26} = \frac{1}{312}.$$

7.5 דוגמה

יהי S צופן הזזה עם מפתח $k \in \mathbb{Z}_{26}$ ויהי M צופן מכפלה עם מפתח $a \in \mathbb{Z}_{26}$. הוכיחו כי הקריפטו-מערכת המורכבת $S \times M$ היא צופן איפני.

פתרון:

$$e_{k,a}(x) = e_k(ax) = ax + k.$$

לכן $e_{k,a}(x)$ זהה לכלל מצפין של צופן אפני.

$$P_{S \times M} = P_S(k)P_M(a) = \frac{1}{26} \cdot \frac{1}{12} = \frac{1}{312}.$$

7.4 משפט האנטרופיה לקריפטו-מערכת

משפט 7.8 משפט האנטרופיה לקריפטו-מערכת

תהי (P, C, K, E, D) קריפטו-מערכת. אז

$$H(K|C) = H(K) + H(P) - H(C) .$$

הוכחה: (*להעשרה בלבד)

לפי משפט 7.6,

$$H(K, P, C) = H(K, P) + H(C|K, P) .$$

בגלל שהכלל מצפין $y = e_k(x)$ הוא פונקציה חד-חד-ערכית, אז המפתח והטקסט גלוי קובעים את הטקסט מוצפן בדרך יחידה. ז"א

$$H(C|K, P) = 0 .$$

לכן

$$H(K, P, C) = H(K, P) . \quad (*1)$$

המשתנים מקריים K ו- P בלתי-תלויים. לכן לפי משפט 7.5, $H(K, P) = H(K) + H(P)$ ולפיכך נקבל

$$H(K, P, C) = H(K) + H(P) . \quad (*2)$$

באותה מידה, לפי משפט 7.6,

$$H(K, P, C) = H(K, C) + H(P|K, C) . \quad (*3)$$

מכיוון שהכלל מפענח $x = d_k(y)$ פונקציה חד-חד ערכית, אז המפתח והטקסט מוצפן קובעים את הטקסט גלוי בדרך יחידה. לכן

$$H(P|K, C) = 0 .$$

ומכאן

$$H(K, P, C) = H(K, C) . \quad (*4)$$

לפי משפט 7.6, $H(K, C) = H(C) + H(K|C)$. לכן

$$\begin{aligned} H(K|C) &= H(K, C) - H(C) \\ &= H(K, P, C) - H(C) && \text{(לפי *4)} \\ &= H(K) + H(P) - H(C) && \text{(לפי *2)} \end{aligned} \quad (7.5)$$

כנדרש.

**דוגמה 7.6 (המשך של דוגמה 7.1 והמשך של דוגמה 7.2)**

עבור דוגמה 7.1 מצאו את $H(K|C)$ ובדקו כי הערך המתקבל תואם עם $H(K|C) = H(K) + H(P) - H(C)$.

פתרון:

בדוגמה 7.2 מצאנו כי $H(P) = 0.81$, $H(K) = 1.5$ ו- $H(C) = 1.85$. ז"א
 $H(K|C) = H(K) + H(P) - H(C) = 0.46$.

כעת נחשב את $H(K|C)$ בעזרת התוצאות של דוגמה 7.1:

$$P(K = k_1|C = 1) = \frac{P(C = 1|K = k_1) P(K = k_1)}{P(C = 1)} = \frac{\left(\frac{1}{4}\right) \left(\frac{1}{2}\right)}{\left(\frac{1}{8}\right)} = 1 ,$$

$$P(K = k_2|C = 1) = \frac{P(C = 1|K = k_2) P(K = k_2)}{P(C = 1)} = \frac{0 \left(\frac{1}{4}\right)}{\left(\frac{1}{8}\right)} = 0 ,$$

$$P(K = k_3|C = 1) = \frac{P(C = 1|K = k_3) P(K = k_3)}{P(C = 1)} = \frac{0 \left(\frac{1}{4}\right)}{\left(\frac{1}{8}\right)} = 0 ,$$

$$P(K = k_1|C = 2) = \frac{P(C = 2|K = k_1) P(K = k_1)}{P(C = 2)} = \frac{\left(\frac{3}{4}\right) \left(\frac{1}{2}\right)}{\left(\frac{7}{16}\right)} = \frac{6}{7} ,$$

$$P(K = k_2|C = 2) = \frac{P(C = 2|K = k_2) P(K = k_2)}{P(C = 2)} = \frac{\left(\frac{1}{4}\right) \left(\frac{1}{4}\right)}{\left(\frac{7}{16}\right)} = \frac{1}{7} ,$$

$$P(K = k_3|C = 2) = \frac{P(C = 2|K = k_3) P(K = k_3)}{P(C = 2)} = \frac{0 \left(\frac{1}{4}\right)}{\left(\frac{7}{16}\right)} = 0 ,$$

$$P(K = k_1|C = 3) = \frac{P(C = 3|K = k_1) P(K = k_1)}{P(C = 3)} = \frac{(0) \left(\frac{1}{2}\right)}{\left(\frac{1}{4}\right)} = 0 ,$$

$$P(K = k_2|C = 3) = \frac{P(C = 3|K = k_2) P(K = k_2)}{P(C = 3)} = \frac{\left(\frac{3}{4}\right) \left(\frac{1}{4}\right)}{\left(\frac{1}{4}\right)} = \frac{3}{4} ,$$

$$P(K = k_3|C = 3) = \frac{P(C = 3|K = k_3) P(K = k_3)}{P(C = 3)} = \frac{\left(\frac{1}{4}\right) \left(\frac{1}{4}\right)}{\left(\frac{1}{4}\right)} = \frac{1}{4} ,$$

$$P(K = k_1|C = 4) = \frac{P(C = 4|K = k_1) P(K = k_1)}{P(C = 4)} = \frac{(0) \left(\frac{1}{2}\right)}{\left(\frac{3}{16}\right)} = 0 ,$$

$$P(K = k_2|C = 4) = \frac{P(C = 4|K = k_2) P(K = k_2)}{P(C = 4)} = \frac{0 \left(\frac{1}{4}\right)}{\left(\frac{3}{16}\right)} = 0 ,$$

$$P(K = k_3|C = 4) = \frac{P(C = 4|K = k_3) P(K = k_3)}{P(C = 4)} = \frac{\left(\frac{3}{4}\right) \left(\frac{1}{4}\right)}{\left(\frac{3}{16}\right)} = 1 .$$

מכאן

$$\begin{aligned}
H(K|C) &= - \sum_{y=1}^4 \sum_{k \in \{k_1, k_2, k_3, k_4\}} P(C=y) P(K=k|C=y) \log_2 P(K=k|C=y) \\
&= - P_C(1) P_{K|C}(k_1|1) \log_2 P_{K|C}(k_1|1) - P_C(2) P_{K|C}(k_1|2) \log_2 P_{K|C}(k_1|2) \\
&\quad - P_C(3) P_{K|C}(k_1|3) \log_2 P_{K|C}(k_1|3) - P_C(4) P_{K|C}(k_1|4) \log_2 P_{K|C}(k_1|4) \\
&\quad - P_C(1) P_{K|C}(k_2|1) \log_2 P_{K|C}(k_2|1) - P_C(2) P_{K|C}(k_2|2) \log_2 P_{K|C}(k_2|2) \\
&\quad - P_C(3) P_{K|C}(k_2|3) \log_2 P_{K|C}(k_2|3) - P_C(4) P_{K|C}(k_2|4) \log_2 P_{K|C}(k_2|4) \\
&\quad - P_C(1) P_{K|C}(k_3|1) \log_2 P_{K|C}(k_3|1) - P_C(2) P_{K|C}(k_3|2) \log_2 P_{K|C}(k_3|2) \\
&\quad - P_C(3) P_{K|C}(k_3|3) \log_2 P_{K|C}(k_3|3) - P_C(4) P_{K|C}(k_3|4) \log_2 P_{K|C}(k_3|4) \\
&= - \frac{1}{8} \log_2 1 - \frac{7}{16} \cdot \frac{6}{7} \log_2 \frac{6}{7} - \frac{1}{4} \cdot 0 \log_2 0 - \frac{3}{16} \cdot 0 \log_2 0 \\
&\quad - \frac{1}{8} 0 \cdot \log_2 0 - \frac{7}{16} \cdot \frac{1}{7} \log_2 \frac{1}{7} - \frac{1}{4} \cdot \frac{3}{4} \log_2 \frac{3}{4} - \frac{3}{16} \cdot 0 \log_2 0 \\
&\quad - \frac{1}{8} \cdot 0 \log_2 0 - \frac{7}{16} \cdot 0 \log_2 0 - \frac{1}{4} \cdot \frac{1}{4} \log_2 \frac{1}{4} - \frac{3}{16} \cdot 1 \cdot \log_2 1 \\
&= 0.461676 .
\end{aligned}$$

הרי

$$H(K|C) = 0.46 = H(K) + H(P) - H(C)$$

■

כנדרש.

שיעור 8

אנטרופיה ומידע

8.1 המושג של מידע

נניח נניח ש- X משתנה מקרי אשר יכול לקבל אחת מארבע אפשרויות:

$$X \in \{a, b, c, a\}.$$

X ידוע לבוב (B) אבל לא ידוע לאליס (A). כל שאליס יודעת הוא ש- X יכול להיות אחת האותיות $\{a, b, c, a\}$ בהסתברות שווה. אנחנו אומרים כי לאליס יש אי-ודאות על הערך של X . כדי שאליס תמצא את הערך של X אליס שואלת סדרת שאלות בינאריות (שאלות כן/לא) לבוב כדי לקבל מידע על המ"מ X עד שהיא תדע את הערך של X עם אי-ודאות אפס.

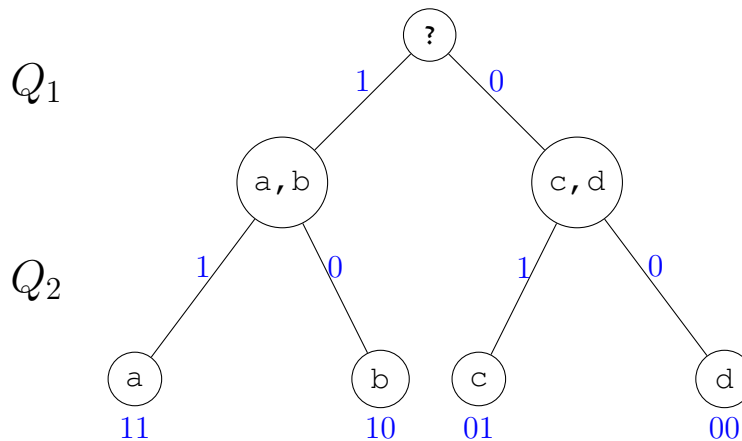
אפשרות אחת לסדרת שאלות היא כך:

$$Q_1: \text{האם } X \in \{a, b\}$$

לפי התשובה אחר כך אליס שואלת

$$Q_2: \text{אם } X \in \{a, b\} \text{ האם } X = a$$

$$\text{אחרת אם } X \notin \{a, b\} \text{ האם } X = c$$



הסדרה של שאלות בינאריות שמאפשרת לאליס למצוא את X ללא שופ אי-ודאות מתוארת בעץ-שאלות למעלה. מספר השאלות הבינאריות $N_Q[X]$, שנדרשות כדי למצוא X ללא אי-ודאות הוא $N_Q[X] = 2$.

כל שאלה היא בינארית, כלומר התשובה היא כן או לא אנחנו מצפינים תשובה כן עם "1" ותשובה לא עם "0". לפי התשובות אנחנו מצפינים את האותיות כך:

$$a \rightarrow 11, \quad b \rightarrow 10, \quad c \rightarrow 01, \quad d \rightarrow 00.$$

מכיוון ששתי תשובות בינאריות נדרשות כדי למצוא את X , אנחנו אורמים כי נדרש שני ביטים (bits) של מידע נדרשים כדי למצוא את X .

במילים אחרות, שתי ספרות בינאריות $X = d_1 d_2$ נדרשות כדי להצפין את X , שערכן הן התשובות לשתי שאלות בינאריות,

לכן המידע המתקבל על מציאת הערך של X הוא 2 bit.

אליס הייתה יכולה לשנות את הסדרת שאלות שלה כך:

Q'_1 האם $X = a$?

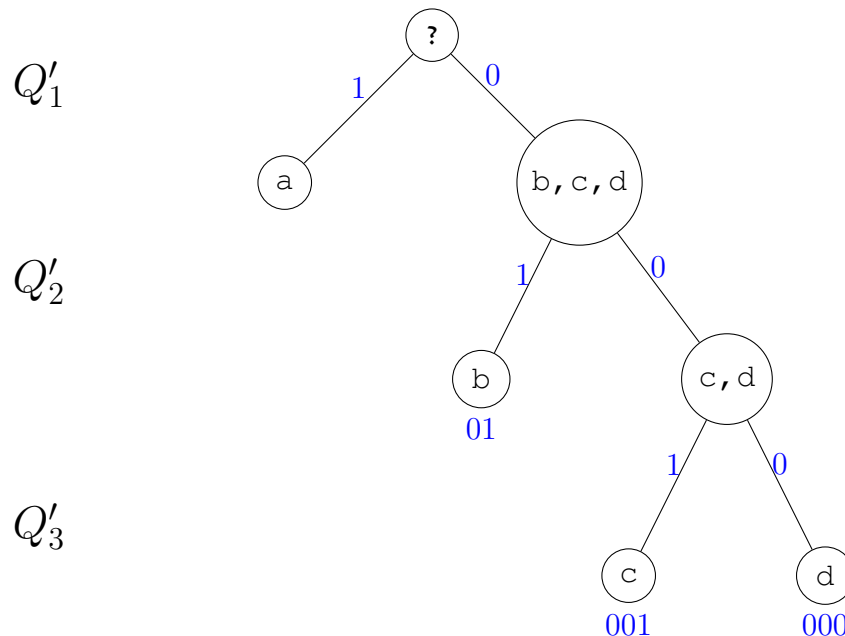
רק אם התשובה היא "לא" אז היא צריכה לשאול שאלה נוספת:

Q'_2 האם $X = b$?

ורק אם התשובה היא "לא" אז היא צריכה לשאול שאלה נוספת:

Q'_3 האם $X = c$?

מספר השאלות הביניאריות הנדרשות למצוא את X תלוי על הערך של X : $N_Q(a) = 1$, $N_Q(b) = 2$ או $N_Q(c) = N_Q(d) = 3$.



X הוא משתנה מקרי בדיד ולכן בהינתן מערכת שאלות, $N_Q(X)$ הוא פונקציה של משתנה מקרי בדיד, ולכן $N_Q[X]$ הוא בעצמו משתנה מקרי בדיד.

כעת נשאל שאלה. נניח כי אליס מעוניינת למצוא מערכת שאלות Q , אשר נותנת את מספר השאלות הממוצע המינימלי. כלומר, כיצד נמצא מערכת שאלות $N_Q[X]$ עבורה התוחלת

$$E[N_Q[X]] = \sum_{k \in X} P_X(k) N_Q[k]$$

תהיה מינימלית.

לפני שנענה על שאלה הזאת נתן דוגמה.

נתון המשתנה מקרי $X = \{a, b, c, d\}$ בעל הפונקציה הסתברות

$$P_X(a) = \frac{1}{2}, \quad P_X(b) = \frac{1}{4}, \quad P_X(c) = P_X(d) = \frac{1}{8}.$$

עם ההצפנה הראשונה $N_Q[k] = 2$ לכל $k \in X$ אז התוחלת תהיה $\frac{1}{2}(2) + \frac{1}{4}(2) + \frac{1}{8}(2) + \frac{1}{8}(2) = 2$ כלומר תוחלת מספר השאלות הוא 2. התוחלת עבור ההצפנה השנייה היא

$$E[N_Q[X]] = \frac{1}{2}(1) + \frac{1}{4}(2) + \frac{1}{8}(3) + \frac{1}{8}(3) = \frac{7}{4}.$$

אשר פחות מהתוחלת עבור ההצפנה הקודמת.

אליס שואלת סדרת שאלות ולכל שאלה נשים ערך בינארי 0 אם התשובה לא ו-1 אם התשובה כן. כך אנחנו נשים לכל ערך של X מספר בינארי $d_1 \dots d_k$ המורכב מספרות בינאריות $d_i = 0, 1$. טרנספורמציה כזאת בין ערכים של X לבין מספרים בינארים נקראת הצפנה. שימו לב כי אורך ההצפנה $\ell_Q[X]$ של כל ערך של X שווה למספר השאלות בינאריות הנדרשות כדי למצוא את X ללא אי-ודאות:

$$\ell_Q[X] = N_Q[X] .$$

התוחלת המינימלית מתקבלת באמצעות מערכת שאלות שבה מספר השאלות שמובילות לערך כלשהו ביחס הפוך להסתברות שלו. במילים פשוטות, ככל שההסתברויות של ערך של X גבוהה מספר השאלות המובילות לערך זה יותר קטן, ולהפך.

אקסיומ 1 מספר ביטים האופטימלי $\ell_{Q^*}(k)$ הנדרש להצפין את הסימן $X = k$ הוא פונקציה של ההסתברות $P_X(k)$.

אקסיומ 2

$$P_X(k) \geq P_X(k') \Rightarrow \ell_{Q^*}(k) \leq \ell_{Q^*}(k') .$$

משפט 8.1 אנטרופיה של שאנון

$$H[X] = - \sum_{k \in X} P_X(k) \log_2 P_X(k) .$$

הוכחה: נניח כי $X = Y \cap Z$, כאשר Y, Z משתנים מקרים בלתי תלויים. אז

$$H[X] = H[Y] + H[Z]$$

נסמן $p_x = P_X(x)$. לפי אקסיומ 1:

$$\ell_Q(x) = f(p_x) .$$

$$H[X] = \sum p_x \ell_Q(x) = \sum p_x f(p_x) .$$

כעת נניח שיש לנו משתנים מקרים Y ו- Z ושהם בלתי תלויים. יהיו $P_Y(y)$ ו- $P_Z(z)$ פונקציות ההסתברות של Y ושל Z בהתאמה. נסמן $p_y = P_Y(y)$ ו- $p_z = P_Z(z)$.

נגדיר את המאורע $X = Y \cap Z$. מכיוון ש- Y ו- Z משתנים בלתי תלויים אז

$$P(X = Y \cap Z) = P_Y(y)P_Z(z) = p_y p_z .$$

ידועה של Y לא נותנת שום מידע על הערך של Z , אז

$$\ell_Q[Y \cap Z] = \ell_Q[Y] + \ell_Q[Z] .$$

לפיכך

$$H[X] = \sum p_x \ell_Q(x) = \sum p_y p_z (\ell_Q(y) + \ell_Q(z))$$

$$H[X] = \sum p_x \ell_Q(x) = \sum p_y p_z (\ell_Q(y) + \ell_Q(z))$$

מכאן

$$H[X] = \sum p_y p_z f(p_y p_z) = \sum p_y p_z [f(p_y) + f(p_z)]$$

לכל p_y ו- p_z . לכן

$$f(p_y p_z) = f(p_y) + f(p_z) .$$

ז"א $f(p) = C \log(p)$. נדרש כי $f\left(\frac{1}{2}\right) = 1$ ונקבל $f(p) = -\log_2(p)$.



8.2 הגדרה של מידע

הגדרה 8.1 מידע של מאורע (שאנון)

נתון משתנה מקרי X . המידע של ערך מסוים של X מסומן $I_X(x)$ ומוגדר להיות

$$I(X = x) = \log_2 \left(\frac{1}{P_X(x)} \right) = -\log_2 (P_X(x))$$

כאשר $P_X(x)$ פונקציית ההסתברות של המשתנה מקרי X .

דוגמה 8.1 המידע המתקבל בגילוי תוצאה של הטלת מטבע

נטיל מטבע הוגנת ונגדיר משתנה מקרי X להיות התוצאה של הניסוי. מכאן X מקבל את הערכים

$$X = \{H, T\} .$$

מצאו את המידע של המאורע $X = H$.

פתרון:

$$P(X = H) = \frac{1}{2} .$$

$$I(X = H) = -\log_2 \left(\frac{1}{2} \right) = 1 .$$

כלומר על קבלת התוצאה " H " אנחנו מקבלים ביט אחד של מידע.

הסבר:

במקום הסימנים " H " ו- " T " בשביל המ"מ X ניתן להצפין את הערכים האפשריים בספרות בינאריות "0" או "1". כלומר

ערך של X	הצפנה בספרות בינאריות
H	0
T	1

ז"א כדי להצפין את הערכים של X אנחנו צריכים ספרה בינארית אחת:

$$d_1 \in \{0, 1\} .$$

אשר יכול להחזיק את הערכים 0 או 1.

ספרה בינארית אחת נדרשת להחזיק את הערך של X לכן המידע של ערך כלשהו של X הוא 1 bit (ביט אחד).



דוגמה 8.2 שליפת קלף מחבילת קלפים תיקנית

בניסוי שליפת קלף אחד מחבילת קלפים תיקנית. נגדיר את המשתנה מקרי X להיות הסוג של הקלף (תלתן, עלה לב או יהלום). חשבו את את המידע של המאורע ששלפני קלף מסוג לב.

פתרון:

ההסתברות לשלוף קלף של הסוג לב מחבילת קלפים סטנדרטית היא

$$P(X = \heartsuit) = \frac{13}{52} = \frac{1}{4}.$$

לכן

$$I(X = \heartsuit) = -\log_2\left(\frac{1}{4}\right) = 2 \text{ bits}$$

הסבר:

יש 4 הערכים האפשריים של X :

$$X = \{\spadesuit, \clubsuit, \heartsuit, \diamondsuit\}$$

כל ספרה בינארית מחזיקה 2 ערכים אפשריים: 0 או 1 לכן ידרש שתי ספרות בינאריות כדי להצפין את ה-4 ערכים האפשריים של X :

$$d_1 d_2, \quad d_1, d_2 \in \{0, 1\}.$$

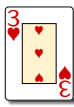
ההצפנה עצמה מתוארת בטבלא למטה:

ערך של X	הצפנה בספרות בינאריות
\spadesuit	00
\clubsuit	01
\heartsuit	10
\diamondsuit	11




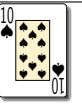

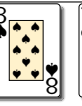
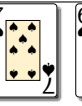
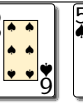
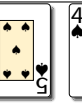
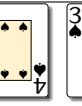
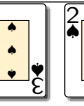
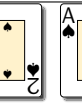
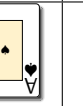



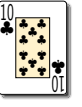
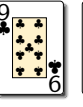
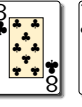
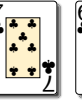
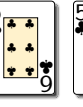
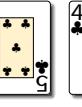
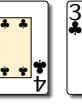
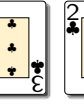
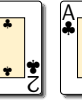
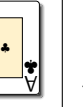





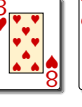
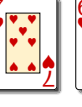
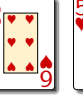
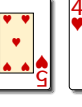
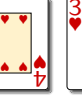
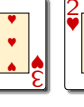
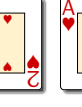
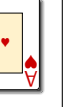










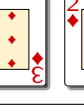
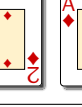
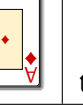
אורך המספר $d_1 d_2$ הוא 2 לכן המידע של המשתנה מקרי X הוא 2 bits (שני ביטים).



דוגמה 8.3 שליפת קלף מחבילת קלפים תיקנית



בניסוי שליפת קלף אחד מחבילת קלפים תיקנית. מצאו את המידע המתקבל אם הקלף נשלף.

תמונות	מספרים	צורה
  	         	עלה
  	         	תלתן
  	         	לב
  	         	יהלום

פתרון:

יהי X המ"מ שמסמן את הקלף הנשלף. ההסתברות לשלוף הקלף שלוש מצורת לב מחבילת קלפים סטנדרטית היא

$$P\left(X = \begin{array}{|c|} \hline 3 \\ \hline \end{array} \begin{array}{|c|} \hline \heartsuit \\ \hline \end{array}\right) = \frac{1}{52}.$$

לכן

$$I\left(X = \begin{array}{|c|} \hline 3 \\ \hline \end{array} \begin{array}{|c|} \hline \heartsuit \\ \hline \end{array}\right) = -\log_2\left(\frac{1}{52}\right) = 5.7 \text{ bits}$$

הסבר:

כדי להצפין את כל הערכים האפשריים של X כרצף סיבית, נדרש רצף סיביתחם אשר מקבל לפחות 52 ערכים שונים. רצף עם 5 סיביות לא מספיק כי יש לו רק $2^5 = 32$ ערכים שונים. אבל רצף עם 6 סיביות נותן $2^6 = 64$ ערכים שונים, אשר מספיק להצפין את כל הערכים האפשריים של X .

$$d_1 d_2 d_3 d_4 d_5 d_6$$

האורך של הרצף סיביות הזה הוא 6 ולכן הרצף סיבית זה נותן 6 bits של מידע. לכל סיבית יש 2 ערכים אפשריים ולכן 64 ערכים שונים בסה"כ.

רק 52 מתוך ה- 64 צירופים נדרשים כדי להצפין את הערכים האפשריים של X לכן נוריד חלק של הסיביות. הקבוצת סיביות הנשארים מכילה 5.7 bits של מידע.



ככל שההסתברות של מאורע יותר קטנה אז המידע המתקבל יותר גבוהה.

כלומר, ככל שהמידע של מאורע יותר גבוהה אז ההסתברות שלו יותר קטנה

8.3 אנטרופיה

הגדרה 8.2 אנטרופיה של מ"מ X

נתון מ"מ בדיד X . נניח כי הערכים האפשריים של X הם

$$X = \{x_1, \dots, x_N\}.$$

האנטרופיה $H(X)$ של מ"מ X מוגדרת להיות התוחלת (הממוצע המשוקלל) של המידע המתקבל על ידי למצוא את הערך של X (כלומר על גילוי התוצאה של הניסוי):

$$H(X) = \sum_{i=1}^N P(X = x_i) I(X = x_i) = - \sum_{i=1}^N P(X = x_i) \log_2 (P(X = x_i))$$

במקרה שההסתברות של כל תוצאה שווה, כלומר

$$P(X = x_i) = \frac{1}{|X|} = \frac{1}{N}$$

אז

$$H(X) = - \sum_{i=1}^N \frac{1}{N} \log_2 \left(\frac{1}{N} \right) = \frac{1}{N} \sum_{i=1}^N \log_2 N = \log_2 N.$$

לכן

$$N = 2^{H(X)}.$$

ניתן להוכיח ש- $\log_2 N$ הוא הערך המקסימלי האפשרי של $H(X)$.

משפט 8.2

נתון מ"מ בדיד X אשר מקבל N ערכים שונים:

$$X = \{x_1, \dots, x_N\}$$

אם ההסתברות של כל ערך שווה, כלומר

$$P(X = x_i) = \frac{1}{N}$$

אז האנטרופיה מקבלת ערך מקסימלי שניתנת על ידי

$$H_{\max}(X) = \log_2 N.$$

ערך זה הוא הערך המקסימלי האפשרי של האנטרופיה.

דוגמה 8.4 אנטרופיה בהטלת מטבע

נניח כי נטיל מטבע עם הסתברות p ($0 \leq p \leq 1$). לקבל H . מצאו את האנטרופיה של המ"מ מקרי X אשר שווה לתוצאת הניסוי.

פתרון:

נסמן $X = \{0, 1\}$ כאשר $X = 0$ מסמן תוצאת H ו- $X = 1$ מסמן תוצאת T . הפונקציה הסתברות היא

$$P_X(0) = p, \quad P_X(1) = 1 - p.$$

לכן המידע של המאורע לקבל תוצאת H הוא

$$I(X = 0) = -\log_2(P_X(0)) = -\log_2(p)$$

והמידע של המאורע לקבל תוצאת H הוא

$$I(X = 1) = -\log_2(P_X(1)) = -\log_2(1 - p)$$

נשים לב שאם המטבע הוגנת אז $p = \frac{1}{2}$ ו- $I(X = 0) = I(X = 1) = 1$. כעת נחשב את האנטרופיה של X :

$$H(X) = -P_X(0) \log_2(P_X(0)) - P_X(1) \log_2(P_X(1)) = -p \log_2 p - (1 - p) \log_2(1 - p).$$

נרשום את האנטרופיה כפונקציה של ההסתברות p :

$$H(X) = -p \log_2 p - (1 - p) \log_2(1 - p) =: h(p).$$

ל- $h(p)$ יש נקודת מקסימום ב- $p = \frac{1}{2}$:

$$h'(p) = -\frac{1}{\ln 2} - \log_2 p + \frac{1}{\ln 2} + \log_2(1 - p) = -\log_2 p + \log_2(1 - p) = \log_2\left(\frac{1}{p} - 1\right) \stackrel{!}{=} 0 \Rightarrow p = \frac{1}{2}.$$

ז"א הערך המקסימלי של האנטרופיה מתקבל כאשר לכל הערכים של X יש הסתברות שווה, $P_X(0) = P_X(1) = \frac{1}{2}$.
אכן

$$h(p = \frac{1}{2}) = -\frac{1}{2} \log_2 \frac{1}{2} - \frac{1}{2} \log_2 \frac{1}{2} = \log_2 2 = 1.$$

8.5 דוגמה

בניסוי הטלת מטבע לא מאוזנת, ההסתברות לקבל תוצאה H היא $p = \frac{1}{1024}$. מצאו את האנטרופיה של X .

פתרון:

נסמן $X = \{0, 1\}$, כאשר $X = 0$ מסמן תוצאת H ו- $X = 1$ מסמן תוצאת T .

$$I(X = 0) = -\log_2 \frac{1}{1024} = 10 \text{ bits}, \quad I(X = 1) = -\log_2(1 - p) = -\log_2 \frac{1023}{1024} = 0.00141 \text{ bits}.$$

לפי זה

$$H(X) = -p \log_2 p - (1 - p) \log_2(1 - p) = -\frac{1}{1024} \log_2 \frac{1}{1024} - \frac{1023}{1024} \log_2 \frac{1023}{1024} = 0.0112 \text{ bits}.$$

המשמעות של התשובה לדוגמה הקודמת היא כך. נניח שנטיל אותה מטבע הלא מאוזנת 100,000 פעמים. בכדי להצפין את כל התוצאות נדרש רצף סיביות של אורך 100,000, כאשר כל ספרה נותנת תוצאה של ניסוי אחד. ז"א 10^5 bits של מידע נדרש כדי להצפין את כל התוצאות.

מצד שני מצאנו כי התוחלת של המידע המתקבל לניסוי (כמות מידע פר ניסוי) הוא 0.0112 bit פר ניסוי. במילים אחרות, ב- 10^5 ניסויים רק 1120 bit של מידע נדרש בממוצע כדי להצפין את כל התוצאות של הרצף ניסויים.

אנטרופיה (בביטים) אומרת לנו את כמות המידע הממוצעת (בביטים) שיש לספק על מנת להעביר את כל התוצאות של המאורע. זהו חסם תחתון על מספר הסיביות שיש להשתמש בהן, בממוצע לקודד (להצפין) את התווים של ההודעה שלנו.

8.4 הצפנת האפמן

נסביר הצפנת האפמן בעזרת הדוגמה הבאה. נתון הטקסט גלוי

$$X = \{a, b, c, d\}$$

ונניח כי הפונקציה הסתברות של X היא לפי הטבלה הבאה:

בחירת אות של $x_i \in X$	$p_i = P_X(x_i)$	$I(X = x_i) = -\log_2(p_i)$
a	$\frac{1}{3}$	1.58 bit
b	$\frac{1}{2}$	1 bit
c	$\frac{1}{12}$	3.58 bit
d	$\frac{1}{12}$	3.58 bit

נשאל את השאלה: כמה ביטים של מידע נדרשים כדי להצפין (בסיביות) רצף של 1000 אותיות של טקסט גלוי X ?

יש 4 אותיות ב- X , כלומר 4 ערכים אפשריים של המ"מ ביד X . לפיכך נדרש רצף של 2 סיביות כדי להצפין טקסט גלוי של תו אחד בהצפנת סיביות קבועה. לדוגמה:

בחירת אות של $x_i \in X$	הצפנה
a	00
b	01
c	10
d	11

ז"א להצפין תו אחד של הטקסט גלוי X נדרש 2 bit. לכן להצפין רצף אותיות של טקסט גלוי נדרש $2 \times 1000 = 2000$ bit, כלומר 2000 סיביות.

האנטרופיה של X היא

$$H(X) = -p_1 \log_2(p_1) - p_2 \log_2(p_2) - p_3 \log_2(p_3) - p_4 \log_2(p_4) = 1.62581 \text{ bit} .$$

ז"א לכל ניסוי המידע הממוצע הנדרש כדי להצפין תו אחד של טקסט גלוי הוא 1.62581 bit. לכן המידע הממוצע הנדרש כדי להצפין רצף אותיות של טקסט גלוי הוא

$$1000 \times 1.62581 = 1625.81 \text{ bit} .$$

לכן, רצף סיביות של אורך 1626 בממוצע יהיה מספיק כדי להעביר את ההודעה.

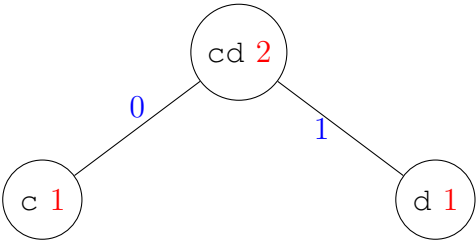
כעת נבנה הצפנה של הטקסט גלוי על ידי האלגוריתם של האפמן.

שלב 1)

	c	d	a	b
	1	1	4	6

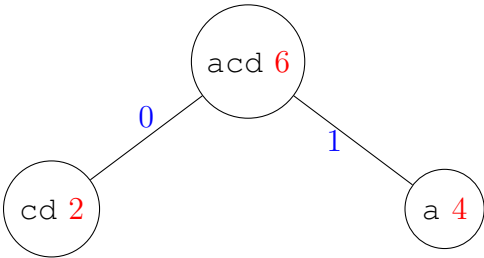
שלב 2)

	c	d	a	b
	1	1	4	6
	0	1		
	2		4	6



שלב 3)

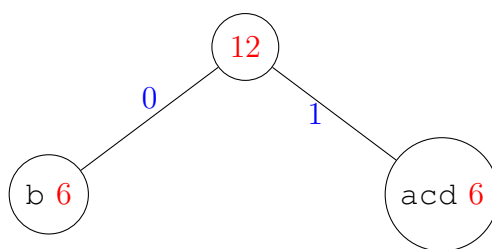
	cd	a	b
	2	4	6
	0	1	
	6		6



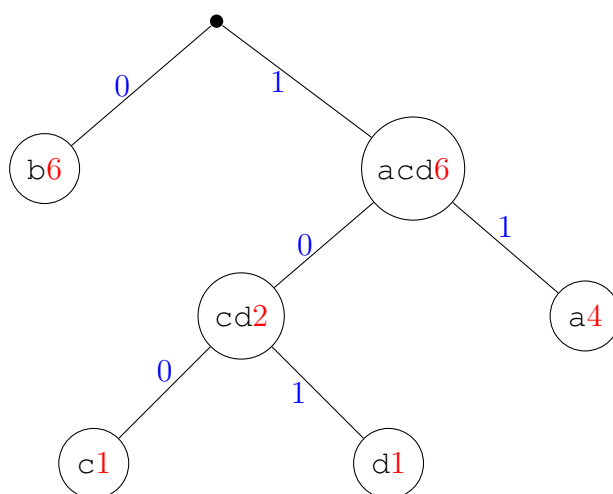
שלב 4)

שלב 5)

	acd	b
	6	6
	0	1
	12	



שלב 6)



בסוף של התהליך האותיות של הטקסט גלוי יהיו בעלים של העץ וההצפנה ניתנת על ידי הרצף סיביות על הענפים במסלול מהנקודת התחלתית של העץ עד העלה בו רשום האות בשאלה.

בחירת אות של $x_i \in X$	הצפנת האפמן
a	11
b	100
c	110
d	101

דוגמה 8.6

נתון הטקסט גלוי הבא

$$X = \{a, b, c, d, e\}$$

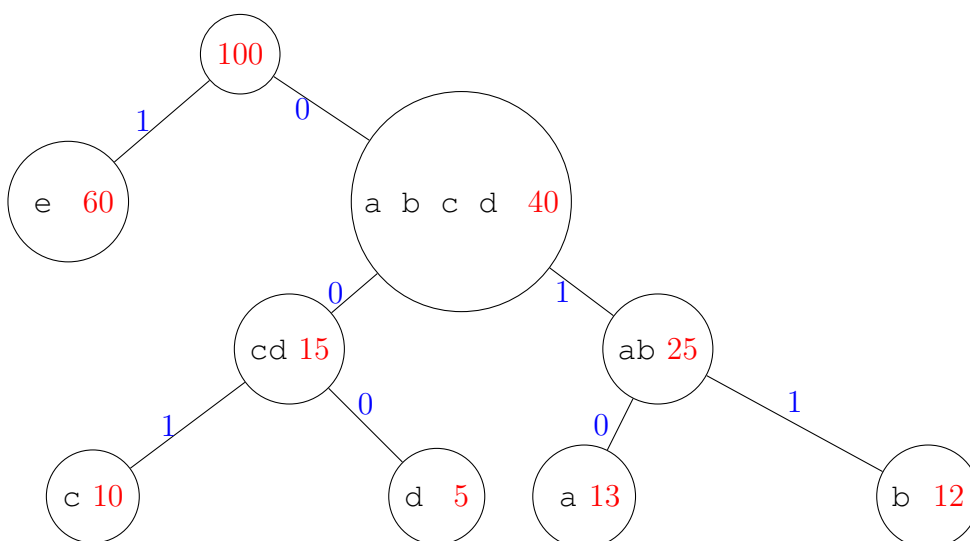
והפונקציה הסתברות

$$P(X = a) = \frac{13}{100} = 0.13, \quad P(X = b) = \frac{3}{25} = \frac{12}{100} = 0.12, \quad P(X = c) = \frac{1}{10} = \frac{10}{100} = 0.1,$$

$$P(X = d) = \frac{1}{20} = \frac{5}{100} = 0.05, \quad P(X = e) = \frac{3}{5} = \frac{60}{100} = 0.6.$$

מצאו את העץ הצפנה וההצפנת האפמן של כל תו של X .

פתרון:



בחירת אות של $x_i \in X$	הצפנת האפמן
a	010
b	011
c	001
d	000
e	1

פורמלי הצפנת האפמן מוגדרת לפי ההגדרה הבאה:

הגדרה 8.3 הצפנת האפמן

נתון משתנה מקרי X . נגדיר הצפנת האפמן של X להיות הפונקציה (כלל מצפין)

$$f : X \rightarrow \{0, 1\}^*$$

כאשר $\{0, 1\}^*$ קבוצת רצפים של סיביות סופיים.

נתון רצף מאורעות x_1, \dots, x_n . נגדיר

$$f(x_1 \dots x_n) = f(x_1) || \dots || f(x_n)$$

כאשר $||$ מסמן שרשור (concatenation).

הגדרה 8.4 תוחלת האורך של הצפנת האפמן

נתונה הצפנת האפמן f . תוחלת האורך של ההצפנה מוגדרת

$$l(f) = \sum_{x \in X} P(X = x) |f(x)|.$$

משפט 8.3 אי שוויון האפמן

נתון קבוצת אותיות של טקסט גלוי X והצפנת האפמן f . נניח כי $l(f)$ תוחלת האורך של ההצפנה ו-
 $H(X)$ האנטרופיה של הטקסט גלוי. מתקיים

$$H(X) \leq l(f) \leq H(X) + 1.$$

דוגמה 8.7 (המשך של דוגמה 8.6)

נתון הטקסט גלוי הבא

$$X = \{a, b, c, d, e\}$$

והפונקציה הסתברות

$$P(X = a) = \frac{13}{100} = 0.13, \quad P(X = b) = \frac{3}{25} = 0.12, \quad P(X = c) = \frac{1}{10} = 0.1, \quad P(X = d) = \frac{1}{20} = 0.05,$$

$$P(X = e) = \frac{3}{5} = 0.6.$$

(1) מצאו את תוחלת האורך של ההצפנת האפמן.

(2) מצאו את האנטרופיה.

(3) הוכיחו כי אי-שוויון האפמן של ההצפנה שמצאתם בדוגמה 8.6 למעלה מתקיים.

פתרון:

סעיף (1)

$$\begin{aligned} l(f) &= \frac{5}{100} \cdot 3 + \frac{10}{100} \cdot 3 + \frac{12}{100} \cdot 3 + \frac{13}{100} \cdot 3 + \frac{60}{100} \cdot 1 \\ &= \frac{15 + 30 + 36 + 39 + 60}{100} \\ &= \frac{180}{100} \\ &= 1.8 \end{aligned}$$

סעיף (2)

$$\begin{aligned} H(X) &= -P(X = a) \log_2 P(X = a) - P(X = b) \log_2 P(X = b) - P(X = c) \log_2 P(X = c) \\ &\quad - P(X = d) \log_2 P(X = d) - P(X = e) \log_2 P(X = e) \\ &= 1.74018. \end{aligned}$$

סעיף (3) $H(X) = 1.74018$, $H(X) + 1 = 1.84018$, $l(f) = 1.8$. לכן

$$H(X) \leq l(f) \leq H(X) + 1$$

מתקיים.