

קריפטוגרפיה

תוכן העניינים

1 תורת המספרים	
3	משפט החילוק של אוקלידס
8	מספרים ראשוניים
10	המחלק המשותף הגדול ביותר
14	האלגוריתם של אוקלידס
19	יחס השקילות המודולרית
2 חוגים מתמטיים	
23	הפונקצית אוילר
25	החוג \mathbb{Z}_m
28	הפיכת מטריצות בחוג \mathbb{Z}_m
3 הצפנים הבסיסיים	
32	מושג של קריפטו-מערכת
32	צופן ההזאה
33	צופן האפיני
35	צופן ויז'ר
41	צופן היל
4 תמורה וצופן אניגמה	
54	תמורים
54	פירוק למחזורים של תמורה
57	תמורים צמודות
60	צופן אניגמה
61	משפט ריבסקי
64	ה衲חות של ריבסקי על צופן האניגמה
5 קריפטו-אנגליזה	
70	סוגים של התקפת סייבר
70	קבוצות אותיות הנפוצים ביותר בטקסט גלי
72	קריפטו-אנגליזה של צופן האפיני
77	קריפטו-אנגליזה של צופן היל
80	מדד צירוף המקרים
81	קריפטו-אנגליזה של צופן ויז'ר - מבחן פרידמן
6 צופן RSA	RSA
86	אלגוריתם RSA
92	משפט השאריות הסיני
93	משפטים של מספרים ראשוניים
96	הוכחה שצופן RSA ניתן לפענוח

97	צופן RSA המוכל	7 הביעית הפירוק של מספרים וצופן רבין
99		הביעית פירוק מספרים
99		צופן רבין
100		8 צופן אל-גמאל
102		9 תורת שאנו
102		סודיות מושלמת
109		המושג של מידע
113		הגדרה של מידע
118		הצפנת האפמן
123		תכוונות של אנתרופיה
127		משפט האנתרופיה לкриpto-מערכת
131		10 צפנים בלוקים ו- DES
131		רשת החלפה-תמורה
135		רשת פייסטל
138		תקן הצפנה מידע (DES)
139		הפונקציית ליבה של DES
140		התזמון המפתח של DES
142		הבלוקים של החלפות של DES
142		דוגמאות
146		IDEA
146		תת מפתחות של IDEA
147		אלגוריתם ההצפנה
148		דוגמאות
151		11 פונקציות תמצות קריפטוגרפיות
151		פונקציות תמצות
151		אמינות המידע
152		12 פונקציות תמצות קריפטוגרפיות המשך
152		פונקציות תמצות איטרטיביות
153		13 שיטות חתימה
153		דרישות בטויות משיטות חתימה
153		שיטות חתימה של אל-גמאל
154		14 סכימות לשיתוף סודות
154		סכמת הסף של שמיר
154		סכמת סף (t, t) פשוטה

שיעור 1

תורת המספרים

1.1 משפט חילוק של אוקלידס

הגדרה 1.1 מספר שלם שמחולק במספר שלם אחר

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

$$a = qb .$$

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

הסימן $a | b$ אומר כי b מחלק את a .

דוגמה 1.1

א) $6 | 3$ בגלל שקיימים מספר שלם $q = 2$ כך ש- $6 = 3q$

ב) $42 | 7$ בgalל שקיימים מספר שלם $q = 6$ כך ש- $42 = 7q$

ג) $8 \nmid 5$ בgalל שלא קיימים מספר שלם q כך ש- $5q = 8$

משפט 1.1 תכונות של חילוק שלמים

יהיו a, b, d שלמים.

(1) אם $d | (a + b)$ ו- $d | b$ אז $d | a$

(2) יהיו x, y שלמים. אם $d | b$ ו- $d | a$ אז $d | (xa + yb)$

(3) אם $a = \pm b$ אז $b | a$ ו- $a | b$

הוכחה:

$$\left. \begin{array}{l} d|a \\ d|b \end{array} \right\} \Rightarrow a = a'd \quad \Rightarrow \quad a \pm b = d(a' + b') \quad \Rightarrow \quad d | (a + b) . \quad (1)$$

$$\left. \begin{array}{l} d|a \\ d|b \end{array} \right\} \Rightarrow a = a'd \quad \Rightarrow \quad ax + by = d(a'x + b'y) \quad \Rightarrow \quad d | (ax + by) . \quad (2)$$

$$\left. \begin{array}{l} a|b \\ b|a \end{array} \right\} \Rightarrow b = ca \quad \Rightarrow \quad b = ca = cc'b \quad \Rightarrow \quad cc' = 1 . \quad (3)$$

ונ- c' הם שלמים לכך $cc' = 1$ אם ורק אם $c = c'$ או $c = -c'$. לפיכך $b = \pm a$.

הגדרה 1.2 השארית

יהיו $a, b > 0$ שלמים. השארית של a בחלוקת b -השאירה b מסומנת $a \bmod b$ ומוגדרת

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

סימון חלופי לשארית בחלוקת a ב- b : $a \% b$

הערה: השארית מוגדרת באופן חד משמעי עבור שלמים חיוביים בלבד!

דוגמה 1.2

$$43 \bmod 10 = 43 - 10 \cdot \left\lfloor \frac{43}{10} \right\rfloor = 43 - 10(4) = 3 ,$$

$$13 \bmod 4 = 13 - 4 \cdot \left\lfloor \frac{13}{4} \right\rfloor = 13 - 4(3) = 1 ,$$

$$8 \bmod 2 = 8 - 2 \cdot \left\lfloor \frac{8}{2} \right\rfloor = 8 - 2(4) = 0 .$$

משפט 1.2 משפט החלוק של אוקלידס

יהיו a, b מספרים שלמים. אם $b \neq 0$ ו- $a \geq b$ אז קיימים מספרים שלמים q, r ייחודיים כך ש-

$$a = qb + r \quad (1.1)$$

כאשר $|r| \leq b$. השם q נקרא המנה של a בחלוקת b -השאירה r של a בחלוקת b -השאירה a .

ההוכחה עצמה היא לא חלק של הקורס.

דוגמה 1.3

יהיו $a = 46, b = 8$. המנה והשאירה הם $q = 5, r = 6$ והפירוק מנה-שאירה הוא

$$46 = 5(8) + 6 .$$

דוגמה 1.4

יהיו $a = -46, b = 8$. המנה והשאירה הם $q = -6, r = 2$ והפירוק מנה-שאירה הוא

$$-46 = (-6)(8) + 2 .$$

משפט 1.3 שיטה מעשית לחישוב החלוקת מנת-שארית

יהיו a, b שלמים ($a \neq 0 \neq b$). אין מנתה q והשארית r במשפט החלוק של אוקלידס ניתנים כך:

$$r = a \bmod b \text{ ו } q = \left\lfloor \frac{a}{b} \right\rfloor \text{ אם } a > 0, b > 0 \quad (1)$$

$$r = a \bmod |b| \text{ ו } q = -\left\lfloor \frac{a}{|b|} \right\rfloor \text{ אם } a > 0, b < 0 \quad (2)$$

$$r = b - |a| \bmod b \text{ ו } q = -\left\lfloor \frac{|a|}{b} \right\rfloor - 1 \text{ אם } a < 0, b > 0 \quad (3)$$

$$r = |b| - |a| \bmod |b| \text{ ו } q = \left\lfloor \frac{|a|}{|b|} \right\rfloor + 1 \text{ אם } a < 0, b < 0 \quad (4)$$

הוכחה: נוכיח בכל אחד מארבעת המקרים.

מצב 1 נניח $0 < a$. לפי משפט החלוק של אוקלידס קיימים שלמים r, q כך ש-

$$a = qb + r, \quad 0 \leq r < b. \quad (*)$$

$$\frac{a}{b} = q + \frac{r}{b}.$$

חלוק ב- b :

$$0 \leq \frac{r}{b} < 1, \text{ מתקיים } 0 \leq r < b, \text{ ולכן}$$

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

$$r = a - b \left\lfloor \frac{a}{b} \right\rfloor = a \bmod b.$$

הצבה חוזרת ב-(*) נותנת

מצב 2 נניח $0 < a$. לפי משפט החלוק של אוקלידס עבור השלמים \bar{r}, \bar{q} כך ש:

$$a = \bar{q}|b| + \bar{r}, \quad 0 \leq \bar{r} < |b|.$$

$$|b| = -b. \bar{r} = a \bmod |b| \text{ ו } \bar{q} = \left\lfloor \frac{a}{|b|} \right\rfloor \text{ מהמקרה הראשון:}$$

$$a = \bar{q}(-b) + \bar{r} \Rightarrow a = -\bar{q}b + \bar{r}. \quad (#)$$

מצד שני משפט החלוק עבור השלמים b, a (כלומר b בלי הערך מוחלט) קיימים שלמים r, q כך ש:

$$a = qb + r, \quad 0 \leq r < |b|.$$

השווואה של משווה (#) ל- $a = qb + r$ נותנת

$$q = -\bar{q} = -\left\lfloor \frac{a}{|b|} \right\rfloor, \quad r = \bar{r} = a \bmod |b|.$$

מצב 3 נניח $a < 0, b > 0$. משפט החלוק עבור הלשימים b , \bar{r} קיימים שלמים \bar{q} כך ש:

$$|a| = \bar{q}b + \bar{r}, \quad 0 \leq \bar{r} < b.$$

מהמקרה הראשון:

$$\bar{q} = \left\lfloor \frac{|a|}{b} \right\rfloor, \quad \bar{r} = |a| \bmod b.$$

$$-a = \bar{q}b + \bar{r} \Rightarrow a = -\bar{q}b - \bar{r}.$$

כעת השארית \bar{r} – שלילית, ואינה עומדת בתנאי $0 \leq r < b$. לכן נוסיף ונחסר ממנה אחת שלמה b :

$$a = -\bar{q}b - \bar{r} = -(\bar{q} + 1)b + (b - \bar{r}). \quad (**)$$

כך קיבלנו את הצורה הנדרשת. מצד שני עבור הלשימים a, b (כלומר a בלי הערך מוחלט) משפט החלוק קיימים שלמים r, q עוברים

$$a = qb + r, \quad 0 \leq r < b.$$

השווואה של זה עם משווה $(**)$ נותנת:

$$q = -\left\lfloor \frac{|a|}{b} \right\rfloor - 1, \quad r = b - |a| \bmod b.$$

מצב 4 נניח $a < 0, b < 0$. לפי משפט החלוק עבור $|a|, |b|$ קיימים שלמים \bar{r}, \bar{q} כך ש:

$$|a| = \bar{q}|b| + \bar{r}, \quad 0 \leq \bar{r} < |b|.$$

מ-(1) קיבל

$$\bar{q} = \left\lfloor \frac{|a|}{|b|} \right\rfloor, \quad \bar{r} = |a| \bmod |b|.$$

$$:|a| = -a, |b| = -b$$

$$-a = -\bar{q}|b| + \bar{r} \Rightarrow a = \bar{q}|b| - \bar{r}.$$

כמו קודם נוסיף ונחסר $|b|$ כדי להפוך את השארית לחיבורית:

$$\begin{aligned} a &= \bar{q}|b| - |b| + |b| - \bar{r} \\ \Rightarrow \quad a &= \bar{q}|b| + b + |b| - \bar{r} \\ \Rightarrow \quad a &= (\bar{q} + 1)|b| + |b| - \bar{r}. \end{aligned} \quad (\#)$$

מצד שני משפט החלוק עבור הלשימים b, a (לא הערכים מוחלטים שלהם) קיימים שלמים r, q עוברים:

$$a = qb + r, \quad 0 \leq r < |b|.$$

השווואה של $a = qb + r$ למשווה $(\#)$ נותנת:

$$q = \bar{q} + 1 = \left\lfloor \frac{|a|}{|b|} \right\rfloor + 1, \quad r = |b| - \bar{r} = |b| - |a| \bmod |b|.$$

שארית r	מנה q	מספר b	סימן a	סימן b	מצב
$a \bmod b$	$\left\lfloor \frac{a}{b} \right\rfloor$	+	+	1	
$a \bmod b $	$- \left\lfloor \frac{a}{ b } \right\rfloor$	-	+	2	
$b - a \bmod b$	$- \left\lfloor \frac{ a }{b} \right\rfloor - 1$	+	-	3	
$ b - a \bmod b $	$\left\lfloor \frac{ a }{ b } \right\rfloor + 1$	-	-	4	



דוגמה 1.5

מצאו את הפירוק מנתה-שארית של השלמים הבאים:

$$a = 46, b = 8 \quad \text{(א)}$$

$$a = -46, b = 8 \quad \text{(ב)}$$

$$a = 101, b = -7 \quad \text{(ג)}$$

$$a = -151, b = -12 \quad \text{(ד)}$$

פתרונות:

(א) במקרה זה $a > 0, b > 0$ אז

$$q = \left\lfloor \frac{a}{b} \right\rfloor = \left\lfloor \frac{46}{8} \right\rfloor = 5, \quad r = a \bmod b = a - b \left\lfloor \frac{a}{b} \right\rfloor = 46 - 8 \left\lfloor \frac{46}{8} \right\rfloor = 6,$$

לכן:

$$46 = (5)(8) + 6.$$

(ב) במקרה זה $a < 0, b > 0$ אז

$$q = - \left\lfloor \frac{|a|}{b} \right\rfloor - 1 = - \left\lfloor \frac{46}{8} \right\rfloor - 1 = -6$$

-1

$$\begin{aligned} r &= b - |a| \bmod b \\ &= b - \left(|a| - b \left\lfloor \frac{|a|}{b} \right\rfloor \right) \\ &= 8 - \left(46 - 8 \left\lfloor \frac{46}{8} \right\rfloor \right) \\ &= 8 - (46 - 8(5)) \\ &= 2. \end{aligned}$$

לכן:

$$-46 = (-6)(8) + 2.$$

ג) במקרה זה $a > 0, b < 0$ אז

$$q = -\left\lfloor \frac{a}{|b|} \right\rfloor = -\left\lfloor \frac{101}{7} \right\rfloor = -14 .$$

-1

$$r = a \bmod |b| = a - |b| \left\lfloor \frac{a}{|b|} \right\rfloor = 101 - 7 \left\lfloor \frac{101}{7} \right\rfloor = 101 - 7(14) = 3 .$$

לכן:

$$101 = (-14)(-7) + 3 .$$

ד) במקרה זה $a < 0, b < 0$ אז

$$q = \left\lfloor \frac{|a|}{|b|} \right\rfloor + 1 = \left\lfloor \frac{151}{12} \right\rfloor + 1 = 12 + 1 = 13 .$$

-1

$$\begin{aligned} r &= |b| - |a| \bmod |b| \\ &= |b| - \left(|a| - |b| \left\lfloor \frac{|a|}{|b|} \right\rfloor \right) \\ &= 12 - \left(151 - 12 \left\lfloor \frac{151}{12} \right\rfloor \right) \\ &= 12 - (151 - 12(12)) \\ &= 12 - 7 \\ &= 5 . \end{aligned}$$

לכן:

$$-151 = (13)(-12) + 5 .$$



1.2 מספרים ראשוניים

הגדרה 1.3 מספר ראשוני

מספר ראשוני הוא מספר שלם וחיוויי $2 \geq p$ שבו המחלקים היחידים שלו הם 1 ו- p בלבד.
ז"א p ראשוני אם התנאי הבא מתקיים:

$$a \mid p \iff a = 1 \vee p .$$

משפט 1.4 משפט הפירוק לראשוניים

כל מספר טבעי $a \geq 2$ הוא מספר ראשוני או שווה למכפלה של מספרים ראשוניים.
ז"א לכל מספר טבעי $a \geq 2$ קיימים טבעיים e_1, \dots, e_n עבורם

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

כאשר p_1, \dots, p_n מספרים ראשוניים.

דוגמה 1.6

הפירוק לראשוניים של 60 הוא:

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

דוגמה 1.7

הפירוק לראשוניים של 98 הוא:

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

הוכחה:

- נניח בשלילה שהטענה לא נכונה. אז קיימים לפחות מספר טבעי אחד שלא ראשוני וגם לא שווה למינימום של ראשוניים.
- יהי $2 \leq m$ הטבעי הקטן ביותר שלא מקיים הטענה זו. (m הוא הדוגמה הנגדית הקטנה ביותר).
- אזי m לא ראשוני וגם לא שווה למינימום של ראשוניים.
- לכן m פריך, ז"א קיימים טבעיים $2 \leq a < m$, $2 \leq b < m$ כך ש:

$$m = ab .$$

- m הוא הטבעי הקטן ביותר מסווג זה שמספריך את הטענה בעוד b , a , m הם קטנים ממש מ- m אז a ו- b בהכרח מקיימים את הטענה: ז"א a או b ראשוני או שווה למינימום של ראשוניים, ואוטו דבר עבור b .

- לכן קיימים טבעיים e_1, e_2, \dots, e_n עבורם

$$a = p_1^{e_1} p_2^{e_2} \dots p_n^{e_n}$$

כאשר p_n, \dots, p_1 מספרים ראשוניים וקיימים טבעיים f_1, \dots, f_n עבורם

$$b = q_1^{f_1} q_2^{f_2} \dots q_n^{f_n}$$

כאשר q_n, \dots, q_1 מספרים ראשוניים.

- מכאן

$$m = ab = p_1^{e_1} p_2^{e_2} \dots p_n^{e_n} q_1^{f_1} q_2^{f_2} \dots q_n^{f_n} .$$

לכן m שווה למינימום של מספרים ראשוניים, בסתיויה לכך m לא שווה למינימום של ראשוניים!**משפט 1.5 קיימים אינסוף מספרים ראשוניים**

קיימים אינסוף מספרים ראשוניים.

הוכחה: נוכיח את הטענה דרך השלילה.

נניח כי $\{p_1, \dots, p_n\} = P$ הוא הקבוצה של כל הראשוניים שקיימים וקבוצה זו נוצרת סופי. נגיד הרسلم $1 + p_n + p_1 p_2 \dots p_n = m$.לפי משפט הפירוק לזרים (ראו משפט 1.4) m הוא秩ני או שווה למינימום של ראשוניים. לפי ההנחה התחולית שלנו, אין מצב ש- m יכול להיות מספר秩ני בغالל ש- m גדול ממש מכל הראשוניים בקבוצת כל הראשוניים P . כלומר, $m > p_i$ לכל $n \leq i \leq 1$. גם לא קיים מספק秩ני p_i אשר מחלק את m . הרי

$$m \pmod{p_i} = 1 \Rightarrow p_i \nmid m .$$

הגענו לסתירה להמשפט הפירוק לזרים. לכן קיימים אינסוף מספרים ראשוניים.

1.3 המחלק המשותף הגדול ביותר

הגדירה 1.4 המחלק המשותף הגדול ביותר (gcd).

יהיו a, b שלמים. המחלק המשותף הגדול ביותר של a ו- b מסומן $\text{gcd}(a, b)$ ומוגדר להיות השם החיוויי grootste gemeenschappelijke deler ביטר. a וגם b .

הסימון gcd מנובע מהשם אנגלי "greatest common divisor".

דוגמה 1.8

$$\text{gcd}(2, 6) = 2 ,$$

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

$$\text{gcd}(24, 5) = 1 ,$$

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

$$\text{gcd}(14, 12) = 2 ,$$

$$\text{gcd}(8, 12) = 4 .$$

הגדירה 1.5 כפולה המשותפת הקטנה ביותר

יהיו a, b שלמים. הcpfולה המשותפת הקטנה ביותר ביטר מסומנת $\text{lcm}(a, b)$ ומוגדרת להיות השם החיוויי kleinste gemeenschappelijke veelvoud ביטר. a וגם b מחלקים אותו.

הסימון lcm מנובע מהשם אנגלי "lowest common multiple".

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

יהיו a, b שלמים. אומרים כי a ו- b **מספרים זרים** אם

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

כלומר, אין אף מספר גדול מאחד שמחלק את שניהם.

משפט 1.6 שיטת פירוק לראשונה לחישוב \gcd

יהיו a, b שלמים חיוביי כך שהפירוק לראשוניים שלהם הם:

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

از ה- $\gcd(a, b)$ הינו

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

הוכחה: נסמן $.d | b$. ראשית נראה כי $d | a$ וגם $d | b$.

$$\begin{aligned} a &= p_1^{e_1} \dots p_i^{e_i} \dots p_n^{e_n} \\ &= (p_1^{e_1 - \min(e_1, f_1)} \dots p_i^{e_i - \min(e_i, f_i)} \dots p_n^{\min(e_n, f_n)}) (p_1^{\min(e_1, f_1)} \dots p_i^{\min(e_i, f_i)} \dots p_n^{\min(e_n, f_n)}) \\ &= qd \end{aligned}$$

כאשר $e_i - \min(e_i, f_i) \geq 0$ החזקה $q = p_1^{e_1 - \min(e_1, f_1)} \dots p_i^{e_i - \min(e_i, f_i)} \dots p_n^{\min(e_n, f_n)}$ הוא מספר שלם. אז $.d | a$.

באופן דומה אפשר להוכיח שגם $.d | b$.

הוכחנו כי d הוא מחלק משותף של a ו- b . כעת נראה כי d הוא המחלק המשותף הגדול ביותר.

נניח בsvilleה שקיימים c שלם כך ש- $c | a$ ו- $c | b$ ו- $c > d$. כלומר נניח שקיימים מחלק c של a ושל b שגדול יותר מ- d . מכיוון ש- $c | a$ ו- $c | b$ אז בפירוק לראשוניים של c מופיע רק אותם ראשוניים $\{p_1, \dots, p_n\}$ שמופיעים בפירוקים של a ושל b . לכן יש לנו:

$$c = p_1^{g_1} \dots p_i^{g_i} \dots p_n^{g_n}.$$

מכיוון ש- $c | a$ אז $g_i \leq e_i$ לכל i , ומכיוון ש- $c | b$ אז $g_i \leq f_i$ לכל i . לכן

$$g_i \leq \min(e_i, f_i) \quad \text{לכל } i.$$

לפיכך

$$c = p_1^{g_1} \dots p_i^{g_i} \dots p_n^{g_n} \leq p_1^{\min(e_1, f_1)} \dots p_i^{\min(e_i, f_i)} \dots p_n^{\min(e_n, f_n)} = d$$

וז"א בסתיו $c > d$.

**דוגמה 1.10**

מצאו את $\gcd(19200, 320)$.

פתרונות:

הפיורוקים הראשונים של 19200 ושל 320 הם

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

לכן

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

דוגמה 1.11

מצאו את $\gcd(154, 36)$

פתרון:

הפיורוקים הראשונים של 154 ושל 36 הם

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

נרשום את 154 ו- 36 כמכפלות של אותם ראשוניים על ידי הוספת חזקות של 0:

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

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

משפט 1.7 \gcd של מספרים ראשוניים

יהיו p, q שני מספרים ראשוניים שונים ($p \neq q$). מתקיים

$$\gcd(p, q) = 1 .$$

הוכחה:

שיטת 1: הוכחה ישירה

p הוא ראשוני אז הפירוק הראשון לשלו הוא

$$p = p^1 q^0 .$$

q הוא ראשוני אז הפירוק הראשון לשלו הוא

$$q = p^0 q^1 .$$

לפי משפט 1.6,

$$\gcd(p, q) = p^{\min(1,0)} q^{\min(0,1)} = p^0 q^0 = 1 .$$

שיטת 2: הוכחה בשילילה

יהי $d = \gcd(p, q)$ ונניח כי $p < q$. אז d נמצא בטוחה של שלמים האפשריים $1 \leq d \leq q$.

נניח בשילילה כי $d > 1$.

.

מכיוון ש- d מחלק משותף של p ושל q אז $d | p$ וגם $d | q$.

$d | p$ אז זה גורר $d | q$, בסתיויה לכך ש- p ראשוני.



משפט 1.8 שיטת פירוק לראשוניים לחישוב lcm

יהיו a, b שלמים חיוביים כך שהפירוק לראשוניים שלהם הם:

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

ה- $\text{lcm}(a, b)$ נתונה על ידי הנוסחה

$$\text{lcm}(a, b) = p_1^{\max(e_1, f_1)} p_2^{\max(e_2, f_2)} \dots p_n^{\max(e_n, f_n)}$$

הוכחה: נסמן $D = p_1^{\max(e_1, f_1)} p_2^{\max(e_2, f_2)} \dots p_n^{\max(e_n, f_n)}$

$$\begin{aligned} D &= p_1^{\max(e_1, f_1)} p_2^{\max(e_2, f_2)} \dots p_n^{\max(e_n, f_n)} \\ &= (p_1^{\max(e_1, f_1) - e_1} \dots p_i^{\max(e_i, f_i) - e_i} \dots p_n^{\max(e_n, f_n) - e_n}) (p_1^{e_1} \dots p_i^{e_i} \dots p_n^{e_n}) \\ &= qa \end{aligned}$$

כאשר $\max(e_i, f_i) - e_i \geq 0$ החזקה $q = p_1^{\max(e_1, f_1) - e_1} \dots p_i^{\max(e_i, f_i) - e_i} \dots p_n^{\max(e_n, f_n) - e_n}$ אז q הוא מספרשלם. $a \mid D$.

באופן דומה אפשר להוכיח שגם $b \mid D$.

הוכחנו כי D הוא כפולה של a ושל b . בעת נראה כי D הוא הכפולה של a ושל b הקטנה ביותר.

נניח בsvilleה שקיימים C שלם כך $a \mid C$ ו- $b \mid C$ ו- $C < D$. כלומר נניח שקיימים C אשר כפולה של a ושל b שקיימת יותר מ- D . מכיוון ש- $b \mid C$ אז כל הראשוניים בקבוצה $\{p_1, \dots, p_n\}$ אשר בפירוקים של a ושל b חייבים להופיע גם בפירוק לראשוניים של C . לכן יש לנו:

$$C = p_1^{g_1} \dots p_i^{g_i} \dots p_n^{g_n} \dots$$

מכיוון ש- $e_i \leq g_i$ לכל i , ומכיון ש- $b \mid C$ אז $f_i \leq g_i$ לכל i . לכן

$$\max(e_i, f_i) \leq g_i \quad \text{לכל } i.$$

לפיכך

$$C = p_1^{g_1} \dots p_i^{g_i} \dots p_n^{g_n} \geq p_1^{\max(e_1, f_1)} \dots p_i^{\max(e_i, f_i)} \dots p_n^{\max(e_n, f_n)} = D$$

ז"א $C \geq D$ בסתירה לכך ש- $C < D$.

משפט 1.9

יהיו a, b שלמים חיוביים. אז $\gcd(a, b) \text{lcm}(a, b) = ab$.

הוכחה: יהיו הירוקים לראשוניים של a ושל b :

$$a = p_1^{e_1} \dots p_n^{e_n}, \quad b = p_1^{f_1} \dots p_n^{f_n}.$$

אזי ממפט 1.6 ומממפט 1.8:

$$\begin{aligned} \gcd(a, b) \operatorname{lcm}(a, b) &= p_1^{\min(e_1, f_1)} \cdots p_n^{\min(e_n, f_n)} p_1^{\max(e_1, f_1)} \cdots p_n^{\max(e_n, f_n)} \\ &= p_1^{\min(e_1, f_1) + \max(e_1, f_1)} \cdots p_n^{\min(e_n, f_n) + \max(e_n, f_n)} \\ &= p_1^{e_1+f_1} \cdots p_n^{e_n+f_n} \\ &= p_1^{e_1} \cdots p_n^{e_n} p_1^{f_1} \cdots p_n^{f_n} \\ &= ab, \end{aligned}$$

כasher נעזרנו בהזהות

$$\min(e, f) + \max(e, f) = e + f.$$



1.4 האלגוריתם של אוקלידס

משפט 1.10 האלגוריתם של אוקלידס

יהיו a, b מספרים שלמים חיוביים. קיים אלגוריתם אשר נותן את $d = \gcd(a, b)$ כדלקמן. ראשית מאותחים:

$:r_1 \rightarrow r_0$

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

אם $r_1 = b \neq 0$ אז מתחילה את הלולאה. בשלב $i = 1$ מחשבים את q_1 ו- r_2 כך:

$$q_1 = \left\lfloor \frac{r_0}{r_1} \right\rfloor, \quad r_2 = r_0 - q_1 r_1 = r_0 - \left\lfloor \frac{r_0}{r_1} \right\rfloor r_1.$$

אם $r_2 \neq 0$ ממשיכים לשלב $i = 2$ שבו מחשבים את q_2 ו- r_3 כך:

$$q_2 = \left\lfloor \frac{r_1}{r_2} \right\rfloor, \quad r_3 = r_1 - q_2 r_2 = r_1 - \left\lfloor \frac{r_1}{r_2} \right\rfloor r_2.$$

התהליק ממשיך עד שנקבל $0 = r_{n+1}$ בשלב ה- n -ית. כל השלבים של התהליק הם כדלקמן:

$$q_1 = \left\lfloor \frac{r_0}{r_1} \right\rfloor \quad r_2 = r_0 - q_1 r_1 = r_0 - \left\lfloor \frac{r_0}{r_1} \right\rfloor r_1 \quad :i = 1$$

$$q_2 = \left\lfloor \frac{r_1}{r_2} \right\rfloor \quad r_3 = r_1 - q_2 r_2 = r_1 - \left\lfloor \frac{r_1}{r_2} \right\rfloor r_2 \quad :i = 2$$

$$q_3 = \left\lfloor \frac{r_2}{r_3} \right\rfloor \quad r_4 = r_2 - q_3 r_3 = r_2 - \left\lfloor \frac{r_2}{r_3} \right\rfloor r_3 \quad :i = 3$$

\vdots

$$q_{n-1} = \left\lfloor \frac{r_{n-2}}{r_{n-1}} \right\rfloor \quad r_n = r_{n-2} - q_{n-1} r_{n-1} = r_{n-2} - \left\lfloor \frac{r_{n-2}}{r_{n-1}} \right\rfloor r_{n-1} \quad :i = n-1$$

$$q_n = \left\lfloor \frac{r_{n-1}}{r_n} \right\rfloor \quad r_{n+1} = 0 \quad :i = n$$

התהליק מסתיים בשלב ה- n -ית אם $0 = r_{n+1}$. ואז הפלט של האלגוריתם הוא

למטה רשום ייצוג פסאודו-קוד של האלגוריתם של אוקלידס:

Algorithm 1 האלגוריתם של אוקליידס

```

1: Input: Integers  $a, b$  .
2:  $r_0 \leftarrow a$ 
3:  $r_1 \leftarrow b$ 
4:  $n \leftarrow 1$ 
5: while  $r_n \neq 0$  do
6:    $q_n \leftarrow \left\lfloor \frac{r_{n-1}}{r_n} \right\rfloor$ 
7:    $r_{n+1} \leftarrow r_{n-1} - q_n r_n$ 
8:    $n \leftarrow n + 1$ 
9: end while
10:  $n \leftarrow n - 1$ 
11: Output:  $r_n = \gcd(a, b)$ 
```

דוגמה 1.12מצאו את $\gcd(1071, 462)$ **פתרון:**

$$a = 1071, b = 462$$

נתחל $r_1 = b = 462$ ו $r_0 = a = 1071$ נבצע את האלגוריתם של אוקליידס:

r_i	q_i	שלב
$r_2 = r_0 - q_1 r_1$ $= 1071 - (2)(462) = 147$	$q_1 = \left\lfloor \frac{r_0}{r_1} \right\rfloor = \left\lfloor \frac{1071}{462} \right\rfloor = 2$: $i = 1$
$r_3 = r_1 - q_2 r_2$ $= 462 - (3)(147) = 21$	$q_2 = \left\lfloor \frac{r_1}{r_2} \right\rfloor = \left\lfloor \frac{462}{147} \right\rfloor = 3$: $i = 2$
$r_4 = r_2 - q_3 r_3$ $= 147 - (7)(21) = 0$	$q_3 = \left\lfloor \frac{r_2}{r_3} \right\rfloor = \left\lfloor \frac{147}{21} \right\rfloor = 7$: $i = 3$

לפיכך $\gcd(1071, 462) = r_3 = 21$ **דוגמה 1.13**מצאו את $\gcd(26, 11)$ **פתרון:**

$$a = 26, b = 11$$

נתחל $r_1 = b = 11$ ו $r_0 = a = 26$ נבצע את האלגוריתם של אוקליידס:

r_i	q_i	שלב
$r_2 = r_0 - q_1 r_1$ $= 26 - (2)(11) = 4$	$q_1 = \left\lfloor \frac{r_0}{r_1} \right\rfloor = \left\lfloor \frac{26}{11} \right\rfloor = 2$: $i = 1$
$r_3 = r_1 - q_2 r_2$ $= 11 - (2)(4) = 3$	$q_2 = \left\lfloor \frac{r_1}{r_2} \right\rfloor = \left\lfloor \frac{11}{4} \right\rfloor = 2$: $i = 2$
$r_4 = r_2 - q_3 r_3$ $= 4 - (1)(3) = 1$	$q_3 = \left\lfloor \frac{r_2}{r_3} \right\rfloor = \left\lfloor \frac{4}{3} \right\rfloor = 1$: $i = 3$
$r_5 = r_3 - q_4 r_4$ $= 3 - (3)(1) = 0$	$q_4 = \left\lfloor \frac{r_3}{r_4} \right\rfloor = \left\lfloor \frac{3}{1} \right\rfloor = 3$: $i = 5$

לפי כן $\gcd(26, 11) = r_4 = 1$



משפט 1.11 משפט בז' (Bezout's identity)

יהיו a, b . קיימים שלמים s, t, d עבורם

$$sa + tb = d , \quad (1.2)$$

כאשר $d = \gcd(a, b)$.

משפט 1.12 האלגוריתם המוכפל של אוקלידס

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

$$d = sa + tb$$

כאשר $d = \gcd(a, b)$. ראשית מתחילה:

$$r_0 = a , \quad r_1 = b , \quad s_0 = 1 , \quad s_1 = 0 , \quad t_0 = 0 , \quad t_1 = 1 .$$

אם $0 \neq r_1 = b$ מבצעים האיטרציה הראשונה של הלולאה. בשלב $i = 1$ מחשבים את q_1, r_2, s_2, t_2 כך:

$$q_1 = \left\lfloor \frac{r_0}{r_1} \right\rfloor , \quad r_2 = r_0 - q_1 r_1 , \quad s_2 = s_0 - q_1 s_1 , \quad t_2 = t_0 - q_1 t_1 .$$

אם $0 \neq r_2$ מבצעים לאיטרציה $i = 2$ שבה מחשבים את q_2, r_3, s_3, t_3 כך:

$$q_2 = \left\lfloor \frac{r_1}{r_2} \right\rfloor , \quad r_3 = r_1 - q_2 r_2 , \quad s_3 = s_1 - q_2 s_2 , \quad t_3 = t_1 - q_2 t_2 .$$

התהlik ממשיך עד השלב ה- n שבו מקבלים r_{n+1} , ו- 0 פולטים $d = r_n = \gcd(a, b)$, $s = s_n$, $t = t_n$. כל השלבים של האלגוריתם הם כדלקמן:

$q_1 = \left\lfloor \frac{r_0}{r_1} \right\rfloor$	$r_2 = r_0 - q_1 r_1$	$s_2 = s_0 - q_1 s_1$	$t_2 = t_0 - q_1 t_1$	שלב 1:
$q_2 = \left\lfloor \frac{r_1}{r_2} \right\rfloor$	$r_3 = r_1 - q_2 r_2$	$s_3 = s_1 - q_2 s_2$	$t_3 = t_1 - q_2 t_2$	שלב 2:
				⋮
$q_i = \left\lfloor \frac{r_{i-1}}{r_i} \right\rfloor$	$r_{i+1} = t_{i-1} - q_i t_i$	$s_{i+1} = s_{i-1} - q_i s_i$	$t_{i+1} = t_{i-1} - q_i r_i$	שלב i :
				⋮
$q_{n-1} = \left\lfloor \frac{r_{n-2}}{r_{n-1}} \right\rfloor$	$r_n = t_{n-2} - q_{n-1} t_{n-1}$	$s_n = s_{n-2} - q_{n-1} s_{n-1}$	$t_n = t_{n-2} - q_{n-1} r_{n-1}$	שלב $n-1$:
$q_n = \left\lfloor \frac{r_{n-1}}{r_n} \right\rfloor$	$r_{n+1} = t_{n-1} - q_n t_n$	$s_{n+1} = s_{n-1} - q_n s_n$	$t_{n+1} = t_{n-1} - q_n r_n$	שלב n :

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

למטה רשום ייצוג פסאודו-קוד של האלגוריתם:

אוקלידס של המוכל האלגוריתם 2

```

1: Input: Integers  $a, b$  .
2:  $r_0 \leftarrow a$ 
3:  $r_1 \leftarrow b$ 
4:  $s_0 \leftarrow 1$ 
5:  $s_1 \leftarrow 0$ 
6:  $t_0 \leftarrow 0$ 
7:  $t_1 \leftarrow 1$ 
8:  $n \leftarrow 1$ 
9: while  $r_n \neq 0$  do
10:    $q_n \leftarrow \left\lfloor \frac{r_{n-1}}{r_n} \right\rfloor$ 
11:    $r_{n+1} \leftarrow r_{n-1} - q_n r_n$ 
12:    $s_{n+1} \leftarrow s_{n-1} - q_n s_n$ 
13:    $t_{n+1} \leftarrow t_{n-1} - q_n t_n$ 
14:    $n \leftarrow n + 1$ 
15: end while
16:  $n \leftarrow n - 1$ 
17: Output:  $r_n, s_n, t_n$   $\triangleright d = r_n = \gcd(a, b)$  and  $d = sa + tb$  where  $s = s_n, t = t_n.$ 

```

דוגמה 1.14 (אלגוריתם המוכל של אוקלידס)

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

פתרונות:

מאתחלים:

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

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

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

$$sa + tb = -9(240) + 47(46) = 2 .$$



דוגמה 1.15 (אלגוריתם המוכל של איוקליידס)

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

פתרונות:
מאתחלים:

$$\begin{array}{ll} r_0 = a = 326 , & r_1 = b = 78 , \\ s_0 = 1 , & s_1 = 0 , \\ t_0 = 0 , & t_1 = 1 . \end{array}$$

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

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

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

1.5 יחס השקילות המודולרית

הגדרה 1.7 שיקילות מודולרית

יהיו n , a, b שלמים ($0 \neq n$). היחס:

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

אומר כי " n מחלק את ההפרש $a - b$ ".
כלומר:

$$a \equiv b \pmod{n} \quad \text{אם ורק אם} \quad n \mid a - b .$$

דוגמה 1.16

הוכחו כי

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

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

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

פתרונות:

(א)

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

(ב)

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

$$(ג) 7 - 2 = 5$$

לא קיימים שלם q כך ש- $7 - 2 = 4q$ אבל $7 - 2 \nmid 5$

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

ההגדרה 1.7 של שיקילות מודולרית בין שלמים גוררת למשפט הבא באופן טבעי:

משפט 1.13

יהיו a, b, r שלמים, $r \neq 0$.

$$a = qr + b \quad \text{קיים שלם } q \text{ עבורו} \quad \text{אם ורק אם} \quad n \mid a - b \quad \text{אם ורק אם} \quad a \equiv b \pmod{n}$$

הוכחה:

הגרירה הראשונה r נובעת יש מההגדרה 1.7 של יחס שקולות.

נראה את הגרירה השנייה:

$$a = qn + b \iff a - b = qn \text{ עבור } q \mid a - b$$

משפט 1.14 תכונות של יחס השקילות המודולרי

יהיו a, b שלמים ו- $0 \neq n$ שלם.

(1) רפלקסיבי:

$.b \equiv a \pmod{n}$ אם ורק אם $a \equiv b \pmod{n}$

(2) סימטרי: אם $a \equiv c \pmod{n}$ אז $b \equiv c \pmod{n}$ אז $a \equiv b \pmod{n}$

(3) טרנזיטיבי: אם $a \equiv b \pmod{n}$ ו- $b \equiv c \pmod{n}$ אז $a \equiv c \pmod{n}$

הוכחה:

(1) רפלקסיבי:

$.a \equiv a \pmod{n}$ מתקיים $a = 0 \cdot n + a$, כלומר $a \mid a - a$, לכן $n \mid a - a$.

(2) סימטרי:

נניח ש- $a \equiv b \pmod{n}$. אז קיימים שלמים q עבורו

$$a = qn + b \iff b = (-q)n + a .$$

זה אומר קיימים שלמים $\bar{q} = -q$ עבורו $b = \bar{q}n + a$, כלומר $a \equiv b \pmod{n}$.

(3) טרנזיטיבי: נניח ש- $a \equiv b \pmod{n}$ ו- $b \equiv c \pmod{n}$

$$\left. \begin{array}{l} a = qn + b \\ b = \bar{q}n + c \end{array} \right\} \Rightarrow a = qn + \bar{q}n + c = (b + \bar{q})n + c$$

זה אומר קיימים שלמים $Q = q + \bar{q}$ עבורו $a = Qn + c$, כלומר $a \equiv c \pmod{n}$.

משפט 1.15 הקשר בין יחס השקילות מודולרי והשארית

יהיו $a, b, n > 0$ שלמים.

$$a \equiv b \pmod{n} \iff a \bmod n = b \bmod n$$

הוכחה:

כיוון \Leftarrow

נניח ש- $a \equiv b \pmod{n}$. אז קיימים שלם Q כך ש:

$$a = qn + b.$$

לפי משפט החילוק של אוקלידס,

$$b = \bar{q}n = r_1, \quad r_1 = b \pmod{n}.$$

לכן

$$a = (q + \bar{q})n + r_1 = Qn + r_1$$

כאשר \bar{q} שלם ו- $r_1 = b \pmod{n}$ הוא השארית n . מכאן נובע ש:

$$a \pmod{n} = a - n \left\lfloor \frac{a}{n} \right\rfloor = Qn + r_1 - Qn = r_1$$

$$a \pmod{n} = r_1 = \pmod{n} \text{ נ"א}$$

כיוון \Rightarrow

נניח ש- $a \pmod{n} = b \pmod{n}$. אז

$$a - n \left\lfloor \frac{a}{n} \right\rfloor = b - n \left\lfloor \frac{b}{n} \right\rfloor \Rightarrow a = \left(\left\lfloor \frac{a}{n} \right\rfloor - \left\lfloor \frac{b}{n} \right\rfloor \right) n + b \Rightarrow a = qn + b$$

כלומר קיימים שלם $q = \left\lfloor \frac{a}{n} \right\rfloor - \left\lfloor \frac{b}{n} \right\rfloor$ עבורו $a = qn + b$ ו- $a \equiv b \pmod{n}$.

משפט 1.16 חיבור וכפל של שלמים השקולים מודולריים

יהיו a, b, c, d שלמים ו- $0 \neq n$ שלם.

(1) חיבור:

אם $a + c \equiv b + d \pmod{n}$ אז $c \equiv d \pmod{n}$ וכן $a \equiv b \pmod{n}$

(2) כפל:

אם $ac \equiv bd \pmod{n}$ אז $c \equiv d \pmod{n}$ וכן $a \equiv b \pmod{n}$

הוכחה:

(1) חיבוריות:

אם $a \equiv b \pmod{n}$ אז קיימים שלם q עבורו $a = qn + b$ וכן אם $c \equiv d \pmod{n}$ אז קיימים שלם q עבורו $c = \bar{q}n + d$.

$$a + c = (q + \bar{q})n + b + d \Rightarrow a + c = Qn + (b + d),$$

כאשר $Q = q + \bar{q}$. הוכחנו שקיימים שלם Q עבורו $a + c = Qn + b + d$ וכך $a + c \equiv b + d \pmod{n}$.

(2) כפל:

אם $a \equiv b \pmod{n}$ אז קיימים שלם q עבורו $a = qn + b$ וכן אם $c \equiv d \pmod{n}$ אז קיימים שלם q עבורו $c = \bar{q}n + d$.

$$ac = (qn + b)(\bar{q}n + d) \Rightarrow ac = (q\bar{q}n^2 + dq + b\bar{q}n + bd) \Rightarrow ac = Qn + bd,$$

כאשר $Q = (q\bar{q}n^2 + dq + b\bar{q})$. הוכחנו שקיימים שלם Q עבורו $ac = Qn + bd$ וכך $ac \equiv bd \pmod{n}$.

שיעור 2

חוגים מתמטיים

2.1 הפונקציה אוילר

הגדרה 2.1 פונקציית אוילר

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

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

דוגמה 2.1

מכיוון ש- $26 = 2 \times 13$, הערכים של a עבורם $\gcd(a, 26) = 1$ הם

$$\{1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25\} .$$

זהו יש בדיק 12 ערכים של a עבורם $\gcd(a, 26) = 1$

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

משפט 2.1 הפרק הראשונים של פונקציית אוילר

יהי $2 \leq m$ מספר שלם ונניח כי הפרק למספרים ראשוניים שלו הוא

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

אז

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

דוגמה 2.2

מצאו את $\phi(60)$.

פתרון:

$$60 = 2^2 \times 3^1 \times 5^1$$

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



דוגמה 2.3

חשבו את $\phi(24)$

פתרונות:

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

לכן

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

משפט 2.2אם p מספר ראשוני אז

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

הוכחה: תרגיל בית.**משפט 2.3**אם p מספר ראשוני אז

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

הוכחה: תרגיל בית.**משפט 2.4**אם a, b שלמים זרים (כלומר $(\gcd(a, b) = 1)$ אז

$$\phi(a \cdot b) = \phi(a) \cdot \phi(b) .$$

הוכחה:

- נניח ש- a, b זרים.
- נניח שהפירוקים הראשוניים של a ו- b הם:

$$a = p_1^{e_1} \cdots p_n^{e_n}, \quad b = q_1^{f_1} \cdots q_m^{f_m} .$$
- a ו- b זרים שכן הראשוניים בין השני הפירוקים יכולים להיות שונים, כלומר $p_i \neq q_j$ לכל $i, j \leq \min(n, m)$.
- לכן אם הפירוק הראשוני של ab הוא

$$ab = p_1^{e_1} \cdots p_n^{e_n} q_1^{f_1} \cdots q_m^{f_m} .$$

- מכאן

$$\phi(ab) = (p_1^{e_1} - p_1^{e_1-1}) \cdots (p_n^{e_n} - p_n^{e_n-1}) (q_1^{f_1} - q_1^{f_1-1}) \cdots (q_m^{f_m} - q_m^{f_m-1}) = \phi(a)\phi(b) .$$

משפט 2.5

אם p ו- q מספרים ראשוניים שונים אז

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

הוכחה: תרגיל בית.

2.2 החוג \mathbb{Z}_m **הגדרה 2.2 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

$$a, b \in \mathbb{Z}_m \quad a \oplus b = (a + b) \bmod m \quad a \odot b = ab \bmod m .$$

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

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

דוגמה 2.4

חשבו את 11×13 ב- \mathbb{Z}_{16} .

פתרונות:

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

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

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

משפט 2.6 תכונות של החוג \mathbb{Z}_m

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

1. סגירה תחת חיבור:

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

2. חוק החלוף 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 $m - a$, א"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 החלוף 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 אומירות כי \mathbb{Z}_m הינו "חבורה מתמטית".
יחד עם תכונה 2, \mathbb{Z}_m הינו חבורה אбелית.
כל התכונות 1-10 אומירות כי \mathbb{Z}_m הוא חוג מתמטי.

הגדלה 2.3 איבר ההופכי ב-

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 2.7

נתון היחס שקולות

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

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

הוכחה:

כיוון

נניח בשילילה כי למשוואה m יש פתרון יחיד $x = x_1$ אבל $1 < x < m$.

אזי $ax_1 \equiv y \pmod{m}$ ולכן קיימים q, r שלם עבורו $ax_1 \equiv qm + y \pmod{m}$
לכן $ax_1 + \frac{am}{d} = qm + y + \frac{am}{d}$ הוא שלם ולכן $\frac{am}{d}$ קיימים שלם $Q = q + \frac{a}{d}$, א"א $a \left(x_1 + \frac{m}{d} \right) = \left(q + \frac{a}{d} \right) m + y$ כך ש-

$$a \left(x_1 + \frac{m}{d} \right) = Qm + y \Rightarrow a \left(x_1 + \frac{m}{d} \right) \equiv y \pmod{m}$$

ולכן $x_2 = x_1 + \frac{m}{d}$ כאשר $ax_2 \equiv y \pmod{m}$

לכן x_2 הוא גם פתרון, בסתירה לכך שיש רק פתרון יחיד.

כיוון ⇒

נניח ש: $\gcd(a, m) = 1$ ונניח בשלילה כי יש שני פתרונות $(x_1 \pmod{26}, x_2 \pmod{26})$. כלומר:

$$ax_1 \equiv y \pmod{m} \quad \text{և} \quad ax_2 \equiv y \pmod{m}.$$

לפי טרנסיטיביות m ולבן $ax_1 \equiv ax_2 \pmod{m}$.

■ $x_1 \not\equiv x_2 \pmod{26}$ לכן $a \nmid m$ שכן $m \mid x_1 - x_2$, בסתירה לכך ש- $\gcd(a, m) = 1$

מסקנה 2.1

יהי $a \in \mathbb{Z}_m$. קיים איבר הופכי $a^{-1} \in \mathbb{Z}_m$ כך ש- 2.3 מקיים את התנאי

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

אם ורק אם $\gcd(a, m) = 1$

הוכחה:

כיוון ⇔

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

כיוון ⇒

נניח ש- $ax + (-q)m = 1$. אז קיימים שלם q עבורו $ax = qm + 1$. נעביר אגפים ונקבל: $ax \equiv 1 \pmod{m}$. לכן $\gcd(a, m) = 1$.

■

דוגמה 2.5

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

פתרונות:

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

$$\begin{array}{ll} r_0 = a = 26, & r_1 = b = 11, \\ s_0 = 1, & s_1 = 0, \\ t_0 = 0, & t_1 = 1. \end{array}$$

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

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

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

מכאן אנחנו רואים כי $1 = \gcd(26, 11)$ ולכן לפי משפט 2.7 ההופכי של 11 קיים ב- \mathbb{Z}_{26} מחשבים את האיבר ההופכי לפי השיטה הבאה:

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

■

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 2.4 פונקציה אוילר ($\phi(m)$)

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

(שםו לב ההגדרה הזאת זהה להגדרה 2.1)

מסקנה 2.2 מספר איברים הפיכיים ב-

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 אולם האיברים הם האיברים הפיכיים של \mathbb{Z}_m .

2.3 הפיכת מטריצות בחוג \mathbb{Z}_m

הגדרה 2.5 המטריצה של קופקטוריים

תהי $A \in \mathbb{R}^{n \times n}$.

הkopקטור 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 .

הגדה 2.6 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 2.8 נוסחת למטריצה ההפכית

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

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

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

2.6 דוגמה

מצאו את הההפכית של

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

פתרון:

$$|A| = 11 \cdot 7 - 8 \cdot 3 = 53 = 1 \mod 26 .$$

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

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

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

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

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

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

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

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

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

לפיכך

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

■

דוגמה 2.7

מצאו את ההפכית של

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

פתרון:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

לפיatz

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

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

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

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

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

לפיatz

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

בדיקה:

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



שיעור 3

הצפנים הבסיסיים

1.3. מושג של קריפטו-מערכת

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

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

הגדרה 3.1 צופן

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

(1) E מסמן קבוצה של טקסט גלי, plaintext,

(2) C מסמן קבוצה של טקסט מוצפן, ciphertext,

(3) K מסמן את מרחב המפתח, keyspace

(4) לכל $k \in K$ יש שתי פונקציות: כלל מצפן $e \in E$ וכלל מפענה $d \in D$:

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

כך ש-

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

לכל איבר של מרחב הטקסט גלי P

נניח כי הודעה הנשלחה על ידי אליס לבוב היא הרץ האותיות

$$X = x_1 x_2 \cdots x_n$$

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

$$y_i = e_k(x_i)$$

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

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

הרץ זהה נשלח מעל גבי העורך. אשר bob מקבל את Y והוא מפענחת אותו באמצעות הפונקציה d_k וכך הוא מקבל הרץ אותיות של טקסט גלי המקורי

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

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

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

כאשר $x_2 \neq x_1$ ואז לבוב לא יוכל לדעת אם y הפענחה של x_1 או x_2 .

3.2 צופן ההזהה

הגדרה 3.2 צופן ההזהה

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

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

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

-1

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

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

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

דוגמה 3.1

נתון טקסט גלי

shamoon

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

פתרונות:

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

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

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

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

שלב 3) נעביר את הרצץ מספרים לטקסט מוצפן:

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

текסט מוצפן המתקבל הוא
DSLXZZY



3.2 דוגמה

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

UJCNQO

מצאו את הטקסט גלי.

פתרונות:

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

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



3.3 דוגמה

נתון הטקסט מוצפן הבא:

QRQXFJANHXD

מצאו את הטסט גלי

פתרונות:

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

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

בשלב זה מצאנו את הטקסט גליוי:
hihowareyou .

המפתח הוא $.k = 9$

משפט 3.1 צופן חזזה ניתן לפענוח

צופן חזזה ניתן לפענוח. ככלומר, אם $d_k(x) = x - k \bmod 26$ ו- $e_k(x) = x + k \bmod 26$ אז

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

הוכחה:

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

נזכיר כי $(x + k) \bmod 26 = x + k - 26q$ כאשר q הוא מספר שלם, ונקבל

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

מכיוון ש- q הוא מספר שלם אז $x - 26q \equiv x \pmod{26}$ לכן לפי משפט :

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

3.3 צופן האפייני

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

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

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

כדי שפונקציה יהיה אפשרי נדרש כי הפונקציה הזאת חד-חד-ערכית. במלילים אחרות, נדרש כי לbijection (יחס שקולות)

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

יש פתרון יחיד ל- x .

למיטה נוכח כי אכן יש פתרון יחיד אם ורק אם $\gcd(a, 26) = 1$

משפט 3.2

לייחס שקולות

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

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

הוכחה:

כיוון \Leftarrow

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

כיוון \Rightarrow

נניח ש- $1 \equiv ax + (-q)(26) \pmod{26}$. אז קיימים שלם q עבורו $1 = q(26) + ax$. נעביר אגפים ונקבל: $ax \equiv 1 - q(26) \pmod{26}$. לכן קיימים שלמים x ו- $y = -q$ כך ש- $1 \equiv ax + y(26) \pmod{26}$. █

דוגמה 3.4

בדקו אם הפונקציה

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

כלל מצפין תקין, כלומר בדקו אם קיים כלל מפענה.

פתרון:

ולכן לא יכולה להיות כלל מצפין. $e(x) = 4x + 7 \pmod{26}$ אינה כלל מצפין תקין, בגלל שהיא לא חד-חד-ערכית $\gcd(4, 26) = 2$, או הפונקציה $e(x) = 4x + 7 \pmod{26}$ היא פונקציה מוגבלת.

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

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

בעוד

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

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

הגדרה 3.3 צופן האפיני

יהי $P = C = \mathbb{Z}_{26}$ ויהי

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

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

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

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

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

כלל 3.1

הפירוק לראשוניים של 26 הינו

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

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

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

ז"א יש בדיק 12 ערכי a עבורם $\gcd(a, 26) = 1$.

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

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

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

דוגמה 3.5

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

1) רשמו את כלל המצפין.

2) רשמו את כלל המעננה.

3) בדקו כי התנאי

מתתקיים.

פתרונות:

1) הכלל מצפין הוא

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

2) הכלל מפענץ 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 מפענץ המתקיים מקיים x

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

**דוגמה 3.6**

בעזרת הצופן של דוגמה 3.5:

1) מצאו את הטקסט מוצפן של הטקסט גליי hot .**2)** בדקו שהפעולה של הכלל מפענץ על הטקסט מוצפן מחזיר את טקסט גליי hot .**פתרונות:****סעיף 1)** נעביר את הواتיות של hot לערכים של \mathbb{Z}_{26} :

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

נפעיל את הכלל מצפין על הערכים x :

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

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

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

מכאן נקבל

$x \in P$	h	\circ	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 המתכבר הוא
 AXG

סעיף 2) הכלל מפענה הוא

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

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

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

נפעיל את הכלל מפענה על הערכים y :

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

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

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

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

לכן הטקסט גלי המתקבל הוא
hot
כנדרש.

3.7 דוגמה

נתון הטקסט מוצפן

ACSE

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

פתרון:

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

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

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

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

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

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

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

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

3.4 צופן ויז'נר

צופן ההזזה וצופן ההחלפה דוגמאות של צופן מונואלפביתי: כל TWO אלפביתיות ב- P נתאים לטו אלפביתית יחיד ב- C . צופן ויז'נר הוא צופן פוליאלפביתי: אין מצפינים כל אות בנפרד, אלא בלוקים, או קבוצות של כמה אותיות באורך קבוע m .

הגדרה 3.4 צופן ויז'נר (Vigenere Cipher)

יהי m מספר שלם חיובי.

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

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

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

ונגידיר כלל מפענה

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

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

דוגמה 3.8

נתון הטקסט גליי

string

והמפתח $.k = \text{ AND }$.

(1) מצאו את הכלל מצפן והכלל מפענה.

(2) מצאו את הטקסט מצפון.

(3) בדקו כי הכלל מפענה מחזיר את הטקסט גליי.

פתרון:

(1) והמפתח הוא

$\text{AND} .$

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

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

לכן $m = 3$.

הכלל מצפן הוא

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

והכלל מפענה הוא

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

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

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

נפרק את הטבלה של התווים של הטקסט גליי יחד עם הערכים המתאימים של \mathbb{Z}_{26} לחת-קבוצות של 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, נattaים לכל TWO 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 שלישי (x_1, x_2, x_3) בבלוק אחד, נפעיל את כלל המיפוי

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

לדוגמא בבלוק הראשון נקבל

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

בלוק השני נקבל

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

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

נעבור את הערכים 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

הтекסט 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 גליי יחד עם הערכים המתאימים של \mathbb{Z}_{26} לחת-קבוצות של 3 תווים:

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

בכל תת-קובוצה, נתאים לכל TWO ערך של המפתח (k_1, k_2, k_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 המיפוי

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

לדוגמה בבלוק הראשון נקבל

$$\begin{aligned} d_k(18, 6, 20) &= (18 - 0, 6 - 13, 20 - 3) \pmod{26} \\ &= (18, 19, 17). \end{aligned}$$

בלוק השני נקבל

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

$y \in C$	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 גלי:

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

הטקסט גלי המתקיים הוא
string.



3.9 דוגמה

נניח כי $m = 6$ והמפתח הוא

CIPHER.

הערכים המתאימים ב- \mathbb{Z}_{26} הינם
 $k = (2, 8, 15, 7, 4, 17)$.

נתון הטקסט גלי

thiscryptosystemisnotsecure.

מצאו את הטקסט מוצפן.

פתרונות:

שלב 1:

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

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

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

שלב 2:

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

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

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

שלב 3:

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

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

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

שלב 3:

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

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

לדוגמה בבלוק הראשון נקבל

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

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

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

שלב 4:

נעביר את הערכים של $y \in \mathbb{Z}_{26}$ 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

הtekst מוצפן המתקין הוא

VPXZGIAKIVWPUBTMJPWIZITWZT



3.5 צופן היל

הגדרה 3.5 צופן היל

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

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

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

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

ונגדיר כלל מפענה

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

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

הגדרה 3.6 המטריצה של קופקטורים

תהי $A \in \mathbb{R}^{n \times n}$

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

המטריצה של קובוקטורים 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} הקובקטור ה- (i,j) של A .

הגדרה 3.7 המטריצה המצורפת

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

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

כאשר C המטריצה של קובוקטורים של A .

משפט 3.3 נוסחת קיילי המילטון

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

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

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

דוגמה 3.10

נתון רצף טקסט גלי

յולן

ונתון המפתח

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

של צופן היל. מצאו את הטקסט מוצפן.

פתרונות:
שלב 1:

נעביר את האותיות של הטקסט גלי 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 גלי יחד עם הערכים המתאימים של \mathbb{Z}_{26} לחת-קבוצות של $2 = m$ תווים:

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

שלב 3:

עבור כל תת-קובוצה המתקבל נחשב

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

עבור התת-קובוצה הראשונה קיבל

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

עבור התת-קובוצה השנייה קיבל

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

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

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

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

הтекסט מוצפן המתקבל הוא

DELW

**דוגמה 3.11**

נתון רצף טקסט מוצפן

DELW

ונתנו המפתח

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

של צופן היל. מצאו את הטקסט גלי.

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

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

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

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

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

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

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

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

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

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

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

לפיכך

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

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

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

שלב 2:נפרק את הtablלה של התווים של הטקסט מוצפן יחד עם הערכים המתאים של \mathbb{Z}_{26} לחת-קבוצות של 2 תווים:

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

שלב 3:

עבור כל תת-קובוצה המתקבל נחשב

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

עבור התת-קובוצה הראשונה נקבל

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

עבור התת-קובוצה השנייה נקבל

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

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

שלב 5: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

הtekst גליי המתקבל הוא

july

**דוגמה 3.12**

נתון רצף טקסט מוצפן

ונתון המפתח

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

של צופן היל. מצאו את הטקסט גליי.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

לפיכך

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

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

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

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

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

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

לפיכך

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

שלב 1:

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

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

שלב 2:

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

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

שלב 3:

עבור כל מת-קבוצה המתקבל נחשב

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

עבור התת-קבוצה הראשונה קיבל

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

עבור התת-קבוצה השנייה קיבל

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

עבור התת-קבוצה השלישי קיבל

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

$y \in C$	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:

עבור 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

הtekst גלי המתקבל הוא

howareyou



שיעור 4

תמורות וצופן אניגמה

4.1 תמורות

הגדרה 4.1 תמורה

תמורה על קבוצה סופית $\Sigma = \{x_1, \dots, x_n\}$ היא פונקציה $\pi : \Sigma \rightarrow \Sigma$ אשר היא חד-חד ערכית ו"על" Σ . בהינתן $x_i \in \Sigma$ ותמורה π . אז

$$\pi(x_i) = x_j \in \Sigma .$$

תזכורת:

- π חד-חד ערכית. ז"א אם $x_i \neq x_j$ אז $\pi(x_i) \neq \pi(x_j)$.
- π "על" Σ . ז"א לכל $y \in \Sigma$ קיים $x \in \Sigma$ כך ש- $y = \pi(x)$.

כתוצאה מכך, אם π פועלת על כל האיברים של Σ אז נקבל אותה קבוצה Σ רק לא באותו בסדר של הסדר המקורי:

$$\{\pi(x_1), \pi(x_2), \dots, \pi(x_n)\} .$$

דוגמה 4.1

x	1	2	3	4	5	6
$\pi(x)$	4	1	6	5	2	3

דוגמה 4.2

x	1	2	3	4	5	6
$\sigma(x)$	2	1	5	4	6	3

דוגמה 4.3

תהי Σ קבוצה סופית ותהי $\Sigma \rightarrow \Sigma$ פונקציה. הוכחו: אם π חד-חד ערכית אז π תמורה.

פתרונות:

נתון לנו הפונקציה $\Sigma \rightarrow \Sigma$ אשר Σ קבוצה נוצר סופית. כדי להוכיח כי π תמורה יש להראות כי π חד-חד-ערכית ו"על" Σ . כבר נתון לנו ש- π חד-חד-ערכית רק להראות כי π על Σ .

Σ היא קבוצה סופית לכן קיימים שלם $0 \leq n \leq |\Sigma|$. תהי $(\Sigma) \pi$ התמונה של π . מכיוון ש- π היא פונקציה מהקבוצה Σ אל הקבוצה Σ , אז התמונה שלה היא תת-קבוצה של Σ , כלומר:

$$\pi(\Sigma) \subseteq \Sigma .$$

לכן

$$|\pi(\Sigma)| \leq |\Sigma| = n .$$

נראה כי $|\pi(\Sigma)| = |\Sigma|$. נניח בשלילה כי $|\pi(\Sigma)| < |\Sigma|$. אז בהכרח קיימים איברים $x_1, x_2 \in \Sigma$ כך ש-

בסטירה לכך ש: π חד-חד-ערכית. לכן הוכחנו דרך השיליה כי $\Sigma(x_1) = \Sigma(x_2)$

$$|\pi(\Sigma)| = |\Sigma| = n.$$

הוכחנו כי $\pi(\Sigma) \subseteq \Sigma$ וגם $|\pi(\Sigma)| = |\Sigma|$ אז בהכרח

$$\pi(\Sigma) = \Sigma$$

ולפיכך $\Sigma \rightarrow \pi$ היא פונקציה "על" Σ .



הגדרה 4.2 הרכבה של תמורה

תהי Σ קבוצה נוצר סופית ותהינה $\Sigma \rightarrow \Sigma : \pi \circ \sigma$ תמורים על הקבוצה Σ . ההרכבה של π ו- σ מוגדרת להיות הפונקציה שמסומנת $\sigma \circ \pi$ ומוגדרת לפי התנאי:
לכל $x \in \Sigma$, אם $\pi(x) = y$ ואם $\sigma(y) = z \in \Sigma$ אז $\sigma \circ \pi(x) = z$.

הסימן $\sigma \circ \pi(x)$ אומר "קודם π פועלת על x ואז σ פועלת על $\pi(x)$ ".

דוגמה 4.4

נתון התמורות π ו- σ :

$\begin{array}{c cccccc} x & 1 & 2 & 3 & 4 & 5 & 6 \\ \hline \pi(x) & 4 & 1 & 6 & 5 & 2 & 3 \end{array}$	$\begin{array}{c cccccc} x & 1 & 2 & 3 & 4 & 5 & 6 \\ \hline \sigma(x) & 3 & 5 & 4 & 2 & 6 & 1 \end{array}$
--	---

אזי ההרבה $\sigma \circ \pi$ היא:

$\begin{array}{c cccccc} x & 1 & 2 & 3 & 4 & 5 & 6 \\ \hline \sigma \circ \pi(x) & 2 & 3 & 1 & 6 & 5 & 4 \end{array}$

לעומת זאת ההרבה ההפוכה $\sigma \circ \pi$ היא:

$\begin{array}{c cccccc} x & 1 & 2 & 3 & 4 & 5 & 6 \\ \hline \pi \circ \sigma(x) & 6 & 2 & 5 & 1 & 3 & 4 \end{array}$

כלומר $\sigma \circ \pi \neq \pi \circ \sigma$.

משפט 4.1 הרכבה של תמורים היא תמורה

תהי Σ קבוצה נוצר סופית ותהינה $\Sigma \rightarrow \Sigma : \pi \circ \sigma$ תמורים על הקבוצה Σ . הרכבה $\sigma \circ \pi$ היא תמורה על Σ .

הוכחה: מספיק להוכיח כי $\sigma \circ \pi$ היא פונקציה חד-חד-ערכית ו"על" Σ .

• חח"ע

נניח בשיליה כי $\sigma \circ \pi$ לא חח"ע.

אזי קיימים $x_1, x_2 \in \Sigma$ כך ש- $\sigma(\pi(x_1)) = \sigma(\pi(x_2))$

נסמן $y_1 = \pi(x_1)$ ו- $y_2 = \pi(x_2)$.

מכיוון ש- π תמורה אז π חח"ע ולכן $y_1 \neq y_2$. ומכיון ש- σ תמורה אזי $\sigma(y_1) \neq \sigma(y_2)$. לכן

$$\sigma(\pi(x_1)) \neq \sigma(\pi(x_2)),$$

בסתירה לכך ש- $\sigma(\pi(x_1)) = \sigma(\pi(x_2))$. לכן הוכחנו דרך השיליה כי π פונקציה חד-ע.

• על

נניח בשלילה כי π לא פונקציה "על". נסמן (Σ) π התמונה של π . אי-

$$\sigma\pi(\Sigma) \neq \Sigma .$$

ראשית מכיוון ש- (Σ) π הוא התמונה של π אי- $\Sigma \subseteq \sigma\pi(\Sigma)$. לכן אם $\Sigma \neq \sigma\pi(\Sigma)$. מכאן

$$|\sigma\pi(\Sigma)| < |\Sigma| .$$

לכן בהכרח קיימים לפחות שני איברים $x_1, x_2 \in \Sigma$ עבורם $\pi(x_1) = \pi(x_2)$. זאת בסתירה לכך ש- π חד-ע, שמכוח בסעיף הקודם.

לכן הוכחנו דרך השיליה כי הפונקציה π היא "על" Σ .

הגדרה 4.3 תמורהות מתחלפות

תהיינה $\Sigma \rightarrow \Sigma : \sigma$ ו- $\Sigma \rightarrow \Sigma : \pi$ תמורהות. אומרים כי π ו- σ מתחלפות אם לכל $x \in \Sigma$ מתקיים

$$\pi\sigma(x) = \sigma\pi(x) .$$

הגדרה 4.4 תמורהות מתחלפות

תהי $\Sigma \rightarrow \Sigma : \pi$ תמורה על הקבוצה Σ . התמורה ההפכית של π מסומנת π^{-1} ומוגדרת:

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

לכל $x \in \Sigma$.

דוגמה 4.5

נתונה התמורה π :

x	1	2	3	4	5	6	7	8
$\pi(x)$	6	3	5	1	2	4	8	7

התמורה ההפכית היא:

x	1	2	3	4	5	6	7	8
$\pi^{-1}(x)$	4	5	2	6	3	1	8	7

הגדרה 4.5 נקודת שבת ונקודת זהה

תהי $\Sigma \rightarrow \Sigma : \pi$ תמורה.

- אם קיימת נקודת $\Sigma \in x$ כך ש: $\pi(x) = x$ אז אומרים כי x היא נקודת שבת של π .
- אם קיימת נקודת $\Sigma \in x$ כך ש: $\pi(x) \neq x$ אז אומרים כי x היא נקודת זהה של π .

הגדרה 4.6 תמורה זהה

התמורהזהה מסומנת $\Sigma \rightarrow \Sigma : \text{id}$ ומוגדרת כך שלכל $\Sigma \in \Sigma$:

$$\text{id}(x) = x .$$

במילים אחרות אם $\Sigma \rightarrow \Sigma : \text{id}$ היא התמורהזהה אז כל נקודת $\Sigma \in \Sigma$ היא נקודת שבת של id .

משפט 4.2 תמורה ההפכית של תמורה מורכבת

תהיינה π_t, \dots, π_1 תמורות על הקבוצה Σ . אז

$$(\pi_1 \cdots \pi_t)^{-1} = \pi_t^{-1} \cdots \pi_1^{-1} .$$

הוכחה: נוכיח את הטענה באינדוקציה.

שלב הבסיס

עבור $t=2$, לכל $\Sigma \in \Sigma$ יש לנו:

$$\pi_2^{-1} \pi_1^{-1} \pi_1 \pi_2(x) = \pi_2^{-1} \text{id} \pi_2(x) = \pi_2^{-1} \pi_2(x) = \text{id}(x) = x .$$

$$\text{לכן הוכחנו כי } (\pi_1 \pi_2)^{-1} = \pi_2^{-1} \pi_1^{-1} .$$

שלב האינדוקציה

נניח כי הטענה מתקיימת עבור $t=k > 2$ (זאת היא ההנחה האינדוקציה). אז נראה כי הטענה נכונה גם במקרה $t=k+1$ באופן הבא. נתבונן על התמורה המורכבת $\pi_k \pi_{k+1} \cdots \pi_1$. נסמן התמורה המורכבת מ- k תמורות כך: $\pi_k \cdots \pi_1 = \sigma$. הסימן זהה מאפשר לנו להביע את התמורה המורכבת מ- $k+1$ תמורות כתמורה המורכבת מ- 2 תמורות באופן הבא:

$$\pi_1 \cdots \pi_k \pi_{k+1} = \sigma \pi_{k+1} .$$

מכאן ולפי שלב הבסיס מהופכית היא

$$(\sigma \pi_{k+1})^{-1} = \pi_{k+1}^{-1} \sigma^{-1} .$$

כעת נחזיר את ההגדרה $\pi_k \cdots \pi_1 = \sigma$ ונשתמש בהנחה האינדוקציה שלנו כדי להוכיח את הטענה עבור $t=k+1$:

$$(\pi_k \pi_{k+1})^{-1} = \pi_{k+1}^{-1} (\pi_1 \cdots \pi_k)^{-1} = \pi_{k+1}^{-1} \pi_k^{-1} \cdots \pi_1^{-1}$$

כאשר במעבר האחרון השתמשנו בהנחה האינדוקציה.

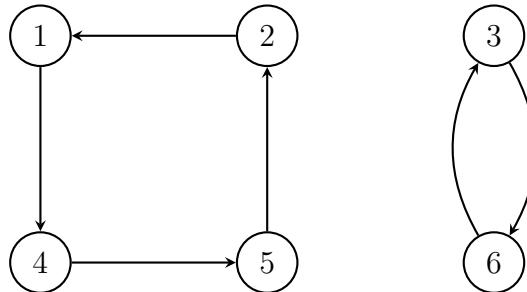
■

4.2 פירוק למחזוריים של תמורה

עד כה ראיינו תמורות בייצוג של טבלה. אבל המבנה האמתי של תמורה נגלה עם נציג תמורה כgraf. לדוגמה, תהי π תמורה הבאה על $\Sigma = \{1, 2, 3, 4, 5, 6\}$:

x	1	2	3	4	5	6
$\pi(x)$	4	1	6	5	2	3

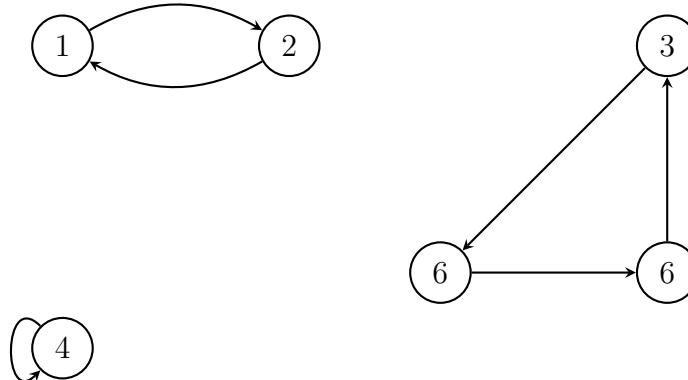
נדיר הגרף המכון $G_\pi = (V, E)$ כאשר הקבוצה הקודקודים היא $V = \Sigma$, ולכל $x \in \Sigma$ נגדיר צלע מ- x ל- $\pi(x)$. נ"א $E = \{e_1, e_2, \dots, e_n\}$ היא הצלע מקודקод x_i לקודקוד $\pi(x_i)$. על פי ההגדרה הזו את הגרף G_π של התמורה π היא כמתואר באIOR למטה.



כדוגמה נוספת אם σ היא התמורה

x	1	2	3	4	5	6
$\sigma(x)$	2	1	5	4	6	3

אז הגרף G_σ הינו:



בגרף של תמורה, כל קודקוד שיעז לבזוק מעגל מכון אחד (שייתכן הוא עובר דרך קודקוד אחד בלבד). הרי קיימים התאמות אחת- אחת בין תמורה על Σ לבין גראフ שמכסה כל המעגלים המכונים של Σ . התופעה זו היא המוטיבציה לסייעון מחזורי של תמורה.

הגזרה 4.7 מחזור

תהי $\Sigma \rightarrow \Sigma$ תמורה על הקבוצה Σ . אם קיימים k איברים שונים Σ כך ש-

$$\pi(a_1) = a_2, \quad \pi(a_2) = a_3, \quad \dots \quad \pi(a_{k-1}) = a_k, \quad \pi(a_k) = a_1$$

אז אומרים כי קיימים מחזור באורך k ב- π שמסומן:

$$(a_1 \ a_2 \ \dots \ a_k).$$

משפט 4.3 פירוק למחזורים של תמורה

כל תמורה $\Sigma \rightarrow \Sigma$ על קבוצה סופית Σ מתפרקת למחזורים זרים.

דוגמה 4.6נתונה התמורה π :

x	1	2	3	4	5	6	7	8
$\pi(x)$	4	5	2	6	3	1	8	7

הפירוק למחזוריים הוא:
 $\pi = (1 \ 4 \ 6) (2 \ 5 \ 3) (8 \ 7)$

משפט 4.4

תהי $\Sigma \rightarrow \pi$ תמורה על קבוצה סופית Σ ויהי $G_\pi = (V, E)$ הגרף של התמורה.
 π מכילה מחזור באורך k אם ורק אם הגרף G_π מכיל מעגל המילטוני באורך k .

הוכחה:
כיוון אם

נניח ש- π מכילה מחזור באורך k .

$$\begin{aligned} & \left. \left(a_1 \ a_2 \ \dots \ \subseteq a_k \right) \in \pi : \text{ש-} \right\} \text{קיים איברים שונים } a_1, \dots, a_k \in \Sigma \\ & . \pi(a_1) = a_2, \quad \pi(a_2) = a_3, \quad \dots \quad \pi(a_{k-1}) = a_k, \quad \pi(a_k) = a_1 \Leftarrow \\ & \text{בגרף } G_\pi = (V, E) \text{ של התמורה קיימות הצלעות} \\ & a_1\pi(a_1), \ a_2\pi(a_2), \ \dots, \ a_{k-1}\pi(a_{k-1}), \ a_k\pi(a_k) \in E. \end{aligned}$$

$$\begin{aligned} & \text{בגרף } G_\pi = (V, E) \text{ קיימות הצלעות} \\ & a_1a_2, \ a_2a_3, \ \dots, \ a_{k-1}a_k, \ a_ka_1 \in E. \end{aligned}$$

כיוון רק אם

נניח ש- G_π מכיל מעגל המילטוני באורך k .

$$\begin{aligned} & \text{קיימות קבוצות } a_1, \dots, a_k \in \Sigma \text{ עבורם} \\ & a_1a_2, \ a_2a_3, \ \dots, \ a_{k-1}a_k, \ a_ka_1 \in E. \end{aligned}$$

מכיוון ש- G_π הוא הגרף של התמורה π איזי

$$\pi(a_1) = a_2, \pi(a_2) = a_3, \quad \dots \quad \pi(a_{k-1}) = a_k, \pi(a_k) = a_1$$

$$\begin{aligned} & \pi \text{ מכילה מחזור באורך } k: \\ & \left(a_1 \ a_2 \ \dots \ \subseteq a_k \right) \subseteq \pi. \end{aligned}$$

הגדרה 4.8 המחלקה של תמורה

תהי $\Sigma \rightarrow \pi$ תמורה. אומרים כי π שיכת למחלקה $[1^{z_1} 2^{z_2} \cdots n^{z_n}]$ אם בפירוק למחזוריים של π יש בדיק z_1 מחזוריים באורך-1, z_2 מחזוריים באורך-2, z_3 מחזוריים באורך-3, וכן הלאה.

במילים אחרות:

$$\pi \in [1^{z_1} 2^{z_2} \cdots n^{z_n}]$$

אם לכל $n = 1, \dots, i$ בפירוק למחזוריים של π יש z_i מחזוריים באורך i .

דוגמה 4.7

תהי $. \Sigma = \{A, B, C, D, E, F\}$

$.(A \ B)(C \ D)(E \ F) \in [2^3]$

$.(A \ B \ C \ D) \in [1^2 4^1]$

$.(A \ D \ C)(E \ F) \in [1^1 2^1 3^1]$

4.3 תמורה צמודות

הגדרה 4.9 תמורה צמודות

תהיינה σ, π תמורות על הקוצה סופית Σ . התמורה הצמודה של σ על ידי π היא המורה המורכבת $\pi \sigma \pi^{-1}$.

משפט 4.5 משפט ההזזה של תמורות צמודות

תהיינה $\Sigma \rightarrow \sigma : \Sigma \rightarrow \pi$ תמורות על הקוצה סופית Σ . לכל Σ אם $\sigma(x) = y$ אז $\pi(\sigma(x)) = \pi(y)$.

$$\pi \sigma \pi^{-1}(\pi(\sigma(x))) = \pi(\sigma(x)) = \pi(y).$$

הוכחה: נניח ש: $\sigma(x) = y$. אז

$$\pi \sigma \pi^{-1}(\pi(\sigma(x))) = \pi \sigma \pi^{-1}\pi(x) = \pi \sigma(x) = \pi(y).$$

משפט 4.6 פירוקים למחזוריים של תמורות צמודות שוויות

תהיינה $\Sigma \rightarrow \sigma : \Sigma \rightarrow \pi$ תמורות על הקוצה סופית Σ . ונניח כי הפירוק למחזוריים של σ הוא

$$\sigma = (a_1 \ a_2 \ \cdots \ a_k) (b_1 \ b_2 \ \cdots \ b_l) \cdots .$$

אז הפירוק למחזוריים של $\pi \sigma \pi^{-1}$ הוא:

$$\pi \sigma \pi^{-1} = (\pi(a_1) \ \pi(a_2) \ \cdots \ \pi(a_k)) (\pi(b_1) \ \pi(b_2) \ \cdots \ \pi(b_l)) \cdots .$$

הוכחה: עבור כל מהזור $(a_1 \ a_2 \ \dots \ a_k)$ של σ , מתקיים

$$\sigma(a_i) = a_{i+1} \quad (1 \leq i \leq k-1), \quad \sigma(a_k) = a_1.$$

מנובע המשפט כי לכל מהזור של σ מתקיים:

$$\pi\sigma\pi^{-1}(\pi(a_i)) = \pi(a_{i+1}) \quad (1 \leq i \leq k-1), \quad \pi\sigma\pi^{-1}(\pi(a_k)) = \pi(a_1).$$

■

משפט 4.7 המחלוקת של תמורה צמודות נשמרת

תהיינה $\Sigma \rightarrow \Sigma : \sigma$ ו- $\Sigma \rightarrow \Sigma : \tau$ תמורים על הקוצה סופית Σ .
 τ צמודה ל- σ אם ורק אם $\sigma \circ \tau$ שייכות לאותה מחלוקת.

הוכחה:

כיוון אם:

נניח ש- σ ו- τ צמודות. אז קיימת תמורה π עבורה $\tau = \pi\sigma\pi^{-1}$.
 אם הפירוק למחוזרים של σ הוא

$$\sigma = (a_1 \ a_2 \ \dots \ a_k) (b_1 \ b_2 \ \dots \ \pi(b_l)) \dots$$

אז לפי משפט 4.6 הפירוק למחוזרים של $\tau = \pi\sigma\pi^{-1}$ הוא

$$\pi\sigma\pi^{-1} = (\pi(a_1) \ \pi(a_2) \ \dots \ \pi(a_k)) (\pi(b_1) \ \pi(b_2) \ \dots \ \pi(b_l)) \dots$$

ולכן ל- τ ול- σ יש אותו מבנה של מחוזרים וכך הוא שייכות לאותה מחלוקת.

כיוון רק אם:

■

4.4 צופן אניגמה

הgalלי האתחול של צופן אניגמה הם 3 תמורים קבועות שמוגדרות:

x	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
$\alpha_1(x)$	E	K	M	F	L	G	D	Q	V	Z	N	T	O	W	Y	H	X	U	S	P	A	I	B	R	C	J

x	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
$\alpha_2(x)$	A	J	D	K	S	I	R	U	X	B	L	H	W	T	M	C	Q	G	Z	N	P	Y	F	V	O	E

x	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
$\alpha_3(x)$	B	D	F	H	J	L	C	P	R	T	X	V	Z	N	Y	E	I	W	G	A	K	M	U	S	Q	O

המשקף הקבוע הוא תמורה הבאה:

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

$$\begin{aligned} \alpha_1 &= (AELTPHQXRU)(BKNW)(CMOY)(DFG)(IV)(JZ)(S) && \in [1^1 2^2 3^1 4^2 10^1], \\ \alpha_2 &= (A)(JB)(CDKLHUP)(ESZ)(FIXVYOMW)(GR)(NT)(Q) && \in [1^2 2^3 3^1 7^1 8^1], \\ \alpha_3 &= (ABDHPEJT)(CFLVMZOYQIRWUKXSG)(N) && \in [1^1 8^1 17^1], \\ \rho &= (AY)(BR)(CU)(DH)(EQ)(FS)(GL)(IP)(JX)(KN)(MO)(TZ)(VW) && \in [2^{13}]. \end{aligned}$$

הגדרה 4.10 כלל מצפין וככלל מפענה של צופן אניגמה

יהי π משקף כלשהו מעל האלפבית $Z = A, \dots, Z$. הבחירה של המשקף מבהווה את הלוח התקעiem. יהי $w = x_1 x_2 \dots x_n$ מילה של טקסט גלי. לכל $i = 1, \dots, n$, הכלל מצפין והכלל מפענה של האות במקומות i -טקסט הם:

$$e(x_i) = \Delta_i(x_i) = d(x_i)$$

כאשר Δ_i היא התמורה המורכבת

$$\Delta_i = \pi [\alpha_3^i]^{-1} \alpha_2^{-1} \alpha_1^{-1} \rho \alpha_1 \alpha_2 \alpha_3^i \pi(x_i)$$

כאשר

$$\alpha_3^i = \sigma_{-i} \alpha_3 \sigma_i, \quad [\alpha_3^i]^{-1} = \sigma_{-i} \alpha_3^{-1} \sigma_i.$$

אם נגדיר את התמורה המורכבת π אי $\tau_i = \sigma_{-i} \alpha_3 \sigma_i \alpha_2 \alpha_1$ ולבסוף

$$\Delta_i = \tau_i^{-1} \rho \tau_i.$$

ז"א לכל $i = 1, \dots, n$ התמורה המורכבת Δ_i היא הצמודה של ρ על ידי τ_i .

דוגמה 4.8 הצפנה על ידי צופן אניגמה

נתון הטקסט גלי,

hello .

נניח כי הלוח התקעiem הוא

$$\pi = (AX)(HF)(LP).$$

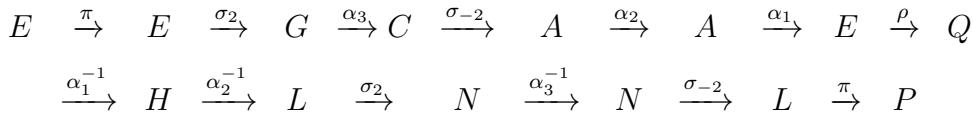
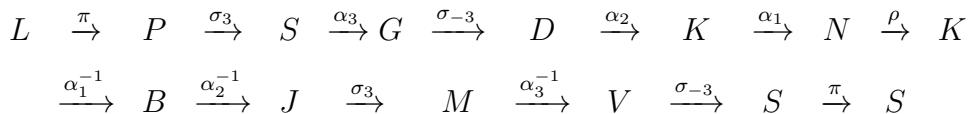
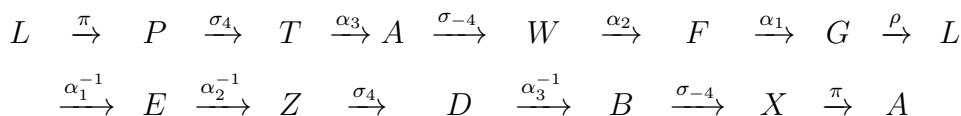
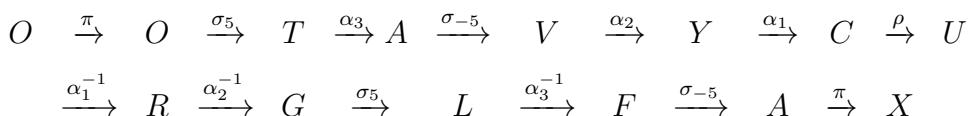
חשבו את הטקסט מוצפן.

פתרונות:

$$x_1 = H \quad (1)$$

$$\begin{array}{ccccccccc} H & \xrightarrow{\pi} & F & \xrightarrow{\sigma_1} & G & \xrightarrow{\alpha_3} C & \xrightarrow{\sigma_{-1}} & B & \xrightarrow{\alpha_2} J \\ & \xrightarrow{\alpha_1^{-1}} & L & \xrightarrow{\alpha_2^{-1}} & K & \xrightarrow{\sigma_1} & L & \xrightarrow{\alpha_3^{-1}} & F \end{array}$$

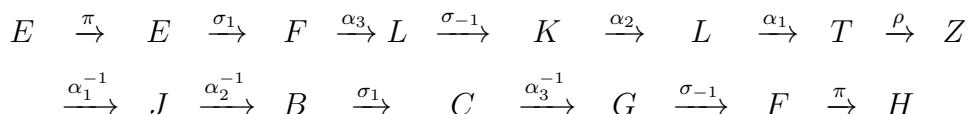
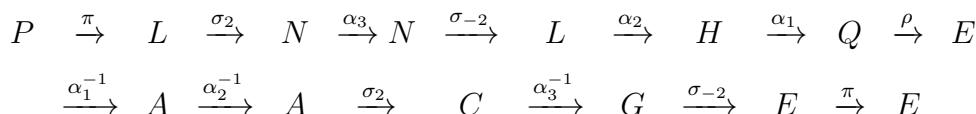
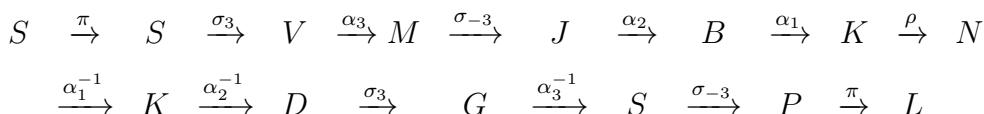
$$x_2 = E \quad (2)$$

 $x_3 = \text{L}$ (3) $x_4 = \text{L}$ (4) $x_5 = \text{O}$ (5)

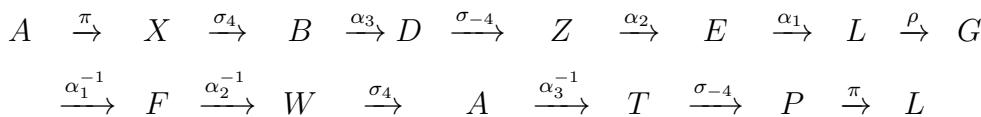
לפייך הטקסט מוצפן הוא: EPSAX.

דוגמה 4.9 הצפנה על ידי צופן איניגמה

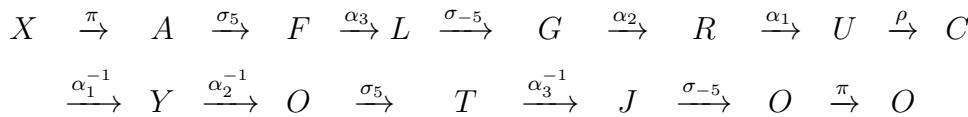
חשבו את הטקסט הגלוי של המילה המתקבלת בדוגמה הקודמת עם אותו לוח-התקעים.

פתרונות: $y_1 = \text{E}$ (1) $y_2 = \text{P}$ (2) $y_3 = \text{S}$ (3)

$$y_4 = \text{A} \quad (4)$$



$$y_5 = \text{X} \quad (5)$$



לפיכך הטקסט המקורי הוא: HELLO.

4.5 משפט ריבסקי

הגדרה 4.11 תמורה משקפת

תהי Σ קבוצה נוצר סופית באורך זוגי. כלומר $|\Sigma| = n$ זוגי. תהי $\Sigma \rightarrow \Sigma : \rho$ תמורה. אומרים כי התמורה ρ היא משקף אם $\rho \in [2^{n/2}]$.

משפט 4.8 תכונות של תמורה משקפת

תהי Σ קבוצה נוצר סופית באורך זוגי, ותהי $\Sigma \rightarrow \Sigma : \rho$ תמורה. אז ρ היא משקף אם ורק אם התנאים הבאים מתקיימים:

$$\rho^{-1} = \rho \quad (1)$$

$$(2) \text{ לכל } \Sigma \in x \text{ מתקיים } \rho(x) \neq x.$$

הוכחה:

כיוון אם

נניח כי ρ משקף. נראה כי $\rho^{-1} = \rho$ באופן הבא. נניח ש:

$$\rho = (x_1 \ y_1) (x_2 \ y_2) \cdots (x_{n/2} \ y_{n/2}).$$

לכל מחרוז $(a_1 \ a_2 \ \cdots \ a_k)$ המחזור ההפוך הוא $(a_k \ a_{k-1} \ \cdots \ a_1)$. לכן

$$\begin{aligned} \rho^{-1} &= (x_1 \ y_1)^{-1} (x_2 \ y_2)^{-1} \cdots (x_{n/2} \ y_{n/2})^{-1} \\ &= (y_1 \ x_1) (y_2 \ x_2) \cdots (y_{n/2} \ x_{n/2}) \\ &= (x_1 \ y_1) (x_2 \ y_2) \cdots (x_{n/2} \ y_{n/2}) \\ &= \rho. \end{aligned}$$

כעת נראה שגם $\rho(x) \neq x$ אז $\rho(x) = x$. נניח בשיילה שקיים נקודה $x \in \Sigma$ עבורה $\rho(x) = x$. אזי $\rho \in [1^{z_1} \ \cdots \ z]$, כאשר $0 < z_1$, כלומר ρ מכילה קים לפחות אחד באורך 1, בסתרה לכך ρ היא משקף.

כיוון רק אם

נניח כי $\Sigma \rightarrow \Sigma : \rho$ היא תמורה כך שלכל $x \in \Sigma$ מתקיים $x \neq \rho(x) \Leftrightarrow \rho^{-1}(\rho(x)) = x$. נוכיח כי ρ היא משקף. בשלילה כי ρ לא משקף. אז ρ מכילה לפחות מחזור אחד באורך $k > 2$. נניח כי קיימים מחזור באורך 1. אז קיימת נקודת שבת של ρ , כלומר קיימת $x \in \Sigma$ עבורו $x = \rho(x)$. והגענו לסתירה. מצד שני נניח כי קיימים מחזור באורך $k > 2$ ב- ρ . אז ניתן לרשום ρ כהרכבה באופן הבא:

$$\rho = (x_1 \ x_2 \ x_3 \ \dots) \rho' ,$$

כאשר (\dots) הוא מחזור באורך $k > 2$. זו ההפכית של ρ היא

$$\rho^{-1} = \rho'^{-1} (x_1 \ x_2 \ x_3 \ \dots)^{-1} = \rho'^{-1} (\dots x_3 \ x_2 \ x_1) \neq \rho ,$$

בסתירה לכך ש- $\rho^{-1} = \rho$.

משפט 4.9 הכלל מצפין של צופן האניגמה הוא תמורה משקפת על האלפבית האנגלית

הכלל מצפין (והכלל מפענה) של צופן האניגמה הוא תמורה משקפת על האלפבית האנגלית.

הוכחה: הכלל מצפין והכלל מפענה של צופן האניגמה הם

$$e(x_i) = \Delta_i(x_i) = \tau_i^{-1} \rho \tau_i(x_i)$$

כאשר $\pi \circ \rho$ המשקף הקבוע של צופן אניגמה.

\Leftarrow לכל $i = 1, \dots, n$ התמורה המורכבת Δ_i היא הצמודה של ρ על ידי τ_i .

\Leftarrow מכיוון ש: ρ הוא משקף על האלפבית האנגלית אז $\rho \in [2^{13}]$.

\Leftarrow לפי משפט 4.7 $\Delta_i \in [2^{13}]$.

\Leftarrow לפי הגדירה 4.11 התמורה Δ_i היא תמורה משקפת.

משפט 4.10 כלל של זוג תמורות משקפות

יהיו ρ_1 ו- ρ_2 תמורות משקפות על הקבוצה סופית Σ .

קיימים Σ עוברים $x, y_1, y_2 \in \Sigma$ ורק אם $\rho_1(x) = y_1$ וגם $\rho_2(x) = y_2$.

הוכחה:
כיוון אם

תהיינה ρ_1, ρ_2 תמורות משקפות ויהי $x \in \Sigma$.

$$\left. \begin{array}{l} y_1 = \rho_1(x) \\ y_2 = \rho_2(x) \end{array} \right\} \xrightarrow{\text{משקפת } \rho_1} x = \rho_1(y_1) \Rightarrow \rho_2(\rho_1(y_1)) = \rho_2(x) = y_2 .$$

כיוון רק אם

נניח ש: $\rho_1(y_1) = \rho_2(y_2)$. מכיוון ש- ρ_2 תמורה משקפת איזומטרית $x \in \Sigma$ קיים $y_1, y_2 \in \Sigma$ כך ש:

$$\left. \begin{array}{l} \rho_1(y_1) = x = \rho_2(y_2) \\ \rho_2(y_2) = x \end{array} \right\} \xrightarrow{\text{משקפות } \rho_1, \rho_2} \left. \begin{array}{l} y_1 = \rho_1(x) \\ y_2 = \rho_2(x) \end{array} \right\} .$$

4.6 ההנחות של ריבסקי על צופן האניגמה

הגדרה 4.12 ההנחות של ריבסקי

1) במהלך מלחמת העולם הראשונה והשנייה, כל הודעה שהוצפנה על ידי צופן האניגמה התחילה במילה סימטרית באורך 6 אותיות שנקראת **מילה משוכפלת**:

$$xyzxyz ,$$

במילה משוכפלת זו - 3 אותיות הראשונות היו זהות ל- 3 אותיות האחרונות.
המילה הזאת נקראת המילה האופיינית של ההודעה.

2) ההצפנה של המילה המשוכפלת נקראת **המילה אופיינית**:

$$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \Delta_1(x)\Delta_2(y)\Delta_3(z)\Delta_4(x)\Delta_5(y)\Delta_6(z) .$$

3) הכלל מצפין אינו משתנה באותו יום.

משפט 4.11 משפט ריבסקי I

יהי $\sigma_6\sigma_5\sigma_4\sigma_3\sigma_2\sigma_1$ המילה האופיינית של טקסט מוצפן כלשהו שהוצפן ע"י צופן האניגמה. אז:

$$\begin{aligned} \sigma_4 &= \Delta_4\Delta_1(\sigma_1) , \\ \sigma_5 &= \Delta_5\Delta_2(\sigma_2) , \\ \sigma_6 &= \Delta_6\Delta_3(\sigma_3) . \end{aligned}$$

הוכחה:

תהי $\sigma_6\sigma_5\sigma_4\sigma_3\sigma_2\sigma_1$ המילה האופיינית אשר היא ההצפנה של המילה המשוכפלת $xyzxyz$. נ"א

$$\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6 = \Delta_1(x)\Delta_2(y)\Delta_3(z)\Delta_4(x)\Delta_5(y)\Delta_6(z) .$$

נ"א

$$\left. \begin{array}{l} \sigma_1 = \Delta_1(x) \\ \sigma_4 = \Delta_4(x) \end{array} \right\} \Rightarrow x = \Delta_1(\sigma_1) \Rightarrow \Delta_4(x) = \Delta_4\Delta_1(\sigma_1) \Rightarrow \sigma_4 = \Delta_4\Delta_1(\sigma_1) .$$

$$\left. \begin{array}{l} \sigma_2 = \Delta_2(y) \\ \sigma_5 = \Delta_5(y) \end{array} \right\} \Rightarrow y = \Delta_2(\sigma_2) \Rightarrow \Delta_5(y) = \Delta_5\Delta_2(\sigma_2) \Rightarrow \sigma_5 = \Delta_5\Delta_2(\sigma_2) .$$

$$\left. \begin{array}{l} \sigma_3 = \Delta_3(z) \\ \sigma_6 = \Delta_6(z) \end{array} \right\} \Rightarrow z = \Delta_3(\sigma_3) \Rightarrow \Delta_6(z) = \Delta_6\Delta_3(\sigma_3) \Rightarrow \sigma_6 = \Delta_6\Delta_3(\sigma_3) .$$

דוגמה 4.10

נתונה הودעה מוצפנת שמתחלפת במילה אופיינית הבאה:

ICPWLV .

ז"א קיימת מילה מושכפלת $xyzxyz$ כך ש:

$$\text{ICPWLV} = \Delta_1(x)\Delta_2(y)\Delta_3(z)\Delta_4(x)\Delta_5(y)\Delta_6(z) ,$$

לכן לפי משפט ריבסקי I :

$$\Delta_4\Delta_1(I) = W , \quad \Delta_5\Delta_2(C) = L , \quad \Delta_6\Delta_3(P) = V .$$

דוגמה 4.11

הטבלה הבאה מראה מילים אופייניות מהודעות מוצפנות מאותו יום.

FDZWOW	YRVSNF	XASAIU	OYDFHH	PXFDBP	REQYUD
BLHGRR	LUBXKI	KGYEQA	APMCMO	JCENEM	KHREJS
HJNQSK	TTGMYL	SZWZXZ	ZFPRVX	QMUBZQ	IWIKFZ
NSXVT	DKJOGV	ENLTWY	CWAIFG	GITPAJ	WOOHDE
VQAU	MVKLLC	UBCJPN			

חשבו את התמורות $\Delta_6\Delta_3$ ו- $\Delta_5\Delta_2$ ו- $\Delta_4\Delta_1$.

פתרונות:

$$\Delta_4\Delta_1 = (ZRYS)(JNVU)(GPDOFWHQB)(ACIKETMLX) ,$$

$$\Delta_5\Delta_2 = (DO)(IA)(STYHJ)(BPMZX)(NWFVLR)(CEUKGQ) ,$$

$$\Delta_6\Delta_3 = (MOE)(CNK)(WBIZ)(AGLY)(VFPXTJ)(DHRSUQ) .$$

משפט 4.12 משפט ריבסקי II

- בכל תמורה כפולה $\Delta_4\Delta_1$ של צופן אנigma קיים זוג מהזורים בסידור מסוים

$$(a_1 \ a_2 \ \cdots \ a_{k-1} \ a_k) (b_1 \ b_2 \ \cdots \ b_{k-1} \ b_k)$$

כך ש:

$$b_k = \Delta_1(a_1) , \quad b_{k-1} = \Delta_1(a_2) , \quad \dots \quad b_2 = \Delta_1(a_{k-1}) , \quad b_1 = \Delta_1(a_k) .$$

הסידור זהה של המהזרים נקרא **סדר ריבסקי**.

- בכל תמורה כפולה $\Delta_5\Delta_2$ של צופן אנigma קיים זוג מוחזרים בסדר ריבסקי

$$(a_1 \ a_2 \ \cdots \ a_{k-1} \ a_k) (b_1 \ b_2 \ \cdots \ b_{k-1} \ b_k)$$

כך ש:

$$b_k = \Delta_2(a_1), \quad b_{k-1} = \Delta_2(a_2), \quad \dots \quad b_2 = \Delta_2(a_{k-1}), \quad b_1 = \Delta_2(a_k).$$

- בכל תמורה כפולה $\Delta_6\Delta_3$ של צופן אנigma קיים זוג מוחזרים בסדר ריבסקי

$$(a_1 \ a_2 \ \cdots \ a_{k-1} \ a_k) (b_1 \ b_2 \ \cdots \ b_{k-1} \ b_k)$$

כך ש:

$$b_k = \Delta_3(a_1), \quad b_{k-1} = \Delta_3(a_2), \quad \dots \quad b_2 = \Delta_3(a_{k-1}), \quad b_1 = \Delta_3(a_k).$$

דוגמה 4.12

$$\Delta_4\Delta_1 = (\text{OGKRYSD})(\text{ZUQWFIB})(\text{MJXCP})(\text{HILNVE})(\text{A})(\text{T})$$

ראשית נשים לב שהפירוק למוחזרים של $\Delta_4\Delta_1$ הוא בדיקת המבנה הנקבע על ידי משפט ריבסקי. בפרט $\Delta_4\Delta_1$ מכילה:

- זוג מוחזרים באורך 7,
- זוג מוחזרים באורך 5,
- זוג מוחזרים באורך 1.

לפי משפט ריבסקי II :

$$(\text{ZUQWFIB}) = \left(\Delta_1(\text{D}) \Delta_1(\text{S}) \Delta_1(\text{Y}) \Delta_1(\text{R}) \Delta_1(\text{K}) \Delta_1(\text{G}) \Delta_1(\text{O}) \right)$$

דוגמה 4.13 קרייפטו-אנליזה של צופן אנigma

נתונות התמורות הבאות של צופן אנigma:

$$\Delta_4\Delta_1 = (\text{ZRYS})(\text{JNVU})(\text{GPDOFWHQB})(\text{ACIKETMLX}),$$

$$\Delta_5\Delta_2 = (\text{DO})(\text{IA})(\text{STYHJ})(\text{BPMZX})(\text{NWFVLR})(\text{CEUKGQ}),$$

$$\Delta_6\Delta_3 = (\text{MOE})(\text{CNK})(\text{WBIZ})(\text{AGLY})(\text{VFPXTJ})(\text{DHRSUQ}).$$

פענו את הקסט מוצפן

ILBDA

פתרונות:

יהי הטקסט הגרפי

$$x_1x_2x_3x_4x_5.$$

אנו

$$\text{ILBDA} = \Delta_1(x_1) \Delta_2(x_2) \Delta_3(x_3) \Delta_4(x_4) \Delta_5(x_5) .$$

אות 1

$$I = \Delta_1(x_1) \xrightarrow{\text{משקפת } \Delta_1} x_1 = \Delta_1(I) \xrightarrow{\text{משפט ריבסקי II}} x_1 = H .$$

אות 2

$$L = \Delta_2(x_2) \xrightarrow{\text{משקפת } \Delta_2} x_2 = \Delta_2(L) \xrightarrow{\text{משפט ריבסקי II}} x_2 = E .$$

אות 3

$$B = \Delta_3(x_3) \xrightarrow{\text{משקפת } \Delta_3} x_3 = \Delta_3(B) \xrightarrow{\text{משפט ריבסקי II}} x_3 = L .$$

אות 4

$$D = \Delta_4(x_4) \xrightarrow{\text{משקפת } \Delta_4} x_4 = \Delta_4(D)$$

$$\Delta_1(D) \xrightarrow{\text{משפט ריבסקי II}} M \xrightarrow{\text{משקפת } \Delta_1} D = \Delta_1(M) \Rightarrow \Delta_4(D) = \Delta_4\Delta_1(M) = L .$$

אות 5

$$A = \Delta_5(x_5) \xrightarrow{\text{משקפת } \Delta_5} x_5 = \Delta_5(A)$$

$$\Delta_2(A) \xrightarrow{\text{משפט ריבסקי II}} D \xrightarrow{\text{משקפת } \Delta_1} A = \Delta_1(D) \Rightarrow \Delta_5(A) = \Delta_5\Delta_2(D) = O .$$

תשובה סופית:

$$x_1x_2x_3x_4x_5 = HELLO .$$



שיעור 5

קריפטו-אליזה

1.5. סוגים של התקפת סייבר

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

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

ישנו 4 סוגי התקפת סייבר.

1) התקפת טקסט מוצפן בלבד.

למתקיף (אוסקר) יש מהריזט של טקסט מוצפן עז.

2) התקפת טקסט גליי ידוע

למתקיף יש מהריזט של טקסט גליי × יחד עם הטקסט מוצפן המתאים עז.

3) התקפת טקסט גליי נבחר

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

4) התקפת טקסט מוצפן נבחר

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

החלק הבא מתעסק עם התקפת טקסט מוצפן.

5.2 קבוצות אותיות הנפוצים ביותר בטקסט גליי

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

כלל 5.1 פונקציית הסתברות של האותיות של האלפיבית

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

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

כלל 5.2 קבוצות תדריות של אותיות בטקסט גליי

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

כלל 5.3 זוגות אותיות הנפוצים ביותר בטקסט גליי

השלושים זוגות אותיות הנפוצים ביותר בטקסט גליי רשומים בטבלה למטה:

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

כלל 5.4 קבוצות שלושת אותיות הנפוצים ביותר בטקסט גלי

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

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

5.3 קריפטו-אנליזה של צופן האפיני

זו דוגמה של התקפת טקסט מוצפן בלבד.

דוגמה 5.1

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

KARSRROHVUKARPFSZFERXERFKREKAFSKARSRROHVUKARURTVEKARVSR

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

פתרון:

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

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

שלב 2) נרשום את האותיות הנפוצות ביותר:

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

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

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

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

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

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

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

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

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

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

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

$$a = 3, b = 5$$

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

- נבנה את הכלל מפענה עם המפתח המתקיים:

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

שלב 4) ננסה לפענה את הטקסט מצפן עם הכלל מפענה

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

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

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



דוגמה 5.2

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

FMXVEDKAPHFERBNDKRXRSREFMORUDSDKDVSHVUFEDKAPRKDLYEVLRHHRH

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

פתרון:

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

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

שלב 2) נרשום את האותיות הנפוצות ביותר:

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

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

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

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

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

• נניח כי

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

• נציב b ונקבל

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

כעת נפתרו את המערכת מעל:

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

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

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

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

• עכשו נחזיר וננסה

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

•

• נציג $e_k = ax + b$ ונקבל

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

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

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

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

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

עכשו נחזור וננסה

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

א"ז •

$$e_k(4) = 17$$

$$e_k(19) = 7.$$

• נציג $e_k = ax + b$ ונקבל

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

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

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

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

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

עכשו נחזור וננסה

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

א"ז •

$$e_k(4) = 17$$

$$e_k(19) = 10.$$

• נציג $e_k = ax + b$ ונקבל

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

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

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

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

$a = 3, b = 5$ א"ז

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

- נבנה את הכלל מפענה עם המפתח המתkeletal:

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

שלב 4) ננסה לפענה את הטקסט מצפונו עם הכלל מפענה

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

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

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



5.4 קרייפטו-אליזה של צופן היל

זו דוגמה של התקפת טקסט גליי ידוע.

משפט 5.1

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

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

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

-1

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

$j \leq 1 \text{ עד ש-}$

$$y_j = e_k(x_j) .$$

נגידר שתי מטריצות

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

אם X הפיכה אז

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

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

נתון הטקסט גלי

friday

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

PQCFKU

מצאו את המפתח של הצופן.

פתרון:

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

א"א

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

נkeh את שני טקסטים גלויים וטקסיום מוצפנים המתאימים נגדיר את המטריצות

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

א"ז

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

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

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

לכן

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

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

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

לכן

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

לבסוף נקבל

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

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

לפיכך

דוגמה 5.4

נתון הטקסט גלי

theresnoplacealikehome

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

FHVTUTGQVRWPSCPSSFGGAMG

מצאו את המפתח של הצופן.

פתרון:

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

ואז

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

נkeh את שני טקסטים גלויים וtekstois מוצפנים המתאימים נגדיר את המטריצות

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

ואז

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

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

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

לכן

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

המטריצת הקופקטורים של X היא

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

לכן

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

לבסוף נקבל

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

לפיכך

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



5.5 מודד צירוף המקרים

הגדרה 5.1 מודד צירוף המקרים I_c

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

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

משפט 5.2 נוסחה לחישוב המודד צירוף המקרים

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

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

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

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

המדד צירוף המקרים של הטקסט גלי x נתון על ידי הנוסחה

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

משפט 5.3 מדד צירוף המקרים בטקסט גלי

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

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

אות	p_i
ג	0.02
ה	0.061
י	0.07
ז	0.002
ק	0.008
ל	0.04

אות	p_i
מ	0.024
נ	0.067
ו	0.075
פ	0.019
ק	0.001
ר	0.06

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

המדד צירוף המקרים מצופה להיות

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

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

דוגמה 5.5

נתון הטקסט מוצפן

MOKSMNXBIUCMQXGCAXOFXMUWLNRNSFMIQBHNCFCGDTAHANTTIJNIERGCHURYHOGGSWTMP
 CCOYISKOGXLQAFMVXNFEDAEMHQTNAAQXUDIXXRSILCIZKGWEFLAWGUJAOAUPLXRQTGATPS
 MKLQSWRGTXJNPXEUNSYIACRGWLQEIMDUBQQGAEEYULEEWXDLIIDUHQFXWEAZJTUOFXWKS
 MTNAAFXTTMFPMUWLNRNSFMOTBIJJTUSFPRMRVBLMQXXRURKCAZGWCWAAGADECGDMMCZJVQS
 NNRTISADILALHOEFWOFTGBSUFDHMZWNKPNUJALAZGWCOKSMXRMRQXNQMFHOGVGAGMR
 AIAFMGWCMRQXUMJXXRPXGCAWILOQAFGZJNOIQXUMVWZUUXWAISLLVIEXWABARVHOGEJNWAV
 LQMAWCOYISUIHIK

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

פתרונות:

שלב 1: נפרק את הטקסט לעמודות של 3 אותיות

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

שלב 2:-Calculating the average length of each row

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

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

כל רצף אותיות \underline{y}_i מתקיים על ידי זהה קבועה של k_i מקומות של הטקסט גלי. לפי זה, הפונקציות הקשורות של האותיות המופיעות,

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

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

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

לכל $g = k_i$ אם $0 \leq g \leq 25$

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

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

\underline{y}_1

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

\underline{y}_2

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

 \underline{Y}_3

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

 \underline{Y}_4

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

 \underline{Y}_5

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

ונסה לפענח את הטקסט מוצפן עם המפתח

JAMES

ונקבל את התשובה

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

עם רוחים וסימני פיסוק:

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

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

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



שיעור 6

צופן RSA

6.1 אלגוריתם RSA

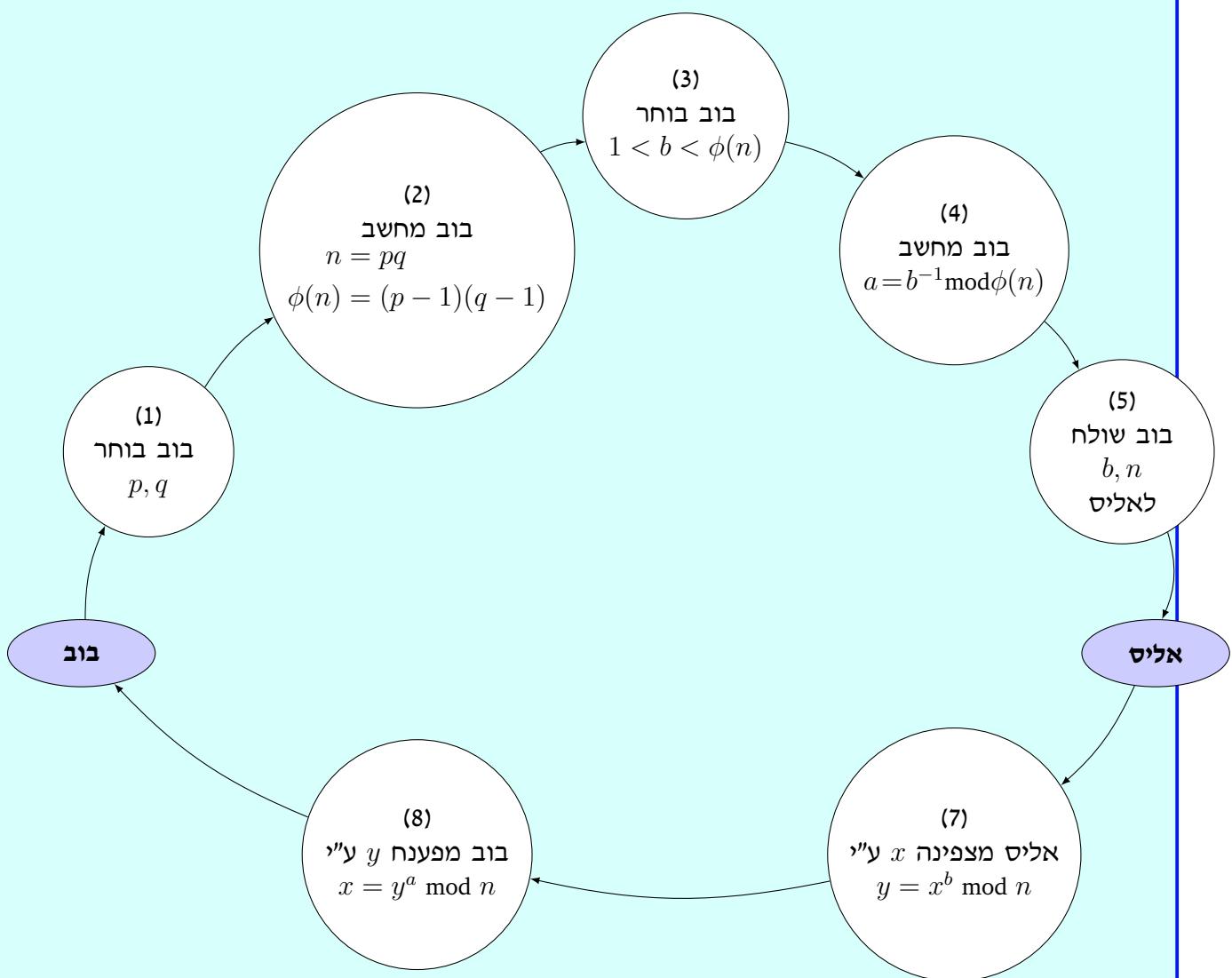
צופן RSA הומצא בשנת 1977 על ידי Ron Rivest, Adi Shamir and Len Adleman.

הגדרה 6.1 צופן RSA

- יהיו p, q מספרים ראשוניים שונים ($p \neq q$).
- יהיה $n = pq$.
- יהיה b שלם כך ש: $1 < b < \phi(n)$ הפונקציה אוילר של n .
- נגדיר $a \equiv b^{-1} \pmod{\phi(n)}$.
- אזי
 - * המפתח הציבורי של צופן RSA הוא הקבוצה (b, n) ,
 - * המפתח הסודי של צופן RSA הוא הקבוצה (a, p, q) .
- יהיה $x \in \mathbb{Z}^+$ שלם אי-שלילי.
 - * הכלל מצפין מוגדר $e_k(x) = x^b \pmod{n}$,
 - * והכלל מפענח מוגדר $d_k(x) = y^a \pmod{n}$.

עכשו נתנו הגדרה מתמטית של הצופן RSA אנחנו נסביר את הסדר של הפעולות של הבניית המפתח, ההצפנה והפענוח באלגוריתם הבא.

הגדלה 6.2 אלגוריתם RSA



נניח שאليس (A) שלחת הודעה לבוב (B).

שלב הבניית המפתח

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

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

[3] B בוחר מספרשלם b באקראי כך שהשני תנאים הבאים מתקיימים:

$$\begin{aligned} 1 < b < \phi(n) &\bullet \\ \gcd(b, \phi(n)) = 1 &\bullet \end{aligned}$$

[4] B מחשב a לפי $a = b^{-1} \bmod \phi(n)$ בעזרת האלגוריתם של אוקלידס (ראו כלל 1.12).

[5] B שלוח את המפתח ציבורי (n, b) לאليس, אך בוב לא מגלה את המפתח הסודי (a, p, q) לאليس.

בנייה מפתח עשויה פעם אחת.

שלב הצפנה

[6] אליס (A) מקבלת את המפתח הציבורי (n, b) מבוב, ומצפינה את הטקסט הגרפי x עם המפתח הציבורי
באמצעות הכלל מצפין

$$y = x^b \pmod{n}.$$

[7] A שולחת את טקסט מוצפן ל- B.

שלב הפענוח

[8] בוב מפענח את הטקסט מוצפן עם המפתח הסודי באמצעות הכלל מפענח $y^a \pmod{n}$.

דוגמה 6.1

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

a) חשבו את n ו- a .

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

c) כעת בוב מפענח את הטקסט מוצפן שהוא קיבל מלאיס בעזרת המפתח (a, p, q) . בדקו כי הפענוח של הטקסט מוצפן מסעיף ב' זהה לטקסט גלי אשר אליס שלחנה.

פתרונות:

סעיף a)

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

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

a. נשתמש באלגוריתם של אוקליד: $a = 47^{-1} \pmod{23940}$

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

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

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

מכאן

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

שיטת 2

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

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

$$17 = 13 + 4$$

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

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

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

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

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

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

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

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

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

$$\text{לכן } a^{-1} = 5603$$

סעיף ב) אליס שולחת את הודעה $2468^{47} \pmod{24257}$. כדי לחשב זה משתמש 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

$$2468^{47} = (2468)^{32} \times (2468)^8 \times (2468)^4 \times (2468)^2 \times 2468 \pmod{24257}$$

$$= 20859 \times 9077 \times 4212 \times 2517 \times 2468 \pmod{24257}$$

$$= 10642 \pmod{24257} .$$

$$\text{לכן הtekסט מוצפן הוא } y = 10642$$

$$\text{סעיף ג) } y = 10642$$

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

לכן

$$x_1 = (y \pmod{p})^{a \pmod{(p-1)}} \pmod{p} = 101^{59} \pmod{127} = 55$$

(ניתן לחשב זה לפי $.101^{32} \times 101^{16} \times 101^8 \times 101^2 \times 101$)

$$(101)^2 \equiv 41 \pmod{127}$$

$$(101)^4 \equiv (41)^2 \pmod{127} \equiv 30 \pmod{127}$$

$$(101)^8 \equiv (30)^2 \pmod{127} \equiv 11 \pmod{127}$$

$$(101)^{16} \equiv (11)^2 \pmod{127} \equiv 121 \pmod{127}$$

$$(101)^{32} \equiv (121)^2 \pmod{127} \equiv 36 \pmod{127}$$

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

$$x_2 = (y \pmod{q})^{a \pmod{(q-1)}} \pmod{q} = 137^{93} \pmod{191} = 176$$

(ניתן לחשב זה לפי $.137^{64} \times 137^{16} \times 137^8 \times 137^4 \times 137$)

$$(137)^2 \equiv 51 \pmod{191}$$

$$(137)^4 \equiv (51)^2 \pmod{191} \equiv 118 \pmod{191}$$

$$(137)^8 \equiv (118)^2 \pmod{191} \equiv 172 \pmod{191}$$

$$(137)^{16} \equiv (172)^2 \pmod{191} \equiv 170 \pmod{191}$$

$$(137)^{32} \equiv (170)^2 \pmod{191} \equiv 59 \pmod{191}$$

$$(137)^{64} \equiv (59)^2 \pmod{191} \equiv 43 \pmod{191}$$

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 עליינו 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 $y_1 = M_1^{-1} \pmod{m_1} = 191^{-1} \pmod{127}$

שיטת 1

$$a = 191, b = 127$$

$$\begin{array}{ll} r_0 = a = 191, & r_1 = b = 127, \\ s_0 = 1, & s_1 = 0, \\ t_0 = 0, & t_1 = 1. \end{array}$$

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

$$\begin{aligned} 191^{-1} &\equiv 2 \pmod{127} \\ 127^{-1} &\equiv (-3) \pmod{191} \equiv 188 \pmod{191}. \end{aligned}$$

שיטת 2

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

$$\begin{aligned} 191 &= 127 \cdot 1 + 64 \\ 127 &= 64 \cdot 1 + 63 \\ 64 &= 63 \cdot 1 + 1 \\ 63 &= 1 \cdot 63 + 0. \end{aligned}$$

לכן

$$\gcd(191, 127) = 1$$

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

לכן

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

נחשב

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

לכן

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

■

6.2 משפט השאריות הסיני

משפט 6.1 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 שקיים

$$\begin{aligned} x &= a_1 \pmod{m_1}, \\ x &= a_2 \pmod{m_2}, \\ &\vdots \\ x &= a_r \pmod{m_r}, \end{aligned}$$

קיימים פתרון יחיד מודולו $M = m_1 m_2 \cdots m_r$ שנייתן על ידי

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

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

דוגמה 6.2

היעזרו במשפט השאריות הסיני כדי לפתור את המערכת

$$\begin{aligned} x &= 22 \pmod{101}, \\ x &= 104 \pmod{113}. \end{aligned}$$

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 באלגוריתם המוכפל של אוקlid.

נסמן $a = 113, b = 101$

$$\begin{array}{ll} r_0 = a = 113, & r_1 = b = 101, \\ s_0 = 1, & s_1 = 0, \\ t_0 = 0, & t_1 = 1. \end{array}$$

$q_1 = 1$	$t_2 = 0 - 1 \cdot 1 = -1$	$s_2 = 1 - 1 \cdot 0 = 1$	$r_2 = 113 - 1 \cdot 101 = 12$	שלב 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 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 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 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 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

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

-1

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

לכז

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

-1

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

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

■

6.3 משפטים של מספרים ראשוניים

משפט 6.2 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 וקובוצת זו נוצרת סופית.

נגידר השלם $M = (p_1 \cdot p_2 \cdot \dots \cdot p_n) + 1$. לפי משפט הפירוק לראשוניים (ראו המשפט 1.4 לעילו או משפט 6.3 למטה) הוא מספר ראשוני או שווה למכפלה של ראשוניים.

M לא מספר ראשוני בגלל ש- $p_i > M$ לכל $i \leq n$. 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 6.3 משפט הפירוק לראשוניים

(ראו משפט 1.4) לכל מספרשלם 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 6.4

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

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

הוכחה: (להעשרה בלבד)

משפט 6.5

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.

בנוסף לכך רק אם m שווה לכפולה של p , כלומר $m \in \{p, 2p, 3p, \dots, p^{n-1}p\}$.

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

משפט 6.6 נוסחה לפונקציית אוילר

(ראו משפט ??) לכל מספרשלם 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 6.4 - 1.

דוגמה 6.3

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 6.7

אם p מספר ראשוני אז

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

הוכחה: משפט 6.4 - 1.

משפט 6.8

אם p ו- q מספרים ראשוניים שונים אז

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

הוכחה: תרגיל בית.

משפט 6.9 המשפט הקטן של פרמה

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

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

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

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

הוכחה:

טענה 1. נוכח באינדוקציה.

בסיס:

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

מעבר:

נניח כי הטענה מתקיימת עבור a .

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

הנחה האינדוקציה אומרת ש- $a^p \equiv a \pmod{p}$ נכון

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

כנדרש.

טענה 2. $\gcd(a, p) = 1$ לפיכך קיים a^{-1} איבר הופכי $a^p \equiv 1 \pmod{p}$ ב- \mathbb{Z}_p 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 6.10 משפט אוילר

אם a, n שלמים ו- $\gcd(a, n) = 1$ אז $a^{\phi(n)} \equiv 1 \pmod{n}$.

משפט 6.11

אם a, n שלמים ו- $\gcd(a, n) = 1$ אז $a^{-1} \equiv a^{\phi(n)-1} \pmod{n}$.

דוגמה 6.4

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

פתרון:

לפי משפט פרימט 6.9:

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

לפי הנוסחת לשארית ?? :

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

$$\text{לכן } 5^{-1} \in \mathbb{Z}_{11} = 9.$$

6.4 הוכחה שצופן RSA ניתן לפענוח

משפט 6.12 קריפטו-מערכת RSA ניתן לפענוח

יהי p, q מספרים ראשוניים שונים, $a, b \in \mathbb{Z}$ שלמים חיוביים כך ש- $(ab)^{-1} \equiv 1 \pmod{\phi(n)}$ אם $x \in \mathbb{Z}_n$ אז

$$(x^b)^a \equiv x \pmod{n}.$$

הוכחה: נתון כי $.ab = 1 \pmod{\phi(n)}$ לפי משפט 6.8 $\phi(n) = \phi(pq) = (p-1)(q-1)$

2

$$ab = 1 \pmod{\phi(n)} = 1 \pmod{(p-1)(q-1)}$$

לכן קיים $t \in \mathbb{Z}$ כך ש-

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

לכל $z \in \mathbb{Z}$ לפי משפט 6.9 $z^{p-1} = 1 \pmod{p}$. בפרט

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

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

משיקולות של סיימטריה באותה מידה

$$x^{ab-1} - 1 = 0 \pmod{q} \text{ ו } x^{ab-1} - 1 = 0 \pmod{p}$$

מכיוון ש- p ו- q זרים אז

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

לפיכך

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

נכפיל ב- x ונקבל

$$(x^a)^b = x \pmod{(pq)} .$$

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

■

6.5 צופן RSA המובלל

משפט 6.13

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

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

נגיד צופן חדש אשר זהה ל- RSA אלא $\lambda(n)$ הוחלף עם $\phi(n)$ וכך לאzioni הקריפטו-מערכת ניתנת לפענה.

הוכחה:

שלב 1) רושמים את הצופן:

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

שלב 2) נתון כי $(p-1, q-1) \cdot d = \gcd(p-1, q-1)$. ז"א שקיימים 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

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

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

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

שלב 4) מכיוון $ab \equiv 1 \pmod{\lambda(n)}$ ניתן למצוא t שולם 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 $y = x^{tq'}$ והשוינו השני מתקיים בಗלל ש- p מספר ראשוני. לפיכך

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

שלב 5) מכיוון $ab \equiv 1 \pmod{\lambda(n)}$ ניתן למצוא t שולם 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 $z = x^{tp'}$ והשוינו השני מתקיים בगלל ש- q מספר ראשוני. לפיכך

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

שלב 6) מכיוון ש- q, p 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 7

הבעית הפירוק של מספרים וצופן רבין

7.1 הבעית פירוק מספרים

7.2 צופן רבין

שיעור 8

צופן אל-גמאל

הגדלה 8.1 צופן אל-גמאל

יהי p מספר ראשוני (גדול), α יוצר של $(\mathbb{Z}_p^*, \times_p)$ ויהי $a \in \{2, 3, \dots, p-2\}$.
יהי הקבוצה טקסט גלי $P = \mathbb{Z}_p^*$ והקבוצה טקסט מוצפן $C = \mathbb{Z}_p^* \times \mathbb{Z}_p^*$. נגידיר קבוצת מפתחות

$$K = \{(p, \alpha, a, \beta) \mid \beta = \alpha^a \pmod{p}\}.$$

לכל $d = \{2, 3, \dots, p-2\}$ ו- $(y_1, y_2) \in P$, $x \in P$, $k = (p, \alpha, a, \beta) \in K$

$$e_k(x, d) = (y_1, y_2)$$

כאשר $y_1 = \beta^d x \pmod{p}$, $y_2 = \alpha^d \pmod{p}$

$$d_k(y_1, y_2) = (y_1^a)^{-1} y_2 \pmod{p}.$$

(p, α, β) מפתח ציבורי ו- a מפתח סודי.

משפט 8.1 צופן אל-גמאל צופן חוקי

אם p מספר ראשוני ו- α יוצר של $(\mathbb{Z}_p^*, \times_p)$, $a \in \{2, 3, \dots, p-2\}$, $x \in \mathbb{Z}_p^*$ אז לכל $d \in \{2, 3, \dots, p-2\}$

$$((\alpha^d)^a)^{-1} \beta^d x = x \pmod{p}.$$

הוכחה: תרגיל בית.

כלל 8.1 אלגורים הצפנה אל-גמאל

נניח שאليس (A) שולחת הودעה לבוב (B).

שלב הרכבת המפתח

- 1 B יוצר מספר ראשוני גדול p , ויווצר α של החבורה $(\mathbb{Z}_p^*, \times_p)$.
- 2 B בוחר באקראי שלם $a \in \{2, 3, \dots, p-2\}$.
- 3 B מחשב $\beta = \alpha^a \pmod{p}$.
- 4 B שומר את המפתח ציבורי (p, α, β) בכתב ציבורי ושמור על a כמפתח סודי.

שלב הצפנה

- 5 אליס (A) קוראת את המפתח ציבורי (p, α, β) מהכתב ציבורי.
- 6 A בוחרת באקראי שלם $d \in \{2, 3, \dots, p-2\}$.
- 7 כדי להצפין הודעה x כאשר $0 \leq x < p$, אליס (A) מחשבת $y_2 = \beta^d x \pmod{p}$ ו- $y_1 = \alpha^d \pmod{p}$.

8 A שולחת הטקסט מוצפן (y_1, y_2) ל- B .

9 כדי לפענח את הטקסט מוצפן (y_1, y_2) , B משמש המפתח הסודי a כדי לחשב את $x = ((y_1)^a)^{-1} y_2 \pmod{p}$.

דוגמה 8.1 הצפנה אל-גמאל

נניח כי אליס שולחת הטקסט גליי $x = 123$. בוב בוחר במספר ראשון $p = 727$, $\alpha = 80$ ומפתח סודי $a = 6$. אליס בוחרת ב- $d = 7$. מצאו את הטקסט מוצפן.

פתרון:

$$\beta = \alpha^a \pmod{p} = 80^6 \pmod{727} = 514 .$$

$$y_1 = \alpha^d \pmod{p} = 80^7 \pmod{727} = 408 , \quad y_2 = \beta^d x \pmod{p} = 514^7 \cdot 123 \pmod{727} = 390 .$$

דוגמה 8.2 הצפנה אל-גמאל

נניח כי בוב מקבל את הטקסט מוצפן $(y_1, y_2) = (408, 390)$. בוב בוחר במספר ראשון $p = 727$, $\alpha = 80$ ומפתח סודי $a = 6$. אליס בחרה ב- $d = 7$. פענחו את הקטע מוצפן.

פתרון:

$$\beta = \alpha^a \pmod{p} = 80^6 \pmod{727} = 514 .$$

$$x = ((y_1^a)^{-1}) y_2 \pmod{p} = ((480^6)^{-1}) \cdot 390 \pmod{727}$$

בעזרת משפט פרמה,

$$(408^6)^{-1} \pmod{727} = 408^{727-1-6} \pmod{727} = 408^{720} \pmod{727} = 375 .$$

שיעור 9

תורת שאנו

1.9. 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 מפענה האפשריים.

אנחנו נתיחס לטקסטים גלויים

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

כמשתנה מקרי (מ"מ) בדיד, אשר ערכו שווה לتوزيعה של בחרית טקסט גלי. כמו כן נתיחס למפתחות

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

כמשתנה מקרי בדיד אשר ערכו שווה למפתח הנבחר.

נסמן את הפונקציית הסתבותות של הטקסט גלי ב-

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

כלומר $P(X = x_i)$ מסמן את ההסתברות לבחור את הטקסט גלי x מתוך X .
נסמן את הפונקציית הסתבותות 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 .

הтекסט מוצפן $y = Y$ המתקבל באמצעות הטקסט גלי $x = X$ הנבחר והמתפתח $K = k$ הנבחר הוא גם משתנה מקרי בדיד שמוגדר

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

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

$$P(Y = y) = \sum_{k \in K} P(K = k) P(X = d_k(y)) . \quad (9.1)$$

ההסתברות מותנית $P(Y = y | X = x)$, כלומר ההסתברות לקבל הטקסט מוצפן y במידע כי הטקסט גלי x , היא בדיקת ההסתברות לבחור מפתח מסויים k אשר באמצעותו מקבלים y על ידי להצפין x עם המפתח זה k .

$$P(Y = y | X = x) = \sum_{\substack{k \in K \\ x = d_k(y)}} P(K = k) . \quad (9.2)$$

מכאן, לפי נוסחת בייס, $P(X = x|Y = y) = \frac{P(Y = y|X = x)P(X = x)}{P(Y = y)}$. נציב את המשוואת (9.1) ומשוואות (9.2) ונקבל את הביטוי

$$P(X = x|Y = y) = \frac{P(X = x) \sum_{\substack{k \in K \\ x = d_k(y)}} P(K = k)}{\sum_{k \in K} P(K = k)P(X = d_k(y))}. \quad (9.3)$$

דוגמה 9.1

נתונה קבוצת טקסט גליי $X = \{a, b\}$ עם פונקציית 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 פונקציית 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 $y \in Y$

פתרונות:

אפשר ליצוג את הкриpto-מערכת כמטריצה הצפנה:

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

נחשב את הפונקציית ההסתברות של Y :

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

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

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

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

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

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

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

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

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

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

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

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

הגדרה 9.1 סודיות מושלמת

אומרים כי לקריפטו-מערכת יש סודיות מושלמת אם

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

לכל $x \in X, y \in Y$.

ז"א הסתברות כי הטקסט גלי $x = X$, בידעה כי הטקסט מוצפן $y = Y$ שווה רק להסתברות כי הטקסט גלי הוא $x = X$ והבחירה של המפתח שבאמצעותו מתקבל הטקסט מוצפן y לא משפייע על הסתברות כי הטקסט גלי $x = X$.

משפט 9.1 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 הסתברות $P(Y = y)$ באמצעות (9.1). הקבוצה 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 ולכן $P(K = k) = \frac{1}{26}$

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

הכלל מצפין והכלל מפענה של צופן קיסר מוגדרים

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

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

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

הסכום בצד הימין הוא רק סכום של $P(X = k)$ מעל כל האיברים $k \in \mathbb{Z}_{26}$. 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 בשווון השני השתמשנו בתכונת הנרמול של הפונקציה הסתברות של המ"מ X .

מצד שני, לפי (9.2),

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

האילוץ על הסכום $x = d_k(y)$ אומר ש-

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

לכל $X \in \mathcal{X}$ ולכל $y \in \mathcal{Y}$ 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, קלומר אם $P_K(k) = \frac{1}{26}$ forall $k \in K$ 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 לפענה בתנאי שימושים בפתח מקורי חדש כל פעם שמצפינים אותן אחד של טקסט גלי.

למה 9.1 תנאי חילופי לסודיות מושלמת

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

$$P(Y = y | X = x) = P(Y = y). \quad (9.4)$$

למה 9.2

נתונה קריפטו-מערכת בעלת סודיות מושלמת.

אם $P(Y = y) > 0$ אז

1 קיים לפחות מפתח אחד $k \in K$ כך ש-

$$e_k(x) = y. \quad (2)$$

הוכחה:

1 לפי (9.4)

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

נציב (9.2) 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 9.2 משפט שאנו

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

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

$$P(K = k) = \frac{1}{|K|} \quad (2)$$

הוכחה:

1) נניח כי $|K| = |Y|$. קלומר

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

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 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 $c - , k_1, k_2, \dots, k_n$ כך ש- $y = e_{k_i}(x_i)$. לפי נוסחת בייס

$$\begin{aligned} P(X = x_i|Y = y) &= \frac{P(Y = y|X = x_i)P(X = x_i)}{P(Y = y)} \\ &\stackrel{(9.2)}{=} \frac{P(K = k_i)P(X = x_i)}{P(Y = y)} \end{aligned}$$

אם ל מערכת 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

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



9.2 המושג של מידע

נניח נניח ש- X משתנה מקרי אשר יכול לקבל אחת מארבע אפשרויות:

$$X \in \{a, b, c, d\} .$$

X ידוע לבוב (B) אבל לא ידוע לאלייס (A). כל שאלות ידעת הוא ש- X יכול להיות אחת האותיות $\{a, b, c, d\}$ בהסתברות שווה. אנחנו אומרים כי לאלייס יש אי-זדאות על הערך של X . כדי שאלייס תמצא את הערך של X אליס שואלת סדרת שאלות בינהירות (שאלות כן/לא) לבוב כדי לקבל מידע על המ"מ X עד שהיא תדע את הערך של X עם אי-זדאות אפס.

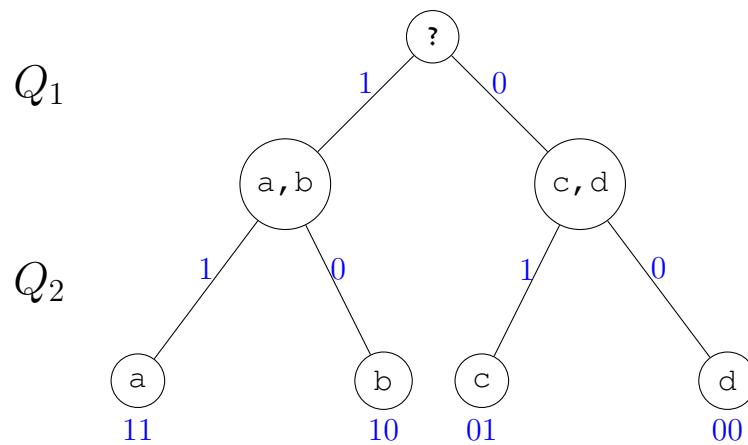
אפשרות אחת לסדרת שאלות היא כך:

$$Q_1: \text{האם } X \in \{a, b\}$$

לפי התשובה אחר כך אליס שואלה

$$Q_2: \text{אם } X = a \text{ האם } X \in \{a, b\}$$

$$Q_3: \text{אחרת אם } X \in \{a, b\}$$



הסדרה של שאלות בינהריות שמאפשרת לאليس למצוא את X ללא שופ אי-ודאות מותוארת בעץ-שאלות מעלה. מספר השאלות הבינהריות $N_Q[X]$, שנדרשות כדי למצוא X ללא אי-ודאות הוא $2 = N_Q[X]$.

כל שאלת היא בינהרית, 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 בינהריות נדרשות כדי למצוא את X , אנחנו אורמים כי נדרש שני ביטים (bits) של מידע כדי למצוא את X .

במילים אחרות, שתי ספרות בינהריות $X = d_1d_2$ נדרשות כדי להצפין את X , שערכן הן התשובות לשתי שאלות בינהריות,

לכן המידע המתקבל על מציאת הערך של X הוא 2 bit.

אליס הייתה יכולה לשנות את הסדרת שאלות שלה כך:

$$?X = a \text{ האם } Q'_1$$

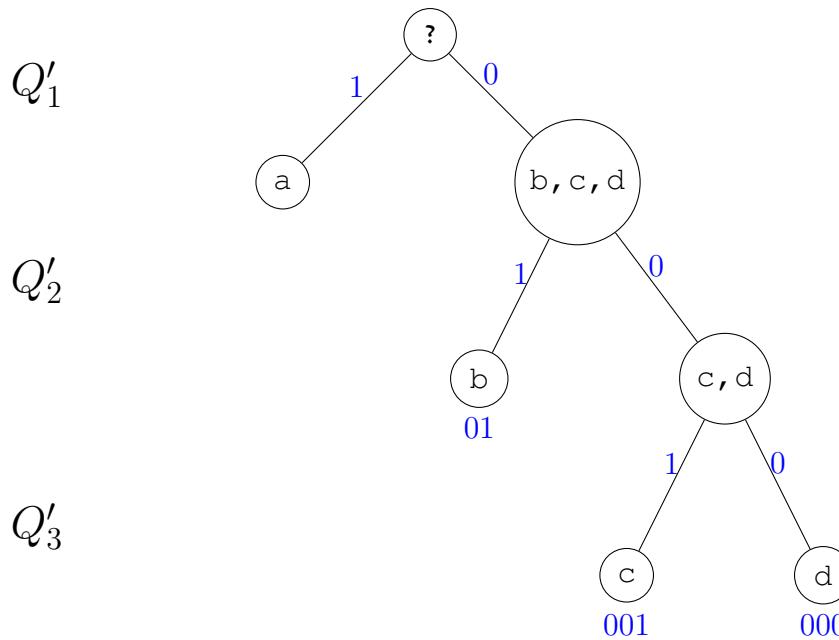
רק אם התשובה היא "לא" אז היא צריכה לשאול שאלה נוספת נוספת:

$$?X = b \text{ האם } Q'_2$$

ורק אם התשובה היא "לא" אז היא צריכה לשאול שאלה נוספת נוספת:

$$?X = c \text{ האם } Q'_3$$

מספר השאלות הבינהריות הנדרשות למצוא את X תלוי על הערך של X : $N_Q(b) = 2$, $N_Q(a) = 1$, $N_Q(c) = N_Q(d) = 3$.



X הוא משתנה מקרי בדיד ולכן בהינתן מערכת שאלות, ($N_Q(X)$) הוא פונקציה של משתנה מקרי בדיד, ולכן $N_Q[X]$ הוא בעצם משתנה מקרי בדיד.

כעת נשאל שאלה. נניח כי אין מעוניינות למצוא מערכת שאלות Q , אשר נותנת את מספר השאלות המומוצע המינימלי. כלומר, כיצד נמצא מערכת שאלות $N_Q[X]$ עבורה התוחלת

$$E[N_Q[X]] = \sum_{k \in X} P_X(k) N_Q[k]$$

תהייה מינימלית.

לפנינו שונעה על שאלה זו זאת נתן דוגמה.

נתון המשתנה מקרי $X = \{a, b, c, d\}$ בעל פונקציית ההסתברות

$$P_X(a) = \frac{1}{2}, \quad P_X(b) = \frac{1}{4}, \quad P_X(c) = P_X(d) = \frac{1}{8}.$$

עבור ההצפנה הראשונה Q , מספר השאלות הנדרשות כדי למצוא כל ערך של X הוא 2, שכן אז התוחלת תהייה

$$E_Q[N_Q[X]] = \frac{1}{2}(2) + \frac{1}{4}(2) + \frac{1}{8}(2) + \frac{1}{8}(2) = 2,$$

כלומר תוחלת המספר השאלות הוא 2.

עבור ההצפנה השנייה Q' תוחלת מספר השאלות 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 פחותה מהתוחלת עבור ההצפנה Q . מכאן אנחנו רואים כי יש קשר בין התוחלת של מספר השאלות הבינאריות לבין מערכת השאלות שאנו שואלים.

אליס שואלת סדרת שאלות ולכל שאלה נשים ערך ביןאיי 0 אם התשובה לא ו- 1 אם התשובה כן. כך אנחנו נשים לכל ערך של X מספר ביןאיי $d_1 \dots d_k$ המורכב מספרות ביןאיריות 0, 1. טרנספורמציה כזו בין ערכיים של X לבין מספרים ביןאירים נקראת הצפנה. שימו לב כי אורך ההצפנה $[X]_Q[\ell]$ של כל ערך של X שווה למספר השאלות ביןאיירות הנדרשות כדי למצוא את X ללא אי-זדאות:

$$\ell_Q[X] = N_Q[X].$$

משפט 9.3

יהי $X = \{x_1, x_2, \dots, x_k\}$ משתנה מקרי בדיד כך ש-

$$p_1 \geq p_2 \geq \dots \geq p_k$$

כאשר $(X = x_i) \ell_Q(x_i) = n_i$, כלומר x_i מוצפן על ידי מספר בינארי עם n_i ספרות בינאריות. התוחלת המינימלית מתקבלת על ידי ההצפנה שמיימת

$$n_1 \leq n_2 \leq \dots \leq n_k .$$

הוכחה: נניח בשלילה שקיימת תמורה $\{p_1, \dots, p_k\}$ של $\{p_{i_1}, \dots, p_{i_k}\}$. כך שהתווחלת

$$E = n_1 p_{i_1} + \dots + n_{j-1} p_{i_{j-1}} + n_j p_{i_j} + \dots + n_k p_{i_k} .$$

היא מינימלית. ללא הגבלת הכלליות נניח כי $p_{i_j} = p_1$. אז

$$E = n_1 p_{i_1} + \dots + n_{j-1} p_{i_{j-1}} + n_j p_1 + \dots + n_k p_{i_k} .$$

לכן אם נחליף p_1 עם n_{j-1} מקבל את התוחלת החדשה $p_{i_{j-1}} \leq p_1 = \max(p_1, \dots, p_n)$

$$E' = n_1 p_{i_1} + \dots + n_{j-1} p_1 + n_j p_{i_{j-1}} + \dots + n_k p_{i_k} .$$

$E < E'$ בסתיו לא ℓ_Q כי E התוחלת המינימלית המתקבלת עבור התמורה $(p_{i_1}, \dots, p_{i_k})$.

■

במשפט הבא אנחנו נוכיח כי אפשר לגוזר ביטוי בשביל התוחלת המינימלית באמצעות הפונקציית הסתברות של המשתנה מקרי X בלבד. נסמן

$$p_x = P_X(X = x) .$$

אנחנו ראיינו לעיל כי אורך ההצפנה של $x = X$ בהצפנה אופטימלית Q^* הוא פונקציה של הסתברות p_x , כלומר

$$\ell_{Q^*}(x) = f(p_x) . \quad (\#)$$

משפט 9.4 אנטרופיה של שאנו

נתון משתנה מקרי X בעל פונקציית הסתברות $P_X(x)$. התוחלת המינימלית של אורך ההצפנה של X מסומן ב- $H[X]$ ונתונה על ידי הנוסחה

$$H[X] = - \sum_{x \in X} P_X(x) \log_2 P_X(x) .$$

נקרא **האנטרופיה** של X .

הוכחה: נניח כי $Z = Y \cap X$, כאשר Y, Z משתנים מקרים בלתי תלויים. לפי משועואה (#):

$$\ell_Q(x) = f(p_x) .$$

$$H[X] = \sum p_x \ell_Q(x) = \sum p_x f(p_x) .$$

תהיינה $P_Z(z)$ ו- $P_Y(y)$ פונקציות הסתברות של Z ושל Y בהתאם. נסמן $p_z = P_Z(z)$ ו- $p_y = P_Y(y)$.

מכיוון ש- Y ו- Z משתנים בלתי תלויים אז

$$P(X = Y \cap Z) = P_Y(y)P_Z(z) = p_y p_z .$$

נשים לב שידיעה של Y לא נותנת שום מידע על הערך של Z , לכן

$$\ell_Q[Y \cap Z] = \ell_Q[Y] + \ell_Q[Z] .$$

לפיכך

$$H[X] = \sum p_x \ell_Q(x) = \sum p_y p_z [\ell_Q(y) + \ell_Q(z)]$$

מכאן

$$H[X] = \sum p_y p_z f(p_y p_z) = \sum p_y p_z [f(p_y) + f(p_z)]$$

$$f(p_y p_z) = f(p_y) + f(p_z) .$$

$$f(p) = C \log(p)$$

כעת נניח כי יש לנו משתנה מקרי $X = \{a, b\}$ בעל פונקציית ההסתברות $P_X(a) = \frac{1}{2}, P_X(b) = \frac{1}{2}$. ההצפנה של X צריכה ספרה אחת, לכן $f(\frac{1}{2}) = 1$ ונקבל $f(Q^*(a)) = f(Q^*(b)) = 1$.

■

9.3 הגדרה של מידע

הגדרה 9.2 מידע של מאורע (שאנו)

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 9.2 המידע המתקיים על קבלת תוצאה של הטלת מטבע

נטיל מטבע הוגנת ונגידר משתנה מקרי X להיות התוצאה. 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.

הסביר:

במקום הסימנים " H " ו- " T " בשביל המ"מ X ניתן להצפין את הערכים האפשריים בספרות בינהיות "0" או "1".
כלומר

ערך של X	הצפנה בספרות בינהיות
0	H
1	T

ז"א כדי להצפין את הערכים של X אנחנו צריכים ספרה בינהיות אחת:

$$d_1 \in \{0, 1\}.$$

אשר יכול להציג את הערכים 0 או 1.
■ ספרה בינהיות אחת נדרשת להצפין את הערך של X שכן המידע של ערך כלשהו של X הוא 1 (בית אחד).

דוגמה 9.3 שליפת קלף מחבילת קלפים תיינית

בניסוי שליפת קלף אחד מחבילת קלפים תיינית. נגיד משטנה מקרי X להיות הסוג של הקלף (תלון, עלה, לב או יהלום). חשבו את את המידע של המאורע שללפנו קלף מסווג לב.

פתרון:

הסתברות 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 ערכים אפשריים של X :

$$X = \{\spadesuit, \clubsuit, \heartsuit, \diamondsuit\}$$

כל ספרה בינהיות מחזיקה 2 ערכים אפשריים: 0 או 1 שכן ידרש שתי ספרות בינהיות כדי להצפין את ה-4 ערכים האפשריים של X :

$$d_1 d_2, \quad d_1, d_2 \in \{0, 1\}.$$

ההצפנה עצמה מתוארת בטבלה למטה:

ערך של X	הצפנה בספרות בינהיות
00	\spadesuit
01	\clubsuit
10	\heartsuit
11	\diamondsuit

אורך המספר $d_1 d_2$ הוא 2 שכן המידע של המשתנה מקרי X הוא 2 bits (שני ביטים).
■

דוגמה 9.4 שליפת קלף מחבילת קלפים תיינית



בניסוי שליפת קלף אחד מחבילת קלפים תיינית. מצאו את המידע המתkeletal אם הקלף נשלף.

תמונה	מספרים	צורה
		עליה
		תלון
		לב
		ילהום

פתרון:

יהי X המ"מ שמסמן את הקלף הנשלף. ההסתברות לשלוフ הקלף שלוש מסוג לב מחבילת קלפים סטנדרטית היא

$$P\left(X = \begin{array}{|c|} \hline 3 \\ \hline \spadesuit \\ \hline \end{array}\right) = \frac{1}{52}.$$

לכן

$$I\left(X = \begin{array}{|c|} \hline 3 \\ \hline \spadesuit \\ \hline \end{array}\right) = -\log_2\left(\frac{1}{52}\right) = 5.7 \text{ bits}$$

הסביר:

כדי להציג את כל הערכים האפשריים של X כמספר בינארי, נדרש רצף סיביות אשר מקבל לפחות 52 ערכים שונים. מספר בעל 5 סיביות לא מספיק מסיבה שיש לו רק $2^5 = 32$ ערכים שונים. אבל מספר בעל 6 סיביות נותן $2^6 = 64$ ערכים שונים, שמספיק להציג את כל הערכים האפשריים של X .

$$d_1 d_2 d_3 d_4 d_5 d_6$$

האורך של מספר זה הוא 6 ולכן הוא מחייב 6 bits של מידע. לכל סיבית יש 2 ערכים אפשריים ולכן 64 ערכים שונים בסה"כ.

נשים לב שرك 52 מותך ה- 64 צירופים נדרשים כדי להציג את הערכים האפשריים של X וכך אפשר להוריד את ■ החלק של הערכים המיוטרים. הקבוצת המספריים הנשארת מכילה 5.7 bits של מידע.

ככל שההסתברות של מאורע יותר קטנה אז המידע המתkeletal יותר גבוהה.

כלומר, ככל שהמידע של מאורע יותר גבוהה אז ההסתברות שלו יותר קטנה

דוגמה 9.5 (המשך של דוגמה 9.1)

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

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

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

■

במקרה שההתברות 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 9.5

נתון מ"מ בדיד X אשר מקבל N ערכים שונים

$$X = \{x_1, \dots, x_N\}$$

בנסיבות שווה, קלומר

$$P(X = x_i) = \frac{1}{N}$$

از האנתרופיה מקבלת ערך מקסימלי שנייה על ידי

$$H_{\max}(X) = \log_2 N .$$

ערך זה הוא הערך המקסימלי האפשרי של האנתרופיה.

דוגמה 9.6 אנתרופיה בהטלת מטבע

נניח כי נטיל מטבע עם הסתברות $p \leq 1$ (0) לקבל "H". יהיו X משתה מקרי ששויה ל吐וצאה הניסוי. מצאו את האנתרופיה של המ"מ מקרי X .

פתרון:

נסמן $\{0, 1\}$ כאשר $0 = X$ מסמן תוצאה H ו- $1 = X$ מסמן תוצאה T . פונקציית ההסתברות היא

$$P_X(0) = p , \quad P_X(1) = 1 - p .$$

לכן המידע של המאורע לקבל תוצאה H הוא

$$I(X = 0) = -\log_2(P_X(0)) = -\log_2(p)$$

והמידע של המאורע לקבל תוצאה H הוא

$$I(X = 1) = -\log_2(P_X(1)) = -\log_2(1 - p)$$

נשים לב שגם המטבע הוגנת או $p = \frac{1}{2}$ ו- $I(X = 0) = I(X = 1) = 1$ ו- $p = \frac{1}{2}$ -cut נחשב את האנתרופיה 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 האנתרופיה כפונקציה של ההסתברות p :

$$H(X) = -p \log_2 p - (1 - p) \log_2(1 - p) =: h(p).$$

ל- $p = \frac{1}{2}$ יש נקודת מקסימום ב-

$$h'(p) = -\frac{1}{\ln 2} - \log_2 p + \frac{1}{\ln 2} + \log_2(1 - p) = -\log_2 p + \log_2(1 - p) = \log_2 \left(\frac{1}{p} - 1 \right) \stackrel{!}{=} 0 \Rightarrow p = \frac{1}{2} .$$

ז"א הערך המקסימלי של האנתרופיה מתקיים כאשר לכל הערכים של X יש הסתברות שווה, ואכן

$$h(p = \frac{1}{2}) = -\frac{1}{2} \log_2 \frac{1}{2} - \frac{1}{2} \log_2 \frac{1}{2} = \log_2 2 = 1 .$$



דוגמה 9.7

בניסוי הטלת מטבח לא מאוזנת, ההסתברות לקבל תוצאה H היא $\frac{1}{1024} = p$. מצאו את האנטרופיה של X .

פתרון:

נסמן T כאשר $X = 0$ מסמן תוצאה H ו- $X = 1$ מסמן תוצאה 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 מטבח ללא מאוזנת 100,000 פעמים. בכדי להציג את כל התוצאות נדרש מספר בינארי עם 100,000 סיביות, כאשר כל ספרה נותנת התוצאה של ניסוי אחד. זו א"א 10^5 bits של מידע נדרש כדי להציג את כל התוצאות.

מצד שני מצאנו כי התוחלת של המידע המתkeletal לניסוי (כמוות מידע פר ניסוי) הוא 0.0112 bit פר ניסוי. במילימט לאחרות, ב- 10^5 ניסויים רק 1120 bit של מידע נדרש בממוצע כדי להציג את כל התוצאות של רצף ההצלחות.

9.4 הצפנה האפמן

סביר הצפנה האפמן בעזרת הדוגמה הבאה. נתון הטקסט גלי

$$X = \{a, b, c, d\}$$

ונניח כי פונקציית ההסתברות של X נתונה בטבלה הבאה:

$I(X = x_i) = -\log_2(p_i)$	$p_i = P_X(x_i)$	בחירה אותן של X
1.58 bit	$\frac{1}{3}$	a
1 bit	$\frac{1}{2}$	b
3.58 bit	$\frac{1}{12}$	c
3.58 bit	$\frac{1}{12}$	d

נשאל את השאלה: כמה ביטים של מידע נדרש כדי להציג (בסיביות) רצף של 1000 אותיות של טקסט גלי X ?

יש 4 אותיות ב- X , כולן 4 ערכים אפשריים של המ"מ בדיד X . לפיכך נדרש רצף של 2 סיביות כדי להציג טקסט גלי של TWO אחד בהצפנה סיביות קבועה. דוגמה:

בחירה אות של X	הצפנה
00	a
01	b
10	c
11	d

וזא להצפיןתו אחד של הטקסט גלי X נדרש bit 2. לכן להצפין רצף אותיות של טקסט גלי נדרש $2 \times 1000 = 2000$ bit, כולל 2000 סיביות.

האנטרופיה של X היא

$$H(X) = -p_1 \log_2(p_1) - p_2 \log_2(p_2) - p_3 \log_2(p_3) - p_4 \log_2(p_4) = 1.62581 \text{ bit} .$$

וזא לכל ניסוי המידע המומוצע הנדרש כדי להצפיןתו אחד של טקסט גלי הוא bit 1.62581. לכן המידע המומוצע הנדרש כדי להצפין רצף אותיות של טקסט גלי הוא

$$1000 \times 1.62581 = 1625.81 \text{ bit} .$$

לכן, רצף סיביות של אורך 1626 ב ממוצע יהיה מספיק כדי להעביר את ההודעה.

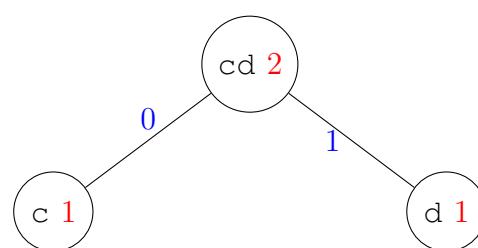
כעת נבנה הצפנה של הטקסט גלי על ידי האלגוריתם של האפמן.

שלב 1)

	c	d	a	b
	1	1	4	6

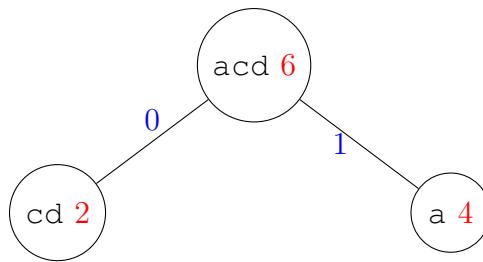
שלב 2)

	c	d	a	b
	1	1	4	6
	0	1		
	2	4	6	



שלב 3)

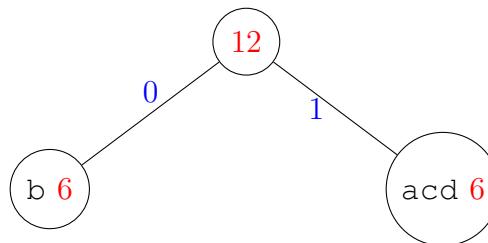
	cd	a	b
	2	4	6
	0	1	
	6	6	



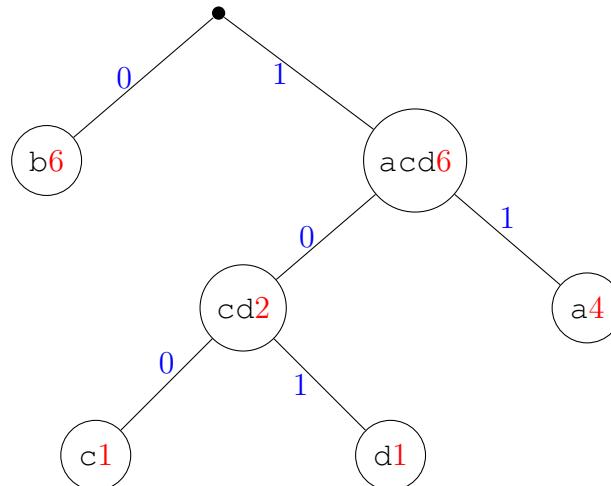
שלב 4)

שלב 5)

	acd	b
6		6
0		1
	12	



שלב 6)



בסוף של התהליך האותיות של הטקסט גלי יהיו בעלים של העץ והחצפנה ניתנת על ידי הריצף סיביות על הענפים במסלול מהנקודות הראשית של העץ עד העלה בו רשום האות בשאלת.

בחירה אות של $x_i \in X$	הצפנה האפמן
11	a
100	b
110	c
101	d

דוגמה 9.8

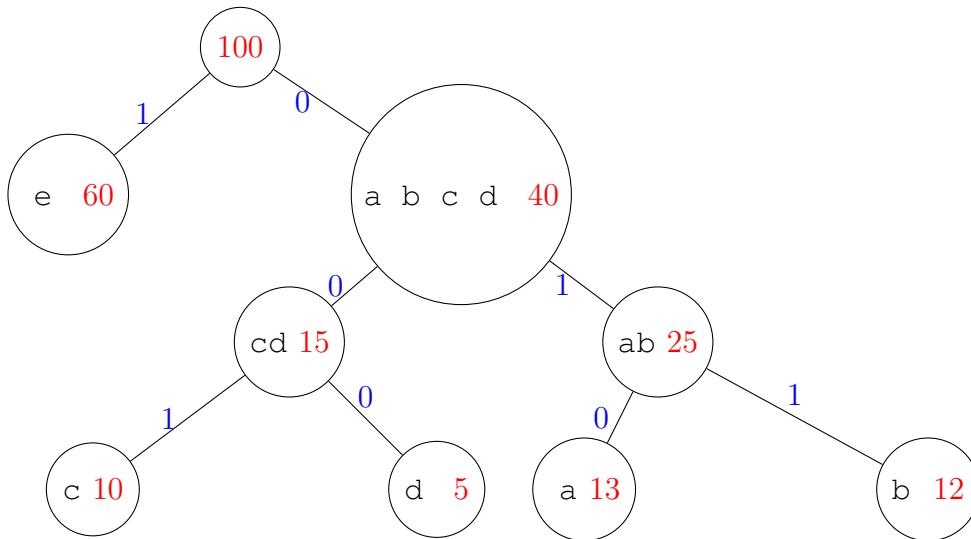
נתון הטקסט גליי הבא

$$X = \{a, b, c, d, e\}$$

והפונקציית 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 וההצפנה האפמן של כל תו של X .**פתרונות:**

בחירה האפמן $x_i \in X$	בחירה אוטומטית
010	a
011	b
001	c
000	d
1	e

פורמלי הבחירה האפמן מוגדרת לפי ההגדרה הבאה:

הגדרה 9.3 הבחירה האפמןנתון משתנה מקרי X . נגידר הבחירה האפמן של X להיות הפונקציה (כלל מיפוי)

$$f : X \rightarrow \{0, 1\}^*$$

כasher $\{0, 1\}^*$ קבוצת רצפים של סיביות סופיים.

נתון רצף מאורעות x_1, \dots, x_n . נגיד

$$f(x_1 \dots x_n) = f(x_1) || \dots || f(x_n)$$

כאשר " $||$ " מסמן שרשור (concatenation).

הגדלה 9.4 תוחלת האורך של הצפנה האפמן

נתונה הצפנה האפמן f . תוחלת האורך של ההצפנה מוגדרת

$$l(f) = \sum_{x \in X} P(X = x) |f(x)| .$$

משפט 9.6 אי-שוויון האפמן

נתון קבוצת אותיות של טקסט גליי X והצפנה האפמן f . נניח כי $l(f)$ תוחלת האורך של ההצפנה ו- $H(X)$ האנטרופיה של הטקסט גליי. מתקיים

$$H(X) \leq l(f) \leq H(X) + 1 .$$

דוגמה 9.9 (המשך דוגמה 9.8)

נתון הטקסט גליי הבא

$$X = \{a, b, c, d, e\}$$

והפונקציית 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 ההצפנה האפמן.

2) מצאו את האנטרופיה.

3) הוכחו כי אי-שוויון האפמן של ההצפנה שמצאתם בדוגמה 9.8 לעלה מותקיים.

פתרונות:

סעיף 1)

$$l(f) = \frac{5}{100} \cdot 3 + \frac{10}{100} \cdot 3 + \frac{12}{100} \cdot 3 + \frac{13}{100} \cdot 3 + \frac{60}{100} \cdot 1 \\ = \frac{15 + 30 + 36 + 30 + 60}{100} \\ = \frac{180}{100} \\ = 1.8$$

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 $H(X) + 1 = 1.84018 , H(X) = 1.74018$ לכן $l(f) = 1.8$

$$H(X) \leq l(f) \leq H(X) + 1$$

מתקיים.



9.5 תכונות של אנטרופיה

הגדרה 9.5 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 9.7 אי-שוויון ינסן

נניח כי f פונקציה רציפה וקעורה ממש בקטע I . נתון מספרים ממשיים $a_1, \dots, a_n > 0$ כך ש- $\sum_{i=1}^n a_i = 1$.

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

אם $x_1 = \dots = x_n$ ורק אם $\sum_{i=1}^n a_i f(x_i) = f\left(\sum_{i=1}^n a_i x_i\right)$ $x \in I$

משפט 9.8

יהי

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

משתנה מקרי בדיד בעל פונקציית הסתברות

$$P_X(x_1) = p_1, \dots, P_X(x_n) = p_n,$$

$1 \leq i \leq n$ לכל $0 < p_i \leq 1$

$$H(X) \leq \log_2 n$$

אם ורק אם

$$p_i = \frac{1}{n}$$

לכל n

הוכחה: לפי אי-שוויון ינסן:

$$\begin{aligned} H(X) &= -\sum_{i=1}^n p_i \log_2 p_i \\ &= \sum_{i=1}^n p_i \log_2 \left(\frac{1}{p_i} \right) \\ &\leq \log_2 \left(\sum_{i=1}^n p_i \cdot \frac{1}{p_i} \right) \\ &= \log_2 \left(\sum_{i=1}^n 1 \right) \\ &= \log_2 n. \end{aligned}$$

בנוסח n אם ורק אם $H(X) = \log_2 n$

משפט 9.9

יהי $X = \{x_1, \dots, x_m\}$ משתנה מקרי בדיד בעל פונקציית הסתברות

$$P_X(x_1) = p_1, \dots, P_X(x_m) = p_m,$$

יהי $Y = \{y_1, \dots, y_n\}$ משתנה מקרי בדיד בעל פונקציית הסתברות

$$P_Y(y_1) = q_1, \dots, P_Y(y_n) = q_n,$$

$1 \leq i \leq n$ לכל $0 < q_i \leq 1$

$$H(X, Y) \leq H(X) + H(Y)$$

אם ורק אם X ו- Y בלתי תלויים.

הוכחה: (*להעשרה בלבד)
 פונקציית הסתברות של X היא $P_X(x_i) = p_i$ ופונקציית הסתברות של X היא $P_Y(y_i) = q_i$. נגדיר הפוקנציית הסתברות של המשתנה מקרי דו-ממדי:

$$r_{ij} = P(X = x_i, Y = y_j).$$

אז הפונקציית הסתבותות שולית של X היא

$$p_i = \sum_{j=1}^n r_{ij} , \quad \forall 1 \leq i \leq m$$

והפונקציית הסתבותות 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

$$\begin{aligned} H(X, Y) - H(X) - H(Y) &= \sum_{i=1}^m \sum_{j=1}^n r_{ij} \log_2 \frac{1}{r_{ij}} + \sum_{i=1}^m \sum_{j=1}^n r_{ij} \log_2 (p_i q_j) \\ &= \sum_{i=1}^m \sum_{j=1}^n r_{ij} \log_2 \left(\frac{p_i q_j}{r_{ij}} \right) \\ &\leq \log_2 \left(\sum_{i=1}^m \sum_{j=1}^n p_i q_j \right) \quad \text{(אי-שוויון ינסן)} \\ &= \log_2 1 \\ &= 0 . \end{aligned}$$

לכן

$$H(X, Y) - H(X) - H(Y) \leq 0 \quad \Rightarrow \quad H(X, Y) \leq H(X) + H(Y) .$$



הגדלה 9.6 אנטרופיה מותנית

יהיו X, Y משתנים מקריים בדים. נגיד

$$H(X|Y = y) = - \sum_{x \in X} P(X = x|Y = y) \log_2 P(X = x|Y = y) .$$

האנטרופיה מותנית תסומן $H(X|y)$ ותוגדר הממוצע המשוקל של $H(X|Y = y)$ ביחס להסתירות $P(Y = y)$

$$H(X|Y) = - \sum_{y \in Y} \sum_{x \in X} P(Y = y) P(X = x|Y = y) \log_2 P(X = x|Y = y) .$$

האנטרופיה המותנית $H(X|Y)$ מכמתת המידע הממוצע של המ"מ X המועברת אשר לא מוגלה באמצעות Y .

משפט 9.10

$$H(X, Y) = H(Y) + H(X|Y) .$$

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

$$H(Y) = - \sum_{j=1}^n q_j \log_2 q_j = - \sum_{i=1}^m \sum_{j=1}^n r_{ij} \log_2 q_j$$

$$H(X, Y) = - \sum_{i=1}^m \sum_{j=1}^n r_{ij} \log_2 r_{ij} .$$

-1

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 9.11

$$H(X|Y) \leq H(X)$$

אם ורק אם X ו- Y משתנים מקיימים בלתי-תלויים.

הוכחה: (*להעשרה בלבד)

לפי משפט 9.9, $H(X, Y) \leq H(X) + H(Y)$. נציב משפט 9.10 ונקבל

$$H(Y) + H(X|Y) \leq H(X) + H(Y) \Rightarrow H(X|Y) \leq H(X) .$$

בנוסף לפי משפט 9.9, $H(X, Y) = H(X) + H(Y)$, לכן

$$H(X|Y) = H(X)$$

אם ורק אם X, Y משתנים בלתי-תלויים.

9.6 משפט האנתרופיה לקריפטו-מערכת

משפט 9.12 משפט האנתרופיה 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 9.10,

$$H(K, P, C) = H(K, P) + H(C|K, P) .$$

בגלל שהכל מציין $y = e_k(x)$ הוא פונקציה חד-חד-ערכית, אז המפתח והטקסט גלי קבועים את הטקסט מוצפן בדרך ייחודית. ז"א

$$H(C|K, P) = 0 .$$

לכן

$$H(K, P, C) = H(K, P) . \quad (*1)$$

המשתנים מקרים K ו- P בלתי-תלויים. לכן לפי משפט 9.9 $H(K, P) = H(K) + H(P)$ ולפיכך נקבל

$$H(K, P, C) = H(K) + H(P) . \quad (*2)$$

באותה מידת, לפי משפט 9.10,

$$H(K, P, C) = H(K, C) + H(P|K, C) . \quad (*3)$$

מכיוון שהכל מפענה $x = d_k(y)$ פונקציה חד-חד ערכית, אז המפתח והטקסט מוצפן קובעים את הטקסט גלו' בדרך ייחודית. לכן

$$H(P|K, C) = 0 .$$

ומכאן

$$H(K, P, C) = H(K, C) . \quad (*4)$$

לפי משפט 9.10. $H(K, C) = H(C) + H(K|C)$

$$\begin{aligned} H(K|C) &= H(K, C) - H(C) \\ &= H(K, P, C) - H(C) \quad (\text{לפי } *4) \\ &= H(K) + H(P) - H(C) \quad (\text{לפי } *2) \end{aligned} \quad (9.5)$$

כנדרש.



דוגמה 9.10 (המשך של דוגמה 9.1 והמשך של דוגמה 9.5)

עבור דוגמה 9.1 מצאו את $H(K|C)$ ובדקו כי הערך המתתקבל תואם עם $H(C)$.

פתרונות:

בדוגמה 9.5 מצאנו כי $H(C) = 1.85$ ו- $H(K) = 1.5$, $H(P) = 0.81$
 $H(K|C) = H(K) + H(P) - H(C) = 0.46$

כעת נחשב את $H(K|C)$ בעזרת התוצאות של דוגמה 9.1:

$$P(K = k_1|C = 1) = \frac{P(C = 1|K = k_1) P(K = k_1)}{P(C = 1)} = \frac{\left(\frac{1}{4}\right) \left(\frac{1}{2}\right)}{\left(\frac{1}{8}\right)} = 1 ,$$

$$P(K = k_2|C = 1) = \frac{P(C = 1|K = k_2) P(K = k_2)}{P(C = 1)} = \frac{0 \left(\frac{1}{4}\right)}{\left(\frac{1}{8}\right)} = 0 ,$$

$$P(K = k_3|C = 1) = \frac{P(C = 1|K = k_3) P(K = k_3)}{P(C = 1)} = \frac{0 \left(\frac{1}{4}\right)}{\left(\frac{1}{8}\right)} = 0 ,$$

$$P(K = k_1|C = 2) = \frac{P(C = 2|K = k_1) P(K = k_1)}{P(C = 2)} = \frac{\left(\frac{3}{4}\right) \left(\frac{1}{2}\right)}{\left(\frac{7}{16}\right)} = \frac{6}{7} ,$$

$$P(K = k_2|C = 2) = \frac{P(C = 2|K = k_2) P(K = k_2)}{P(C = 2)} = \frac{\left(\frac{1}{4}\right) \left(\frac{1}{4}\right)}{\left(\frac{7}{16}\right)} = \frac{1}{7} ,$$

$$P(K = k_3|C = 2) = \frac{P(C = 2|K = k_3) P(K = k_3)}{P(C = 2)} = \frac{0 \left(\frac{1}{4}\right)}{\left(\frac{7}{16}\right)} = 0 ,$$

$$P(K = k_1|C = 3) = \frac{P(C = 3|K = k_1) P(K = k_1)}{P(C = 3)} = \frac{(0) \left(\frac{1}{2}\right)}{\left(\frac{1}{4}\right)} = 0 ,$$

$$P(K = k_2|C = 3) = \frac{P(C = 3|K = k_2) P(K = k_2)}{P(C = 3)} = \frac{\left(\frac{3}{4}\right) \left(\frac{1}{4}\right)}{\left(\frac{1}{4}\right)} = \frac{3}{4} ,$$

$$P(K = k_3|C = 3) = \frac{P(C = 3|K = k_3) P(K = k_3)}{P(C = 3)} = \frac{\left(\frac{1}{4}\right) \left(\frac{1}{4}\right)}{\left(\frac{1}{4}\right)} = \frac{1}{4} ,$$

$$P(K = k_1|C = 4) = \frac{P(C = 4|K = k_1) P(K = k_1)}{P(C = 4)} = \frac{(0) \left(\frac{1}{2}\right)}{\left(\frac{3}{16}\right)} = 0 ,$$

$$P(K = k_2|C = 4) = \frac{P(C = 4|K = k_2) P(K = k_2)}{P(C = 4)} = \frac{0 \left(\frac{1}{4}\right)}{\left(\frac{3}{16}\right)} = 0 ,$$

$$P(K = k_3|C = 4) = \frac{P(C = 4|K = k_3) P(K = k_3)}{P(C = 4)} = \frac{\left(\frac{3}{4}\right) \left(\frac{1}{4}\right)}{\left(\frac{3}{16}\right)} = 1 .$$

מבחן

$$\begin{aligned}
 H(K|C) &= - \sum_{y=1}^4 \sum_{k \in \{k_1, k_2, k_3, k_4\}} P(C=y)P(K=k|C=y) \log_2 P(K=k|C=y) \\
 &= - P_C(1)P_{K|C}(k_1|1) \log_2 P_{K|C}(k_1|1) - P_C(2)P_{K|C}(k_1|2) \log_2 P_{K|C}(k_1|2) \\
 &\quad - P_C(3)P_{K|C}(k_1|3) \log_2 P_{K|C}(k_1|3) - P_C(4)P_{K|C}(k_1|4) \log_2 P_{K|C}(k_1|4) \\
 &\quad - P_C(1)P_{K|C}(k_2|1) \log_2 P_{K|C}(k_2|1) - P_C(2)P_{K|C}(k_2|2) \log_2 P_{K|C}(k_2|2) \\
 &\quad - P_C(3)P_{K|C}(k_2|3) \log_2 P_{K|C}(k_2|3) - P_C(4)P_{K|C}(k_2|4) \log_2 P_{K|C}(k_2|4) \\
 &\quad - P_C(1)P_{K|C}(k_3|1) \log_2 P_{K|C}(k_3|1) - P_C(2)P_{K|C}(k_3|2) \log_2 P_{K|C}(k_3|2) \\
 &\quad - P_C(3)P_{K|C}(k_3|3) \log_2 P_{K|C}(k_3|3) - P_C(4)P_{K|C}(k_3|4) \log_2 P_{K|C}(k_3|4) \\
 &= - \frac{1}{8} \log_2 1 - \frac{7}{16} \cdot \frac{6}{7} \log_2 \frac{6}{7} - \frac{1}{4} \cdot 0 \log_2 0 - \frac{3}{16} \cdot 0 \log_2 0 \\
 &\quad - \frac{1}{8} 0 \cdot \log_2 0 - \frac{7}{16} \cdot \frac{1}{7} \log_2 \frac{1}{7} - \frac{1}{4} \cdot \frac{3}{4} \log_2 \frac{3}{4} - \frac{3}{16} \cdot 0 \log_2 0 \\
 &\quad - \frac{1}{8} \cdot 0 \log_2 0 - \frac{7}{16} \cdot 0 \log_2 0 - \frac{1}{4} \cdot \frac{1}{4} \log_2 \frac{1}{4} - \frac{3}{16} \cdot 1 \cdot \log_2 1 \\
 &= 0.461676 .
 \end{aligned}$$

הרי

$$H(K|C) = 0.46 = H(K) + H(P) - H(C)$$

כנדרש.



שיעור 10

צפנים בлокים ו- DES

10.1 רשות החלפה-תמורה

הגדרה 10.1 רשות החלפה-תמורה

נתון טקסט גליי $x \in \{0,1\}^n$ כרצף סיביות. מחלקים x ל- m קבוצות של אורך ℓ :

$$x = x_{<1>} || x_{<2>} || \cdots || x_{<m>}$$

כאשר

$$x_{<1>} = x_1 x_2 \cdots x_\ell, \quad x_{<2>} = x_{\ell+1} x_{\ell+2} \cdots x_{2\ell}, \quad x_{<m>} = x_{(m-1)\ell+1} x_{(m-1)\ell+2} \cdots x_{m\ell}.$$

ברשות החלפה-תמורה יש 4 מרכיבים:

- החלפה של אורך m , שנסמך $\pi_S : \{0,1\}^\ell \rightarrow \{0,1\}^\ell$
- תמורה של אורך $\ell m = n$ שנסמך $\pi_P : \{1, \dots, \ell m\} \rightarrow \{1, \dots, \ell m\}$
- מפתח התחלתי $.k$.
- זמן המפתחות (k^1, \dots, k^{N+1}) , אחד לכל שלב של ההצפנה.

האלגוריתם של ההצפנה הוא כמוerten להלן:

$$(1) \text{ מגדרים } w^0 = x.$$

$$(2) \text{ מחשבים } w^1 = w^0 \oplus k^1 \text{ כאשר } \oplus \text{ האופרטור XOR.}$$

$$(3) \text{ מבצעים את החלפה } \pi_S \text{ על כל תת-קבוצה } u_{<i>}^1 \text{ לכל } 1 \leq i \leq m \text{ עבור } .v_{<i>}^1 = \pi_S(u_{<i>}^1)$$

$$(4) \text{ מבצעים את התמורה } \pi_P \text{ על תת-קבוצה } v^1 \text{ עבור } .w_i^1 = v_{\pi_P(i)}^1$$

cut חזרים על שלבים (2)-(4):

$$(2') \text{ מחשבים } w^2 = w^1 \oplus k^2 \text{ כאשר } \oplus \text{ האופרטור XOR.}$$

$$(3') \text{ מבצעים את החלפה } \pi_S \text{ על כל תת-קבוצה } u_{<i>}^2 \text{ לכל } 1 \leq i \leq m \text{ עבור } .v_{<i>}^2 = \pi_S(u_{<i>}^2)$$

$$(4') \text{ מבצעים את התמורה } \pi_P \text{ על תת-קבוצה } v^2 \text{ עבור } .w_i^2 = v_{\pi_P(i)}^2$$

התהליך ממשיך עד שמניגים לסופי שלב ה- N -ית. בשלב N לא מוחשבים את w^N אלא מקבלים את הטקסט מוצפן לפי

$$y = v^N \oplus k^{N+1}.$$

דוגמה 10.1

נתון הטקסט גלי

$$x = 00100110.$$

נתונה ההחלפה $\pi_S : \{0,1\}^4 \rightarrow \{0,1\}^4$ שמוגדרת

z	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$\pi_S(z)$	D	4	3	1	2	F	B	8	3	A	6	C	5	9	0	7

נתונה התמורה $\pi_P : \{1, \dots, 8\} \rightarrow \{1, \dots, 8\}$ שמוגדרת

z	1	2	3	4	5	6	7	8
$\pi_P(z)$	8	5	4	2	3	6	1	7

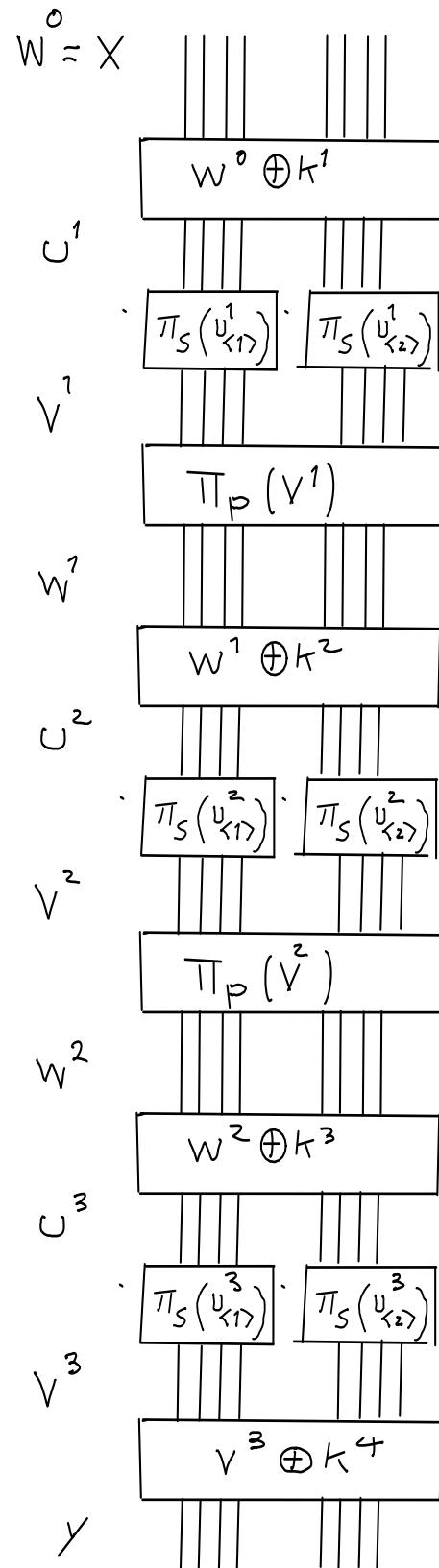
או בסימון מחזורי

$$(1 \ 8 \ 7) (2 \ 5 \ 3 \ 4) (6)$$

ונתנו מפתח התחלתי

$$k = 0011 \ 1010 \ 1001 \ 0100 \ 1111.$$

מספר השלבים בהצפנה הוא $N + 1$ כאשר $N = 2$. נגדיר תיזמו המפתחות (k^1, k^2, k^3) כאשר המפתח k^i רצף סיביות של אורך 8 אשר מתחילה עם הסיבית ה- $(4i - 3)$ ית של k . מצטו את הטקסט מוצפן.

**פתרונות:**

המפתחות של כל שלב של ההצפנה הם

$$\begin{aligned}k^1 &= 0011 \ 1010, \\k^2 &= 1010 \ 1001, \\k^3 &= 1001 \ 0100, \\k^4 &= 0100 \ 1111.\end{aligned}$$

שלב (1)

$$\begin{aligned}w^0 &= 0010 \ 0110 \\k^1 &= 0011 \ 1010 \\u^1 = w^0 \oplus k^1 &= 0001 \ 1100\end{aligned}$$

$$u^1 = u_{<1>} || u_{<2>} = 0001 || 1100$$

בבסיס הקסדצימלי:

$$u^1 = u_{<1>} || u_{<2>} = 1 || C$$

$$v^1 = \pi_S(u_{<1>}) || \pi_S(u_{<2>}) = \pi_S(1) || \pi_S(C) = 4 || 5$$

בבסיס בינארי:

$$v^1 = 0100 || 0101$$

$$w^1 = \pi_P(0100 \ 0101) = 1001 \ 0100$$

שלב (2)

$$\begin{aligned}w^1 &= 1001 \ 0100 \\k^2 &= 1010 \ 1001 \\u^2 = w^1 \oplus k^2 &= 0011 \ 1101\end{aligned}$$

$$u^2 = u_{<1>}^2 || u_{<2>}^2 = 0011 || 1101$$

בבסיס הקסדצימלי:

$$u^2 = u_{<1>}^2 || u_{<2>}^2 = 3 || D$$

$$v^2 = \pi_S(u_{<2>}^2) || \pi_S(u_{<2>}^2) = \pi_S(3) || \pi_S(D) = 1 || 9$$

בbasis בינארי:

$$v^2 = 0001 || 1001$$

$$w^2 = \pi_P(0001 \ 1001) = 1110 \ 0000$$

שלב (3)

$$\begin{aligned} w^2 &= 1110 \quad 0000 \\ k^3 &= 1001 \quad 0100 \\ u^3 = w^2 \oplus k^3 &= 0111 \quad 0100 \end{aligned}$$

$$u^3 = u_{<1>}^3 || u_{<2>}^3 = 0111 || 0100$$

בבסיס הקסדצימלי:

$$u^3 = u_{<1>}^3 || u_{<2>}^3 = 7 || 4$$

$$v^3 = \pi_S(u_{<2>}^3) || \pi_S(u_{<2>}^3) = \pi_S(7) || \pi_S(4) = 8 || 2$$

בבסיס בינארי:

$$v^3 = 1000 || 0010$$

$$\begin{aligned} v^3 &= 1000 \quad 0010 \\ k^4 &= 0100 \quad 1111 \\ y = v^3 \oplus k^4 &= 1100 \quad 1101 \end{aligned}$$



10.2 רשות פייסטל

הגדרה 10.2 רשות פייסטל (Feistel)

נתון טקסט גליי $x = \{0, 1\}^{2n}$ כרכף סיביות.

$$x = \underbrace{x_1 \dots x_n}_{L_0} \quad \underbrace{x_n \dots x_{2n}}_{R_0}$$

מחלקים את x לשני חצאים שננסמן ו- R_0 ו- L_0 :

ברשות פייסטל יש 4 מרכיבים:

- מספר שלם N אשר קובע את המספר של שלבים בתהליך הצפנה.

- מפתח התחלתי k .

- מערכת של N תת-מפתחות (k_1, \dots, k_N) , אחד לכל שלב של התהליך הצפנה.

- פונקציית ליבה $f : \{0, 1\}^n \rightarrow \{0, 1\}^n$.

$$1) \text{ מגדירים } R_0 = x_n \dots x_{2n}, L_0 = x_1 \dots x_n$$

$$. L_i = R_{i-1}, \quad R_i = L_{i-1} \oplus f(R_{i-1}, k_i)$$

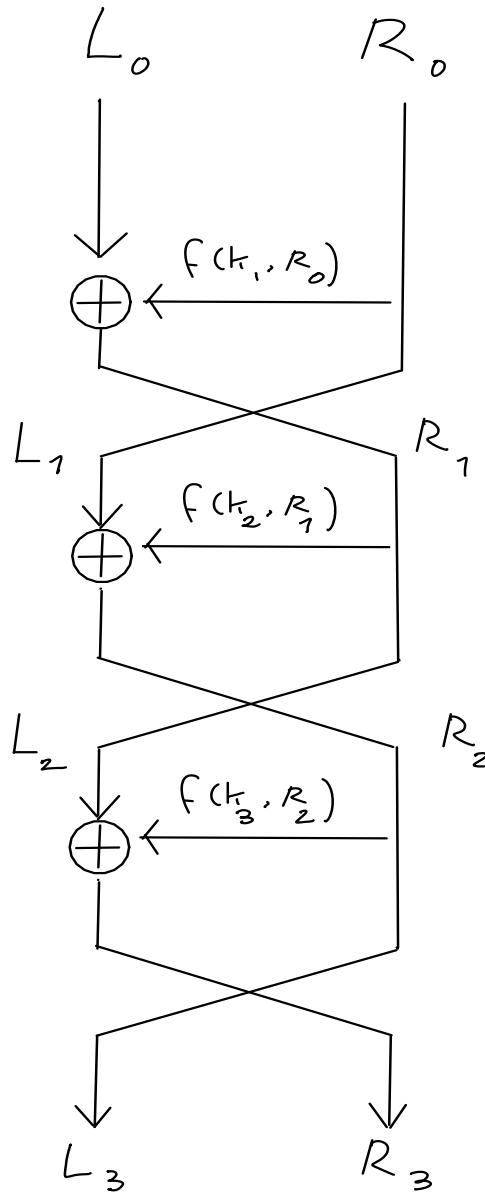
בשלב ה- i ית $(1 \leq i \leq N)$:

$$y = R_N L_N$$

בשלב ה- N קיבל את הטקסט מוצפן לפי

לדוגמה, עבור תהליך הצפנה עם $N = 3$ שלבים:

$$\begin{aligned} L_1 &= R_0 , & L_2 &= R_1 , & L_3 &= R_2 , \\ R_1 &= L_0 \oplus f(R_0, k_1) , & R_2 &= L_1 \oplus f(R_1, k_2) , & R_3 &= L_2 \oplus f(R_2, k_3) . \end{aligned}$$



דוגמה 10.2

נתון צופן פיזיטל שמוגדר עם הפונקציית ליבה המפתח הראשוני הוא התמורה π . כל תת-מפתח k_i הוא התמורה המתקבלת על ידי לבצע i פעמים את התמורה π . מצאו את טקסט מוצפן של הטקסט גליי 0010111001.

פתרונות:

הת מפתחות הם $R_0 = 11001$ ו- $L_0 = 00101$.

$$k_1 = (135)(24) , \quad k_2 = (153)(2)(4) , \quad k_3 = (1)(3)(5)(24) .$$

מכאן

$$L_1 = R_0 = 11001 .$$

$$R_1 = L_0 \oplus f(R_0, k_1) = 00101 \oplus 00111 = 00010 .$$

$$L_2 = R_1 = 00010 .$$

$$R_2 = L_1 \oplus f(R_1, k_2) = 11001 \oplus 00010 = 11011 .$$

$$L_3 = R_2 = 11011 .$$

$$R_3 = L_2 \oplus f(R_2, k_3) = 00010 \oplus 11011 = 11001 .$$

$$y = R_3 L_3 = 1100111011$$

■

משפט 10.1 משוואות פיסטל

משוואות פיסטל להצפנה:

נתון טקסט גלי $x = L_0 R_0$:
 $1 \leq i \leq N$.
 $L_i = R_{i-1}$, $R_i = L_{i-1} \oplus f(R_{i-1}, k_i)$, $y = R_N L_N$

משוואות פיסטל לענוה:

נתון טקסט גלי $y = R_N L_N$:
 $1 \leq i \leq N$.
 $R_i = L_{i+1}$, $L_i = R_{i+1} \oplus f(R_i, k_{i+1})$, $x = L_0 R_0$

דוגמה 10.3 ענוה של צופן פיסטל

текסט גלי של bit 10 היה מוצפן באמצעות צופן צוף פיסטל עם מפתח התחלה $(35)(124)$. כל תת מפתח $k = (124)(35)$ מתקבל על ידי לבצע התמורה התחלה i פעמים. הטקסט מוצפן הוא 1100001010 . מצאו את הטקסט גלי.

פתרונות:

התת מפתחות הם:

$$k_1 = (124)(35) , \quad k_2 = (142)(3)(5) , \quad k_3 = (1)(2)(4)(35) .$$

הtekסט מוצפן התקבל על ידי להפוך את השני חצאים, $R_3 = 11000$, $L_3 = 01010$. לכן, השלב 1 הוא:

$$R_2 = L_3 = 01010$$

-1

$$L_2 = R_3 \oplus f(R_2, k_3) = 11000 \oplus 01010 = 10010 .$$

שלב 2:

$$R_1 = L_2 = 10010 .$$

$$L_1 = R_2 \oplus f(R_1, k_2) = 01010 \oplus 11000 = 10010$$

שלב 3:

$$R_0 = L_1 = 10010 .$$

$$L_0 = R_1 \oplus f(R_0, k_1) = 10010 \oplus 01010 = 11000$$

לכן הטקסט גלי הוא

$$X = L_0 R_0 = 1100010010 .$$



10.3 תקן הצפנה מיידע (DES)

התקן הצפנה מיידע, באנגלית Data Encryption Standard ובראשי תיבות (DES), הוא צופן בלוקים סימטרי שפותח ב- 1974 במרכז המחבר של IBM בשיתוף פעולה עם הסוכנות לביטחון לאומי של ממשלת ארצות הברית.

שלב (1) נתון טקסט גלי $x = x_1 \dots x_{64}$ כרצף סיביות של 64 ביטים. בונים רצף סיביות x_0 באמצעות תמורה של הביטים של x לפי תמורה סטטistica הנקראת IP (initial permutation):

$$IP = \begin{pmatrix} 58 & 50 & 42 & 34 & 26 & 18 & 10 & 2 & 60 & 52 & 44 & 36 & 28 & 20 & 12 & 4 \\ 62 & 54 & 46 & 38 & 30 & 22 & 14 & 6 & 64 & 56 & 48 & 40 & 32 & 24 & 16 & 8 \\ 57 & 49 & 41 & 33 & 25 & 17 & 9 & 1 & 59 & 51 & 43 & 35 & 27 & 19 & 11 & 3 \\ 61 & 53 & 45 & 37 & 29 & 21 & 13 & 5 & 63 & 55 & 47 & 39 & 31 & 23 & 15 & 7 \end{pmatrix}$$

ז"א, לפי הטבלה,

$$IP \left(x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9, x_{10}, x_{11}, x_{12}, x_{13}, x_{14}, x_{15}, x_{16}, \right. \\ \left. x_{17}, x_{18}, x_{19}, x_{20}, x_{21}, x_{22}, x_{23}, x_{24}, x_{25}, x_{26}, x_{27}, x_{28}, x_{29}, x_{30}, x_{31}, x_{32}, \right. \\ \left. x_{33}, x_{34}, x_{35}, x_{36}, x_{37}, x_{38}, x_{39}, x_{40}, x_{41}, x_{42}, x_{43}, x_{44}, x_{45}, x_{46}, x_{47}, x_{48}, \right. \\ \left. x_{49}, x_{50}, x_{51}, x_{52}, x_{53}, x_{54}, x_{55}, x_{56}, x_{57}, x_{58}, x_{59}, x_{60}, x_{61}, x_{62}, x_{63}, x_{64} \right)$$

$$= x_{58}, x_{50}, x_{42}, x_{34}, x_{26}, x_{18}, x_{10}, x_2, x_{60}, x_{52}, x_{44}, x_{36}, x_{28}, x_{20}, x_{12}, x_4 \\ x_{62}, x_{54}, x_{46}, x_{38}, x_{30}, x_{22}, x_{14}, x_6, x_{64}, x_{56}, x_{48}, x_{40}, x_{32}, x_{24}, x_{16}, x_8 \\ x_{57}, x_{49}, x_{41}, x_{33}, x_{25}, x_{17}, x_9, x_1, x_{59}, x_{51}, x_{43}, x_{35}, x_{27}, x_{19}, x_{11}, x_3 \\ x_{61}, x_{53}, x_{45}, x_{37}, x_{29}, x_{21}, x_{13}, x_5, x_{63}, x_{55}, x_{47}, x_{39}, x_{31}, x_{23}, x_{15}, x_7$$

שלב (2) מחלקים $x_0 = IP(x)$ לשני חצאים:

$$x_0 = IP(x) = L_0 R_0 ,$$

כאשר L_0 ה-32 ביטים הראשונים של x_0 ו- R_0 ה-32 ביטים האחרונים:

$$L_0 = x_{58}, x_{50}, x_{42}, x_{34}, x_{26}, x_{18}, x_{10}, x_2, x_{60}, x_{52}, x_{44}, x_{36}, x_{28}, x_{20}, x_{12}, x_4$$

$$x_{62}, x_{54}, x_{46}, x_{38}, x_{30}, x_{22}, x_{14}, x_6, x_{64}, x_{56}, x_{48}, x_{40}, x_{32}, x_{24}, x_{16}, x_8 ,$$

$$R_0 = x_{57}, x_{49}, x_{41}, x_{33}, x_{25}, x_{17}, x_9, x_1, x_{59}, x_{51}, x_{43}, x_{35}, x_{27}, x_{19}, x_{11}, x_3$$

$$x_{61}, x_{53}, x_{45}, x_{37}, x_{29}, x_{21}, x_{13}, x_5, x_{63}, x_{55}, x_{47}, x_{39}, x_{31}, x_{23}, x_{15}, x_7 .$$

שלב (3) מבצעים 16 מחזוריים של אלגוריתם פיסטול מסוימים. מחשבים את $i \leq 16$ L_i, R_i לפי הכלל

$$L_i = R_{i-1}, \quad R_i = L_{i-1} \oplus f(R_{i-1}, k_i)$$

כאשר \oplus מסמן XOR ו- k_1, \dots, k_{16} התח-מפתחות שבנויים מרצפי סיביות, כל אחד של אורך 48 שמתקבלים ממפתח התחלתי k .

שלב (4) בסוף מפעילים התמורה ההפוכה IP^{-1} על הרצף סיביות $R_{16}L_{16}$ כדי לקבל הטקסט מוצפן הסופי y . ז"א

$$y = IP^{-1}(R_{16}L_{16}) .$$

כאשר

$$IP^{-1} = \begin{pmatrix} 40 & 8 & 48 & 16 & 56 & 24 & 64 & 32 & 39 & 7 & 47 & 15 & 55 & 23 & 63 & 31 \\ 38 & 6 & 46 & 14 & 54 & 22 & 62 & 30 & 37 & 5 & 45 & 13 & 53 & 21 & 61 & 29 \\ 36 & 4 & 44 & 12 & 53 & 20 & 60 & 28 & 35 & 3 & 43 & 11 & 51 & 19 & 59 & 27 \\ 34 & 2 & 42 & 10 & 50 & 18 & 58 & 26 & 33 & 1 & 41 & 9 & 49 & 17 & 57 & 25 \end{pmatrix}$$

הפונקציית ליבה של DES

בכל מחזור של DES מבצעים את הפונקציית ליבה

$$R_i = L_{i-1} \oplus f(R_{i-1}, k_i) .$$

מקבלת ארגומנט ראשון A אשר הוא רצף סיביות של אורך 32, וארגומנט שני J אשר רצף סיביות של אורך 48, ומהזירה רצף סיביות של אורך 32.

$$f : \{0, 1\}^{32} \times \{0, 1\}^{48} \rightarrow \{0, 1\}^{32} .$$

שלב (1) ראשית הפונקציית ליבה f הופכת A לרצף סיביות של אורך 48 באמצעות הפונקציה

$$E : \{0, 1\}^{32} \rightarrow \{0, 1\}^{48} .$$

היא תמורה של הסיביות של A עבורה 16 ספרות מופיעות פעמיים.

$$E = \begin{pmatrix} 32 & 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 6 & 7 & 8 & 9 \\ 8 & 9 & 10 & 11 & 12 & 13 \\ 12 & 13 & 14 & 15 & 16 & 17 \\ 16 & 17 & 18 & 19 & 20 & 21 \\ 20 & 21 & 22 & 23 & 24 & 25 \\ 24 & 25 & 26 & 27 & 28 & 29 \\ 28 & 29 & 30 & 31 & 32 & 1 \end{pmatrix}$$

שלב (2) מחשבים J ורושמים התוצאה כשירשור של שמונה רצפי סיביות של 6 ביטים

$$B = B_1B_2B_3B_4B_5B_6B_7B_8 .$$

שלב (3) בשלב זה משתמשים בkopfsאות הוחלפות $.S_1, S_2, S_3, S_4, S_5, S_6, S_7, S_8$

כל S_i היא מטריצה 4×16 אשר איבריה הם שלמים $0, 1, \dots, 15$.

כל S_i עובדת כפונקציה

$$S_j : \{0, 1\}^2 \times \{0, 1\}^4 \rightarrow \{0, 1\}^4 .$$

ספרטיבי, נתון רצף סיביות של אורך 6, $B_j = b_1 b_2 b_3 b_4 b_5 b_6$, אז

$$S_j(B_j) = S_j(r, c)$$

כאשר $S_j(r, c)$ הוא האיבר בשורה ה- r ועמודה ה- c של המטריצה S_i .

הביטויים $b_1 b_6$ קובעים את היצוג הבינארי של שורה r של S_j , והביטויים $b_2 b_3 b_4 b_5$ קובעים את היצוג הבינארי של עמודה c של S_j .

מגדירים

$$C_j = S_j(B_j) , \quad 1 \leq j \leq 8 .$$

שלב (4) מבצעים תמורה הסטי P על הרצף $C = C_1 C_2 C_3 C_4 C_5 C_6 C_7 C_8$ כאשר התמורה נתונה בטבלה למטה:

$$P = \begin{pmatrix} 16 & 7 & 20 & 21 \\ 29 & 12 & 28 & 17 \\ 1 & 15 & 23 & 26 \\ 5 & 18 & 31 & 10 \\ 2 & 8 & 24 & 14 \\ 32 & 27 & 3 & 9 \\ 19 & 13 & 30 & 6 \\ 22 & 11 & 4 & 25 \end{pmatrix}$$

הרץף סיביות המתקובל $P(C)$ מוגדר להיות $.f(A, J)$

התזמון המפתח של DES

נתון מפתח התחלתי k של 64 ביטים. משתמשים בו 56 סיביות של k בהרכבת התת-מפתחות k_1 .

שלב (1) מבצעים התמורה

$$PC_1 = \begin{pmatrix} 57 & 49 & 41 & 33 & 25 & 17 & 9 \\ 1 & 58 & 50 & 42 & 34 & 26 & 18 \\ 10 & 2 & 59 & 51 & 43 & 35 & 27 \\ 19 & 11 & 3 & 60 & 52 & 44 & 36 \\ 63 & 55 & 47 & 39 & 31 & 23 & 15 \\ 7 & 62 & 54 & 46 & 38 & 30 & 22 \\ 14 & 6 & 61 & 53 & 45 & 37 & 29 \\ 21 & 13 & 5 & 28 & 20 & 12 & 4 \end{pmatrix}$$

שלב (2) נסמן

$$PC_1(k) = C_0 D_0$$

כאשר C_0 הוא 28 סיביות הראשונות ו- D_0 הוא 28 סיביות האחרונות.

שלב (3) לכל $1 \leq i \leq 16$, מחשבים

$$C_i = LS_i(C_{i-1}) , \quad D_i = LS_i(D_{i-1}) .$$

$$k_i = PC_2(C_i D_i) .$$

הוא הזהה של מקום אחד או שני מקומות שמאליה:

$$LS_i = \begin{cases} \text{זהה מקום אחד שמאליה} & i = 1, 2, 9, 16, \\ \text{זהה שני מקומות שמאליה} & i = 3, 4, 5, 6, 7, 8, 10, 11, 12, 13, 14, 15 . \end{cases}$$

התמורה PC_2 היא

$$PC_2 = \begin{pmatrix} 14 & 17 & 11 & 24 & 1 & 5 \\ 3 & 28 & 15 & 6 & 21 & 10 \\ 23 & 19 & 12 & 4 & 26 & 8 \\ 16 & 7 & 27 & 20 & 13 & 2 \\ 41 & 52 & 31 & 37 & 47 & 55 \\ 30 & 40 & 51 & 45 & 33 & 48 \\ 44 & 49 & 39 & 56 & 34 & 53 \\ 46 & 42 & 50 & 36 & 29 & 32 \end{pmatrix}$$

הבלוקים של החלפות של DES

S_1	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13
S_2	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9
S_3	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12
S_4	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14
S_5	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3
S_6	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13
S_7	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12
S_8	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

דוגמאות

10.4

בצעו את האלגוריתם ליצירת תת-מפתחות לחשב k_1 מהמפתח המקורי

$$k = 133457799\text{BBCDF}FF1$$

פתרונות:

hex	1	3	3	4	5	7	7	9
binary	0001	0011	0011	0100	0101	0111	0111	1001

hex	9	B	B	C	D	F	F	1
binary	1001	1011	1011	1100	1101	1111	1111	0001

מכאן

$$k = 0001 \ 0011 \ 0011 \ 0100 \ 0101 \ 0111 \ 0111 \ 1001 \\ 1001 \ 1011 \ 1011 \ 1100 \ 1101 \ 1111 \ 1111 \ 0001 .$$

$$PC_1(k) = C_0 D_0$$

כasher

$$C_0 = 1111 \ 0000 \ 1100 \ 1100 \ 1010 \ 1010 \ 1111$$

$$D_0 = 0101 \ 0101 \ 0110 \ 0110 \ 0111 \ 1000 \ 1111 .$$

נבעז הזהה של ספרה אחד לשמאלו לקבול

$$C_1 = 111 \ 0000 \ 1100 \ 1100 \ 1010 \ 1010 \ 1111 \ 1$$

$$D_1 = 101 \ 0101 \ 0110 \ 0110 \ 0111 \ 1000 \ 1111 \ 0 .$$

$$PC_2(C_1 D_1) = k_1 = 0001 \ 1011 \ 0000 \ 0010 \ 1110 \ 1111 \ 1111 \ 1100 \ 0111 \ 0000 \ 0111 \ 0010 .$$

■

דוגמה 10.5

מצאו את ההצפנה אחורי מחזיר אחד של קריפטו-מערכת DES של הטקסט גלי

0123456789ABCDEF

עם מפתח התחלתי

133457799BBCDFF1

פתרונות:

תחליה נרשום את הטקסט מוצפן בסיביות:

hex	0	1	2	3	4	5	6	7
binary	0000	0001	0010	0011	0100	0101	0110	0111

hex	8	9	A	B	C	D	E	F
binary	1000	1001	1010	1011	1100	1101	1110	1111

אנחנו כבר חישבנו את התת-מפתח k_1 בדוגמה 10.4

$$k_1 = 0001 \ 1011 \ 0000 \ 0010 \ 1110 \ 1111 \ 1111 \ 1100 \ 0111 \ 0000 \ 0111 \ 0010 .$$

נפעיל תמורה הסטטיטית IP על הרץ סיביות 64 ביטים ונקבל

$$IP(x) = L_0 R_0$$

כasher

$$L_0 = 1100 \ 1100 \ 0000 \ 0000 \ 1100 \ 1100 \ 1111 \ 1111 ,$$

1

$$R_0 = 1111 \ 0000 \ 1010 \ 1010 \ 1111 \ 0000 \ 1010 \ 1010 ,$$

cut נחשב את $f(R_0, k_1)$

שלב (1)

$$E(R_0) = 0111 \ 1010 \ 0001 \ 0101 \ 0101 \ 0101 \ 0111 \ 1010 \ 0001 \ 0101 \ 0101 \ 0101 ,$$

שלב (2)

$$E(R_0) \oplus k_1 = 011000 \ 010001 \ 011110 \ 111010 \ 100001 \ 100110 \ 010100 \ 100111 ,$$

שלב (3) בעזרת הקופסאות S_i נחליף כל רצף 6- ביטים אם רצף 4- ביטים.

שלב (4) עברור הרצף 6- ביטים הראשון:

$$b_1 b_2 b_3 b_4 b_5 b_6 = 011000 ,$$

נקה שורה 00 ועמודה $b_1 b_6 = 00$ ועמודה $b_2 b_3 b_4 b_5 = 1100$ של הקופסה S_2 . זהי 5, אשר הוא 0101 בבסיס בינארי.
חזרים ומבצעים אותו חישוב על כל רצף 6- ביטים של $E(R_0) \oplus k_1$ כדי לקבל הרצף 32- ביטים:

$$C = 0101 \ 1100 \ 1000 \ 0010 \ 1011 \ 0101 \ 1001 \ 0111$$

שלב (5) מפעלים התמורה על C :

$$f(R_0, k_1) = P(C) = 0010 \ 0011 \ 0100 \ 1010 \ 1010 \ 1001 \ 1011 \ 1011$$

בסיום ו- $L_1 = R_0$

$$R_1 = L_0 \oplus f(R_0, k_1) = 1110 \ 1111 \ 0100 \ 1010 \ 0110 \ 0101 \ 0100 \ 0100$$



10.6 דוגמה

נתון הטקסט גלי

02468ACE13579BDF ,

נתון המפתח ההתחלתי

$$k = 010145458989CD\text{CD} ,$$

ונתנו כי התת-מפתח הראשון של קריפטו-מערכת DES הוא

$$k_1 = 0000 \ 1011 \ 0000 \ 0010 \ 0100 \ 0011 \ 1001 \ 1001 \ 0100 \ 1000 \ 0010 \ 0100 .$$

בצעו את המחרוז הראשון של הצפנה DES.

פתרון:

hex	0	2	4	6	8	A	C	E
binary	0000	0010	0100	0110	1000	1010	1100	1110
hex	1	3	5	7	9	B	D	F
binary	0001	0011	0101	0111	1001	1011	1101	1111

$$\text{כasher } IP(x) = L_0 R_0$$

$$L_0 = 1010 \ 1010 \ 1111 \ 0000 \ 1010 \ 1010 \ 1111 \ 0000$$

$$R_0 = 1100 \ 1100 \ 0000 \ 0000 \ 1100 \ 1100 \ 1111 \ 1111$$

כדי

להשתמש במשוואות פיזיטל נציגן לחשב את הפונקציית ליבת $f(R_0, k_1)$. תחילת משבבים את

$$E(R_0) = 1111 \ 1111 \ 0111 \ 1001 \ 0101 \ 0110 \ 0001 \ 0000 \ 0000 \ 1000 \ 0101 \ 1110.$$

מבצעים XOR של $E(R_0)$ עם k_1 ורושמים את התוצאה בקבוצות של 6 ביטים:

$$E(R_0) \oplus k_1 = 111011 \ 101000 \ 001001 \ 000010 \ 111111 \ 001101 \ 111111 \ 011011.$$

קופסה החלפה S1 שורה 11, عمودה 1101, ומקבלים את האיבר 0.

קופסה החלפה S2 שורה 10, عمودה 0100, ומקבלים את האיבר 10.

קופסה החלפה S3 שורה 01, عمودה 0100, ומקבלים את האיבר 3.

קופסה החלפה S4 שורה 00, عمودה 0001, ומקבלים את האיבר 13.

קופסה החלפה S5 שורה 11, عمودה 1111, ומקבלים את האיבר 3.

קופסה החלפה S6 שורה 01, عمودה 0110, ומקבלים את האיבר 9.

קופסה החלפה S7 שורה 11, عمودה 1111, ומקבלים את האיבר 12.

קופסה החלפה S8 שורה 01, عمودה 1101, ומקבלים את האיבר 14.

לכן

$$C = 0000 \ 1010 \ 0011 \ 1101 \ 0011 \ 1001 \ 1100 \ 1110$$

מבצעים את התמורה הסטטיטית: C

$$P(C) = f(R_0, k_1) = 1111 \ 1100 \ 0001 \ 1010 \ 0011 \ 0000 \ 1110 \ 0101$$

לבסוף אנחנו מקבלים

$$L_1 = R_0 = 1100 \ 1100 \ 0000 \ 0000 \ 1100 \ 1100 \ 1111 \ 1111$$

$$R_1 = L_0 \oplus f(R_0, k_1) = 0101 \ 0110 \ 1110 \ 1010 \ 1001 \ 1010 \ 0001 \ 0101$$

■

IDEA 10.4

הגדרה 10.3 פעולות בינאריות של IDEA

או מוציא XOR	\oplus
חיבור מודולו 2^n כאשר n שלים השווה לאורך של הבלוקים	\boxplus
כפל מודולו $1 + 2^n$	\odot

דוגמה 10.7

$$0110 \oplus 1011 = 1101 .$$

דוגמה 10.8

$$0110 \boxplus 1011 \xrightarrow{\text{ספרות דצימליות}} 6 \boxplus 11 = 6 + 11 \mod 2^4 = 1 \xrightarrow{\text{סיביות}} 0001 .$$

דוגמה 10.9

$$0110 \odot 1011 \xrightarrow{\text{ספרות דצימליות}} 6 \odot 11 = 6 \cdot 11 \mod 2^4 + 1 = 66 \mod 17 = 15 \xrightarrow{\text{סיביות}} 1111 .$$

דוגמה 10.10

$$0000 \odot 1011 \xrightarrow{\text{ספרות דצימליות}} 2^4 \odot 11 = 16 \cdot 11 \mod 2^4 + 1 = 176 \mod 17 = 6 \xrightarrow{\text{סיביות}} 0110 .$$

תת מפתחות של IDEA

נתון מפתח התחלתי k של IDEA של אורך 128 ביטים. כל הצפנה משתמשת ב- 6 תת מפתחות, וכל תפקoka משתמשת ב- 4 תת מפתחות. התת מפתחות מסומנות ב- $k_i^{(r)}$, $1 \leq i \leq 4$, $1 \leq r \leq 8$. התת מפתחות לדוגמה $k_1^{(9)}$, $k_2^{(1)}$, $k_3^{(4)}$, $k_4^{(1)}$. התת מפתחות מתקובלים על ידי לחלק k לשמונה תת-מפתחות, כל אחד של אורך 16 ביטים, ולאחר כך להזיז 25 בits מקום שמאלה. התת מפתחות המתקובלים מתוארים בטבלה למטה.

r	k_1	k_2	k_3	k_4	k_5	k_6
1	0 – 15	16 – 31	32 – 47	48 – 63	64 – 79	80 – 95
2	96 – 111	112 – 127	25 – 40	41 – 56	57 – 72	73 – 88
3	89 – 104	105 – 120	121 – 8	9 – 24	50 – 65	66 – 81
4	82 – 97	98 – 113	114 – 1	2 – 17	18 – 33	34 – 49
5	75 – 90	91 – 106	107 – 122	123 – 10	11 – 26	27 – 42
6	43 – 58	59 – 74	100 – 115	116 – 3	4 – 19	20 – 35
7	36 – 51	52 – 67	68 – 83	84 – 99	125 – 12	13 – 28
8	29 – 44	45 – 60	61 – 76	77 – 92	93 – 108	109 – 124
9	22 – 37	38 – 53	54 – 69	70 – 85	–	–

אלגוריתם ההצפנה

- נתון טקסט גליי P של אורך 64 ביטים.
 - מחלקים X לארבע בלוקים, כל אחד של אורך 16 ביטים:
- $$P = P_1 P_2 P_3 P_4 .$$
- בתחילה של מחזור ה- 1, נסמן את הטקסט מוצפן המתקבל ממחזור הקודם (מחזור $r - 1$) ב- $C^{(1)}, C^{(r)}$, בלבד מ-
 - כל מחזור r מורכב מהשלבים הבאים:

$$Y_1 = C_1^{(r)} \odot k_1^{(r)} = C_1^{(r)} \cdot k_1^{(r)} \pmod{2^{16} + 1} \quad [1]$$

$$Y_2 = C_2^{(r)} \boxplus k_2^{(r)} = C_2^{(r)} + k_2^{(r)} \pmod{2^{16}} \quad [2]$$

$$Y_3 = C_3^{(r)} \boxplus k_3^{(r)} = C_3^{(r)} + k_3^{(r)} \pmod{2^{16}} \quad [3]$$

$$Y_4 = C_4^{(r)} \odot k_4^{(r)} = C_4^{(r)} \cdot k_4^{(r)} \pmod{2^{16} + 1} \quad [4]$$

$$Y_5 = Y_1 \oplus Y_3 \quad [5]$$

$$Y_6 = Y_2 \oplus Y_4 \quad [6]$$

$$Y_7 = Y_5 \odot k_5^{(r)} = Y_5 \cdot k_5^{(r)} \pmod{2^{16} + 1} \quad [7]$$

$$Y_8 = Y_6 \boxplus Y_7 = Y_6 + Y_7 \pmod{2^{16}} \quad [8]$$

$$Y_9 = Y_8 \odot k_6^{(r)} = Y_8 \cdot k_6^{(r)} \pmod{2^{16} + 1} \quad [9]$$

$$Y_{10} = Y_7 \boxplus Y_9 = Y_7 + Y_9 \pmod{2^{16}} \quad [10]$$

$$C_1^{(r+1)} = Y_1 \oplus Y_9 \quad [11]$$

$$C_2^{(r+1)} = Y_3 \oplus Y_9 \quad [12]$$

$$C_3^{(r+1)} = Y_2 \oplus Y_{10} \quad [13]$$

$$C_4^{(r+1)} = Y_4 \oplus Y_{10} \quad [14]$$

הערכים Y_i נקראים הערכים הביניים. התפקיד i נקראות הטקסטים מוצפנים הביניים.

- בכדי לקבל את הטקסט מוצפן הסופי, אחרי השלבים של כל מחזור r מבצעים את השלב התפקיד:

$$C_1 = C_1^{(9)} \odot k_1^{(9)} = C_1^{(9)} \cdot k_1^{(9)} \pmod{2^{16} + 1} \quad [1]$$

$$C_2 = C_3^{(9)} \boxplus k_2^{(9)} = C_3^{(9)} + k_2^{(9)} \pmod{2^{16}} \quad [2]$$

$$C_3 = C_2^{(9)} \boxplus k_3^{(9)} = C_2^{(9)} + k_3^{(9)} \pmod{2^{16}} \quad [3]$$

$$C_4 = C_4^{(9)} \odot k_4^{(9)} = C_4^{(9)} \cdot k_4^{(9)} \pmod{2^{16} + 1} \quad [4]$$

- לבסוף הטקסט מוצפן 64- ביטים מתקבל מהארבע בלוקים 16- ביטים

$$C = C_1 C_2 C_3 C_4 .$$

דוגמאות

דוגמה 10.11

נתון מפתח התחלתי

$$k = 01010303030301010123\text{cdef}00110011$$

בצעו את המחזור הראשון של הצפנה IDEA על הטקסט גלי

$$P = 000f11111111000f$$

פתרונות:

רושמים את המפתח במונחי סיביות:

hex	0	1	0	1	0	3	0	3
binary	0000	0001	0000	0001	0000	0011	0000	0011
hex	0	3	0	3	0	1	0	1
binary	0000	0011	0000	0011	0000	0001	0000	0001
hex	0	1	2	3	c	d	e	f
binary	0000	0001	0010	0011	1100	1101	1110	1111
hex	0	0	1	1	0	0	1	1
binary	0000	0000	0001	0001	0000	0000	0001	0001

יצרים את התת מתחות למחזור הראשון:

$$k_1^{(1)} = 0000000100000001 = 257$$

$$k_2^{(1)} = 0000001100000011 = 771$$

$$k_3^{(1)} = 0000001100000011 = 771$$

$$k_4^{(1)} = 0000000100000001 = 257$$

$$k_5^{(1)} = 0000000100100011 = 291$$

$$k_6^{(1)} = 1100110111101111 = 52719$$

רושמים את הטקסט גלי במונחי סיביות:

hex	0	0	0	f	1	1	1	1
binary	0000	0000	0000	1111	0001	0001	0001	0001
hex	1	1	1	1	0	0	0	f
binary	0001	0001	0001	0001	0000	0000	0000	1111

מוצאים מחזור ראשון של ההצפנה:

$$\begin{aligned}
 P_1 &= C_1^{(1)} = 0000000000001111 = 15 , \\
 P_2 &= C_2^{(1)} = 0001000100010001 = 4369 , \\
 P_3 &= C_3^{(1)} = 0001000100010001 = 4369 , \\
 P_4 &= C_4^{(1)} = 0000000000001111 = 15 ,
 \end{aligned}$$

$$\begin{aligned}
 Y_1 &= C_1^{(1)} \odot k_1^{(1)} = 15 \cdot 257 \pmod{65537} = 3855 \Rightarrow Y_1 = 0000\ 1111\ 0000\ 1111 , \\
 Y_2 &= C_2^{(1)} \boxplus k_2^{(1)} = 4369 + 771 \pmod{65536} = 5140 \Rightarrow Y_2 = 0001\ 0100\ 0001\ 0100 , \\
 Y_3 &= C_3^{(1)} \boxplus k_3^{(1)} = 4369 + 771 \pmod{65536} = 5140 \Rightarrow Y_3 = 0001\ 0100\ 0001\ 0100 , \\
 Y_4 &= C_4^{(1)} \odot k_4^{(1)} = 15 \cdot 257 \pmod{65537} = 3855 \Rightarrow Y_4 = 0000\ 1111\ 0000\ 1111 , \\
 Y_5 &= Y_1 \oplus Y_3 = 0001\ 1011\ 0001\ 1011 = 6939 , \\
 Y_6 &= Y_2 \oplus Y_4 = 0001\ 1011\ 0001\ 1011 = 6939 , \\
 Y_7 &= Y_5 \odot k_5^{(1)} = 6939 \cdot 291 \pmod{65537} = 53139 \Rightarrow Y_7 = 1100\ 1111\ 1001\ 0011 , \\
 Y_8 &= Y_6 \boxplus Y_7 = 6939 + 53139 \pmod{65536} = 60078 \Rightarrow Y_8 = 1110\ 1010\ 1010\ 1110 , \\
 Y_9 &= Y_8 \odot k_6^{(1)} = 60078 \cdot 52719 \pmod{65537} = 45483 \Rightarrow Y_9 = 1011\ 0001\ 1010\ 1011 , \\
 Y_{10} &= Y_7 \boxplus Y_9 = 53139 + 45483 \pmod{65536} = 33086 \Rightarrow Y_{10} = 1000\ 0001\ 0011\ 1101 .
 \end{aligned}$$

התפוקה של מחזור הראשון הינה

$$\begin{aligned}
 C_1^{(2)} &= Y_1 \oplus Y_9 = 1011111010100100 \\
 C_2^{(2)} &= Y_3 \oplus Y_9 = 1010010110111111 \\
 C_3^{(2)} &= Y_2 \oplus Y_{10} = 1001010100101010 \\
 C_4^{(2)} &= Y_4 \oplus Y_{10} = 1000111000110001
 \end{aligned}$$

10.12 דוגמה

מצאו את המפתחות פענו של המחזור הראשון של IDEA בעזרת המפתח ההתחלתי

$$k = 00112233445566778899aabbcdddeeff .$$

פתרונות:

המפתחות לפענו הם

$$DK_1^{(1)} = \left(K_1^{(9)} \right)^{-1} ,$$

$$DK_2^{(1)} = - \left(K_2^{(9)} \right) ,$$

$$DK_3^{(1)} = - \left(K_3^{(9)} \right) ,$$

$$DK_4^{(1)} = \left(K_4^{(9)} \right)^{-1} ,$$

$$DK_5^{(1)} = K_5^{(8)} ,$$

$$DK_6^{(1)} = K_6^{(8)} .$$

hex	0	0	1	1	2	2	3	3	4	4	5
binary	0000	0000	0001	0001	0010	0010	0011	0011	0100	0100	0101
hex	5	6	6	7	7	8	8	9	9	a	a
binary	0101	0110	0110	0111	0111	1000	1000	1001	1001	1010	1010
hex	b	b	c	c	d	d	e	e	f	f	
binary	1011	1011	1100	1100	1101	1101	1110	1110	1111	1111	

$$k_1^{(9)} = 0100\ 0110\ 0110\ 1000 = 18024 . \quad :22 - 37$$

$$k_2^{(9)} = 1000\ 1010\ 1010\ 1100 = 35500 . \quad :38 - 53$$

$$k_3^{(9)} = 1100\ 1110\ 1111\ 0001 = 52977 . \quad :54 - 69$$

$$k_4^{(9)} = 0001\ 0011\ 0011\ 0101 = 4917 . \quad :70 - 85$$

$$k_5^{(8)} = 1011\ 1100\ 1100\ 1101 . \quad :93 - 108$$

$$k_6^{(8)} = 1101\ 1110\ 1110\ 1111 . \quad :109 - 124$$

$$DK_1^{(1)} = \left(K_1^{(9)}\right)^{-1} = (18024)^{-1} \mod 65537 = 45753 = 1011\ 0010\ 1011\ 1001 ,$$

$$DK_2^{(1)} = -\left(K_2^{(9)}\right) = -35500 \mod 65536 = 30036 = 0111\ 0101\ 0101\ 0100 .$$

$$DK_3^{(1)} = -\left(K_3^{(9)}\right) = -52977 \mod 65536 = 12559 = 0011\ 0001\ 0000\ 1111 .$$

$$DK_4^{(1)} = \left(K_4^{(9)}\right)^{-1} = (4917)^{-1} \mod 65537 = 18047 = 0100\ 0110\ 0111\ 1111 .$$

$$DK_5^{(1)} = K_5^{(8)} = 1011\ 1100\ 1100\ 1101 .$$

$$DK_6^{(1)} = K_6^{(8)} = 1101\ 1110\ 1110\ 1111 .$$

■

שיעור 11

פונקציות תמצות קריפטוגרפיות

11.1 פונקציות תמצות

11.2 אמינות המידע

שיעור 12

פונקציות תמצות קריפטוגרפיות המשך

12.1 פונקציות תמצות איטרטיביות

שיעור 13

שיטות חתימה

13.1 דרישות בטויות משיטות חתימה

13.2 שיטות חתימה של אל-גמאל

שיעור 14 סכבות לשיתוף סודות

14.1 סכמת הסך של שמיר

14.2 סכמת סך פשוטה (t, t)