קריפטוגרפיה

תוכן העניינים

1 תורת המספרים **3**
משפט החילוק של אוקלידס 3
מספרים ראשוניים 8
המחלק המשותף הגדול ביותר 10
האלגוריתם של אוקלידס 14
יחס השקילות המודולרית 19

2 חוגים מתמטיים **23**
הפונקצית אוילר 23
החוג $\mathbb{Z}_m$ 25
הפיכת מטריצות בחוג $\mathbb{Z}_m$ 28

3 הצפנים הבסיסיים **32**
מושג של קריפטו-מערכת 32
צופן ההזזה 33
צופן האפיני 35
צופן ויז'נר 41
צופן היל 45

4 תמורות וצופן אניגמה **54**
תמורות 54
פירוק למחזורים של תמורה 57
תמורות צמודות 60
צופן אניגמה 61
משפט רייבסקי 64
ההנחות של רייבסקי על צופן האניגמה 66

5 קריפטו-אנליזה **70**
סוגים של התקפת סייבר 70
קבוצות אותיות הנפוצים ביותר בטקסט גלוי 70
קריפטו-אנליזה של צופן האפיני 72
קריפטו-אנליזה של צופן היל 77
מדד צירוף המקרים 80
קריפטו-אנליזה של צופן ויז'נר - מבחן פרידמן 81

6 צופן RSA **86**
אלגוריתם RSA 86
משפט השאריות הסיני 92
משפטים של מספרים ראשוניים 93
הוכחה שצופן RSA ניתן לפענוח 96

צופן RSA המוכלל . . . 97

7 הבעיית הפירוק של מספירם וצופן רבין 99
הבעיית פירוק מספרים . . . 99
צופן רבין . . . 99

8 צופן אל-גמאל 100

9 תורת שאנון 102
סודיות מושלמת . . . 102
המושג של מידע . . . 109
הגדרה של מידע . . . 113
הצפנת האפמן . . . 118
תכונות של אנטרופיה . . . 123
משפט האנטרופיה לקריפטו-מערכת . . . 127

10 צפנים בלוקים ו- DES 131
רשת החלפה-תמורה . . . 131
רשת פייסטל . . . 135
תקן הצפנת מידע (DES) . . . 138
הפונקציית ליבה של DES . . . 139
התזמון המפתח של DES . . . 140
הבלוקים של ההחלפות של DES . . . 142
דוגמאות . . . 142
IDEA . . . 146
תת מפתחות של IDEA . . . 146
אלגוריתם ההצפנה . . . 147
דוגמאות . . . 148

11 פונקציות תמצות קריפטוגרפיות 151
פונקציות תמצות . . . 151
אמינות המידע . . . 151

12 פונקציות תמצות קריפטוגרפיות המשך 152
פונקציות תמצות איטרטיביות . . . 152

13 שיטות חתימה 153
דרישות בטיות משיטות חתימה . . . 153
שיטות חתימה של אל-גמאל . . . 153

14 סכמות לשיתוף סודות 154
סכמת הסף של שמיר . . . 154
סכמת סף (t,t) פשוטה . . . 154

שיעור 1
תורת המספרים

1.1 משפט החילוק של אוקלידס

הגדרה 1.1 מספר שלם שמחלק מספר שלם אחר

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

$$a = qb \ .$$

כלומר $\frac{a}{b}$ שווה למספר שלם q.

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

דוגמה 1.1

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

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

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

משפט 1.1 תכונות של חילוק שלמים

יהיו a, b, d שלמים.

1) אם $a \mid d$ ו- $b \mid d$ אזי $(a+b) \mid d$.

2) יהיו x, y שלמים. אם $a \mid d$ ו- $b \mid d$ אזי $(xa+yb) \mid d$.

3) אם $b \mid a$ ו- $a \mid b$ אזי $a = \pm b$.

הוכחה:

1)

$$\left.\begin{array}{lll} d|a & \Rightarrow & a = a'd \\ d|b & \Rightarrow & b = b'd \end{array}\right\} \quad \Rightarrow \quad a \pm b = d\,(a' + b') \quad \Rightarrow \quad d \mid (a+b) \ .$$

2)

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

3)

$$\left.\begin{array}{lll} a|b & \Rightarrow & b = ca \\ b|a & \Rightarrow & a = c'b \end{array}\right\} \quad \Rightarrow \quad b = ca = cc'b \quad \Rightarrow \quad cc' = 1 \ .$$

c ו- c' הם שלמים לכן $cc' = 1$ אם ורק אם $c = 1 = c'$ או $c = -1 = c'$. לפיכך

$$b = \pm a \ .$$

■

הגדרה 1.2 השארית

יהיו $a, b > 0$ שלמים. השארית של a בחלוקה ב- 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 עובר שלמים חיוביים בלבד!

דוגמה 1.2

$$\begin{aligned} 43 \bmod 10 &= 43 - 10 \cdot \left\lfloor \frac{43}{10} \right\rfloor &&= 43 - 10(4) &&= 3 \ , \\ 13 \bmod 4 &= 13 - 4 \cdot \left\lfloor \frac{13}{4} \right\rfloor &&= 13 - 4(3) &&= 1 \ , \\ 8 \bmod 2 &= 8 - 2 \cdot \left\lfloor \frac{8}{2} \right\rfloor &&= 8 - 2(4) &&= 0 \ . \end{aligned}$$

משפט 1.2 משפט החילוק של אוקלידס

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

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

כאשר $0 \leq r < |b|$. השלם q נקרא **המנה** של a בחלוקה ב- b ו- r נקרא **השארית** של a בחלוקה ב- b.
המשוואה (1.1) נקרא ה**פירוק מנה-שארית** של השלמים a ו- b.

ההוכחה עצמה היא לא חלק של הקורס.

דוגמה 1.3

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

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

דוגמה 1.4

יהיו $a = -46$, $b = 8$. המנה והשארית הם $q = -6$, $r = 2$ והפירוק מהן-שארית הוא

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

משפט 1.3 שיטה מעשית לחישוב הפירוק מנה–שארית

יהיו a,b שלמים (עם $b\neq 0$). אזי המנה q והשארית r במשפט החילוק של אוקלידס ניתנים כך:

1) אם $a>0,b>0$ אז $q=\left\lfloor\frac{a}{b}\right\rfloor$ ו- $r=a \bmod b$.

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

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

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

הוכחה: נוכיח בכל אחד מארבעת המקרים.

מצב 1) נניח $a>0,b>0$. לפי משפט החילוק של אוקלידס קיימים שלמים r, q כך ש-

(*)
$$a=qb+r,\qquad 0\le r<b.$$

נחלק ב-b:

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

מכיוון ש-$0\le r<b$, מתקיים $0\le\frac{r}{b}<1$, ולכן

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

הצבה חזרה ב-(*) נותנת

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

מצב 2) נניח $a>0,b<0$. לפי משפט החילוק של אוקלידס עבור הלשמים $|b|$, a קיימים שלמים $\bar{r}$, $\bar{q}$ כך ש:

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

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

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

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

$$a=qb+r\ ,\qquad 0\le r<|b|\ .$$

השוואה של משוואה (#) ל-$a=qb+r$ נותנת

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

מצב 3) נניח $a<0, b>0$. ממשפט החילוק עבור הלשמים $|a|$, b קיימים שלמים $\bar{r}$, $\bar{q}$ כך ש:

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

מהמקרה הראשון:

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

נציב $|a| = -a$:

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

כעת השארית $-\bar{r}$ שלילית, ואינה עומדת בתנאי $0 \le r < b$. לכן נוסיף ונחסר מנה אחת שלמה b:

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

כך קיבלנו את הצורה הנדרשת. מצד שני עבור השלמים a , b (כלומר a בלי הערך מוחלט) ממשפט החילוק קיימים שלמים q, r עבורם

$$a = qb + r \ , \qquad 0 \le r < b \ .$$

השוואה של זה עם משוואה (**) נותנת:

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

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

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

מ־(1) נקבל

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

נציב $|a| = -a, |b| = -b$:

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

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

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

מצד שני ממשפט החילוק עבור השלמים a , b (לא הערכים מוחלטים שלהם) קיימים שלמים q, r עבורם:

$$a = qb + r \ , \qquad 0 \le r < |b| \ .$$

השוואה של $a = qb + r$ למשוואה (##) נותנת:

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

לסיכום, מתקבלת הטבלה הבאה:

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

■

דוגמה 1.5

מצאו את הפירוק מנה-שארית של השלמים הבאים:

א) $a = 46\,,\ b = 8$.

ב) $a = -46\,,\ b = 8$.

ג) $a = 101\,,\ b = -7$.

ד) $a = -151\,,\ b = -12$.

פתרון:

א) במקרה זה $a > 0\,,\ b > 0$ אז

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

לכן:

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

ב) במקרה זה $a < 0\,,\ b > 0$ אז

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

ו-

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

לכן:

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

ג) במקרה זה $b<0$, $a>0$ אז

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

ו-

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

לכן:

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

ד) במקרה זה $b<0$, $a<0$ אז

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

ו-

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

לכן:

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

■

1.2 מספרים ראשוניים

הגדרה 1.3 מספר ראשוני

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

$$a\mid p \qquad \Longleftrightarrow \qquad a=1\vee p\ .$$

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 $e_1,\ldots,e_n$ עבור

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

כאשר $p_1,\ldots,p_n$ 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. אזי קיים לפחות מספר טבעי אחד שלא ראשוני וגם לא שווה למכפלה של ראשוניים.
- יהי $m \geq 2$ הטבעי הקטן ביותר שלא מקיים הטענה זו. (m הוא הדוגמה הנגדית הקטנה ביותר.)
- אזי m לא ראשוניי וגם לא שווה למכפלת ראשוניים.
- לכן m פריק, ז"א קיימים טבעיים $2 \leq a < m, \ 2 \leq b < m$ כך ש:
$$m = ab \ .$$
- m הוא הטבעי הקטן ביותר מסוג זה שמפריך את הטענה בעוד a, b הם קטנים ממש מ- m אז a ו- b בהכרח מקיימים את הטענה: ז"א a הוא או ראשוני או שווה למכפלת ראשוניים, ואותו דבר עבור b.
- לכן קיימים טבעיים $e_1, \ldots, e_n$ עבורם
$$a = p_1^{e_1} \ p_2^{e_2} \ \ldots \ p_n^{e_n}$$
כאשר $p_1, \ldots, p_n$ מספרים ראשוניים וקיימים טבעיים $f_1, \ldots, f_n$ עבורם
$$b = q_1^{f_1} \ q_2^{f_2} \ \ldots \ q_n^{f_n}$$
כאשר $q_1, \ldots, q_n$ מספרים ראשוניים.
- מכאן
$$m = ab = p_1^{e_1} \ p_2^{e_2} \ \ldots \ p_n^{e_n} \ q_1^{f_1} \ q_2^{f_2} \ \ldots \ q_n^{f_n} \ .$$
לכן m שווה למכפלה של מספרים ראשוניים, בסתירה לכך ש- m לא שווה למכפלה של ראשוניים!

■

משפט 1.5 קיימים אינסוף מספרים ראשוניים

קיימים אינסוף מספרים ראשוניים.

הוכחה: נוכיח את הטענה דרך השלילה.
נניח כי $P = \{p_1, \ldots, p_n\}$ הוא הקבוצה של כל הראשוניים שקיימים וקבוצה זו נוצרת סופי.
נגדיר השלם $m = p_1 p_2 \ldots p_n + 1$.
לפי משפט הפירוק לראשוניים (ראו משפט 1.4) m הוא ראשוני או שווה למכפלה של ראשוניים.
לפי ההנחה ההתחלתית שלנו, אין מצב ש- m יכול להיות מספר ראשוני בגלל ש- m גדול ממש מכל הראשוניים בקבוצת כל ראשוניים P. כלומר, $m > p_i$ לכל $1 \leq i \leq n$.
גם לא קיים מספר ראשוני p_i אשר מחלק את m. הרי

$$m \ (\text{mod} \ p_i) = 1 \quad \Rightarrow \quad p_i \nmid m \ .$$

הגענו לסתירה להמשפט הפירוק לראשוניים. לכן קיימים אינסוף מספרים ראשוניים. ■

1.3 המחלק המשותף הגדול ביותר

הגדרה 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 השלם החיובי הגדול ביותר שמחלק גם a וגם b.

הסימון gcd מנובע מהשם אנגלית "greatest common divisor".

דוגמה 1.8

$$\text{gcd}(2,6) = 2 ,$$
$$\text{gcd}(3,6) = 3 ,$$
$$\text{gcd}(24,5) = 1 ,$$
$$\text{gcd}(20,10) = 10 ,$$
$$\text{gcd}(14,12) = 2 ,$$
$$\text{gcd}(8,12) = 4 .$$

הגדרה 1.5 כפולה המשותפת הקטנה ביותר

יהיו a,b שלמים. הכפולה המשותפת הקטנה ביותר מסומנת $\text{lcm}(a,b)$ ומוגדרת להיות השלם החיובי החיובי הקטן ביותר עבורו גם a וגם b מחלקים אותו.

הסימון lcm מנובע מהשם אנגלית "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 לראשוניים לחישוב gcd

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

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

אז ה- $\gcd(a,b)$ הינו

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

הוכחה: נסמן $d=p_1^{\min(e_1,f_1)}p_2^{\min(e_2,f_2)}\ldots {p_n}^{\min(e_n,f_n)}$. ראשית נראה כי $a\mid d$ וגם $b\mid d$.

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

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

באופן דומה אפשר להוכיח שגם $b\mid d$.

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

ניניח בשלילה שקיים c שלם כך ש- $a\mid c$ ו- $b\mid c$ ו- $d>c$. כלומר נניח שקיים מחלק משותף c של a ושל b שגדול יותר מ- d. מכיוון ש- $a\mid c$ ו- $b\mid c$ אז בפירוק לראשוניים של c מופיע רק אותם ראשוניים $\{p_1,\ldots,p_n\}$ שמופיעים בפירוקים של a ושל b. לכך יש לנו:

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

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

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

לפיכך

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

ז"א $c\leq d$ בסתירה לכך ש- $d>c$. ■

דוגמה 1.10

מצאו את $\gcd(19200,320)$.

פתרון:

הפירוקים לראשוניים של 19200 ושל 320 הם

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

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:

הפירוקים לראשוניים של 154 ושל 36 הם

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

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

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

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

■

משפט 1.7 gcd של מספרים ראשוניים

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

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

הוכחה:

<u>שיטה 1: הוכחה ישרה</u>

p הוא ראשוני אז הפירוק לראשונים שלו הוא

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

q הוא ראשוני אז הפירוק לראשונים שלו הוא

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

לפי משפט 1.6,

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

<u>שיטה 2: הוכחה בשלילה</u>

יהי $d = \gcd(p, q)$ ונניח כי $q < p$. אז d נמצא בטווח של שלמים האפשריים $1 \leq d \leq q$.
נניח בשלילה כי $d > 1$.
מכיוון ש- d מחלק משותף של p ושל q אז $d \mid p$ וגם $d \mid q$.
q הוא ראשוני אז $d \mid q$ רק אם $d = q$. לכן אם גם $d \mid p$ אז זה גורר ל- $p \mid q$, בסתירה לכך ש- p ראשוני. ■

משפט 1.8 שיטת פירוק לראשוניים לחישוב lcm

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

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

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

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

הוכחה: נסמן $D = p_1^{\max(e_1,f_1)} p_2^{\max(e_2,f_2)} \ldots p_n{}^{\max(e_n,f_n)}$. ראשית נראה כי $D \mid a$ וגם $D \mid b$.

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

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

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

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

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

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

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

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

לפיכך

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

ז"א $C \geq D$ בסתירה לכך ש- $D < C$. ■

משפט 1.9

יהיו a,b שלמים חיוביים. אזי

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

הוכחה: יהיו הירוקים לראשוניים של a ושל b:

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

אזי ממשפט 1.6 וממשפט 1.8:

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

כאשר 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 מאתחלים r_0 ו- r_1:

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

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

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

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

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

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

$$\begin{array}{llll} \text{שלב } i=1: & r_2 = r_0 - q_1 r_1 = r_0 - \left\lfloor \frac{r_0}{r_1} \right\rfloor r_1 & & q_1 = \left\lfloor \frac{r_0}{r_1} \right\rfloor \\ \text{שלב } i=2: & r_3 = r_1 - q_2 r_2 = r_1 - \left\lfloor \frac{r_1}{r_2} \right\rfloor r_2 & & q_2 = \left\lfloor \frac{r_1}{r_2} \right\rfloor \\ \text{שלב } i=3: & r_4 = r_2 - q_3 r_3 = r_2 - \left\lfloor \frac{r_2}{r_3} \right\rfloor r_3 & & q_3 = \left\lfloor \frac{r_2}{r_3} \right\rfloor \\ \vdots & & & \\ \text{שלב } i=n-1: & r_n = r_{n-2} - q_n r_n = r_{n-2} - \left\lfloor \frac{r_{n-2}}{r_{n-1}} \right\rfloor r_{n-1} & & q_{n-1} = \left\lfloor \frac{r_{n-2}}{r_{n-1}} \right\rfloor \\ \text{שלב } i=n: & r_{n+1} = 0 & & q_n = \left\lfloor \frac{r_{n-1}}{r_n} \right\rfloor \end{array}$$

התהליך מסתיים בשלב ה-n-ית אם $r_{n+1}=0$. ואז הפלט של האלגוריתם הוא $r_n = \gcd(a,b)$.

למטה רשום ייצוג פסאודו-קוד של האלגוריתם של אוקלידס:

Algorithm 1 האלגוריתם של אוקלידס

Input: Integers a, b .
$r_0 \leftarrow a$
$r_1 \leftarrow b$
$n \leftarrow 1$
while $r_n \neq 0$ **do**
    $q_n \leftarrow \left\lfloor \frac{r_{n-1}}{r_n} \right\rfloor$
    $r_{n+1} \leftarrow r_{n-1} - q_n r_n$
    $n \leftarrow n + 1$
end while
$n \leftarrow n - 1$
Output: $r_n = \gcd(a, b)$

דוגמה 1.12

מצאו את ה- $\gcd(1071, 462)$.

פתרון:

$a = 1071, b = 462$.

נאתחל $r_0 = a = 1071$ ו- $r_1 = b = 462$ נבצע את האלגוריתם של אוקלידס:

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

לפיכך $\gcd(1071, 462) = r_3 = 21$.

■

דוגמה 1.13

מצאו את $\gcd(26, 11)$.

פתרון:

$a = 26, b = 11$.

נאתחל $r_0 = a = 26$ ו- $r_1 = b = 11$ נבצע את האלגוריתם של אוקלידס:

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

לפיכך $\gcd(26,11) = r_4 = 1$.

■

משפט 1.11 משפט בזו (Bezout's identity)

יהיו a,b. קיימים שלמים s,t,d עבור

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

כאשר $d = \gcd(a,b)$. משוואה (1.2) נראת ה**פירוק אוקלידס** של a ו- b.

משפט 1.12 האלגוריתם המוכלל של אוקלידס

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

$$d = sa + tb$$

כאשר $d = \gcd(a,b)$, כדלקמן. ראשית מאתחלים:

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

אם $r_1 = b \neq 0$ אז 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 $r_2 \neq 0$ אז עוברים לאיטרציה $i=2$ שבה מחשבים את q_2, r_3, s_3, t_3 כך:

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

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

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

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

למטה רשום ייצוג פסאודו-קוד של האלגוריתם:

Algorithm 2 האלגוריתם המוכלל של אוקלידס

Input: Integers a, b .
$r_0 \leftarrow a$
$r_1 \leftarrow b$
$s_0 \leftarrow 1$
$s_1 \leftarrow 0$
$t_0 \leftarrow 0$
$t_1 \leftarrow 1$
$n \leftarrow 1$
while $r_n \neq 0$ **do**
  $q_n \leftarrow \left\lfloor \frac{r_{n-1}}{r_n} \right\rfloor$
  $r_{n+1} \leftarrow r_{n-1} - q_n r_n$
  $s_{n+1} \leftarrow s_{n-1} - q_n s_n$
  $t_{n+1} \leftarrow t_{n-1} - q_n t_n$
  $n \leftarrow n + 1$
end while
$n \leftarrow n - 1$
Output: r_n, s_n, t_n ▷ $d = r_n = \gcd(a,b)$ and $d = sa + tb$ where $s = s_n$, $t = t_n$.

דוגמה 1.14 (אלגוריתם המוכלל של איוקלידס)

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

פתרון:

מאתחלים:

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

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

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

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

■

דוגמה 1.15 (אלגוריתם המוכלל של איוקלידס)

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

פתרון:

מאתחלים:

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

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

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

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

■

1.5 יחס השקילות המודולרית

הגדרה 1.7 שקילות מודולרית

יהיו a,b,n שלמים ($n \neq 0$). היחס:

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

אומר כי "n מחלק את ההפרש $a-b$".

כלומר:

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

דוגמה 1.16

הוכיחו כי

א) $5 \equiv 2 \pmod{3}$

ב) $43 \equiv 23 \pmod{10}$

ג) $7 \not\equiv 2 \pmod{4}$

פתרון:

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

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

■

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

משפט 1.13

יהיו a,b,r שלמים, $b \neq 0$.

$a \equiv b \pmod{n}$ אם ורק אם $n \mid a-b$ אם ורק אם קיים שלם q עבורו $a = qn+b$.

הוכחה:
הגרירה הראשונה $a-r \mid b \Leftrightarrow a\equiv r \pmod b$ נובעת ישר מההגדרה 1.7 של יחס שקילות.
נראה את הגרירה השנייה:
$b-a \mid n$ אם ורק אם קיים שלם q עבורו $a-b=qn \quad\Longleftrightarrow\quad a=qn+b$.

■

משפט 1.14 תכונות של יחס השקילות המודולרית

יהיו a,b שלמים ו- $n\neq 0$ שלם.

1) <u>רפלקסיבי:</u> $a\equiv a \pmod n$.
2) <u>סימטרי:</u> $a\equiv b \pmod n$ אם ורק אם $b\equiv a \pmod n$.
3) <u>טרנזיטיבי:</u> אם $a\equiv b \pmod n$ וכן $b\equiv c \pmod n$ אזי $a\equiv c \pmod n$.

הוכחה:

1) <u>רפלקסיבי:</u>

לכל שלם $n\neq 0$ מתקיים $a-a \mid n$, או במילים אחרות $a=0\cdot n+a$, לכן $a\equiv a \pmod n$.

2) <u>סימטרי:</u>

נניח ש- $a\equiv b \pmod n$. אזי קיים שלם q עבורו

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

ז"א קיים שלם $\bar q=-q$ עבורו $b=\bar q n+a$ לכן $b\equiv a \pmod n$.

3) <u>טרנזיטיבי:</u> נניח ש- $a\equiv b \pmod n$ וכן $b\equiv c \pmod n$.

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

ז"א קיים שלם $Q=q+\bar q$ עבורו $a=Qn+c$ לכן $a\equiv c \pmod n$.

■

משפט 1.15 הקשר בין יחס שקילות מודולרית והשארית

יהיו $a,b,n>0$ שלמים.

$$a\equiv b \pmod n \quad\Longleftrightarrow\quad a \bmod n = b \bmod n$$

הוכחה:
<u>כיוון $\Leftarrow$</u>

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

$$a = qn + b \ .$$

לפי משפט החילוק של אוקלידס,

$$b = \bar{q}n = r_1 \ , \qquad r_1 = b \bmod n \ .$$

לכן

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

כאשר $Q = q + \bar{q}$ שלם ו- $0 \leq r_1 < b$ הוא השארית $r_1 = b \bmod n$. מכאן נובע ש:

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

ז"א $a \bmod n = r_1 = \text{mod} n$.

<u>כיוון $\Rightarrow$</u>

נניח ש- $a \bmod n = b \bmod n$. אזי

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

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

משפט 1.16 חיבור וכפל של שלמים השקולים מודולריים

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

1) <u>חיבור:</u>

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

2) <u>כפל:</u>

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

הוכחה:

1) <u>חיבוריות:</u>

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

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

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

2) <u>כפל:</u>

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

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

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

■

שיעור 2
חוגים מתמטיים

2.1 הפונקצית אוילר

הגדרה 2.1 פונקצית אוילר

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

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

דוגמה 2.1

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

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

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

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

משפט 2.1 הפירוק לראשוניים של פונקצית אוילר

יהי $m \geq 2$ מספר שלם ונניח כי הפירוק למספרים ראשוניים שלו הוא

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

אזי

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

דוגמה 2.2

מצאו את $\phi(60)$.

פתרון:

$60 = 2^2 \times 3^1 \times 5^1$ לכן

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

■

דוגמה 2.3

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 2.2

אם p מספר ראשוני אז

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

הוכחה: תרגיל בית. ■

משפט 2.3

אם p מספר ראשוני אז

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

הוכחה: תרגיל בית. ■

משפט 2.4

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

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

הוכחה:

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

$$a = p_1^{e_1}\ldots p_n^{e_n} \ , \qquad b = q_1^{f_1}\ldots q_m^{f_m} \ .$$

- a ו- b זרים לכן הראשוניים בין השני הפירוקים כולם שונים, כלומר $p_i\neq q_j$ לכל $1\leq i,j\leq \min n,m$.
- לכן אם הפירוק לראשונים של ab הוא

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

- מכאן

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

■

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

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

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

לכל $a,b\in\mathbb{Z}_m$,

$$a\oplus b=(a+b)\bmod m \qquad a\odot b=ab \bmod m\ .$$

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

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

דוגמה 2.4

חשבו את 11×13 ב- $\mathbb{Z}_{16}$.

פתרון:

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

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

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

■

משפט 2.6 תכונות של החוג $\mathbb{Z}_m$

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

1. סגירה תחת חיבור:
$$a+b\in\mathbb{Z}_m\ .$$
2. חוק החילוף לחיבור:
$$a+b=b+a\ .$$
3. חוק הקיבוץ לחיבור:
$$(a+b)+c=a+(b+c)\ .$$
4. קיום איבר הניטרלי ביחס לחיבור:
$$a+0=0+a=a\ .$$

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

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

ב- $\mathbb{Z}_m$.

.6 סגירה תחת כפל:

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

.7 חוק החילוף לכפל:

$$ab=ba\ .$$

.8 חוק הקיבוץ לכפל:

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

.9 קיום איבר הניטרלי ביחס לכפל:

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

.10 חוק הפילוג:

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

תכונות 1, 3-5 אומרות כי $\mathbb{Z}_m$ הינו "חבורה מתמטית".
יחד עם תכונה 2, $\mathbb{Z}_m$ הוא חבורה אָבֶּלִית.
כל התכונות 1-10 אומרות כי $\mathbb{Z}_m$ הוא חוג מתמטי.

הגדרה 2.3 איבר ההופכי ב- $\mathbb{Z}_m$

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

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

משפט 2.7

נתון היחס שקילות

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

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

הוכחה:

<u>כיוון $\Leftarrow$</u>

נניח בשלילה כי למשוואה $ax\equiv y \pmod{m}$ יש פתרון יחיד $x=x_1$ אבל $\gcd(a,m)=d>1$.

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

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

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

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

<u>כיוון $\Rightarrow$</u>

נניח ש: $\gcd(a,m)=1$ ונניח בשלילה כי יש שני פתרונות $x_1 \not\equiv x_2 \pmod{26}$. כלומר:

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

לפי טרנזיטיביות $ax_1 \equiv ax_2 \pmod{m}$ ולכן $m \mid a(x_1-x_2)$.
$\gcd(a,m)=1$ לכן $m \nmid a$ לכן $m \mid x_1-x_2$ לכן $x_1 \equiv x_2 \pmod{26}$, בסתירה לכך ש- $x_1 \not\equiv x_2 \pmod{26}$. ■

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

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

אם ורק אם $\gcd(a,m)=1$.

הוכחה:

<u>כיוון $\Leftarrow$</u>

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

<u>כיוון $\Rightarrow$</u>

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

דוגמה 2.5

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

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

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

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

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

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

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

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

■

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 פונקצית אוילר $\phi(m)$

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

(שימו לב ההגדרה הזאת זהה להגדרה 2.1.)

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

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

הוכחה: $\phi(m)$ שווה למספר איברים $a \in \mathbb{Z}_m$
עבורם $\gcd(a, m)$, ולפי משפט 2.1 אותם האיברים הם האיברים ההפיכים של $\mathbb{Z}_m$. ■

2.3 הפיכת מטריצות בחוג $\mathbb{Z}_m$

הגדרה 2.5 המטריצה של קופקטורים

תהי $A \in \mathbb{R}^{n \times n}$.

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

המטריצה של קופקטורים של המטריצה A מוגדרת

$$C = \begin{pmatrix} C_{11} & \cdots & C_{1n} \\ \vdots & \ddots & \vdots \\ C_{n1} & \cdots & C_{nn} \end{pmatrix}$$

כאשר C_{ij} הקופקטור ה- (i,j) של A.

הגדרה 2.6 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 הופכית

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

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

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

דוגמה 2.6

מצאו את ההופכית של

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

פתרון:

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

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

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

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

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

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

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

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

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

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

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 ההופכית של

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

פתרון:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

לפיכך

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

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

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

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

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

לפיכך

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

בדיקה:

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

■

שיעור 3
הצפנים הבסיסיים

3.1 מושג של קריפטו-מערכת

אליס ובוב, לתקשר מעל גבי ערוץ תקשורת בלתי אמין (נאמר קו טלפון או דואר אלקטרוני), ומבקשים ליהנות מסודיות. כלומר , הם מעוניינים ש שום גורם עוין, אוסקר, שעלול לצותת לשיחתם , לא יוכל להבין את תוכנה.

לשם כך משתמשים אליס ובוב בצופן (cryptosystem). אליס ובוב מסכימים ביניהם מראש על שיטה מסויימת להצפנה ועל מפתח, (key) שהוא ערך מספרי (או כמה ערכים מספריים). כעת , נניח שאליס מעוניינת לשלוח לבוב הודעה מסוימת. היא מצפינה encrypt את ההודעה בשיטה שהיא ובוב בחרו בה תוך כדי שימוש במפתח שהם קבעו. לאחר ההצפנה, ההודעה שינתה את צורתה. להודעה המקורית אנו קוראים טקסט גלוי (plaintext) ואילו ההודעה לאחר ההצפנה נקראת טקסט מוצפן (ciphertext). אליס שולחת את הטקסט המוצפן לבוב. בוב מפענח (decrypt) אותו ומשחזר את הטקסט הגלוי , המקורי. אוסקר, המצותת לערוץ , איננו יודע את ערכו של המפתח שנעשה בו שימוש (למרות ש י יתכן בהחלט ואף סביר להניח שהוא י ודע מהו הצופן ש השתמשו בו אליס ובוב).

הגדרה 3.1 צופן

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

(1 E מסמן קבוצה של טקסט גלוי plaintext,

(2 C מסמן קבוצה של טקסט מוצפן ciphertext,

(3 K מסמן את מרחב המפתח keyspace,

(4 לכל $k \in K$ יש שתי פונקציות: כלל מצפין $e \in E$ וכלל מפענח $d \in D$:

$$e : P \to C \ , \qquad d : C \to P \ ,$$

כך ש-

$$d\left(e\left(x\right)\right) = x$$

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

נניח כי ההודעה הנשלחה על ידי אליס לבוב היא הרצף האותיות

$$X = x_1 x_2 \cdots x_n$$

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

$$y_i = e_k(x_i)$$

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

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

הרצף הזה נשלח מעל גבי הערוץ. כאשר בוב מקבל את Y הוא מפענח אותו באמצעות הפונקציה d_k וכך הוא מקבל הרצף אותיות של טקסט גלוי המקורי

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

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

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

כאשר $x_1 \neq x_2$ ואז לבוב לא יכול לדעת אם y ההפענחה של x_1 או x_2.

3.2 צופן ההזזה

הגדרה 3.2 צופן ההזזה

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

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

ו-

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

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

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

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

דוגמה 3.1

נתון טקסט גלוי

shamoon

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

פתרון:

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

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

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

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

שלב 3) נעבור את הרצץ מספרים לטקסט מוצפן:

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

הטקסט מוצפן המתקבל הוא

DSLXZZY

■

דוגמה 3.2

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

UJCNQO

מצאו את הטקסט גלוי.

פתרון:
ננסה לפענח את הטקסט מוצפן בעזרת הצופן הזזה עם המפתחות $d_0 = 0, d_1 = 1, d_2 = 2 \ldots$ בתור.

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

■

דוגמה 3.3

נתון הטקסט מוצפן הבא:

QRQXFJANHXD

מצאו את הטסטק גלוי

פתרון:
ננסה לפענח את הטקסט מוצפן בעזרת הצופן הזזה עם המפתחות $d_0, d_1, \ldots$ בתור.

d_0 `qrqxfjanhxd`

d_1 `pqpweizmgwc`

d_2 `opovdhylfvb`

d_3 `nonucgxkeua`

d_4 `mnmtbfwjdtz`

d_5 `lmlsaevicsy`

d_6 `klkrzduhbrx`

d_7 `jkjqyctgaqw`

d_8 `ijipxbsfzpv`

d_9 `hihowareyou`

בשלב זה מצאנו את הטקסט גלוי:

$$\texttt{hihowareyou} \ .$$

המפתח הוא $k = 9$. ■

משפט 3.1 צופן הזזה ניתן לפענוח

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

$$d_k\left(e_k(x)\right) = x \mod 26 \ .$$

הוכחה:

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

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

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

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

$$d_k\left(e_k(x)\right) = \left(x - 26q\right) \mod 26 = x \mod 26 \ .$$

■

3.3 צופן האפיני

באופן כללי, בצופן האפיני הכלל מצפין נתון ע"י הפונקציה מצורה

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

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

כדי שפענוח יהיה אפשרי נדרוש כי הפונקציה הזאת חד-חד-ערכית. במילים אחרות, נדרוש כי לביטוי (יחס שקילות)

$$ax+b\equiv y \mod 26$$

יש פתרון יחיד ל-x.

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

משפט 3.2

ליחס שקילות

$$ax+b\equiv y \mod 26$$

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

הוכחה:

כיוון $\Leftarrow$

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

כיוון $\Rightarrow$

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

דוגמה 3.4

בדקו אם הפונקציה

$$e(x)=4x+7 \mod 26$$

כלל מצפין תקין, כלומר בדקו אם קיים כלל מפענח.

פתרון:

$\gcd(4,26)=2$, אז הפונקציה $e(x)=4x+7 \mod 26$ אינה כלל מצפין תקין, בגלל שהיא לא חד-חד ערכית ולכן לא יכולה להיות כלל מצפין.

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

$$e(x)=4x+7 \mod 26$$

בעוד

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

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

$$K=\left\{a,b\in\mathbb{Z}_{26}\middle|\gcd(a,26)=1\right\} .$$

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

$$e_k(x)=(ax+b) \mod 26 ,$$

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

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

כלל 3.1

הפירוק לראשוניים של 26 הינו

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

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

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

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

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

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

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

דוגמה 3.5

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

1) רשמו את כלל המצפין.

2) רשמו את כלל המפענח.

3) בדקו כי התנאי

מתקיים.

פתרון:

1) כלל המצפין הוא

$$e_k(x) = 7x + 3 \mod 26 ,$$

2) כלל המפענח הוא

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

3) נבדוק כי הכלל מפענח המתקבל מקיים $d_k(e_k(x)) = x$:

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

■

דוגמה 3.6

בעזרת הצופן של דוגמה 3.5:

1) מצאו את הטקסט מוצפן של הטקסט גלוי

hot .

2) בדקו שהפעולה של הכלל מפענח על הטקסט מוצפן מחזיר את טקסט גלוי

hot .

פתרון:

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

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

נפעיל את הכלל מצפין על הערכים x:

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

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

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

מכאן נקבל

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

לכן הטקסט מוצפן המתקבל הוא

AXG

סעיף 2) הכלל מפענח הוא

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

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

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

נפעיל את הכלל מפענח על הערכים y:

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

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

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

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

לכן הטקסט גלוי המתקבל הוא

hot

כנדרש.

■

דוגמה 3.7

נתון הטקסט מוצפן

ACSE

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

פתרון:

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

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

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

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

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

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

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

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

■

3.4 צופן ויז'נר

צופן ההזזה וצופן ההחלפה דוגמאות של צופן מונואלפביתי: כל תו אלפביתי ב- P נתאים לתו אלפביתי יחיד ב- C. צופן ויז'נר הוא צופן פוליאלפיביתי: אין מצפינים כל אות בנפרד, אלא בלוקים, או קבוצות של כמה אותיות באורך קבוע m.

הגדרה 3.4 צופן ויז'נר (Vigenere Cipher)

יהי m מספר שלם חיובי.
נגדיר $P=C=K=\mathbb{Z}_{26}^m$.
עבור מפתח $k=(k_1,k_2,\ldots,k_m)$ נגדיר כלל מצפין

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

ונגדיר כלל מפענח

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

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

דוגמה 3.8

נתון הטקסט גלוי

string

והמפתח AND $=k$.

1) מצאו את הכלל מצפין והכלל מפענח.

2) מצאו את הטקסט מצפון.

3) בדקו כי הכלל מפענח מחזיר את הטקסט גלוי.

פתרון:

1) והמפתח הוא

AND .

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

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

לכן $m=3$.
הכלל מצפין הוא

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

והכלל מפענח הוא

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

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

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

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

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

בכל תת-קבוצה, נתאים לכל תו ערך של המפתח $k=(0,13,3)$:

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

על כל שלישיה (x_1,x_2,x_3) בבלוק אחד, נפעיל את כלל המצפין

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

לדוגמה בבלוק הראשון נקבל

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

בבלוק השני נקבל

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

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

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

$\mathrm{x}\in P$	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
$\mathrm{y}\in C$	S	G	U	I	A	J

הטקסט מוצפן המתקבל הוא

$$\text{SGUIAJ}\ .$$

3) נעביר את האותיות של הטקסט מוצפן לערכים של $\mathbb{Z}_{26}$:

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

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

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

בכל תת-קבוצה, נתאים לכל תו ערך של המפתח $k = (0, 13, 3)$:

$x \in P$	S	G	U	I	A	J
$y \in \mathbb{Z}_{26}$	18	6	20	8	0	9
$k_i \in k$	0	13	3	0	13	3

על כל שלישיה (y_1, y_2, y_3) בבלוק אחד, נפעיל את כלל המצפין

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

לדוגמה בבלוק הראשון נקבל

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

בבלוק השני נקבל

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

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

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

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

הטקסט גלוי המתקבל הוא

string .

■

דוגמה 3.9

נניח כי $m = 6$ והמפתח הוא

CIPHER.

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

$$k = (2, 8, 15, 7, 4, 17) \ .$$

נתון הטקסט גלוי

thiscryptosystemisnotsecure.

מצאו את הטקסט מוצפן.

פתרון:

<u>שלב 1:</u>

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

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

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

<u>שלב 2:</u>

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

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

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

<u>שלב 3:</u>

בכל תת-קבוצה, נתאים לכל תו ערך של המפתח $k = (2, 8, 15, 7, 4, 17)$:

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

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

<u>שלב 3:</u>

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

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

לדוגמה בבלוק הראשון נקבל

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

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

x ∈ 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

<u>שלב 4:</u>

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

x ∈ 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 ∈ ℂ	V	P	X	Z	G	I	A	X	I	V	W	P	U	B	T	T	M	J

x ∈ 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 ∈ ℂ	P	W	I	Z	I	T	W	Z	T

הטקסט מוצפן המתקבל הוא

VPXZGIAXIVWPUBTTMJPWIZITWZT

■

3.5 צופן היל

הגדרה 3.5 צופן היל

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

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

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

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

ונגדיר כלל מפענח

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

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

הגדרה 3.6 המטריצה של קופקטורים

תהי $A \in \mathbb{R}^{n \times n}$.

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

המטריצה של קופקטורים של המטריצה A מוגדרת

$$C = \begin{pmatrix} C_{11} & \cdots & C_{1n} \\ \vdots & \ddots & \vdots \\ C_{n1} & \cdots & C_{nn} \end{pmatrix}$$

כאשר C_{ij} הקופקטור ה- (i,j) של A.

הגדרה 3.7 המטריצה המצורפת

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

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

כאשר C המטריצה של קופקטורים של A.

משפט 3.3 נוסחת קיילי המילטון

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

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

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

דוגמה 3.10

נתון רצף טקסט גלוי

```
july
```

ונתון המפתח

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

של צופן היל. מצאו את הטקסט מוצפן.

פתרון:

<u>שלב 1:</u>

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

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

<u>שלב 2:</u>

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

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

<u>שלב 3:</u>

עבור כל תת-קבוצה המתקבל נחשב

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

עבור התת-קבוצה הראשונה נקבל

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

עבור התת-קבוצה השנייה נקבל

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

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

<u>שלב 4:</u>

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

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

הטקסט מוצפן המתקבל הוא

DELW

■

דוגמה 3.11

נתון רצף טקסטת מוצפן

DELW

ונתון המפתח

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

של צופן היל. מצאו את הטקסט גלוי.

פתרון:

<u>שלב 0:</u>

נחשב את ההופכית k^{-1}:

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

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

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

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

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

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

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

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

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

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

לפיכך

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

<u>שלב 1:</u>

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

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

<u>שלב 2:</u>

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

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

<u>שלב 3:</u>

עבור כל תת-קבוצה המתקבל נחשב

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

עבור התת-קבוצה הראשונה נקבל

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

עבור התת-קבוצה השנייה נקבל

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

$\mathrm{y} \in C$	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

<u>שלב 5:</u>

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

$\mathrm{y} \in C$	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
$\mathrm{x} \in P$	j	u	l	y

הטקסט גלוי המתקבל הוא

july

■

דוגמה 3.12

נתון רצף טקטסת מוצפן

PGRFGGCSY

ונתון המפתח

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

של צופן היל. מצאו את הטקסט גלוי.

פתרון:

<u>שלב 0:</u>

נחשב את ההופכית k^{-1}:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

לפיכך

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

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

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

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

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

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

לפיכך

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

<u>שלב 1:</u>

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

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

<u>שלב 2:</u>

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

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

<u>שלב 3:</u>

עבור כל תת-קבוצה המתקבל נחשב

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

עבור התת-קבוצה הראשונה נקבל

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

עבור התת-קבוצה השנייה נקבל

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

עבור התת-קבוצה השלישי נקבל

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

$\mathrm{y} \in C$	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

<u>שלב 5:</u>

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

$\mathrm{y} \in C$	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
$\mathrm{x} \in P$	h	o	w	a	r	e	y	o	u

הטקסט גלוי המתקבל הוא

howareyou

■

שיעור 4
תמורות וצופן אניגמה

4.1 תמורות

הגדרה 4.1 תמורה

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

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

תזכורות:

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

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

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

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 $\pi : \Sigma \to \Sigma$ פונקציה. הוכיחו: אם π חד-חד ערכית אז היא תמורה.

פתרון:
נתון לנו הפונקציה $\pi : \Sigma \to \Sigma$ כאשר Σ קבוצה נוצר סופית. כדי להוכיח כי π תמורה יש להראות כי π חד-חד-ערכית ו"על" Σ. כבר נתון לנו ש- π חח"ע אז נשאר רק להראות כי π על Σ.

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

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

לכן

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

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

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

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

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

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

ולפיכך $\pi : \Sigma \to \Sigma$ היא פונקציה "על" Σ.

■

הגדרה 4.2 הרכבה של תמורות

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

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

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

דוגמה 4.4

נתון התמורות π ו- σ:

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

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

אזי ההרבה $\sigma\pi$ היא:

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

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

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

כלומר $\sigma\pi \neq \pi\sigma$.

משפט 4.1 הרכבה של תמורות היא תמורה

תהי Σ קבוצה נוצר סופית ותהיינה $\pi : \Sigma \to \Sigma$ ו- $\sigma : \Sigma \to \Sigma$ תמורות על הקבוצה Σ. ההרכבה $\sigma\pi$ היא תמורה על Σ.

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

- **חח"ע**

  נניח בשלילה כי $\sigma\pi$ 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 $y_1 \neq y_2$. ומכיוון ש- σ תמורה אזי $\sigma(y_1) \neq \sigma(y_2)$. לכן

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

בסתירה לכך ש- $\sigma\left(\pi(x_1)\right)=\sigma\left(\pi(x_2)\right)$.

לכן הוכחנו דרך השלילה כי $\sigma\pi$ פונקציה חח"ע.

- **על**

ניח בשלילה כי $\sigma\pi$ לא פונקצית "על". נסמן $\sigma\pi\left(\Sigma\right)$ התמונה של $\sigma\pi$. אזי

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

ראשית מכיוון ש- $\sigma\pi\left(\Sigma\right)$ הוא התמונה של $\sigma\pi$ אזי $\sigma\pi\left(\Sigma\right)\subseteq\Sigma$.

לכן אם $\sigma\pi\left(\Sigma\right)\neq\Sigma$ אז $\sigma\pi\left(\Sigma\right)\subset\Sigma$. מכאן

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

לכן בהכרח קיים לפחות שני איברים $x_1,x_2\in\Sigma$ עבורם $\sigma\pi\left(x_1\right)=\sigma\pi\left(x_2\right)$. זאת בסתירה לכך ש- $\sigma\pi$ חח"ע, שמוכח בסעיף הקודם.

לכן הוכחנו דרך השלילה כי הפונקציה $\sigma\pi$ היא "על" Σ.

■

הגדרה 4.3 תמורות מתחלפות

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

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

הגדרה 4.4 תמורות מתחלפות

תהי $\pi:\Sigma\to\Sigma$ תמורה על הקבוצה Σ. התמורה ההופכית 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 ההופכית 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 ונקודה זזה

תהי $\pi:\Sigma\to\Sigma$ תמורה.

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

הגדרה 4.6 תמורה הזהות

התמורה הזהות מסומנת $\mathrm{id}:\Sigma\to\Sigma$ ומוגדרת כך שלכל $x\in\Sigma$:

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

במילים אחרות אם $\mathrm{id}:\Sigma\to\Sigma$ היא התמורה הזהות אזי כל נקודה $x\in\Sigma$ היא נקודת שבת של id.

משפט 4.2 תמורה ההופכית של תמורה מורכבת

תהיינה $\pi_1,\cdots,\pi_t$ תמורות על הקבוצה Σ. אזי

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

הוכחה: נוכיח את הטענה באינדוקציה.

<u>שלב הבסיס</u>

עבור $t=2$, לכל $x\in\Sigma$ יש לנו:

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

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

<u>שלב האינדוקציה</u>

נניח כי הטעהה מתקיימת עבור $t=k>2$ (זאת היא ההנחת האינדוקציה). אז נראה כי הטענה נכונה גם כן עבור $t=k+1$ באופן הבא. נתבונן על ההתמורה המורכבת $\pi_1\cdots\pi_k\pi_{k+1}$. נסמן התמורה המורכבת מ- k תמורות כך: $\sigma=\pi_1\cdots\pi_k$. הסימון הזה 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 השלב הבסיס מהופכית היא

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

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

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

כאשר במעבר האחרון השתמשנו בההנחת האינדוקציה.

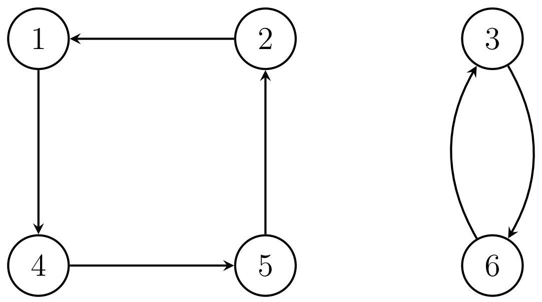
■

4.2 פירוק למחזורים של תמורה

עד כה ראינו תמורות בייצוג של טבלה. אבל המבנה האמיתי של תמורה נגלה עם נציג תמורה כגרף. 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

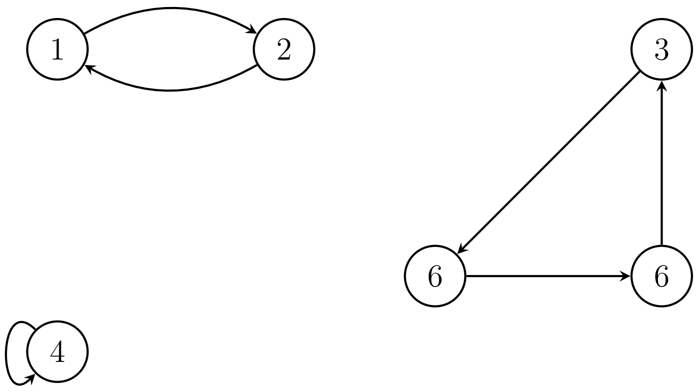
נגדיר הגרף המכוון $G_\pi = (V, E)$ כאשר הקבוצת הקודקודים היא $V = \Sigma$, ולכל $x \in \Sigma$ נגדיר צלע מ- x ל- $\pi(x)$. ז"א $E = \{e_1, e_2, \ldots, e_n\}$ כאשר $e_i = x_i\pi(x_i)$ היא הצלע מקודקוד x_i לקודקוד $\pi(x_i)$. על פי ההגדרה הזאת הגרף G_π של התמורה π היא כמתוארת באיור למטה.



כדוגמה נוספת אם σ היא התמורה

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

אזי הגרף G_σ הינו:



בגרף של תמורה, כל קודקוד שייך לבדיוק מעגל מכוון אחד (שייתכן הוא עובר דרך קודקוד אחד בלבד). הרי קיים התאמה אחת-אחת בין תמורה על Σ לבין גרף שמכסה כל המעגלים המכוונים של Σ. התופעה זו היא המוטיבציה לסימון מחזורים של תמורות.

הגדרה 4.7 מחזור

תהי $\pi : \Sigma \to \Sigma$ תמורה על הקבוצה Σ. אם קיימים k איברים שונים $a_1, \ldots, a_k \in \Sigma$ כך ש-

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

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

$$\begin{pmatrix} a_1 & a_2 & \cdots & a_k \end{pmatrix} .$$

משפט 4.3 פירוק למחזורים של תמורה

כל תמורה $\pi : \Sigma \to \Sigma$ על קבוצה סופית Σ מתפרקת למחזורים זרים.

הוכחה: שאלה לעבודת הגשה. ■

דוגמגה 4.6

נתונה התמורה π:

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

הפירוק למחזורים הוא:

$$\pi = (1 \quad 4 \quad 6)\,(2 \quad 5 \quad 3)\,(8 \quad 7)$$

משפט 4.4

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

הוכחה:

<u>כיוון אם</u>

נניח ש- π מכילה מחזור באורך k.

$\Leftarrow$ קיימים איברים שונים $a_1, \ldots, a_k \in \Sigma$ כך ש: $\pi \in (a_1 \quad a_2 \quad \ldots \quad \subseteq a_k)$.

$\Leftarrow$ $\pi(a_k) = a_1$, $\pi(a_{k-1}) = a_k$, $\ldots$ $\pi(a_2) = a_3$, $\pi(a_1) = a_2$.

$\Leftarrow$ בגרף $G_\pi = (V, E)$ של התמורה קיימות הצלעות

$$a_1\pi(a_1) \ , \ a_2\pi(a_2) \ , \quad \cdots \quad , \ a_{k-1}\pi(a_{k-1}) \ , \ a_k\pi(a_k) \in E \ .$$

$\Leftarrow$ בגרף $G_\pi = (V, E)$ קיימות הצלעות

$$a_1a_2 \ , \ a_2a_3 \ , \quad \cdots \quad , \ a_{k-1}a_k \ , \ a_ka_1 \in E \ .$$

$\Leftarrow$ G_π מכילה מעגל המילטוני באורך k.

<u>כיוון רק אם</u>

נניח ש- G_π מכיל מעגל המילטוני באורך k.

$\Leftarrow$ קיימים קבוצות $a_1, \ldots, a_k \in \Sigma$ עבורם

$$a_1a_2 \ , \ a_2a_3 \ , \quad \cdots \quad , \ a_{k-1}a_k \ , \ a_ka_1 \in E \ .$$

$\Leftarrow$ מכיוון ש- G_π הוא הגרף של התמורה π אזי

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

$\Leftarrow$ π מכילה מחזור באורך k:

$$(a_1 \quad a_2 \quad \ldots \quad \subseteq a_k) \subseteq \pi \ .$$

■

הגדרה 4.8 המחלקה של תמורה

תהי $\pi : \Sigma \to \Sigma$ תמורה. אומרים כי π שייכת למחלקה $[1^{z_1}2^{z_2}\cdots n^{z_n}]$ אם בפירוק למחזורים של π יש בדיוק z_1 מחזורים באורך- 1, z_2 מחזורים באורך- 2, z_3 מחזורים באורך- 3, וכן הלה.

במילים אחרות:

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

אם לכל $i = 1, \ldots, n$ בפירוק למחזורים של π יש z_i מחזורים באורך i.

דוגמה 4.7

תהי $\Sigma = \{A, B, C, D, E, F\}$.

- התמורה $(A\ B)(C\ D)(E\ F) \in [2^3]$.
- התמורה $(A\ B\ C\ D) \in [1^2 4^1]$.
- התמורה $(A\ D\ C)(E\ F) \in [1^1 2^1 3^1]$.

4.3 תמורות צמודות

הגדרה 4.9 תמורות צמודות

תהיינה π, σ תמורות על הקבוצה 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 $\sigma : \Sigma \to \Sigma$ ו- $\pi : \Sigma \to \Sigma$ תמורות על הקוצה סופית Σ. לכל $x, y \in \Sigma$ אם $\sigma(x) = y$ אזי

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

הוכחה: נניח ש: $\sigma(x) = y$. אזי

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

■

משפט 4.6 פירוקים למחזורים של תמורות צמודות שוויום

תהיינה $\sigma : \Sigma \to \Sigma$ ו- $\pi : \Sigma \to \Sigma$ תמורות על הקוצה סופית Σ. ונניח כי הפירוק למחזורים של σ הוא

$$\sigma = \begin{pmatrix} a_1 & a_2 & \cdots & a_k \end{pmatrix} \begin{pmatrix} b_1 & b_2 & \cdots & b_l \end{pmatrix} \cdots \qquad .$$

אזי הפירוק למחזורים של $\pi\sigma\pi^{-1}$ הוא:

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

הוכחה: עבור כל מחזור $\left(a_1 \ a_2 \ \ldots \ a_k\right)$ של σ, מתקיים

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

מנובע ממשפט כי לכל מחזור של σ מתקיים:

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

■

משפט 4.7 המחלקה של תמורות צמודות נשמרת

תהיינה $\sigma : \Sigma \to \Sigma$ ו- $\tau : \Sigma \to \Sigma$ תמורות על הקוצה סופית Σ.
τ צמודה ל- σ אם ורק אם σ ו- τ שייכות לאותה מחלקה.

הוכחה:
כיוון אם:

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

$$\sigma = \left(a_1 \ \ a_2 \ \ \cdots \ \ a_k\right)\left(b_1 \ \ b_2 \ \ \cdots \ \ \pi\left(b_l\right)\right)\cdots$$

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

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

ולכן ל- τ ולי- σ יש אותו מבנה של מחזורים ולכן הן שייכות לאותה מחלקה.

כיוון רק אם:

■

4.4 צופן אניגמה

הגלגלי האתחול של צופן אניגמה הם 3 תמורות 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

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

הגדרה 4.10 כלל מצפין וכלל מפענח של צופן אניגמה

יהי π משקף כלשהו מעל האלפבית $A,\ldots,Z$. הבחירה של המשקף מהווה את הלוח התקעים.
יהי $w = x_1x_2\ldots x_n$ מילה של טקסט גלוי. לכל $i = 1,\ldots,n$ הכלל מצפין והכלל מפענח של האות במיקום ה-i בטקסט הם:

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

כאשר Δ_i היא התמורה המורכבת

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

כאשר

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

אם נגדיר את התמורה המורכבת $\tau_i = \sigma_{-i}\,\alpha_3\,\sigma_i\,\alpha_2\,\alpha_1\,\pi$ אזי $\tau_i^{-1} = \pi\,\alpha_1^{-1}\,\alpha_2^{-1}\,\sigma_{-i}\,\alpha_3^{-1}\ \sigma_i$ ולכן

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

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

דוגמה 4.8 הצפנה על ידי צופן אניגמה

נתון הטקסט גלוי

$$\texttt{hello}\ .$$

נניח כי הלוח התקעים הוא

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

חשבו את הטקסט מוצפן.

פתרון:

(1 $x_1 = \texttt{H}$

$$H \xrightarrow{\pi} F \xrightarrow{\sigma_1} G \xrightarrow{\alpha_3} C \xrightarrow{\sigma_{-1}} B \xrightarrow{\alpha_2} J \xrightarrow{\alpha_1} Z \xrightarrow{\rho} T$$
$$\xrightarrow{\alpha_1^{-1}} L \xrightarrow{\alpha_2^{-1}} K \xrightarrow{\sigma_1} L \xrightarrow{\alpha_3^{-1}} F \xrightarrow{\sigma_{-1}} E \xrightarrow{\pi} E$$

(2 $x_2 = \texttt{E}$

$$E \xrightarrow{\pi} E \xrightarrow{\sigma_2} G \xrightarrow{\alpha_3} C \xrightarrow{\sigma_{-2}} A \xrightarrow{\alpha_2} A \xrightarrow{\alpha_1} E \xrightarrow{\rho} Q$$
$$\xrightarrow{\alpha_1^{-1}} H \xrightarrow{\alpha_2^{-1}} L \xrightarrow{\sigma_2} N \xrightarrow{\alpha_3^{-1}} N \xrightarrow{\sigma_{-2}} L \xrightarrow{\pi} P$$

(3 $x_3 = \texttt{L}$

$$L \xrightarrow{\pi} P \xrightarrow{\sigma_3} S \xrightarrow{\alpha_3} G \xrightarrow{\sigma_{-3}} D \xrightarrow{\alpha_2} K \xrightarrow{\alpha_1} N \xrightarrow{\rho} K$$
$$\xrightarrow{\alpha_1^{-1}} B \xrightarrow{\alpha_2^{-1}} J \xrightarrow{\sigma_3} M \xrightarrow{\alpha_3^{-1}} V \xrightarrow{\sigma_{-3}} S \xrightarrow{\pi} S$$

(4 $x_4 = \texttt{L}$

$$L \xrightarrow{\pi} P \xrightarrow{\sigma_4} T \xrightarrow{\alpha_3} A \xrightarrow{\sigma_{-4}} W \xrightarrow{\alpha_2} F \xrightarrow{\alpha_1} G \xrightarrow{\rho} L$$
$$\xrightarrow{\alpha_1^{-1}} E \xrightarrow{\alpha_2^{-1}} Z \xrightarrow{\sigma_4} D \xrightarrow{\alpha_3^{-1}} B \xrightarrow{\sigma_{-4}} X \xrightarrow{\pi} A$$

(5 $x_5 = \texttt{O}$

$$O \xrightarrow{\pi} O \xrightarrow{\sigma_5} T \xrightarrow{\alpha_3} A \xrightarrow{\sigma_{-5}} V \xrightarrow{\alpha_2} Y \xrightarrow{\alpha_1} C \xrightarrow{\rho} U$$
$$\xrightarrow{\alpha_1^{-1}} R \xrightarrow{\alpha_2^{-1}} G \xrightarrow{\sigma_5} L \xrightarrow{\alpha_3^{-1}} F \xrightarrow{\sigma_{-5}} A \xrightarrow{\pi} X$$

לפיכך הטקסט מוצפן הוא: EPSAX. ■

דוגמה 4.9 הצפנה על ידי צופן אניגמה

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

פתרון:

(1 $y_1 = \texttt{E}$

$$E \xrightarrow{\pi} E \xrightarrow{\sigma_1} F \xrightarrow{\alpha_3} L \xrightarrow{\sigma_{-1}} K \xrightarrow{\alpha_2} L \xrightarrow{\alpha_1} T \xrightarrow{\rho} Z$$
$$\xrightarrow{\alpha_1^{-1}} J \xrightarrow{\alpha_2^{-1}} B \xrightarrow{\sigma_1} C \xrightarrow{\alpha_3^{-1}} G \xrightarrow{\sigma_{-1}} F \xrightarrow{\pi} H$$

(2 $y_2 = \texttt{P}$

$$P \xrightarrow{\pi} L \xrightarrow{\sigma_2} N \xrightarrow{\alpha_3} N \xrightarrow{\sigma_{-2}} L \xrightarrow{\alpha_2} H \xrightarrow{\alpha_1} Q \xrightarrow{\rho} E$$
$$\xrightarrow{\alpha_1^{-1}} A \xrightarrow{\alpha_2^{-1}} A \xrightarrow{\sigma_2} C \xrightarrow{\alpha_3^{-1}} G \xrightarrow{\sigma_{-2}} E \xrightarrow{\pi} E$$

(3 $y_3 = \texttt{S}$

$$S \xrightarrow{\pi} S \xrightarrow{\sigma_3} V \xrightarrow{\alpha_3} M \xrightarrow{\sigma_{-3}} J \xrightarrow{\alpha_2} B \xrightarrow{\alpha_1} K \xrightarrow{\rho} N$$
$$\xrightarrow{\alpha_1^{-1}} K \xrightarrow{\alpha_2^{-1}} D \xrightarrow{\sigma_3} G \xrightarrow{\alpha_3^{-1}} S \xrightarrow{\sigma_{-3}} P \xrightarrow{\pi} L$$

(4 $\underline{y_4 = \texttt{A}}$

$$A \xrightarrow{\pi} X \xrightarrow{\sigma_4} B \xrightarrow{\alpha_3} D \xrightarrow{\sigma_{-4}} Z \xrightarrow{\alpha_2} E \xrightarrow{\alpha_1} L \xrightarrow{\rho} G$$
$$\xrightarrow{\alpha_1^{-1}} F \xrightarrow{\alpha_2^{-1}} W \xrightarrow{\sigma_4} A \xrightarrow{\alpha_3^{-1}} T \xrightarrow{\sigma_{-4}} P \xrightarrow{\pi} L$$

(5 $\underline{y_5 = \texttt{X}}$

$$X \xrightarrow{\pi} A \xrightarrow{\sigma_5} F \xrightarrow{\alpha_3} L \xrightarrow{\sigma_{-5}} G \xrightarrow{\alpha_2} R \xrightarrow{\alpha_1} U \xrightarrow{\rho} C$$
$$\xrightarrow{\alpha_1^{-1}} Y \xrightarrow{\alpha_2^{-1}} O \xrightarrow{\sigma_5} T \xrightarrow{\alpha_3^{-1}} J \xrightarrow{\sigma_{-5}} O \xrightarrow{\pi} O$$

לפיכך הטקסט הגלוי הוא: HELLO. ■

4.5 משפט רייבסקי

הגדרה 4.11 תמורה משקפת

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

משפט 4.8 תכונות של תמורה משקפת

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

(1 $\rho^{-1} = \rho$.

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

הוכחה:

<u>כיוון אם</u>

נניח כי ρ משקף. נראה כי $\rho = \rho^{-1}$ באופן הבא. נניח ש:
$$\rho = (x_1\ y_1)\,(x_2\ y_2) \cdots (x_{n/2}\ y_{n/2}) \ .$$

לכל מחזור $(a_1\ a_2\ \cdots\ a_k)$ המחזור ההפוכי הוא $(a_k\ a_{k-1}\ \cdots\ a_1)$ $(a_1\ a_2\ \cdots\ a_k)^{-1} =$. 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 שאם $x \in \Sigma$ אז $\rho(x) \neq x$. נניח בשלילה שקיימת נקודה $x \in \Sigma$ עבורה $\rho(x) = x$. אזי $\rho \in [1^{z_1} \cdots]$ כאשר $z_1 > 0$, כלומר ρ מכילה קיים לפחות מחזור אחד באורך 1, בסתירה לכך ש- ρ היא משקף.

כיוון רק אם

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

$$\rho=(x_1\ x_2\ x_3\ \ldots\ )\,\rho' \quad ,$$

כאשר $(x_1\ x_2\ x_3\ \ldots\ )$ הוא מחזור באורך $k>2$. ז"א ההופכית של ρ היא

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

בסתירה לכך ש- $\rho^{-1}=\rho$. ■

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

הכלל מצפין (והכלל מפענח) של צופן אניגמה הוא תמורה משקפת על האלפבית האנגלית.

הוכחה: הכלל מצפין והכלל מפענח של צופן אניגמה הם

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

כאשר $\pi\ \alpha_1\ \alpha_2\ \sigma_i\ \alpha_3\ \sigma_{-i}=\tau_i$ ו- ρ המשקף הקבוע של צופן אניגנה.

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

⇐ מכיוון ש: ρ הוא משקף על האלפיבית האנגלית אזי $\rho\in[2^{13}]$.

⇐ לפי משפט 4.7 $\Delta_i\in[2^{13}]$.

⇐ לפי הגדרה 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 $x,y_1,y_2\in\Sigma$ עבורם $\rho_1(x)=y_1$ וגם $\rho_2(x)=y_2$ אם ורק אם $\rho_2\rho_1(y_1)=y_2$.

הוכחה:

כיוון אם

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

$$\left.\begin{aligned} y_1&=\rho_1(x)\\ y_2&=\rho_2(x)\end{aligned}\right\}\ \xRightarrow{\rho_1\ \text{משקפת}}\ x=\rho_1(y_1)\ \Rightarrow\ \rho_2(\rho_1(y_1))=\rho_2(x)=y_2\ .$$

<u>כיוון רק אם</u>

נניח ש: $y_2 = \rho_2(\rho_1(y_1))$. מכיוון ש- ρ_2 תמורה משפקת אזי $\rho_1(y_1) = \rho_2(y_2)$ לכן קיים $x \in \Sigma$ כך ש:

$$\left.\begin{aligned} y_1 &= \rho_1(x) \\ y_2 &= \rho_2(x) \end{aligned}\right\} \xRightarrow{\text{משקפות } \rho_1,\rho_2} \left.\begin{aligned} \rho_1(y_1) &= x \\ \rho_2(y_2) &= x \end{aligned}\right\} \Rightarrow \rho_1(y_1) = x = \rho_2(y_2) .$$

■

4.6 ההנחות של רייבסקי על צופן האניגמה

הגדרה 4.12 ההנחות של רייבסקי

(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 ה- 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 רייבסקי I

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

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

הוכחה:

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

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

ז"א

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

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

$$\left.\begin{aligned}\sigma_3 &= \Delta_3(z)\\ \sigma_6 &= \Delta_6(z)\end{aligned}\right\} \quad\Rightarrow\quad z=\Delta_3\left(\sigma_3\right) \quad\Rightarrow\quad \Delta_6\left(z\right)=\Delta_6\Delta_3\left(\sigma_3\right) \quad\Rightarrow\quad \sigma_6=\Delta_6\Delta_3\left(\sigma_3\right) \ .$$

■

דוגמה 4.10

נתונה הודעה מוצפנת שמתחילה במילה אופיינית הבאה:

$$\texttt{ICPWLV} \ .$$

ז"א קיימת מילה מושכפלת $xyzxyz$ כך ש:

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

לכן לפי משפט רייבסקי I :

$$\Delta_4\Delta_1\left(\texttt{I}\right)=\texttt{W} \ , \qquad \Delta_5\Delta_2\left(\texttt{C}\right)=\texttt{L} \ , \qquad \Delta_6\Delta_3\left(\texttt{P}\right)=\texttt{V} \ .$$

דוגמה 4.11

הטבלה הבאה מראה מילים אופיינות מהודעות מוצפנות מאותו יום.

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

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

פתרון:

$$\Delta_4\Delta_1=\left(\texttt{ZRYS}\right)\left(\texttt{JNVU}\right)\left(\texttt{GPDOFWHQB}\right)\left(\texttt{ACIKETMLX}\right) \ ,$$

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

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

■

משפט 4.12 משפט רייבסקי II

- בכל תמורה כפולה $\Delta_4\Delta_1$ של צופן אניגמה קיים זוג מחזורים בסידור מסוים

$$\begin{pmatrix}a_1 & a_2 & \cdots & a_{k-1} & a_k\end{pmatrix}\begin{pmatrix}b_1 & b_2 & \cdots & b_{k-1} & b_k\end{pmatrix}$$

כך ש:

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

הסידור הזה של המחזורים נקרא **סדר רייבסקי**.

- בכל תמורה כפולה $\Delta_5\Delta_2$ של צופן אניגמה קיים זוג מחזורים בסדר רייבסקי

$$\begin{pmatrix} a_1 & a_2 & \cdots & a_{k-1} & a_k \end{pmatrix} \begin{pmatrix} b_1 & b_2 & \cdots & b_{k-1} & b_k \end{pmatrix}$$

כך ש:

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

- בכל תמורה כפולה $\Delta_6\Delta_3$ של צופן אניגמה קיים זוג מחזורים בסדר רייבסקי

$$\begin{pmatrix} a_1 & a_2 & \cdots & a_{k-1} & a_k \end{pmatrix} \begin{pmatrix} b_1 & b_2 & \cdots & b_{k-1} & b_k \end{pmatrix}$$

כך ש:

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

דוגמה 4.12

$$\Delta_4\Delta_1 = (\mathtt{OGKRYSD})(\mathtt{ZUQWFIB})(\mathtt{MJXCP})(\mathtt{HLNVE})(\mathtt{A})(\mathtt{T})$$

ראשית נשים לב שהפירוק למחזורים של $\Delta_4\Delta_1$ הוא בדיוק המבנה הנקבע על ידי משפט רייבסקי. בפרט $\Delta_4\Delta_1$ מכילה:

- זוג מחזורים באורך 7,
- זוג מחזורים באורך 5,
- וזוג מחזורים באורך 1.

לפי משפט רייבסקי II :

$$(\mathtt{ZUQWFIB}) = \Big(\Delta_1(\mathtt{D})\,\Delta_1(\mathtt{S})\,\Delta_1(\mathtt{Y})\,\Delta_1(\mathtt{R})\,\Delta_1(\mathtt{K})\,\Delta_1(\mathtt{G})\,\Delta_1(\mathtt{O})\Big)$$

דוגמה 4.13 קריפטו-אנליזה של צופן אניגמה

נתונות התמורות הבאות של צופן אניגמה:

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

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

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

פענחו את הקסט מוצפן

ILBDA

פתרון:

יהי הטקסט הגלוי

$$x_1x_2x_3x_4x_5 \ .$$

אזי

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

אות 1)

$$\texttt{I} = \Delta_1(x_1) \xRightarrow{\Delta_1\text{משקפת}} x_1 = \Delta_1(\texttt{I}) \xRightarrow{\text{משפט רייבסקי II}} x_1 = \texttt{H}\ .$$

אות 2)

$$\texttt{L} = \Delta_2(x_2) \xRightarrow{\Delta_2\text{משקפת}} x_2 = \Delta_2(\texttt{L}) \xRightarrow{\text{משפט רייבסקי II}} x_2 = \texttt{E}\ .$$

אות 3)

$$\texttt{B} = \Delta_3(x_3) \xRightarrow{\Delta_3\text{משקפת}} x_3 = \Delta_3(\texttt{B}) \xRightarrow{\text{משפט רייבסקי II}} x_3 = \texttt{L}\ .$$

אות 4)

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

$$\Delta_1(\texttt{D}) \overset{\text{משפט רייבסקי II}}{=} \texttt{M} \xRightarrow{\Delta_1\text{משקפת}} \texttt{D} = \Delta_1(\texttt{M}) \Rightarrow \Delta_4(\texttt{D}) = \Delta_4\Delta_1(\texttt{M}) = \texttt{L}\ .$$

אות 5)

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

$$\Delta_2(\texttt{A}) \overset{\text{משפט רייבסקי II}}{=} \texttt{D} \xRightarrow{\Delta_1\text{משקפת}} \texttt{A} = \Delta_1(\texttt{D}) \Rightarrow \Delta_5(\texttt{A}) = \Delta_5\Delta_2(\texttt{D}) = \texttt{O}\ .$$

תשובה סופית:

$$x_1x_2x_3x_4x_5 = \texttt{HELLO}\ .$$

■

שיעור 5
קריפטו-אנליזה

5.1 סוגים של התקפת סייבר

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

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

ישנם 4 סוגים של התקפת סייבר.

1) **התקפת טקסט מוצפן בלבד.**

למתקיף (אוסקר) יש מחרוזת של טקסט מוצפן y .

2) **התקפת טקסט גלוי ידוע**

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

3) **התקפת טקסט גלוי נבחר**

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

4) **התקפת טקסט מוצפן נבחר**

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

החלק הבא מתעסק עם התקפת טקסט מוצפן.

5.2 קבוצות אותיות הנפוצים ביותר בטקסט גלוי

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

כלל 5.1 פונקציית הסתברות של האותיות של האלפיבית

אות	הסתברות
a	0.082
b	0.015
c	0.028
d	0.043
e	0.127
f	0.022
g	0.02
h	0.061
i	0.07
j	0.002
k	0.008
l	0.04
m	0.024

אות	הסתברות
n	0.067
o	0.075
p	0.019
q	0.001
r	0.06
s	0.063
t	0.091
u	0.028
v	0.01
w	0.023
x	0.001
y	0.02
z	0.001

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

כלל 5.2 קבוצות תדירות של אותיות בטקסט גלוי

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

כלל 5.3 זוגות אותיות הנפוצים ביותר בטקסט גלוי

השלושים זוגות אותיות הנפוצים ביותר בטקסט גלוי רשומים בטבלה למטה:

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

כלל 5.4 קבוצות שלשת אותיות הנפוצים ביותר בטקסט גלוי

ה12 שלשות של אותיות הנפוצים ביותר בטקסט גלוי 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

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

פתרון:

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

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

שלב 2) נרשום את האותיות הנפוצות ביותר:

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

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

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

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

- נניח כי

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

- ז"א

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

- נציב $e_k=ax+b$ ונקבל

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

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

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

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

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

$a = 3, b = 5$.

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

- נבנה את הכלל מפענח עם המפתח המתקבל:

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

שלב 4) ננסה לפענח את הטקסט מצפון עם הכלל מפענח

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

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

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

■

דוגמה 5.2

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

FMXVEDKAPHFERBNDKRXRSREFMORUDSDKDVSHVUFEDKAPRKDLYEVLRHHRH

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

פתרון:

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

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

שלב 2) נרשום את האותיות הנפוצות ביותר:

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

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

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

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

- נניח כי

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

- ז"א

$$e_k(4) = 17$$
$$e_k(19) = 3 \ .$$

- נציב $e_k = ax + b$ ונקבל

$$4a + b = 17 \ ,$$
$$19a + b = 3 \ .$$

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

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

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

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

- עכשיו נחזור וננסה

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

- ז"א

$$e_k(4) = 17$$
$$e_k(19) = 4 \ .$$

- נציב $e_k = ax + b$ ונקבל

$$4a + b = 17 \ ,$$
$$19a + b = 4 \ .$$

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

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

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

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

עכשיו נחזור וננסה

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

- ז"א

$$e_k(4) = 17$$
$$e_k(19) = 7 \ .$$

- נציב $e_k = ax + b$ ונקבל

$$4a + b = 17 \ ,$$
$$19a + b = 7 \ .$$

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

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

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

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

עכשיו נחזור וננסה

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

- ז"א

$$e_k(4) = 17$$
$$e_k(19) = 10 \ .$$

- נציב $e_k = ax + b$ ונקבל

$$4a + b = 17 \ ,$$
$$19a + b = 10 \ .$$

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

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

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

ז"א $a = 3, b = 5$.

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

- נבנה את הכלל מפענח עם המפתח המתקבל:

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

שלב 4) ננסה לפענח את הטקטסט מצפון עם הכלל מפענח

$\mathrm{y} \in C$	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
$\mathrm{x} \in P$	a	l	g	o	r	i	t	h	m	s	a	r	e	q	u	i	t	e	g	e

$\mathrm{y} \in C$	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
$\mathrm{x} \in P$	n	e	r	a	l	d	e	f	i	n	i	t	i	o	n	s	o	f	a	r

$\mathrm{y} \in C$	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
$\mathrm{x} \in P$	i	t	h	m	e	t	i	c	p	r	o	c	e	s	s	e	s

■

5.4 קריפטו-אנליזה של צופן היל

זו דוגמה של התקפת טקסט גלוי ידוע.

משפט 5.1

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

נניח שיש למתקיף לפחות m טקסטים גלוים וטקסטים מוצפנים. של הטקטסט גלוי:

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

ו-

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

$1 \leq j \leq m$ כך ש-

$$y_j = e_k\left(x_j\right) \ .$$

נגדיר שתי מטריצות

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

אם X הפיכה אז
$$Y = XK \qquad \Leftrightarrow \qquad K = X^{-1}Y \ .$$
כאשר $K \in \mathbb{Z}_{26}^{m\times m}$ המפתח של הצופן היל.

דוגמה 5.3

נתון הטקסט גלוי

friday

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

PQCFKU

מצאו את המפתח של הצופן.

פתרון:

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

ז"א
$$e_k(5,17) = (15,16)\ , \qquad e_k(8,3) = (2,5)\ , \qquad e_k(0,24) = (10,20)\ .$$
נקח את שני טקסטים גלוים וטקסוים מוצפנים המתאימיפו נגדיר את המטריצות
$$X = \begin{pmatrix} 5 & 17 \\ 8 & 3 \end{pmatrix}\ , \qquad Y = \begin{pmatrix} 15 & 16 \\ 2 & 5 \end{pmatrix}\ .$$

אזי
$$K = X^{-1}Y\ .$$
נחשב את ההופכית X^{-1} באמצעות נוסחת קיילי $X^{-1} = |X|^{-1}\text{adj}(X)$.
$$\begin{aligned}|X| =& 15 - 136 \mod 26\\ =& -121 \mod 26\\ =& -4(26) - 17 \mod 26\\ =& -17 \mod 26\\ =& 9 \mod 26\ .\end{aligned}$$

לכן
$$|K|^{-1} \mod 26 = 9^{-1} \mod 26 = 3.$$
המטריצת הקופקטורים של X היא $C = \begin{pmatrix} C_{11} & C_{12} \\ C_{21} & C_{22} \end{pmatrix}$ כאשר
$$C_{11} = 3\ , \qquad C_{12} = -8\ , \qquad C_{21} = -17\ , \qquad C_{22} = 5\ .$$

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

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

לפיכך

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

■

דוגמה 5.4

נתון הטקסט גלוי

`theresnoplacelikehome`

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

`FHVTUTGQVRWPCPSFGGAMG`

מצאו את המפתח של הצופן.

פתרון:

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

ז"א

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

נקח את שני טקסטים גלוים וטקסוים מוצפנים המתאימיפו נגדיר את המטריצות

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

אזי

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

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

$$|X| = 15 - 136 \mod 26$$
$$= -3051 \mod 26$$
$$= 17 .$$

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

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

לבסוף נקבל

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

לפיכך

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

■

5.5 מדד צירוף המקרים

הגדרה 5.1 מדד צירוף המקרים I_c

נתון מחרוזת של טקסט גלוי $\mathrm{x} = x_1 x_2 \cdots x_n$ של אורך n.

המדד צירוף המקרים של x מסומן $I_c(\mathrm{x})$ ומוגדר להיות ההסתברות ששתי אותיות הנבחורת באקראי מתוך x יהיו זהות.

משפט 5.2 נוסחה לחישוב המדד צירוף המקרים

נתון מחרוזת של טקסט גלוי $\mathrm{x} = x_1 x_2 \cdots x_n$ של אורך n.
יהי f_k מספר הפעמים שהאות מספר k באלפיבית מופיעה במחרוזת x. למשל, f_0 מסמן את מסםר הפעמים שהאות a מופיעה, f_1 מסמן את מסםר הפעמים שהאות b מופיעה, וכן הלא.

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

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

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

המדד צירוף המקרים של הטקסט גלוי x נתון על ידי הנוסחה

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

משפט 5.3 מדד צירוף המקרים בטקסט גלוי

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

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

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

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

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

המדד צירוף המקרים מצופה להיות

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

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

דוגמה 5.5

נתון הטקטסט מוצפן

```
MOKSMNXBIUCMQXGCAXOFXMUWLNRNSFMIQBHNCFCGDTAHANTTIJNIERGCHURYHOGGSWTMP
CCOYISKOGXLQAFMVXNFEDAEMHQTNAAQXUDIXXRSILCIZKGWEFLAWGUJAOAUPLXRQTGATPS
MKLQSWRGTXJNPXEUNSYIACRGWLQEIMDUBQQGAEEYULEEWXDLIIDUHQOFXWEAZJTUOFXWKS
MTNAAFXTTMFPMUWLNRNSFMOBIJJTUSFPRMRVBLMQXXRURKCAZGWCWAAGADECGDMMCZJVQS
NNRTISADILALHOEFWOFTGBSUFDHHMZWJNKWAPNUJALAZGWCOKSMXRMRQXNQMFHOGVGAGMR
AIAFMGWCMRQXUMJXXRPXGCAWILQAFGZJNOIQXUMVWZUUXWAISLLVIEXWABARVHOGEJNWAV
LQMAVWCOYISUIHIK
```

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

פתרון:

שלב 1: נפרק את הטקסט לעמודות של 3 אותיות

y_1	M	N	C	C	X	N	M	N	D	N	N	C	H	W	C	K	Q	X	A	T	X	X	C	W	W	O	X	A	K	R	⋯
y_2	O	X	M	A	M	R	I	C	T	T	I	H	O	T	O	O	A	N	E	N	U	R	I	E	G	A	R	T	L	G	⋯
y_3	K	B	Q	X	U	N	Q	F	A	T	E	U	G	M	Y	G	F	F	M	A	D	S	Z	F	U	U	Q	P	Q	T	⋯
y_4	S	I	X	O	W	S	B	C	H	I	R	R	G	P	I	X	M	E	H	A	I	I	K	L	J	P	T	S	S	X	⋯
y_5	M	U	G	F	L	F	H	G	A	J	G	Y	S	C	S	L	V	D	Q	Q	X	L	G	A	A	L	G	M	W	J	⋯

שלב 2: נחשב את המדד המשותף של כל שורה

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

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

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

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

תהיו קרובות להסתברויות $p_0, \ldots, p_{25}$ של אותיות בטקסט גלוי.

כעת נגדיר את המדד המשותף

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

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

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

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

$\underline{y_1}$

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				

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				

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	0.0.0372529	z	0.0352184				

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				

ננסה לפענח את הטקסט מוצפן עם המפתח

JAMES

ונקבל את התשובה

doyouexpectmetotalknomisterbondiexpectyoutodiethereisnothingyoucantalk
tomeaboutthatidontalreadyknowyoureforgettingonethingififailtoreportdou
bleoeightreplacesmeitrusthewillbemoresuccessfulwellheknowswhatiknowyou
knownothingmisterbondoperationgrandslamforinstancetwowordsyoumayhaveov
erheardwhichcannotpossiblyhaveanysignificancetoyouoranyoneinyourorgani
zationcanyouaffordtotakethatchanceyouarequiterightmisterbondyouarewort
hmoretomealives

עם רווחים וסימני פיסוק:

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

```python
def letterToZ26(a):
    if a.isalpha():
        if a.isupper():
            return ord(a) - 65
        if a.islower():
            return ord(a) - 97

def Z26ToUpperLetter(a):
    return chr(a+65)

def Z26ToLowerLetter(a):
    return chr(a+97)

probabilities = [0.082, 0.015, 0.028, 0.043, 0.127, 0.022, 0.02, 0.061, 0.07, 0.002,
    0.008, 0.04, 0.024, 0.067, 0.075, 0.019, 0.001, 0.06, 0.063, 0.091,  0.028, 0.01,
    0.023, 0.001, 0.02, 0.001]

alphabetLower = ['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']
alphabetUpper = ['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']

def P(a):
    i = alphabetLower.index(a)
    return probabilities[i]

cipherText = "
    MOKSMNXBIUCMQXGCAXOFXMUWLNRNSFMIQBHNCFCGDTAHANTTIJNIERGCHURYHOGGSWTMPCCOYISKOGXLQAFMVXNFEDAE
    "

cipherTextList = list(cipherText)

y= [None]*5
for i in range(0,6):
    y[i] = cipherTextList[i::5]

```

```
print( len(y[0]) == len(y[1]) == len(y[2]) ==  len(y[3]) == len(y[4]) )

f = [None]*26

n = len(y[0])

My = [None]*5

for k, yi in enumerate(y):
    for i,X in enumerate(alphabetUpper):
            f[i] = yi.count(X)

    A = [None]*26

    for g in range(0,26):
        Sum = 0;
        b = alphabetLower[g]

        for i in range(0,26):
            a = alphabetLower[i]
            Sum += P(a)*f[(i+g) % 26]

        Sum = Sum / n

        A[g] = [b , Sum   ]

    My[k] = A

keyWord = 'james'

keyZ26 = [letterToZ26(a) for a in list(keyWord)]

Y = [letterToZ26(a) for a in cipherTextList]

X = []

for i,y in enumerate(Y):
    x = ( y - keyZ26[ i%5 ] ) % 26
    X.append(x)

plainTextList = [Z26ToLowerLetter(a) for a in X]
plainText = ''.join(plainTextList)
```

■

שיעור 6
צופן RSA

6.1 אלגוריתם RSA

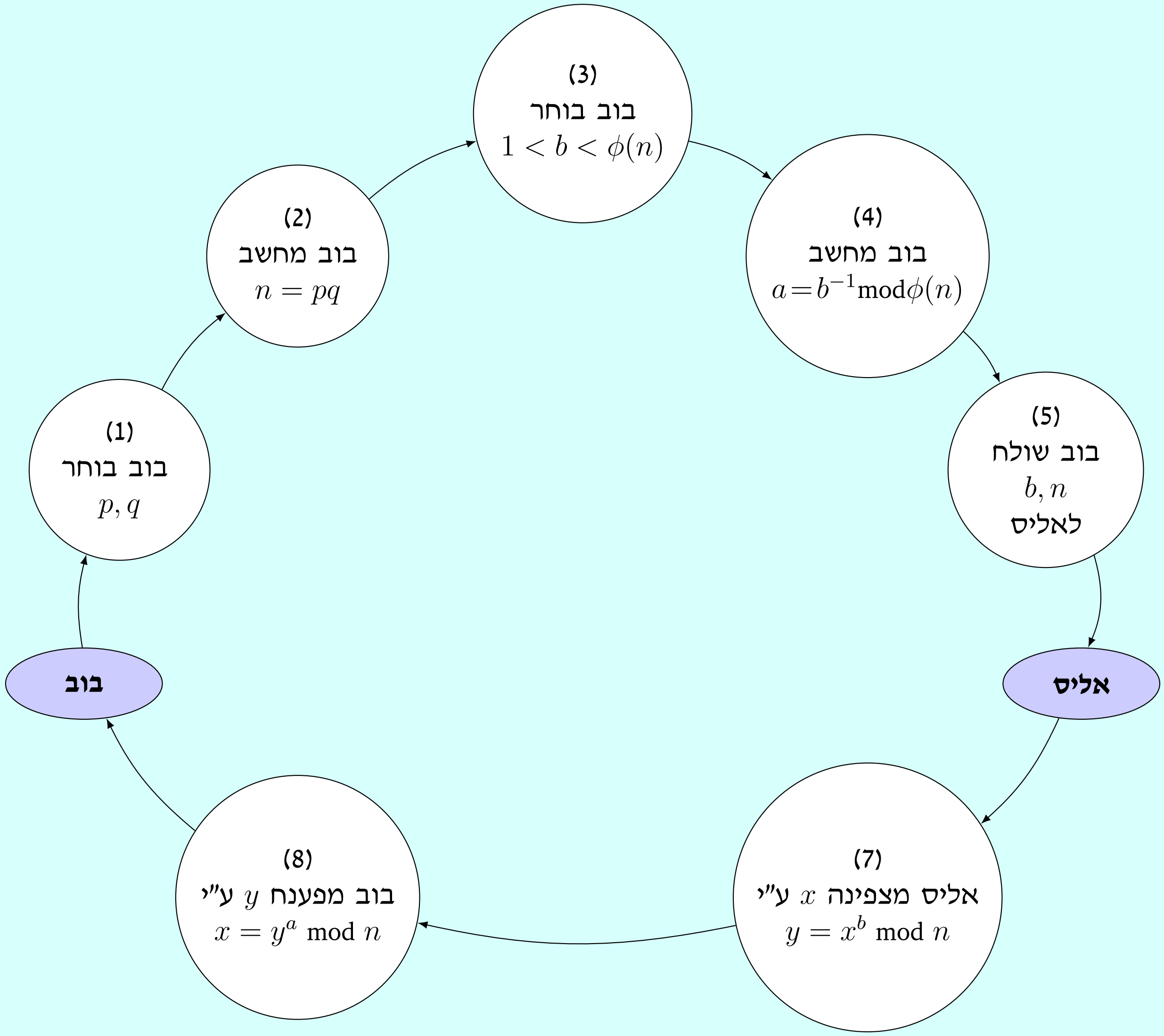
צופן RSA הומצא בשנה 1977 על ידי Ron Rivest, Adi Shamir and Len Adleman .

הגדרה 6.1 צופן RSA

- יהיו p,q מספרים ראשוניים שונים ($p\neq q$).
- יהי $n=pq$.
- יהי b שלם כך ש: $1<b<\phi(n)$ כאשר $\phi(n)$ הפונקצית 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).
- יהי $x\in\mathbb{Z}^+$ שלם אי-שלילי.
  * הכלל מצפין מוגדר
  $$e_k(x)=x^b \mod n\ ,$$
  * והכלל מפענח מוגדר
  $$d_k(x)=y^a \mod n\ .$$

עכשיו שנתנו הגדרה מתמטית של הצופן RSA אנחנו נסביר את הסדר של הפעולות של הבניית המפתח, ההצפנה והפענוח באלגוריתם הבא.

הגדרה 6.2 אלגוריתם RSA



נניח שאליס (A) שולחת הודעה לבוב (B).

<u>שלב הבניית המפתח</u>

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

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

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

[4] B מחשב a כך ש- $a = b^{-1} \mod \phi(n)$ בעזרת האלגוריתם של אוקלידס, (ראו כלל 1.12) ולכן $0 \leq a < \phi(n)$.

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

בניית מפתח עשוי פעם אחת.

<u>שלב הצפנה</u>

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

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

[8] A שולחת טקסט מוצפן ל- B.

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

דוגמה 6.1

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

א) חשבו את n, $\phi(n)$ ו- a.

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

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

פתרון:

סעיף א)

$$n=pq=191\times 127=24257$$
$$\phi(n)=\phi(pq)=(p-1)(q-1)=190\times 126=23940\ .$$

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

<u>שיטה 1</u>

$a=23940, b=47$.

$$r_0=a=23940\ ,\qquad r_1=b=47\ ,$$
$$s_0=1\ ,\qquad s_1=0\ ,$$
$$t_0=0\ ,\qquad t_1=1\ .$$

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

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

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

מכאן

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

<u>שיטה 2</u>

$$\begin{aligned}23940 &=509(47)+17\\ 47 &=2(17)+13\\ 17 &=13+4\\ 13 &=3(4)+1\\ 4 &=4(1)+0\ .\end{aligned}$$

$$\begin{aligned}1 &=13-3(4)\\ &=13-3(17-13)\\ &=4(13)-3(17)\\ &=4(47-2(17))-3(17)\\ &=4(47)-11(17)\\ &=4(47)-11(23940-509(47))\\ &=5603(47)-11(23940)\end{aligned}$$

לכן $a^{-1}=5603$.

סעיף ב) אליס שולחת את ההודעה $2468^{47}\mod 24257$. כדי לחשב זה נשתמש בשיטת ריבועים:
$47=32+8+4+2+1$.

$$\begin{aligned}(2468)^2 & &=2517\mod 24257\\ (2468)^4 &=(2517)^2 &=4212\mod 24257\\ (2468)^8 &=(4212)^2 &=9077\mod 24257\\ (2468)^{16} &=(9077)^2 &=15157\mod 24257\\ (2468)^{32} &=(15157)^2 &=20859\mod 24257\end{aligned}$$

לכן

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

לכן הטקסט מוצפן הוא $y=10642$.

סעיף ג) $y=10642$.

$$y\mod p=10642\mod 127=101\ ,\qquad a\mod (p-1)=5603\mod 126=59\ .$$

לכן

$$x_1 = (y \mod p)^{a \mod (p-1)} \mod p = 101^{59} \mod 127 = 55$$

(ניתן לחשב זה לפי $101 \times 101^2 \times 101^8 \times 101^{16} \times 101^{32}$.)

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

לכן

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

$$y \mod q = 10642 \mod 191 = 137 , \qquad a \mod (p-1) = 5603 \mod 190 = 93 .$$

לכן

$$x_2 = (y \mod q)^{a \mod (q-1)} \mod q = 137^{93} \mod 191 = 176$$

(ניתן לחשב זה לפי $137 \times 137^4 \times 137^8 \times 137^{16} \times 137^{64}$.)

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

לכן

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

בנוסף

$$y \mod q = 9625 \mod 127 = 100 , \qquad a \mod (q-1) = 5603 \mod 126 = 59 .$$

לכן

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

לכן עלינו לפתור את המערכת

$$\begin{aligned}
x =& x_1 \mod p = 55 \mod 127\\
x =& x_2 \mod q = 176 \mod 191
\end{aligned}$$

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

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

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

<u>שיטה 1</u>

$a=191, b=127$.

$$\begin{aligned} r_0 &= a = 191 \ , \qquad & r_1 = b = 127 \ , \\ s_0 &= 1 \ , & s_1 = 0 \ , \\ t_0 &= 0 \ , & t_1 = 1 \ . \end{aligned}$$

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

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

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

לכן

$$\begin{aligned} &191^{-1} \equiv 2 \mod 127 \\ &127^{-1} \equiv (-3) \mod 191 \equiv 188 \mod 191 \ . \end{aligned}$$

<u>שיטה 2</u>

נחשב $y_1 = 191^{-1} \mod 127$ ו- $y_2 = 127^{-1} \mod 191$ 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

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

נחשב

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

לכן

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

■

6.2 משפט השאריות הסיני

משפט 6.1 משפט השאריות הסיני

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

$$\begin{aligned} x =& a_1 \mod m_1 , \\ x =& a_2 \mod m_2 , \\ & \vdots \\ x =& a_r \mod m_r , \end{aligned}$$

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

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

כאשר $M_i = \dfrac{M}{m\, i}$ ו- $y_i = M_i^{-1} \mod m_i$ לכל $1 \leq i \leq r$.

דוגמה 6.2

היעזרו במשפט השאריות הסיני כדי לפתור את המערכת

$$\begin{aligned} x =& 22 \mod 101 , \\ x =& 104 \mod 113 . \end{aligned}$$

פתרון:

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

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

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

כדי לחשב את האיברים ההופכיים נשתמש בהאלגוריתם המוכלל של אוקליד.

נסמן $a=113, b=101$.

$$\begin{aligned} r_0 &= a = 113 \ , \qquad & r_1 = b = 101 \ , \\ s_0 &= 1 \ , & s_1 = 0 \ , \\ t_0 &= 0 \ , & t_1 = 1 \ . \end{aligned}$$

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

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

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

מכאן

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

ו-

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

לכן

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

ו-

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

$$\begin{aligned} x &= a_1M_1y_1+a_2M_2y_2 \mod M \\ &= 22\cdot 113\cdot 59+104\cdot 111\cdot 47 \mod 11413 \\ &= 640362 \mod 11413 \\ &= 1234 \ . \end{aligned}$$

■

6.3 משפטים של מספרים ראשוניים

משפט 6.2 קיימים אינסוף מספרים ראשוניים

קיימים אינסוף מספרים ראשוניים.

הוכחה: נוכיח הטענה דרך השלילה.
נניח כי $\{p_1,\ldots,p_n\}$ הוא הקבוצה של כל הראשוניים שקיימים וקבוצה זו נוצרת סופי.

נגדיר השלם $M=(p_1\cdot p_2\cdot\ldots\cdot p_n)+1$.
לפי משפט הפירוק לראשוניים (ראו משפט 1.4 למעלה או משפט 6.3 למטה) M הוא מספר ראשוני או שווה למכפלה של ראשוניים.
M לא מספר ראשוני בגלל ש- $M>p_i$ לכל $1\leq i\leq n$.
גם לא קיים מספר ראשוני p_i אשר מחלק את M. הרי

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

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

משפט 6.3 משפט הפירוק לראשוניים

(ראו משפט 1.4) לכל מספר שלם n קיימים שלמים e_i וראשוניים p_i כך ש-

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

הוכחה: אינדוקציה. ■

משפט 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 $1,p,p^2,\ldots,p^n$. בסה"כ יש p^n אפשרויות.

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

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

■

משפט 6.6 נוסחה לפונקצית אוילר

(ראו משפט **??**) לכל מספר שלם n בעל פירוק לראשוניים

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

פונקציית אוילר ניתנת על ידי

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

הוכחה: משפט 6.4 ו- 6.5. ■

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 ו- 6.5. ■

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:

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

הוכחה:

טענה 1. נוכיח באינדוקציה.

בסיס:

עבור $a = 0$ הטענה $0^p \equiv 0 \mod p$ מתקיימת.

מעבר:

נניח כי הטענה מתקיימת עבור a.

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

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

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

כנדרש.

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

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

טענה 3.

$$a^{p-1} \equiv 1 \mod p \qquad \Leftrightarrow \qquad 1 \equiv a^{p-1} \mod p \quad \Rightarrow \quad a^{-1} \equiv a^{p-2} \mod p\ .$$

■

משפט 6.10 משפט אוילר

אם a,n שלמים ו- $\gcd(a,n) = 1$ אז

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

משפט 6.11

אם a,n שלמים ו- $\gcd(a,n) = 1$ אז

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

דוגמה 6.4

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

פתרון:

לפי משפט פרמט 6.9:

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

לפי הנוסחת לשארית ?? :

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

לכן $5^{-1} \in \mathbb{Z}_{11} = 9$. ■

6.4 הוכחה שצופן RSA ניתן לפענוח

משפט 6.12 קריפטו-מערכת RSA ניתן לפענוח

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

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

הוכחה: נתון כי $ab = 1 \mod \phi(n)$.
לפי משפט 6.8, $\phi(n) = \phi(pq) = (p-1)(q-1)$.

ז"א
$$ab = 1 \mod \phi(n) = 1 \mod (p-1)(q-1)$$
לכן קיים $t \in \mathbb{Z}$ כך ש-
$$ab - 1 = t(p-1)(q-1) \ .$$
לכל $z \neq 0 \in \mathbb{Z}$ לפי משפט 6.9, $z^{p-1} = 1 \mod p$. בפרט
$$x^{ab-1} = x^{t(p-1)(q-1)} = \left(x^{t(q-1)}\right)^{p-1} = y^{p-1}$$
כאשר $y = x^{t(q-1)}$. מכאן $x^{ab-1} = 1 \mod p$.

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

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

מכיוון ש- p ו- q זרים אז
$$x^{ab-1} - 1 = 0 \mod (pq) \ .$$
לפיכך
$$x^{ab-1} = 1 \mod (pq) \ .$$
נכפיל ב- x ונקבל
$$(x^a)^b = x \mod (pq) \ .$$
ז"א הוכחנו כי לכל טקסט גלוי x, אם נצפין אותו ואז אחר כך נפענח את הטקסט מוצפן המתקבל מאלגוריתם RSA, נקבל אותו טקסט גלוי המקורי בחזרה. ■

6.5 צופן RSA המוכלל

משפט 6.13

יהיו p, q מספרים ראשוניים ויהי $n = pq$. יהי
$$\lambda(n) = \frac{(p-1)(q-1)}{\gcd(p-1, q-1)} \ .$$
נגדיר צופן חדש אשר זהה ל- RSA אלא $\phi(n)$ הוחלף עם $\lambda(n)$ כך ש- $ab \equiv 1 \mod \lambda(n)$. אזי הקריפטו-מערכת ניתן לפענח.

הוכחה:

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

שלב 2) נתון כי $d = \gcd(p-1, q-1)$. ז"א שקיים p' שלם כך ש-
$$p - 1 = p'd \quad \Leftrightarrow \quad \frac{p-1}{d} = p' \quad \Leftrightarrow \quad d = \frac{p-1}{p'} \ . \qquad (\#1)$$
באותה מידה קיים q' שלם כך ש-
$$q - 1 = q'd \quad \Leftrightarrow \quad \frac{q-1}{d} = q' \quad \Leftrightarrow \quad d = \frac{q-1}{q'} \ . \qquad (\#2)$$

שלב 3)

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

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

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

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

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

לכן

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

מכאן

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

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

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

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

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

לכן

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

מכאן

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

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

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

שלב 6) מכיוון ש- p,q ראשוניים אז

$$\left.\begin{aligned} x^{ab-1}&\equiv 1 \mod q\\ x^{ab-1}&\equiv 1 \mod q\end{aligned}\right\}\quad\Rightarrow\quad x^{ab-1}\equiv 1 \mod pq$$

לפיכך

$$x^{ab-1}\equiv 1 \mod n\quad\Rightarrow\quad \left(x^b\right)^a\equiv x \mod n$$

כנדרש.

■

שיעור 7
הבעיית הפירוק של מספירם וצופן רבין

7.1 הבעיית פירוק מספרים

7.2 צופן רבין

שיעור 8
צופן אל-גמאל

הגדרה 8.1 צופן אל-גמאל

יהי p מספר ראשוני (גדול), α יוצר של $\left(\mathbb{Z}_p^*, \times_p\right)$ ויהי $a \in \{2,3,\ldots,p-2\}$.
יהי הקבוצת טקסט גלוי $P=\mathbb{Z}_p^*$ והקבוצת טקסט מוצפן $C=\mathbb{Z}_p^* \times Z_p^*$. נגדיר קבוצת מפתחות

$$K=\left\{(p,\alpha,a,\beta) \,\middle|\, \beta=\alpha^a \mod p\right\} .$$

לכל $k=(p,\alpha,a,\beta)\in K$, $x\in P$, $(y_1,y_2)\in P$ ו- $d=\{2,3,\ldots,p-2\}$ נגדיר

$$e_k\left(x,d\right)=\left(y_1,y_2\right)$$

כאשר $y_1=\alpha^d \mod p$, $y_2=\beta^d x \mod p$ ו-

$$d_k(y_1,y_2)=\left(y_1^a\right)^{-1} y_2 \mod p .$$

(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 $\left(\mathbb{Z}_p^*, \times_p\right)$, $a\in\{2,3,\ldots,p-2\}$, $\beta=\alpha^a \mod p$ ו- $x\in\mathbb{Z}_p^*$ אז לכל $d\in\{2,3,\ldots,p-2\}$

$$\left(\left(\alpha^d\right)^a\right)^{-1}\beta^d x = x \mod p .$$

הוכחה: תרגיל בית. ■

כלל 8.1 אלגוריתם הצפנת אל-גמאל

נניח שאליס (A) שולחת הודעה לבוב (B).

שלב הרכבת המפתח

1 B יוצר מספר ראשוני גדול p, ויוצר α של החבורה $\left(\mathbb{Z}_p^*, \times_p\right)$.

2 B בוחר באקראי שלם $a\in\{2,3,\ldots,p-2\}$,

3 B מחשב β כך ש- $\beta=\alpha^a \mod p$.

4 B שומר את המפתח ציבורי (p,α,β) בכתובת ציבורית ושמור על a כמפתח סודי.

שלב הצפנה

5 אליס (A) קוראת את המפתח ציבורי (p,α,β) מהכתובת ציבורית.

6 A בוחרת באקראי שלם $d\in\{2,3,\ldots,p-2\}$.

7 כדי להצפין הודעה x כאשר $0\leq x<p$, אליס (A) מחשבת $y_1=\alpha^d \mod p$ ו- $y_2=\beta^d x \mod p$.

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 $x = ((y_1)^a)^{-1} y_2$ $\mod p$.

דוגמה 8.1 הצפנת אל-גמאל

נניח כי אליס שולחת הטקסט גלוי $x = 123$. בוב בוחר במספר ראשוני $p = 727$, יוצר $\alpha = 80$ ומפתח סודי $a = 6$. אליס בוחרת ב- $d = 7$. מצאו את הטקסט מוצפן.

פתרון:

$$\beta = \alpha^a \mod p = 80^6 \mod 727 = 514 \ .$$

$$y_1 = \alpha^d \mod p = 80^7 \mod 727 = 408 \ , \qquad y_2 = \beta^d x \mod p = 514^7 \cdot 123 \mod 727 = 390 \ .$$

■

דוגמה 8.2 הצפנת אל-גמאל

נניח כי בוב מקבל את הטקסט מוצפן $(y_1, y_2) = (408, 390)$. בוב בחר במספר ראשוני $p = 727$, יוצר $\alpha = 80$ ומפתח סודי $a = 6$. ואליס בחרה ב- $d = 7$. פענחו את הקטסט מוצפן.

פתרון:

$$\beta = \alpha^a \mod p = 80^6 \mod 727 = 514 \ .$$

$$x = \left((y_1^a)^{-1}\right) y_2 \mod p = \left(\left(480^6\right)^{-1}\right) \cdot 390 \mod 727$$

בעזרת משפט פרמה,

$$\left(408^6\right)^{-1} \mod 727 = 408^{727-1-6} \mod 727 = 408^{720} \mod 727 = 375 \ .$$

■

שיעור 9
תורת שאנון

9.1 סודיות מושלמת

נתונה קריפטו-מערכת

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

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

אנחנו נתייחס לטקסטים גלויים

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

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

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

כמשתנה מקרי בדיד אשר ערכו שווה למפתח הנבחר.

נסמן את הפונקציית הסתברות של הטקסט גלוי ב-

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

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

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

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

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

$$Y(k) = \left\{ e_k(x) \middle| \ x \in X \right\} \ .$$

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

$$P(Y = y) = \sum_{k \in K} P(K = k) P\left(X = d_k(y)\right) \ . \tag{9.1}$$

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

$$P(Y = y|X = x) = \sum_{\substack{k \in K \\ x = d_k(y)}} P(K = k) \ . \tag{9.2}$$

מכאן, לפי נוסחת בייס, $P(X=x|Y=y)=\dfrac{P(Y=y|X=x)P(X=x)}{P(Y=y)}$. נציב את משוואת (9.1) ומשוואות (9.2) ונקבל את הביטוי

$$P(X=x|Y=y)=\frac{P(X=x)\displaystyle\sum_{\substack{k\in K\\ x=d_k(y)}}P(K=k)}{\displaystyle\sum_{k\in K}P(K=k)P\left(X=d_k(y)\right)}\ . \tag{9.3}$$

דוגמה 9.1

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

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

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

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

ונתונה קבוצת טקסט מוצפן

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

נניח כי הכלל מצפין מוגדר כך ש-

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

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

פתרון:

אפשר לייצג את הקריפטו-מערכת כמטריצת הצפנה:

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

נחשב את הפונקצית ההסתברות של Y:

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

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

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

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

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

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

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

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

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

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

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

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

■

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

משפט 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 ההסתברות $P(Y=y)$ באמצעות (9.1). הקבוצת מפתחות בצופן קיסר היא

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

לכן
$$P(Y=y)=\sum_{k\in\mathbb{Z}_{26}} P(K=k)P\left(X=d_k(y)\right) \ .$$
אם ההסתברות של כל מפתח שווה אז $P(K=k)=\dfrac{1}{26}$ ולכן
$$P(Y=y)=\frac{1}{26}\sum_{k\in\mathbb{Z}_{26}} P\left(X=d_k(y)\right) \ .$$
הכלל מצפין והכלל מפענח של צופן קיסר מוגדרים
$$e_k(x)=x+k \mod 26 \ , \qquad d_k(y)=y-k \mod 26 \ .$$
כאשר $k\in\mathbb{Z}_{26}$. לכן $P(X=d_k(y))=P(X=y-k \mod 26)$. לפיכך
$$P(Y=y)=\frac{1}{26}\sum_{k\in\mathbb{Z}_{26}} P\left(X=y-k \mod 26\right) \ .$$
הסכום בצד הימין הוא רק סכום של $P(X=k)$ מעל כל האיברים k ב- $\mathbb{Z}_{26}$. לכן
$$P(Y=y)=\frac{1}{26}\sum_{k\in\mathbb{Z}_{26}} P\left(X=k\right)=\frac{1}{26}\cdot 1=\frac{1}{26} \ .$$
כאשר בשוויון השני השתמשנו בתכונת הנרמול של הפונקצית 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-
$$x=k-y \mod 26 \qquad \Rightarrow \qquad k=x+y \mod 26 \ .$$
לכל $x\in X$ ולכל $y\in Y$ קיים רק מפתח אחד אשר מקיים תנאי זה. ז"א רק איבר אחד של הסכום נשאר ולפיכך
$$P(Y=y|X=x)=\sum_{\substack{k\in\mathbb{Z}_{26}\\ x=d_k(y)}} P(K=k)=P(K=y-x \mod 26) \ .$$
אם ההסתברות של כל מפתח שווה, כלומר אם $P_K(k)=\dfrac{1}{26}$ לכל $k\in K$, אז
$$P(Y=y|X=x)=P(K=y-x \mod 26)=\frac{1}{26} \ .$$
לכן
$$P(Y=y)=\frac{1}{26}=P(Y=y|X=x)$$
ז"א לצופן קיסר יש סודיות מושלמת. ■

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

למה 9.1 תנאי חילופי לסודיות מושלמת

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

$$P(Y=y|X=x)=P(Y=y) \ . \tag{9.4}$$

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- $e_k(x)=y$

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

הוכחה:

1) לפי (9.4),

$$P(Y=y|X=x)=P(Y=y)>0 \tag{\#1}$$

נציב (9.2) בצד שמאל ונקבל

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

ז"א

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

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

$$|K|\geq|Y| \ . \tag{\#4}$$

■

משפט 9.2 משפט שאנון

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

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

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

הוכחה:

1) נניח כי $|K|=|Y|$. כלומר

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

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

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

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

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

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

$$P(X=x_i|Y=y)=\frac{P(Y=y|X=x_i)P(X=x_i)}{P(Y=y)}$$
$$\stackrel{\text{לפי (9.2)}}{=}\frac{P(K=k_i)P(X=x_i)}{P(Y=y)}$$

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

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

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 אפשריות:

$$X\in\{\mathrm{a},\mathrm{b},\mathrm{c},\mathrm{a}\} \ .$$

X ידוע לבוב (B) אבל לא ידוע לאליס (A). כל שאליס יודעת הוא ש- X יכול להיות אחת האותיות $\{\mathrm{a},\mathrm{b},\mathrm{c},\mathrm{a}\}$ בהסתברות שווה. אנחנו אומרים כי לאליס יש אי-ודאות על הערך של X. כדי שאליס תמצא את הערך של X אליס שואלת סדרת שאלות בינאריות (שאלות כן/לא) לבוב כדי לקבל מידע על המ"מ X עד שהיא תדע את הערך של X עם אי-ודאות אפס.

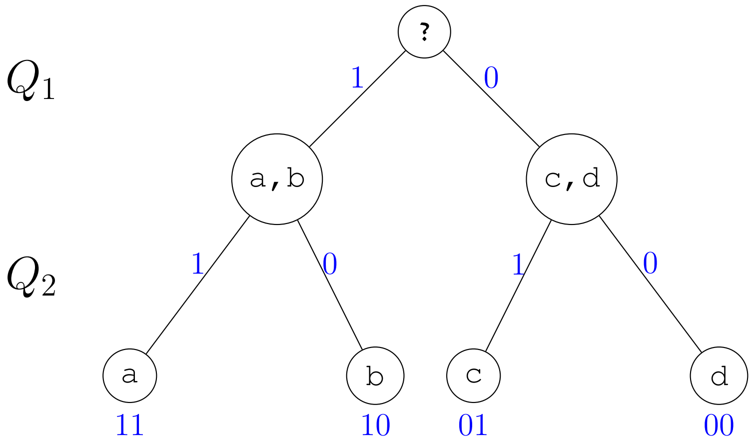
אפשרות אחת לסדרת שאלות היא כך:

Q_1: האם $X\in\{\mathrm{a},\mathrm{b}\}$?

לפי התשובה אחר כך אליס שואלת

Q_2: אם $X\in\{\mathrm{a},\mathrm{b}\}$ האם $X=\mathrm{a}$?

אחרת אם $X\notin\{\mathrm{a},\mathrm{b}\}$ האם $X=\mathrm{c}$?



הסדרה של שאלות בינאריות שמאפשרת לאליס למצוא את X ללא שוף אי-ודאות מתוארת בעץ-שאלות למעלה. מספר השאלות הבינאריות $N_Q[X]$, שנדרשות כדי למצוא X ללא אי-ודאות הוא $N_Q[X]=2$.

כל שאלה היא בינארית, כלומר התשובה היא כן או לא אנחנו מצפינים תשובה כן עם "1" ותשובה לא עם "0". לפי התשובות אנחנו מצפינים את האותיות כך:

$$a \to 11\ , \quad b \to 10\ , \quad c \to 01\ , \quad d \to 00\ .$$

מכיוון ששתי תשובות בינאריות נדרשות כדי למצוא את X, אנחנו אורמים כי נדרש שני ביטים (bits) של מידע נדרשים כדי למצוא את X.
במילים אחרות, שתי ספרות ביניאריות $X=d_1d_2$ נדרשות כדי להצפין את X, שערכן הן התשובות לשתי שאלות ביניאריות,
לכן המידע המתקבל על מציאת הערך של X הוא 2 bit.

אליס הייתה יכולה לשנות את הסדרת שאלות שלה כך:

Q_1' האם $X=\mathtt{a}$?

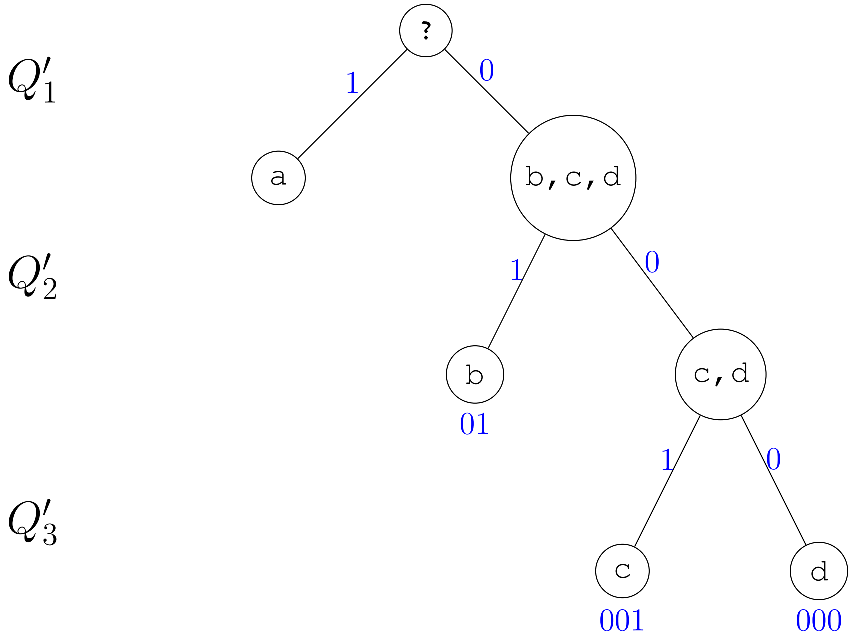
רק אם התשובה היא "לא" אז היא צריכה לשאול שאלה נוספת:

Q_2' האם $X=\mathtt{b}$?

ורק אם השתובה היא "לא" אז היא צריכה לשאול שאלה נוספת:

Q_3' האם $X=\mathtt{c}$?

מספר השאלות הביניאריות הנדרשות למצוא את X תלוי על הערך של X: $N_Q(\mathtt{a})=1$, $N_Q(\mathtt{b})=2$ או $N_Q(\mathtt{c})=N_Q(\mathtt{d})=3$.



X הוא משתנה מקרי בדיד ולכן בהינתן מערכת שאלות, $N_Q(X)$ הוא פונקציה של משתנה מקרי בדיד, ולכן $N_Q[X]$ הוא בעצמו משתנה מקרי בדיד.

כעת נשאל שאלה. נניח כי אליס מעוניינת למצוא מערכת שאלות Q, אשר נותנת את מספר השאלות הממוצע המינימלי. כלומר, כיצד נמצא מערכת שאלות $N_Q[X]$ עבורה התוחלת

$$E\left[N_Q[X]\right] = \sum_{k\in X} P_X(k)N_Q[k]$$

תהיה מינימלית.

לפני שנענה על שאלה הזאת נתן דוגמה.

נתון המשתנה מקרי $X = \{\mathtt{a}, \mathtt{b}, \mathtt{c}, \mathtt{d}\}$ בעל פונקצית ההסתברות

$$P_X\left(\mathtt{a}\right) = \frac{1}{2} \ , \quad P_X\left(\mathtt{b}\right) = \frac{1}{4} \ , \quad P_X\left(\mathtt{c}\right) = P_X\left(\mathtt{d}\right) = \frac{1}{8} \ .$$

עבור ההצפנה הראשונה Q, מספר השאלות הנדרשות כדי למצוא כל ערך של X הוא $N_Q[k] = 2$, לכן אז התוחלת תהיה

$$E_Q\left[N_Q[X]\right] = \frac{1}{2}(2) + \frac{1}{4}(2) + \frac{1}{8}(2) + \frac{1}{8}(2) = 2 \ ,$$

כלומר תוחלת המספר השאלות הוא 2.
עבור ההצפנה השנייה Q' תוחלת מספר השאלות היא

$$E\left[N_{Q'}[X]\right] = \frac{1}{2}(1) + \frac{1}{4}(2) + \frac{1}{8}(3) + \frac{1}{8}(3) = \frac{7}{4} \ .$$

אשר פחות מהתוחלת עבור ההצפנה Q. מכאן אנחנו רואים כי יש קשר בין התוחלת של מספר השאלות הבינאריות לבין מערכת השאלות שאנחנו שואלים.

אליס שואלת סדרת שאלות ולכל שאלה נשים ערך בינארי 0 אם התשובה לא ו- 1 אם התשובה כן. כך אנחנו נשים לכל ערך של X מספר בינארי $d_1 \ldots d_k$ המורכב מספרות בינאריות $d_i = 0, 1$. טרנספורמציה כזרת בין ערכים של X לבין מספרים בינארים נקראת הצפנה. שימו לב כי אורך ההצפנה $\ell_Q[X]$ של כל ערך של X שווה למספר השאלות בינאריות הנדרשותת כדי למצוא את X ללא אי-ודאות:

$$\ell_Q[X] = N_Q[X] \ .$$

משפט 9.3

יהי $X=\{x_1,x_2,\ldots,x_k\}$ משתנה מקרי בדיד כך ש-

$$p_1\geq p_2\geq\cdots\geq p_k$$

כאשר $p_i=P\left(X=x_i\right)$. תהי $\ell_Q[X]$ הצפנה כך ש- $\ell_Q(x_i)=n_i$, כלומר x_i מוצפן על ידי מספר בינארי עם n_i ספרות ביניאריות. התוחלת המינימלית מתקבלת על ידי ההצפנה שמקיימת

$$n_1\leq n_2\leq\ldots\leq n_k\ .$$

הוכחה: נניח בשלילה שקיימת תמורה $\{p_{i_1},\ldots,p_{i_k}\}$ של $\{p_1,\ldots,p_k\}$. כך שהתוחלת

$$E=n_1p_{i_1}+\ldots+n_{j-1}p_{i_{j-1}}+n_jp_{i_j}+\ldots+n_kp_{i_k}\ .$$

היא מינימלית. ללא הגבלת הכלליות נניח כי $p_1=p_{i_j}$. אזי

$$E=n_1p_{i_1}+\ldots+n_{j-1}p_{i_{j-1}}+n_jp_1+\ldots+n_kp_{i_k}\ .$$

$p_1=\max(p_1,\ldots,p_n)$ אז בהכרח $p_{i_{j-1}}\leq 1$. לכן אם נחליף p_1 עם שכנו נקבל את התוחלת החדשה

$$E'=n_1p_{i_1}+\ldots+n_{j-1}p_1+n_jp_{i_{j-1}}+\ldots+n_kp_{i_k}\ .$$

$E'<E$ בסתירה לכך כי E התוחלת המינימלית המתקבלת עבור התמורה $(p_{i_1},\ldots,p_{i_k})$.

■

במשפט הבא אנחנו נוכיח כי אפשר לגזור ביטוי בשביל התוחלת המינימלית באמצעות הפונקצית ההסתברות של המשתנה מקרי X בלבד. נסמן

$$p_x=P_X(X=x)\ .$$

אנחנו ראינו למעלה כי אורך ההצפנה של $X=x$ בהצפנה אופטימלית Q^* הוא פונקציה של ההסתברות של p_x, כלומר

$$\ell_{Q^*}(x)=f\left(p_x\right)\ . \qquad (\#\#)$$

משפט 9.4 אנטרופיה של שאנון

נתון משתנה מקרי X בעל פונקצית ההסתברות $P_X(x)$. התוחלת המינימלית של אורך ההצפנה של X מסומן ב- $H[X]$ ונתונה על ידי הנוסחה

$$H[X]=-\sum_{x\in X}P_X(x)\log_2 P_X(x)\ .$$

$H[X]$ נקרא **האנטרופיה** של X.

הוכחה: נניח כי $X=Y\cap Z$, כאשר Y,Z משתנים מקרים בלתי תלויים.
לפי משוואה (##):

$$\ell_Q(x)=f\left(p_x\right)\ .$$

$$H[X]=\sum p_x\ell_Q(x)=\sum p_xf\left(p_x\right)\ .$$

תהיינה $P_Y(y)$ ו- $P_Z(z)$ פונקציות ההסתברות של Y ושל Z בהתאמה.
נסמן $P_Y(y)=p_y$ ו- $P_Z(z)=p_z$.

מכיוון ש- Y ו- Z משתנים בלתי תלויים אז

$$P\left(X=Y\cap Z\right)=P_Y(y)P_Z(z)=p_yp_z\ .$$

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

$$H[X]=\sum p_x\ell_Q(x)=\sum p_yp_z\left[\ell_Q(y)+\ell_Q(z)\right]$$

מכאן

$$H[X]=\sum p_yp_zf\left(p_yp_z\right)=\sum p_yp_z\left[f\left(p_y\right)+f\left(p_z\right)\right]$$

לכל p_y ו- p_z. לכן

$$f\left(p_yp_z\right)=f\left(p_y\right)+f\left(p_z\right)\ .$$

ז"א $f(p)=C\log(p)$.

כעת נניח כי יש לנו משתנה מקרי $X=\{a,b\}$ בעל פונקצית ההסתברות $P_X(b)=\frac{1}{2},\ P_X(a)=\frac{1}{2}$. ההצפנה של X צריכה ספרה אחת, לכן $\ell_{Q^*}(a)=\ell_{Q^*}(b)=1$. לכן נשים $f\left(\frac{1}{2}\right)=1$ ונקבל $f(p)=-\log_2(p)$.

■

9.3 הגדרה של מידע

הגדרה 9.2 מידע של מאורע (שאנון)

נתון משתנה מקרי X. המידע של ערך מסוים של X מסומן $I_X(x)$ ומוגדר להיות

$$I\left(X=x\right)=\log_2\left(\frac{1}{P_X(x)}\right)=-\log_2\left(P_X(x)\right)$$

כאשר $P_X(x)$ פונקצית ההסתברות של המשתנה מקרי X.

דוגמה 9.2 המידע המתקבל על קבלת תוצאה של הטלת מטבע

נטיל מטבע הוגנת ונגדיר משתנה מקרי X להיות התוצאה. X מקבל את הערכים

$$X=\{H,T\}\ .$$

מצאו את המידע של המאורע $X=H$.

פתרון:

$P(X=H)=\frac{1}{2}$. לכן

$$I(X=H)=-\log_2\left(\frac{1}{2}\right)=1\ .$$

כלומר על קבלת התוצאה "H" אנחנו מקבלים ביט אחד של מידע.

הסבר:

במקום הסימנים "H" ו- "T" בשביל המ"מ X ניתן להצפין את הערכים האפשריים בספרות בינאריות "0" או "1". כלומר

ערך של X	הצפנה בספרות בינאריות
H	0
T	1

ז"א כדי להצפין את הערכים של X אנחנו צריכים ספרה בינארית אחת:

$$d_1 \in \{0,1\} \ .$$

אשר יכול להחזיק את הערכים 0 או 1.
ספרה ביניארית אחת נדרשת להצפין את הערך של X לכן המידע של ערך כלשהו של X הוא 1 bit (ביט אחד). ■

דוגמה 9.3 שליפת קלף מחבילת קלפים תיקנית

בניסוי שליפת קלף אחד מחבילת קלפים תיקנית. נגדיר משתנה מקרי X להיות הסוג של הקלף (תלתן, עלה, לב או יהלום). חשבו את את המידע של המאורע ששלפנו קלף מסוג לב.

פתרון:
ההסתברות לשלוף קלף של הסוג לב מחבילת קלפים סטנדרטית היא

$$P(X=\heartsuit) = \frac{13}{52} = \frac{1}{4} \ .$$

לכן

$$I(X=\heartsuit) = -\log_2\left(\frac{1}{4}\right) = 2 \text{ bits}$$

הסבר:

יש 4 ערכים אפשריים של X:

$$X = \{\spadesuit, \clubsuit, \heartsuit, \diamondsuit\}$$

כל ספרה בינארית מחזיקה 2 ערכים אפשריים: 0 או 1 לכן ידרש שתי ספרות בינאריות כדי להצפין את ה-4 ערכים האפשריים של X:

$$d_1 d_2 \ , \qquad d_1, d_2 \in \{0,1\} \ .$$

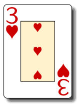
ההצפנה עצמה מתוארת בטבלא למטה:

ערך של X	הצפנה בספרות בינאריות
$\spadesuit$	00
$\clubsuit$	01
$\heartsuit$	10
$\diamondsuit$	11

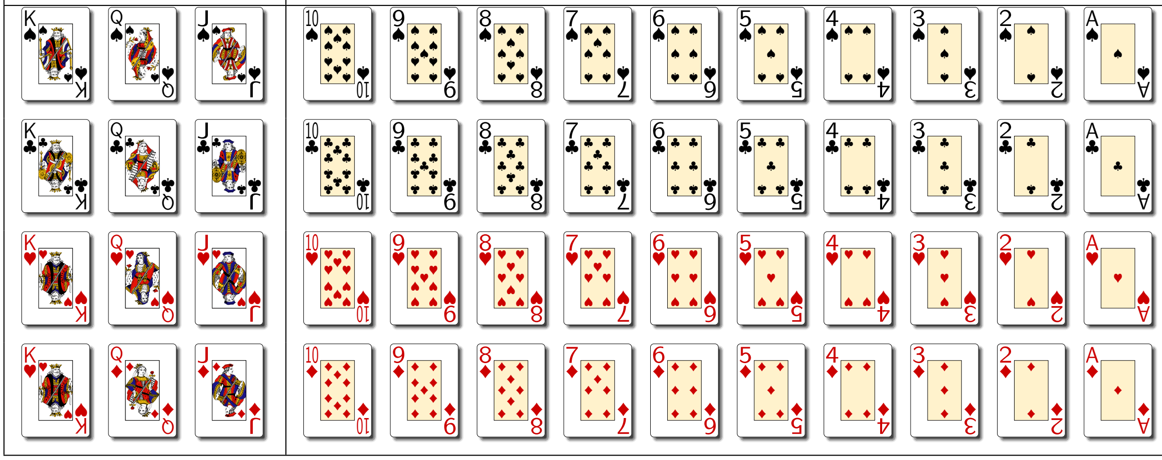
אורך המספר d_1d_2 הוא 2 לכן המידע של המשתנה מקרי X הוא 2 bits (שני ביטים).

■

דוגמה 9.4 שליפת קלף מחבילת קלפים תיקנית

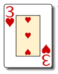
בניסוי שליפת קלף אחד מחבילת קלפים תיקנית. מצאו את המידע המתקבל אם הקלף  נשלף.

צורה	מספרים	תמונות
עלה		
תלתן		
לב		
יהלום		

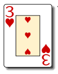


פתרון:

יהי X המ"מ שמסמן את הקלף הנשלף. ההסתברות לשלוף הקלף שלוש מסוג לב מחבילת קלפים סטנדרטית היא

$P\Big(X =$  $\Big) = \frac{1}{52}$.

לכן

$I\Big(X =$  $\Big) = -\log_2\left(\frac{1}{52}\right) = 5.7 \text{ bits}$

הסבר:

כדי להצפין 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 להצפין 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 מחזיק 6 bits של מידע.
לכל סיבית יש 2 ערכים אפשריים ולכן 64 ערכים שונים בסה"כ.

נשים לב שרק 52 מתוך ה- 64 צירופים נדרשים כדי להצפין את הערכים האפשריים של X לכן אפשר להוריד את החלק של הערכים המיותרים. הקבוצת המספרים הנשארת מכילה 5.7 bits של מידע. ■

ככל שההסתברות של מאורע יותר קטנה אז המידע המתקבל יותר גבוהה.

כלומר, ככל שהמידע של מאורע יותר גבוהה אז ההסתברות שלו יותר קטנה

דוגמה 9.5 (המשך של דוגמה 9.1)

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

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

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

■

במקרה שההסתברות של כל תוצאה שווה, כלומר

$$P(X=x_i) = \frac{1}{|X|} = \frac{1}{N}$$

אז

$$H(X) = -\sum_{i=1}^{N}\frac{1}{N}\log_2\left(\frac{1}{N}\right) = \frac{1}{N}\sum_{i=1}^{N}\log_2 N = \log_2 N\ .$$

לכן

$$N = 2^{H(X)}\ .$$

ניתן להוכיח ש- $\log_2 N$ הוא הערך המקסימלי האפשרי של $H(X)$.

משפט 9.5

נתון מ"מ בדיד X אשר מקבל N ערכים שונים

$$X=\{x_1,\ldots,x_N\}$$

בהסתברות שווה, כלומר

$$P(X=x_i)=\frac{1}{N}$$

אז האנטרופיה מקבלת ערך מקסימלי שניתנת על ידי

$$H_{\text{max}}(X)=\log_2 N\ .$$

ערך זה הוא הערך המקסימלי האפשרי של האנטרופיה.

דוגמה 9.6 אנטרופיה בהטלת מטבע

נניח כי נטיל מטבע עם הסתברות p $(0\leq p\leq 1)$ לקבל "H". יהי X משתה מקרי ששווה לתוצאת הניסוי. מצאו את האנטרופיה של המ"מ מקרי X.

פתרון:
נסמן $X=\{0,1\}$ כאשר $X=0$ מסמן תוצאת H ו- $X=1$ מסמן תוצאת T. פונקצית ההסתברות היא

$$P_X(0)=p\ ,\qquad P_X(1)=1-p\ .$$

לכן המידע של המאורע לקבל תוצאת H הוא

$$I(X=0)=-\log_2\left(P_X(0)\right)=-\log_2\left(p\right)$$

והמידע של המאורע לקבל תוצאת H הוא

$$I(X=1)=-\log_2\left(P_X(1)\right)=-\log_2\left(1-p\right)$$

נשים לב שאם המטבע הוגנת אז $p=\frac{1}{2}$ ו- $I(X=0)=I(X=1)=1$.
כעת נחשב את האנטרופיה של X:

$$H(X)=-P_X(0)\log_2 P_X(0)-P_X(1)\log_2 P_X(1)=-p\log_2 p-(1-p)\log_2(1-p)\ .$$

נרשום את האנטרופיה כפונקציה של ההסתברות p:

$$H(X)=-p\log_2 p-(1-p)\log_2(1-p)\ =:h(p).$$

ל- $h(p)$ יש נקודת מקסימום ב- $p=\frac{1}{2}$:

$$h'(p)=-\frac{1}{\ln 2}-\log_2 p+\frac{1}{\ln 2}+\log_2(1-p)=-\log_2 p+\log_2(1-p)=\log_2\left(\frac{1}{p}-1\right)\stackrel{!}{=}0\Rightarrow p=\frac{1}{2}\ .$$

ז"א הערך המקסימלי של האנטרופיה מתקבל כאשר לכל הערכים של X יש הסתברות שווה, $P_X(0)=P_X(1)=\frac{1}{2}$.
אכן

$$h(p=\tfrac{1}{2})=-\frac{1}{2}\log_2\frac{1}{2}-\frac{1}{2}\log_2\frac{1}{2}=\log_2 2=1\ .$$

■

דוגמה 9.7

בניסוי הטלת מטבע לא מאוזנת, ההסתברות לקבל תוצאה H היא $p=\frac{1}{1024}$. מצאו את האנטרופיה של X.

פתרון:
נסמן $X=\{0,1\}$, כאשר $X=0$ מסמן תוצאת H ו- $X=1$ מסמן תוצאת T.

$$I(X=0)=-\log_2\frac{1}{1024}=10 \text{ bits} , \qquad I(X=1)=-\log_2(1-p)=-\log_2\frac{1023}{1024}=0.00141 \text{ bits} .$$

לפי זה

$$H(X)=-p\log_2 p-(1-p)\log_2(1-p)=-\frac{1}{1024}\log_2\frac{1}{1024}-\frac{1023}{1024}\log_2\frac{1023}{1024}=0.0112 \text{ bits} .$$

■

המשמעות של התשובה לדוגמה הקודמת היא כך. נניח שנטיל אותה מטבע הלא מאוזנת $100,000$ פעמים. בכדי להצפין את כל התוצאות נדרש מספר ביניארי עם $100,000$ סיביות, כאשר כל ספרה נותנת התוצאה של ניסוי אחד. ז"א 10^5 bits של מידע נדרש כדי להצפין את כל התוצאות.

מצד שני מצאנו כי התוחלת של המידע המתקבל לניסוי (כמות מידע פר ניסוי) הוא 0.0112 bit פר ניסוי. במילים אחרות, ב- 10^5 ניסוים רק 1120 bit של מידע נדרש בממוצע כדי להצפין את כל התוצאות של רצף ההטלות.

9.4 הצפנת האפמן

נסביר הצפנת האפמן בעזרת הדוגמה הבאה. נתון הטקסט גלוי

$$X=\{\mathrm{a},\mathrm{b},\mathrm{c},\mathrm{d}\}$$

ונניח כי פונקצית ההסתברות של X נתונה בטבלא הבאה:

בחירת אות של $x_i\in X$	$p_i=P_X(x_i)$	$I(X=x_i)=-\log_2(p_i)$
a	$\frac{1}{3}$	1.58 bit
b	$\frac{1}{2}$	1 bit
c	$\frac{1}{12}$	3.58 bit
d	$\frac{1}{12}$	3.58 bit

נשאל את השאלה: כמה ביטים של מידע נדרשים כדי להצפין (בסיביות) רצף של 1000 אותיות של טקסט גלוי X?

יש 4 אותיות ב- X, כלומר 4 ערכים אפשריים של המ"מ בדיד X. לפיכך נדרש רצף של 2 סיביות כדי להצפין טקסט גלוי של תו אחד בהצפנת סיביות קבועה. לדוגמה:

בחירת אות של $x_i \in X$	הצפנה
a	00
b	01
c	10
d	11

ז"א להצפין תו אחד של הטקסט גלוי X נדרש 2 bit. לכן להצפין רצף אותיות של טקסטט גלוי נדרש $2 \times 1000 =$ 2000 bit, כלומר 2000 סיביות.

האנטרופיה של X היא

$$H(X) = -p_1 \log_2(p_1) - p_2 \log_2(p_2) - p_3 \log_2(p_3) - p_4 \log_2(p_4) = 1.62581 \text{ bit} .$$

ז"א לכל ניסוי המידע הממוצע הנדרש כדי להצפין תו אחד של טקסט גלוי הוא 1.62581 bit. לכן המידע הממוצע הנדרש כדי להצפין רצף אותיות של טקסט גלוי הוא

$$1000 \times 1.62581 = 1625.81 \text{ bit} .$$

לכן, רצף סיביות של אורך 1626 בממוצע יהיה מספיק כדי להעביר את ההודעה.

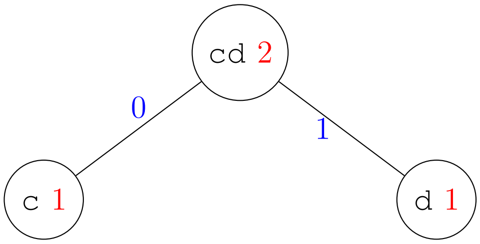
כעת נבנה הצפנה של הטקסט גלוי על ידי האלגוריתם של האפמן.

שלב 1)

	c	d	a	b
	1	1	4	6

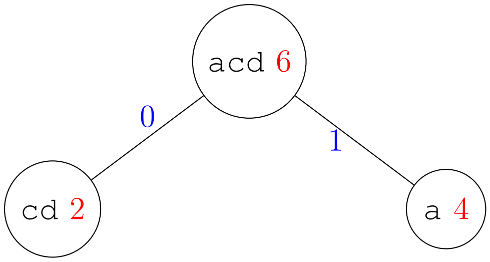
שלב 2)

	c	d	a	b
	1	1	4	6
	0	1		
	2		4	6



שלב 3)

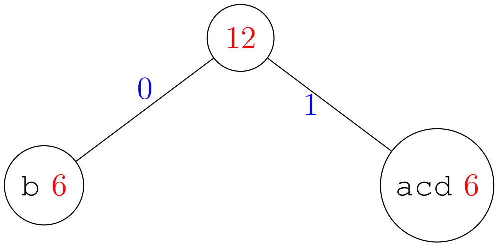
	cd	a	b
	2	4	6
	0	1	
	6		6



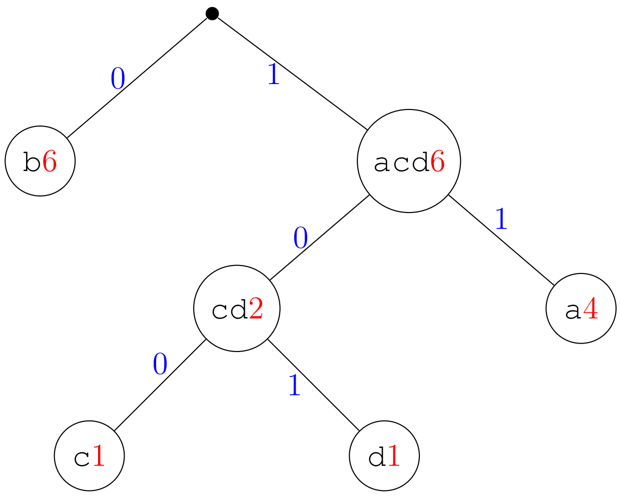
שלב 4)

שלב 5)

	acd	b
	6	6
	0	1
	12	



שלב 6)



בסוף של התהליך האותיות של הטקסט גלוי יהיו בעלים של העץ וההצפנה ניתנת על ידי הרצף סיביות על הענפים במסלול מהנקודה התחלתית של העץ עד העלה בו רשום האות בשאלה.

בחירת אות של $x_i \in X$	הצפנת האפמן
a	11
b	100
c	110
d	101

דוגמה 9.8

נתון הטקסט גלוי הבא

$$X = \{\mathrm{a}, \mathrm{b}, \mathrm{c}, \mathrm{d}, \mathrm{e}\}$$

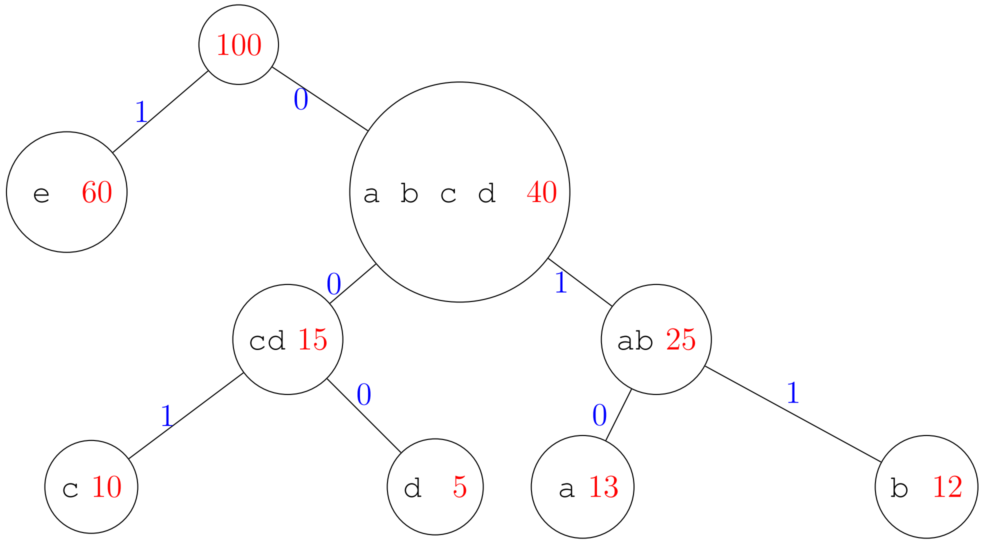
והפונקצית הסתברות

$$P(X=\mathrm{a}) = \frac{13}{100} = 0.13 \ , \quad P(X=\mathrm{b}) = \frac{3}{25} = \frac{12}{100} = 0.12 \ , \quad P(X=\mathrm{c}) = \frac{1}{10} = \frac{10}{100} = 0.1 \ ,$$

$$P(X=\mathrm{d}) = \frac{1}{20} = \frac{5}{100} = 0.05 \ , \quad P(X=\mathrm{e}) = \frac{3}{5} = \frac{60}{100} = 0.6 \ .$$

מצאו את העץ הצפנה וההצפנת האפמן של כל תו של X.

פתרון:



בחירת אות של $x_i \in X$	הצפנת האפמן
a	010
b	011
c	001
d	000
e	1

■

פורמלי הצפנת האפמן מוגדרת לפי ההגדרה הבאה:

הגדרה 9.3 הצפנת האפמן

נתון משתנה מקרי X. נגדיר הצפנת האפמן של X להיות הפונקציה (כלל מצפין)

$$f : X \to \{0,1\}^*$$

כאשר $\{0,1\}^*$ קבוצת רצפים של סיביות סופיים.

נתון רצף מאורעות $x_1,\ldots,x_n$. נגדיר

$$f(x_1\ldots x_n)=f(x_1)||\ldots||f(x_n)$$

כאשר "||" מסמן שרשור (concatenation).

הגדרה 9.4 תוחלת האורך של הצפנת האפמן

נתונה הצפנת האפמן f. תוחלת האורך של ההצפנה מוגדרת

$$l(f)=\sum_{x\in X}P(X=x)\,|f(x)|\ .$$

משפט 9.6 אי שוויון האפמן

נתון קבוצת אותיות של טקסט גלוי X והצפנת האפמן f. נניח כי $l(f)$ תוחלת האורך של ההצפנה ו-$H(X)$ האנטרופיה של הטקסט גלוי. מתקיים

$$H(X)\leq l(f)\leq H(X)+1\ .$$

דוגמה 9.9 (המשך של דוגמה 9.8)

נתון הטקסט גלוי הבא

$$X=\{\mathrm{a},\mathrm{b},\mathrm{c},\mathrm{d},\mathrm{e}\}$$

והפונקצית הסתברות

$$P(X=\mathrm{a})=\frac{13}{100}=0.13\ ,\quad P(X=\mathrm{b})=\frac{3}{25}=0.12\ ,\quad P(X=\mathrm{c})=\frac{1}{10}=0.1\ ,\quad P(X=\mathrm{d})=\frac{1}{20}=0.05\ ,$$

$$P(X=\mathrm{e})=\frac{3}{5}=0.6\ .$$

1) מצאו את תוחלת האורך של ההצפנת האפמן.

2) מצאו את האנטרופיה.

3) הוכיחו כי אי-שוויון האפמן של ההצפנה שמצאתם בדוגמה 9.8 למעלה מתקיים.

פתרון:

סעיף 1)

$$\begin{aligned}l(f)=&\frac{5}{100}\cdot 3+\frac{10}{100}\cdot 3+\frac{12}{100}\cdot 3+\frac{13}{100}\cdot 3+\frac{60}{100}\cdot 1\\=&\frac{15+30+36+30+60}{100}\\=&\frac{180}{100}\\=&1.8\end{aligned}$$

סעיף 2)

$$\begin{aligned} H(X) =& - P(X=\mathtt{a})\log_2 P(X=\mathtt{a}) - P(X=\mathtt{b})\log_2 P(X=\mathtt{b}) - P(X=\mathtt{c})\log_2 P(X=\mathtt{c}) \\ & - P(X=\mathtt{d})\log_2 P(X=\mathtt{d}) - P(X=\mathtt{e})\log_2 P(X=\mathtt{e}) \\ =& 1.74018 \ . \end{aligned}$$

סעיף 3) $H(X)=1.74018$, $H(X)+1=1.84018$, $l(f)=1.8$. לכן

$$H(X) \leq l(f) \leq H(X)+1$$

מתקיים.

■

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 $a_i>0$, $i=1,\ldots,n$ כך ש- $\sum\limits_{i=1}^n a_i=1$. אז

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

לכל $x\in I$. $\sum\limits_{i=1}^n a_i f(x_i) = f\left(\sum\limits_{i=1}^n a_i x_i\right)$ אם ורק אם $x_1=\cdots=x_n$.

משפט 9.8

יהי

$$X=\{x_1,\cdots,x_n\}$$

משתנה מקרי בדיד בעל פונקצית הסתברות

$$P_X(x_1) = p_1 \ , \ldots \ , P_X(x_n) = p_n \ ,$$

$1 \leq p_i < 0$ לכל $1 \leq i \leq n$. אז

$$H(X) \leq \log_2 n$$

אם ורק אם

$$p_i = \frac{1}{n}$$

לכל $1 \leq i \leq n$.

הוכחה: לפי אי-שוויון ינסן:

$$\begin{aligned} H(X) &= -\sum_{i=1}^{n} p_i \log_2 p_i \\ &= \sum_{i=1}^{n} p_i \log_2 \left(\frac{1}{p_i}\right) \\ &\leq \log_2 \left(\sum_{i=1}^{n} p_i \cdot \frac{1}{p_i}\right) \\ &= \log_2 \left(\sum_{i=1}^{n} 1\right) \\ &= \log_2 n \ . \end{aligned}$$

בנוסף $H(X) = \log_2 n$ אם ורק אם $p_i = \frac{1}{n}$ לכל $1 \leq i \leq n$. ■

משפט 9.9

יהי $X = \{x_1, \cdots, x_m\}$ משתנה מקרי בדיד בעל פונקצית הסתברות

$$P_X(x_1) = p_1 \ , \ldots \ , P_X(x_m) = p_m \ ,$$

$1 \leq p_i < 0$ לכל $1 \leq i \leq m$, ויהי $Y = \{y_1, \cdots, y_n\}$ משתנה מקרי בדיד בעל פונקצית הסתברות

$$P_Y(y_1) = q_1 \ , \ldots \ , P_Y(y_n) = q_n \ ,$$

$1 \leq q_i < 0$ לכל $1 \leq i \leq n$. אז

$$H(X,Y) \leq H(X) + H(Y)$$

ו- $H(X,Y) = H(X) + H(Y)$ אם ורק אם X ו- Y בלתי תלויים.

הוכחה: (*להעשרה בלבד)

פונקצית הסתברות של X היא $P_X(x_i) = p_i$ ופונקצית הסתברות של X היא $P_Y(y_i) = q_i$. נגדיר הפונקצית הסתברות של המשתנה מקרי דו-ממדי:

$$r_{ij} = P(X = x_i, Y = y_j) \ .$$

אז הפונקצית הסתברות שולית של X היא

$$p_i=\sum_{j=1}^{n} r_{ij}\ , \qquad \forall 1\leq i\leq m$$

והפונקצית הסתברות שולית של Y היא

$$q_j=\sum_{i=1}^{m} r_{ij}\ , \qquad \forall 1\leq j\leq m\ .$$

מכאן

$$\begin{aligned}
H(X)+H(Y) &= -\sum_{i=1}^{m} p_i\log_2 p_i-\sum_{j=1}^{n} q_j\log_2 q_j\\
&= -\sum_{i=1}^{m}\left(\sum_{j=1}^{n} r_{ij}\right)\log_2 p_i-\sum_{j=1}^{n}\left(\sum_{i=1}^{m} r_{ij}\right)\log_2 q_j\\
&= -\sum_{i=1}^{m}\sum_{j=1}^{n} r_{ij}\log_2 p_i-\sum_{j=1}^{n}\sum_{i=1}^{m} r_{ij}\log_2 q_j\\
&= -\sum_{i=1}^{m}\sum_{j=1}^{n} r_{ij}\left(\log_2 p_i+\log_2 q_j\right)\\
&= -\sum_{i=1}^{m}\sum_{j=1}^{n} r_{ij}\log_2\left(p_iq_j\right)\ .
\end{aligned}$$

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

$$\begin{aligned}
H(X,Y)-H(X)-H(Y) &= \sum_{i=1}^{m}\sum_{j=1}^{n} r_{ij}\log_2\frac{1}{r_{ij}}+\sum_{i=1}^{m}\sum_{j=1}^{n} r_{ij}\log_2\left(p_iq_j\right)\\
&= \sum_{i=1}^{m}\sum_{j=1}^{n} r_{ij}\log_2\left(\frac{p_iq_j}{r_{ij}}\right)\\
&\leq \log_2\left(\sum_{i=1}^{m}\sum_{j=1}^{n} p_iq_j\right) && \text{(אי-שוויון ינסן)}\\
&= \log_2 1\\
&= 0\ .
\end{aligned}$$

לכן

$$H(X,Y)-H(X)-H(Y)\leq 0 \qquad \Rightarrow \qquad H(X,Y)\leq H(X)+H(Y)\ .$$

■

הגדרה 9.6 אנטרופיה מותנית

יהיו X,Y משתנים מקריים בדידים. נגדיר

$$H(X|Y=y) = -\sum_{x\in X} P(X=x|Y=y)\log_2 P(X=x|Y=y) \ .$$

האנטרופיה מותנית תסומן $H(X|y)$ ותוגדר הממוצע המשוקללת של $H(X|Y=y)$ ביחס להתברויות $P(Y=y)$, כלומר התוחלת של $H(X|Y=y)$:

$$H(X|Y) = -\sum_{y\in Y}\sum_{x\in X} P(Y=y)P(X=x|Y=y)\log_2 P(X=x|Y=y) \ .$$

האנטרופיה המותנית $H(X|Y)$ מכמתת המידע הממוצע של המ"מ X המועברת אשר לא מוגלה באמצעות Y.

משפט 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

$$H(Y) = -\sum_{j=1}^{n} q_j\log_2 q_j = -\sum_{i=1}^{m}\sum_{j=1}^{n} r_{ij}\log_2 q_j$$

ו-

$$H(X,Y) = -\sum_{i=1}^{m}\sum_{j=1}^{n} r_{ij}\log_2 r_{ij} \ .$$

לכן

$$\begin{aligned}
H(Y)+H(X|Y) &= -\sum_{i=1}^{m}\sum_{j=1}^{n} r_{ij}\log_2\frac{r_{ij}}{q_j} - \sum_{i=1}^{m}\sum_{j=1}^{n} r_{ij}\log_2 q_j\\
&= -\sum_{i=1}^{m}\sum_{j=1}^{n} r_{ij}\left(\log_2\frac{r_{ij}}{q_j}+\log_2 q_j\right)\\
&= -\sum_{i=1}^{m}\sum_{j=1}^{n} r_{ij}\log_2\left(\frac{r_{ij}}{q_j}\cdot q_j\right)\\
&= -\sum_{i=1}^{m}\sum_{j=1}^{n} r_{ij}\log_2 r_{ij}\\
&=H(X,Y)\ .
\end{aligned}$$

■

משפט 9.11

$$H(X|Y)\leq H(X)$$

ו- $H(X|Y)=H(X)$ אם ורק אם X ו- Y משתנים מקיים בלתי-תלויים.

הוכחה: (*להעשרה בלבד)
לפי משפט 9.9, $H(X,Y)\leq H(X)+H(Y)$. נציב משפט 9.10 ונקבל

$$H(Y)+H(X|Y)\leq H(X)+H(Y) \qquad \Rightarrow \qquad H(X|Y)\leq H(X)\ .$$

בנוסף לפי משפט 9.9, $H(X,Y)=H(X)+H(Y)$ אם ורק אם X,Y משתנים בלתי תלויים, לכן

$$H(X|Y)=H(X)$$

אם ורק אם X,Y משתנים בלתי תלויים.

■

9.6 משפט האנטרופיה לקריפטו-מערכת

משפט 9.12 משפט האנטרופיה לקריפטו-מערכת

תהי (P,C,K,E,D) קריפטו-מערכת. אז

$$H(K|C)=H(K)+H(P)-H(C)\ .$$

הוכחה: (*להעשרה בלבד)
לפי משפט 9.10,

$$H(K,P,C)=H(K,P)+H(C|K,P)\ .$$

בגלל שהכלל מצפין $y=e_k(x)$ הוא פונקציה חד-חד-ערכית, אז המפתח והטקסט גלוי קובעים את הטקסט מוצפן בדרך יחידה. ז"א

$$H(C|K,P)=0\ .$$

לכן

$$H(K,P,C)=H(K,P)\ . \tag{*1}$$

המשתנים מקריים K ו- P בלתי-תלויים. לכן לפי משפט 9.9, $H(K,P)=H(K)+H(P)$ ולפיכך נקבל

$$H(K,P,C)=H(K)+H(P)\ . \tag{*2}$$

באותה מידה, לפי משפט 9.10,

$$H(K,P,C)=H(K,C)+H(P|K,C)\ . \tag{*3}$$

מכיוון שהכלל מפענח $x=d_k(y)$ פונקציה חד-חד ערכית, אז המפתח והטקסט מוצפן קובעים את הטקסט גלוי בדרך יחידה. לכן

$$H(P|K,C)=0\ .$$

ומכאן

$$H(K,P,C)=H(K,C)\ . \tag{*4}$$

לפי משפט 9.10, $H(K,C)=H(C)+H(K|C)$. לכן

$$\begin{aligned} H(K|C) =& H(K,C)-H(C) \\ =& H(K,P,C)-H(C) && \text{(לפי *4)} \\ =& H(K)+H(P)-H(C) && \text{(לפי *2)} \end{aligned} \tag{9.5}$$

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 המתקבל תואם עם $H(K|C)=H(K)+H(P)-H(C)$.

פתרון:

בדוגמה 9.5 מצאנו כי $H(P)=0.81$, $H(K)=1.5$ ו- $H(C)=1.85$. ז"א $H(K|C)=H(K)+H(P)-H(C)=0.46$.

כעת נחשב את $H(K|C)$ בעזרת התוצאות של דוגמה 9.1:

$$P\left(K=k_1|C=1\right)=\frac{P\left(C=1|K=k_1\right)P(K=k_1)}{P(C=1)}=\frac{\left(\frac{1}{4}\right)\left(\frac{1}{2}\right)}{\left(\frac{1}{8}\right)}=1\ ,$$

$$P\left(K=k_2|C=1\right)=\frac{P\left(C=1|K=k_2\right)P(K=k_2)}{P(C=1)}=\frac{0\left(\frac{1}{4}\right)}{\left(\frac{1}{8}\right)}=0\ ,$$

$$P\left(K=k_3|C=1\right)=\frac{P\left(C=1|K=k_3\right)P(K=k_3)}{P(C=1)}=\frac{0\left(\frac{1}{4}\right)}{\left(\frac{1}{8}\right)}=0\ ,$$

$$P\left(K=k_1|C=2\right)=\frac{P\left(C=2|K=k_1\right)P(K=k_1)}{P(C=2)}=\frac{\left(\frac{3}{4}\right)\left(\frac{1}{2}\right)}{\left(\frac{7}{16}\right)}=\frac{6}{7}\ ,$$

$$P\left(K=k_2|C=2\right)=\frac{P\left(C=2|K=k_2\right)P(K=k_2)}{P(C=2)}=\frac{\left(\frac{1}{4}\right)\left(\frac{1}{4}\right)}{\left(\frac{7}{16}\right)}=\frac{1}{7}\ ,$$

$$P\left(K=k_3|C=2\right)=\frac{P\left(C=2|K=k_3\right)P(K=k_3)}{P(C=2)}=\frac{0\left(\frac{1}{4}\right)}{\left(\frac{7}{16}\right)}=0\ ,$$

$$P\left(K=k_1|C=3\right)=\frac{P\left(C=3|K=k_1\right)P(K=k_1)}{P(C=3)}=\frac{(0)\left(\frac{1}{2}\right)}{\left(\frac{1}{4}\right)}=0\ ,$$

$$P\left(K=k_2|C=3\right)=\frac{P\left(C=3|K=k_2\right)P(K=k_2)}{P(C=3)}=\frac{\left(\frac{3}{4}\right)\left(\frac{1}{4}\right)}{\left(\frac{1}{4}\right)}=\frac{3}{4}\ ,$$

$$P\left(K=k_3|C=3\right)=\frac{P\left(C=3|K=k_3\right)P(K=k_3)}{P(C=3)}=\frac{\left(\frac{1}{4}\right)\left(\frac{1}{4}\right)}{\left(\frac{1}{4}\right)}=\frac{1}{4}\ ,$$

$$P\left(K=k_1|C=4\right)=\frac{P\left(C=4|K=k_1\right)P(K=k_1)}{P(C=4)}=\frac{(0)\left(\frac{1}{2}\right)}{\left(\frac{3}{16}\right)}=0\ ,$$

$$P\left(K=k_2|C=4\right)=\frac{P\left(C=4|K=k_2\right)P(K=k_2)}{P(C=4)}=\frac{0\left(\frac{1}{4}\right)}{\left(\frac{3}{16}\right)}=0\ ,$$

$$P\left(K=k_3|C=4\right)=\frac{P\left(C=4|K=k_3\right)P(K=k_3)}{P(C=4)}=\frac{\left(\frac{3}{4}\right)\left(\frac{1}{4}\right)}{\left(\frac{3}{16}\right)}=1\ .$$

מכאן

$$\begin{aligned}
H(K|C) =& -\sum_{y=1}^{4}\sum_{k\in\{k_1,k_2,k_3,k_4\}} P(C=y)P(K=k|C=y)\log_2 P(K=k|C=y)\\
=& -P_C(1)P_{K|C}(k_1|1)\log_2 P_{K|C}(k_1|1) - P_C(2)P_{K|C}(k_1|2)\log_2 P_{K|C}(k_1|2)\\
&-P_C(3)P_{K|C}(k_1|3)\log_2 P_{K|C}(k_1|3) - P_C(4)P_{K|C}(k_1|4)\log_2 P_{K|C}(k_1|4)\\
&-P_C(1)P_{K|C}(k_2|1)\log_2 P_{K|C}(k_2|1) - P_C(2)P_{K|C}(k_2|2)\log_2 P_{K|C}(k_2|2)\\
&-P_C(3)P_{K|C}(k_2|3)\log_2 P_{K|C}(k_2|3) - P_C(4)P_{K|C}(k_2|4)\log_2 P_{K|C}(k_2|4)\\
&-P_C(1)P_{K|C}(k_3|1)\log_2 P_{K|C}(k_3|1) - P_C(2)P_{K|C}(k_3|2)\log_2 P_{K|C}(k_3|2)\\
&-P_C(3)P_{K|C}(k_3|3)\log_2 P_{K|C}(k_3|3) - P_C(4)P_{K|C}(k_3|4)\log_2 P_{K|C}(k_3|4)\\
=& -\frac{1}{8}\log_2 1 - \frac{7}{16}\cdot\frac{6}{7}\log_2\frac{6}{7} - \frac{1}{4}\cdot 0\log_2 0 - \frac{3}{16}\cdot 0\log_2 0\\
&-\frac{1}{8}0\cdot\log_2 0 - \frac{7}{16}\cdot\frac{1}{7}\log_2\frac{1}{7} - \frac{1}{4}\cdot\frac{3}{4}\log_2\frac{3}{4} - \frac{3}{16}\cdot 0\log_2 0\\
&-\frac{1}{8}\cdot 0\log_2 0 - \frac{7}{16}\cdot 0\log_2 0 - \frac{1}{4}\cdot\frac{1}{4}\log_2\frac{1}{4} - \frac{3}{16}\cdot 1\cdot\log_2 1\\
=& 0.461676\ .
\end{aligned}$$

הרי

$$H(K|C) = 0.46 = H(K) + H(P) - H(C)$$

כנדרש. ■

שיעור 10
צפנים בלוקים ו- DES

10.1 רשת החלפה-תמורה

הגדרה 10.1 רשת החלפה-תמורה

נתון טקסט גלוי $x=\{0,1\}^n$ כרצף סיביות. מחלקים x ל- m קבוצות של אורך ℓ:

$$x = x_{<1>}||x_{<2>}||\cdots||x_{<m>}$$

כאשר

$$x_{<1>} = x_1x_2\cdots x_{\ell}, \qquad x_{<2>} = x_{\ell+1}x_{\ell+2}\cdots x_{2\ell}, \qquad x_{<m>} = x_{(m-1)\ell+1}\ x_{(m-1)\ell+2}\ \cdots\ x_{m\ell}\ .$$

ברשת החלפה-תמורה יש 4 מרכיבים:

- החלפה של אורך m, שנסמן $\pi_S:\{0,1\}^{\ell}\to\{0,1\}^{\ell}$
- תמורה של אורך $n=\ell m$ שנסמן $\pi_P:\{1,\ldots,\ell m\}\to\{1,\ldots,\ell m\}$
- מפתח התחלתי k.
- תזמון המפתחות $\left(k^1,\ldots,k^{N+1}\right)$, אחד לכל שלב של ההצפנה.

האלגוריתם של ההצפנה הוא כמפורט להלן:

1) מגדירים $w^0=x$.

2) מחשבים $u^1=w^0\oplus k^1$ כאשר $\oplus$ האופרטור XOR .

3) מבצעים את ההחלפה π_S על כל תת-קבוצה $u^1_{<i>}$ לכל $1\leq i\leq m$: $\mathrm{v}^1_{<i>}=\pi_S\left(u^1_{<i>}\right)$.

4) מבצעים את התמורה π_P על תת-קבוצה v^1: $w^1_i=\mathrm{v}^1_{\pi_P(i)}$.

כעת חוזרים על שלבים 2)-4):

2') מחשבים $u^2=w^1\oplus k^2$ כאשר $\oplus$ האופרטור XOR .

3') מבצעים את ההחלפה π_S על כל תת-קבוצה $u^2_{<i>}$ לכל $1\leq i\leq m$: $\mathrm{v}^2_{<i>}=\pi_S\left(u^2_{<i>}\right)$.

4') מבצעים את התמורה π_P על תת-קבוצה v^2. $w^2_i=\mathrm{v}^2_{\pi_P(i)}$.

התהליך ממשיך עד שמגיעים לסוף שלב ה- N -ית. בשלב N לא משחבים את w^N אלא מקבלים את הטקסט מוצפן לפי

$$y=\mathrm{v}^N\oplus k^{N+1}\ .$$

דוגמה 10.1

נתון הטקסט גלוי

$$x = \texttt{00100110}\ .$$

נתונה ההחלפה $\pi_S : \{0,1\}^4 \to \{0,1\}^4$ שמוגדרת

z	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
π_S(z)	D	4	3	1	2	F	B	8	3	A	6	C	5	9	0	7

נתונה התמורה $\pi_P\{1,\ldots,8\} \to \{1,\ldots,8\}$ שמוגדרת

z	1	2	3	4	5	6	7	8
π_P(z)	8	5	4	2	3	6	1	7

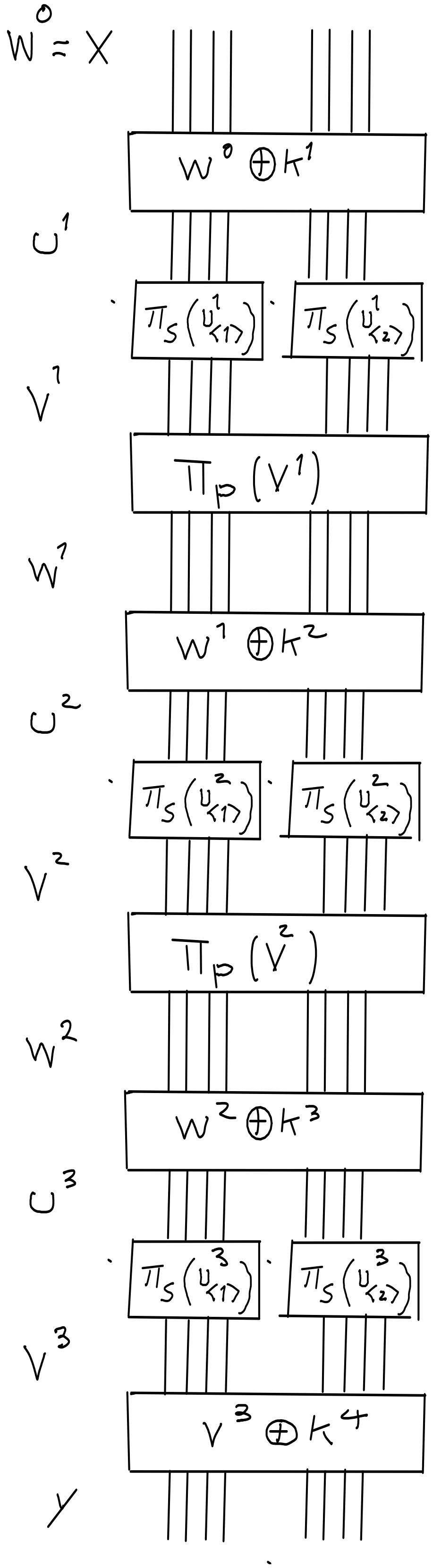
או בסימון מחזורי

$$\begin{pmatrix}1 & 8 & 7\end{pmatrix}\begin{pmatrix}2 & 5 & 3 & 4\end{pmatrix}\begin{pmatrix}6\end{pmatrix}$$

ונתון מפתח התחלתי

$$k = \texttt{0011 1010 1001 0100 1111}\ .$$

מספר השלבים בהצפנה הוא $N+1$ כאשר $N=2$. נגדיר תזמון המפתחות (k^1,k^2,k^3) כאשר המפתח k^i רצף סיביות של אורך 8 אשר מתחיל עם הסיבית ה- $(4i-3)$ ית של k. מצטו את הטקסט מוצפן.



פתרון:

המפתחות של כל שלב של ההצפנה הם

$$\begin{aligned} k^1 =& \texttt{0011 1010} , \\ k^2 =& \texttt{1010 1001} , \\ k^3 =& \texttt{1001 0100} , \\ k^4 =& \texttt{0100 1111} . \end{aligned}$$

שלב (1)

$$\begin{aligned} w^0 =& \texttt{0010 0110} \\ k^1 =& \texttt{0011 1010} \\ u^1 = w^0 \oplus k^1 =& \texttt{0001 1100} \end{aligned}$$

$$u^1 = u_{<1>} || u_{<2>} = \texttt{0001}||\texttt{1100}$$

בבסיס הקסדצימלי:

$$u^1 = u_{<1>} || u_{<2>} = \texttt{1}||\texttt{C}$$

$$\text{v}^1 = \pi_S(u_{<1>})||\pi_S(u_{<2>}) = \pi_S(\texttt{1})||\pi_S(\texttt{C}) = \texttt{4}||\texttt{5}$$

בבסיס בינארי:

$$\text{v}^1 = \texttt{0100}||\texttt{0101}$$

$$w^1 = \pi_P(\texttt{0100 0101}) = \texttt{1001 0100}$$

שלב (2)

$$\begin{aligned} w^1 =& \texttt{1001 0100} \\ k^2 =& \texttt{1010 1001} \\ u^2 = w^1 \oplus k^2 =& \texttt{0011 1101} \end{aligned}$$

$$u^2 = u^2_{<1>} || u^2_{<2>} = \texttt{0011}||\texttt{1101}$$

בבסיס הקסדצימלי:

$$u^2 = u^2_{<1>} || u^2_{<2>} = \texttt{3}||\texttt{D}$$

$$\text{v}^2 = \pi_S\left(u^2_{<2>}\right)||\pi_S\left(u^2_{<2>}\right) = \pi_S(\texttt{3})||\pi_S(\texttt{D}) = \texttt{1}||\texttt{9}$$

בבסיס בינארי:

$$\text{v}^2 = \texttt{0001}||\texttt{1001}$$

$$w^2 = \pi_P(\texttt{0001 1001}) = \texttt{1110 0000}$$

שלב (3)

$$\begin{aligned} w^2 &= 1110 \ \ 0000 \\ k^3 &= 1001 \ \ 0100 \\ u^3 = w^2 \oplus k^3 &= 0111 \ \ 0100 \end{aligned}$$

$$u^3 = u^3_{<1>} || u^3_{<2>} = 0111||0100$$

בבסיס הקסדצימלי:

$$u^3 = u^3_{<1>} || u^3_{<2>} = 7||4$$

$$\text{v}^3 = \pi_S\left(u^3_{<2>}\right) || \pi_S\left(u^3_{<2>}\right) = \pi_S(7) || \pi_S(4) = 8||2$$

בבסיס בינארי:

$$\text{v}^3 = 1000||0010$$

$$\begin{aligned} \text{v}^3 &= 1000 \ \ 0010 \\ k^4 &= 0100 \ \ 1111 \\ y = \text{v}^3 \oplus k^4 &= 1100 \ \ 1101 \end{aligned}$$

■

10.2 רשת פייסטל

הגדרה 10.2 רשת פייסטל (Feistel)

נתון טקסט גלוי $x = \{0,1\}^{2n}$ כרצף סיביות.

מחלקים את x לשני חצאים שנסמן L_0 ו- R_0:
$$x = \underbrace{x_1 \ldots x_n}_{L_0} \ \underbrace{x_n \ldots x_{2n}}_{R_0}.$$

ברשת פייסטל יש 4 מרכיבים:

- מספר שלם N אשר קובע את המספר השלבים בתהליך הצפנה.
- מפתח התחלתי k.
- מערכת של N תת-מפתחות $(k_1, \ldots, k_N)$, אחד לכל שלב של התהליך הצפנה.
- פונקציית ליבה $f : \{0,1\}^n \to \{0,1\}^n$.

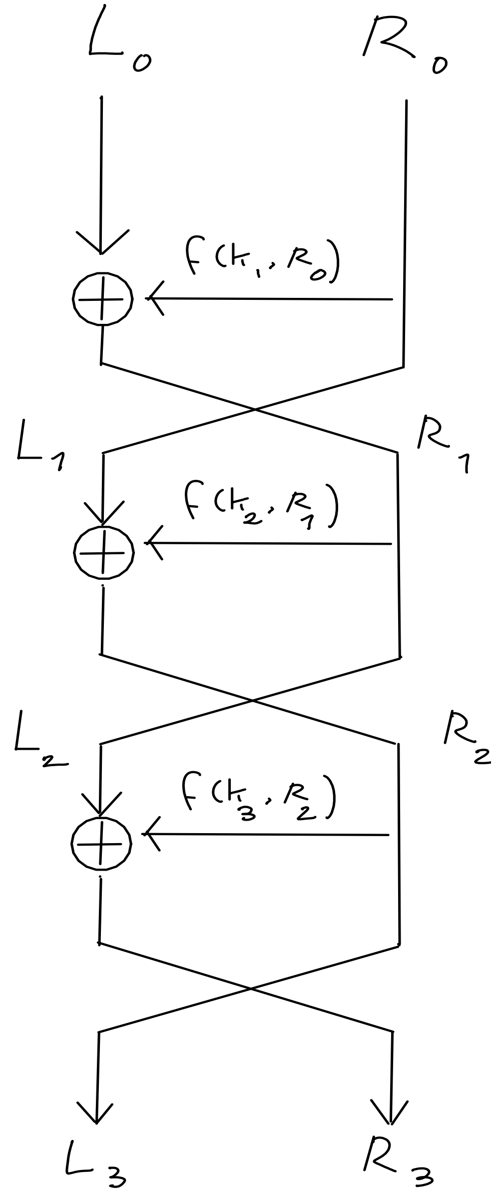
1) מגדירים $L_0 = x_1 \cdots x_n$, $R_0 = x_n \cdots x_{2n}$.

2) בשלב ה- i ית $(1 \leq i \leq N)$:
$$R_i = L_{i-1} \oplus f(R_{i-1}, k_i) \ , \qquad L_i = R_{i-1}.$$

3) בשלב ה- N נקבל את הטקסט מוצפן לפי
$$y = R_N L_N.$$

לדוגמה, עבור תהליך הצפנה עם $N=3$ שלבים:

$$L_1 = R_0\ , \qquad L_2 = R_1\ , \qquad L_3 = R_2\ ,$$
$$R_1 = L_0 \oplus f(R_0,k_1)\ , \quad R_2 = L_1 \oplus f(R_1,k_2)\ , \quad R_3 = L_2 \oplus f(R_2,k_3)\ .$$



דוגמה 10.2

נתון צופן פייסטל שמוגדר עם הפונקציית ליבה $f(x_1x_2x_3x_4x_5,\pi) = x_{\pi(1)}x_{\pi(2)}x_{\pi(3)}x_{\pi(4)}x_{\pi(5)}$ המפתח ההתחלתי הוא התמורה $(135)(24)$. כל תת-מפתח k_i הוא התמורה המתקבלת על ידי לבצע i פעמים את התמורה π. מצאו את טקסט מוצפן של הטקסט גלוי 0010111001.

פתרון:

$L_0 = 00101$ ו- $R_0 = 11001$. התת מפתחות הם

$$k_1 = (135)(24)\ , \qquad k_2 = (153)(2)(4)\ , \qquad k_3 = (1)(3)(5)(24)\ .$$

מכאן

$$L_1 = R_0 = \texttt{11001} \ .$$
$$R_1 = L_0 \oplus f(R_0, k_1) = \texttt{00101} \oplus \texttt{00111} = \texttt{00010} \ .$$

$$L_2 = R_1 = \texttt{00010} \ .$$
$$R_2 = L_1 \oplus f(R_1, k_2) = \texttt{11001} \oplus \texttt{00010} = \texttt{11011} \ .$$

$$L_3 = R_2 = \texttt{11011} \ .$$
$$R_3 = L_2 \oplus f(R_2, k_3) = \texttt{00010} \oplus \texttt{11011} = \texttt{11001} \ .$$
$$y = R_3 L_3 = \texttt{1100111011}$$

■

משפט 10.1 משוואות פייסטל

<u>משוואות פייסטל להצפנה:</u>

נתון טקסט גלוי $x = L_0 R_0$. לכל $1 \leq i \leq N$:

$$L_i = R_{i-1} \ , \qquad R_i = L_{i-1} \oplus f(R_{i-1}, k_i) \ , \qquad y = R_N L_N$$

<u>משוואות פייסטל לפענוח:</u>

נתון טקסט גלוי $y = R_N L_N$. לכל $1 \leq i \leq N$:

$$R_i = L_{i+1} \ , \qquad L_i = R_{i+1} \oplus f(R_i, k_{i+1}) \ , \qquad x = L_0 R_0$$

דוגמה 10.3 פענוח של צופן פייסטל

טקסט גלוי של 10 bit היה מוצפן באמצעות צופן פייסטל עם מפתח התחלתי $k = (124)(35)$. כל תת מפתח k_i מתקבל על ידי לבצע התמורה ההתחלתית i פעמים. הטקסט מוצפן הוא $\texttt{1100001010}$. מצאו את הטקסט גלוי.

פתרון:

התת מפתחות הם:

$$k_1 = (124)(35) \ , \qquad k_2 = (142)(3)(5) \ , \qquad k_3 = (1)(2)(4)(35) \ .$$

הטקסט מוצפן התקבל על ידי להפוך את השני חצאים, $L_3 = 01010$, $R_3 = 11000$. לכן, השלב 1 הוא:

$$R_2 = L_3 = 01010$$

ו-

$$L_2 = R_3 \oplus f(R_2, k_3) = 11000 \oplus 01010 = 10010 \ .$$

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 גלוי הוא

$$X = L_0 R_0 = 1100010010 \ .$$

■

10.3 תקן הצפנת מידע (DES)

התקן הצפנת מידע, באנגלית Data Encryption Standard ובראשי תיבות (DES), הוא צופן בלוקים סימטרי שפותח ב- 1974 במרכז המחקר של IBM בשיתוף פעולה עם הסוכנות לביטחון לאומי של ממשלת ארצות הברית.

שלב (1) נתון טקסט גלוי $x = x_1 \ldots x_{64}$ כרצף סיביות של 64 ביטים. בונים רצף סיביות x_0 באמצעות תמורה של הביטים של x לפי תמורה סטטית 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,

$$\begin{aligned} IP\Big(& x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9, x_{10}, x_{11}, x_{12}, x_{13}, x_{14}, x_{15}, x_{16}, \\ & x_{17}, x_{18}, x_{19}, x_{20}, x_{21}, x_{22}, x_{23}, x_{24}, x_{25}, x_{26}, x_{27}, x_{28}, x_{29}, x_{30}, x_{31}, x_{32}, \\ & x_{33}, x_{34}, x_{35}, x_{36}, x_{37}, x_{38}, x_{39}, x_{40}, x_{41}, x_{42}, x_{43}, x_{44}, x_{45}, x_{46}, x_{47}, x_{48}, \\ & x_{49}, x_{50}, x_{51}, x_{52}, x_{53}, x_{54}, x_{55}, x_{56}, x_{57}, x_{58}, x_{59}, x_{60}, x_{61}, x_{62}, x_{63}, x_{64} \Big) \end{aligned}$$

$$\begin{aligned} = & x_{58}, x_{50}, x_{42}, x_{34}, x_{26}, x_{18}, x_{10}, x_2, x_{60}, x_{52}, x_{44}, x_{36}, x_{28}, x_{20}, x_{12}, x_4 \\ & x_{62}, x_{54}, x_{46}, x_{38}, x_{30}, x_{22}, x_{14}, x_6, x_{64}, x_{56}, x_{48}, x_{40}, x_{32}, x_{24}, x_{16}, x_8 \\ & x_{57}, x_{49}, x_{41}, x_{33}, x_{25}, x_{17}, x_9, x_1, x_{59}, x_{51}, x_{43}, x_{35}, x_{27}, x_{19}, x_{11}, x_3 \\ & x_{61}, x_{53}, x_{45}, x_{37}, x_{29}, x_{21}, x_{13}, x_5, x_{63}, x_{55}, x_{47}, x_{39}, x_{31}, x_{23}, x_{15}, x_7 \end{aligned}$$

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:

$$\begin{aligned} L_0 = & x_{58}, x_{50}, x_{42}, x_{34}, x_{26}, x_{18}, x_{10}, x_2, x_{60}, x_{52}, x_{44}, x_{36}, x_{28}, x_{20}, x_{12}, x_4 \\ & x_{62}, x_{54}, x_{46}, x_{38}, x_{30}, x_{22}, x_{14}, x_6, x_{64}, x_{56}, x_{48}, x_{40}, x_{32}, x_{24}, x_{16}, x_8 \ , \end{aligned}$$

$$\begin{aligned} R_0 = & x_{57}, x_{49}, x_{41}, x_{33}, x_{25}, x_{17}, x_9, x_1, x_{59}, x_{51}, x_{43}, x_{35}, x_{27}, x_{19}, x_{11}, x_3 \\ & x_{61}, x_{53}, x_{45}, x_{37}, x_{29}, x_{21}, x_{13}, x_5, x_{63}, x_{55}, x_{47}, x_{39}, x_{31}, x_{23}, x_{15}, x_7 \ . \end{aligned}$$

שלב (3) מבצעים 16 מחזורים של אלגוריתם פייסטל מסוים. מחשבים את L_i, R_i $1 \leq i \leq 16$ לפי הכלל

$$L_i = R_{i-1} \ , \qquad R_i = L_{i-1} \oplus f\left(R_{i-1}, k_i\right)$$

כאשר $\oplus$ מסמן XOR ו- $k_1, \ldots, k_{16}$ התת-מפתחות שבנויים מרצפי סיביות, כל אחד של אורך 48 שמתקבלים ממפתח התחלתי k.

שלב (4) בסוף מפעילים התמורה ההופכית IP^{-1} על הרצף סיביות $R_{16}L_{16}$ כדי לקבל הטקסט מוצפן הסופי y. ז"א

$$y = IP^{-1}\left(R_{16}L_{16}\right) \ .$$

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

$$R_i = L_{i-1} \oplus f\left(R_{i-1}, k_i\right) \ .$$

f מקבלת ארגומנט ראשון A אשר הוא רצף סיביות של אורך 32, וארגומנט שני J אשר רצף סיביות של אורך 48, ומחזירה רצף סיביות של אורך 32.

$$f : \{0,1\}^{32} \times \{0,1\}^{48} \to \{0,1\}^{32} \ .$$

שלב (1) ראשית הפונקציית ליבה f הופכת A לרצף סיביות של אורך 48 באמצעות הפונקציה

$$E : \{0,1\}^{32} \to \{0,1\}^{48} \ .$$

$E(A)$ 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 $E(A) \oplus J$ 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 בקופסאות ההחלפות $S_1,S_2,S_3,S_4,S_5,S_6,S_7,S_8$.

כל S_i היא מטריצה 16×4 אשר איבריה הם שלמים $0,1,\ldots,15$.

כל S_i עובדת כפונקציה

$$S_j:\{0,1\}^2\times\{0,1\}^4\to\{0,1\}^4\ .$$

ספציפי, נתון רצף סיביות של אורך 6, $B_j=b_1b_2b_3b_4b_5b_6$, אז

$$S_j\left(B_j\right)=S_j(r,c)$$

כאשר $S_j(r,c)$ הוא האיבר בשורה ה- r ועמושדה ה- c של המטריצה S_i.

הביטים b_1b_6 קובעים את היצוג הבינארי של שורה r של S_j, והביטים $b_2b_3b_4b_5$ קובעים את היצוג הבינארי של עמודה c של S_j.

מגדירים

$$C_j=S_j\left(B_j\right)\ ,\qquad 1\le j\le 8\ .$$

שלב (4) מבצעים תמורה הסטטי P על הרצף $C=C_1C_2C_3C_4C_5C_6C_7C_8$ כאשר התמורה P נתונה בטבלה למטה:

$$P=\begin{pmatrix}16&7&20&21\\29&12&28&17\\1&15&23&26\\5&18&31&10\\2&8&24&14\\32&27&3&9\\19&13&30&6\\22&11&4&25\end{pmatrix}$$

הרצף סיביות המתקבל $P(C)$ מוגדר להיות $f(A,J)$.

התזמון המפתח של DES

נתון מפתח התחלתי k של 64 ביטים. משתמשים ב- 56 סיביות של k בהרכב 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

$$PC_1(k)=C_0D_0$$

כאשר C_0 ה- 28 סיביות הראשונות ו- D_0 ה- 28 סיביות האחרונות.

שלב (3) לכל $1 \leq i \leq 16$, מחשבים

$$C_i = LS_i\left(C_{i-1}\right)\ , \qquad D_i = LS_i\left(D_{i-1}\right)\ .$$

ו-

$$k_i = PC_2\left(C_i D_i\right)\ .$$

LS_i הוא הזזה של מקום אחד או שתי מקומות שמאולה:

$$LS_i = \begin{cases} \text{הזזה מקום אחת שמאולה} & i = 1, 2, 9, 16, \\ \text{הזזה שתי מקומות שמאלה} & i = 3, 4, 5, 6, 7, 8, 10, 11, 12, 13, 14, 15\ . \end{cases}$$

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 ההחלפות 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

דוגמה 10.4

בצעו את האלגוריתם ליצירת תת-מפתחות לחשב k_1 מהמפתח ההתחלתי

$$k = \texttt{133457799BBCDFF1}$$

פתרון:

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

$$k = \texttt{0001 0011 0011 0100 0101 0111 0111 1001}$$
$$\texttt{1001 1011 1011 1100 1101 1111 1111 0001}\ .$$

$$PC_1(k) = C_0 D_0$$

כאשר

$$C_0 = \texttt{1111 0000 1100 1100 1010 1010 1111}$$

$$D_0 = \texttt{0101 0101 0110 0110 0111 1000 1111}\ .$$

נבצע הזזה של ספרה אחד לשמאל לקבל

$$C_1 = \texttt{111 0000 1100 1100 1010 1010 1111 1}$$
$$D_1 = \texttt{101 0101 0110 0110 0111 1000 1111 0}\ .$$

$$PC_2\left(C_1 D_1\right) = k_1 = \texttt{0001 1011 0000 0010 1110 1111 1111 1100 0111 0000 0111 0010}\ .$$

■

דוגמה 10.5

מצאו את ההצפנה אחרי מחזור אחד של קריפטו-מערכת DES של הטקסט גלוי

0123456789ABCDEF

עם מפתח התחלתי

133457799BBCDFF1

פתרון:
תחילה 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:

$$k_1 = \texttt{0001 1011 0000 0010 1110 1111 1111 1100 0111 0000 0111 0010}\ .$$

נפעיל תמורה הסטטית IP על הרצף סיביות 64 ביטים ונקבל

$$IP(x) = L_0 R_0$$

כאשר

$$L_0 = 1100\ 1100\ 0000\ 0000\ 1100\ 1100\ 1111\ 1111\ ,$$

ו-

$$R_0 = 1111\ 0000\ 1010\ 1010\ 1111\ 0000\ 1010\ 1010\ ,$$

כעת 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) עבור הרצף 6- ביטים הראשון:

$$b_1b_2b_3b_4b_5b_6 = 011000\ ,$$

נקח שורה $b_1b_6 = 00$ ועמודה $b_2b_3b_4b_5 = 1100$ של הקופסה S_2. זוהי 5, אשר הוא 0101 בבסיס בינארי. חוזרים 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) מפעילים התמורה P על C:

$$f(R_0, k_1) = P(C) = 0010\ 0011\ 0100\ 1010\ 1010\ 1001\ 1011\ 1011$$

בסוף $L_1 = R_0$ ו-

$$R_1 = L_0 \oplus f(R_0, k_1) = 1110\ 1111\ 0100\ 1010\ 0110\ 0101\ 0100\ 0100$$

■

דוגמה 10.6

נתון הטקסט גלוי

02468ACE13579BDF ,

נתון המפתח ההתחלתי

$$k = \texttt{010145458989CDCD} \ ,$$

ונתון כי התת-מפתח הראשון של קריפטו-מערכת DES הוא

$$k_1 = \texttt{0000 1011 0000 0010 0100 0011 1001 1001 0100 1000 0010 0100} \ .$$

בצעו את המחזור הראשון של הצפנת 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

כאשר $IP(x) = L_0 R_0$

$$L_0 = \texttt{1010 1010 1111 0000 1010 1010 1111 0000}$$
$$R_0 = \texttt{1100 1100 0000 0000 1100 1100 1111 1111}$$

כדי
להשתמש במשוואות פייסטל נצטרך לחשב את הפונקציית ליבה $f(R_0, k_1)$. תחילה משחבים את

$$E(R_0) = \texttt{1111 1111 0111 1001 0101 0110 0001 0000 0000 1000 0101 1110}.$$

מבצעים XOR של $E(R_0)$ עם k_1 ורושמים את התוצאה בקבוצות של 6 ביטים:

$$E(R_0) \oplus k_1 = \texttt{111011 101000 001001 000010 111111 001101 111111 011011}.$$

<u>קופסה החלפה S1</u> שורה 11, עמודה 1101, ומקבלים את האיבר 0.

<u>קופסה החלפה S2</u> שורה 10, עמודה 0100, ומקבלים את האיבר 10.

<u>קופסה החלפה S3</u> שורה 01, עמודה 0100, ומקבלים את האיבר 3.

<u>קופסה החלפה S4</u> שורה 00, עמודה 0001, ומקבלים את האיבר 13.

<u>קופסה החלפה S5</u> שורה 11, עמודה 1111, ומקבלים את האיבר 3.

<u>קופסה החלפה S6</u> שורה 01, עמודה 0110, ומקבלים את האיבר 9.

<u>קופסה החלפה S7</u> שורה 11, עמודה 1111, ומקבלים את האיבר 12.

<u>קופסה החלפה S8</u> שורה 01, עמודה 1101, ומקבלים את האיבר 14.

לכן

$$C = \texttt{0000 1010 0011 1101 0011 1001 1100 1110}$$

מבצעים את התמורה הסטטית C:

$$P(C) = f(R_0, k_1) = \texttt{1111 1100 0001 1010 0011 0000 1110 0101}$$

לבסוף אנחנו מקבלים

$$\begin{aligned} L_1 = R_0 &= \texttt{1100 1100 0000 0000 1100 1100 1111 1111} \\ R_1 = L_0 \oplus f(R_0, k_1) &= \texttt{0101 0110 1110 1010 1001 1010 0001 0101} \end{aligned}$$

■

10.4 IDEA

הגדרה 10.3 פעולות בינאריות של IDEA

$\oplus$	או מוציא XOR
$\boxplus$	חיבור מודולו 2^n כאשר n שלם השווה לאורך של הבלוקים
$\odot$	כפל מודולו 2^n+1

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 תפוקה משתמשת ב- 4 תת מפתחות. התת מפתחות מסומנות ב- $k_i^{(r)}$ $1 \leq r \leq 8$, $1 \leq i \leq 4$, ו- $k_i^{(9)}$, $1 \leq i \leq 4$. התת מפתחות מתקבלים על ידי לחלק k לשמונה תת-מפתחות, כל אחד של אורך 16 ביטים, ואחר כך להזיז k 25 מקומות שמאלה. התת מפתחות המתקבלים 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 גלוי P של אורך 64 ביטים.
- מחלקים X לארבע בלוקים, כל אחד של אורך 16 ביטים:

$$P = P_1P_2P_3P_4 \ .$$

- בתחילה של מחזור ה- r $1 \leq r \leq 9$, נסמן את הטקסט מוצפן המתקבל ממחזור הקודם (מחזור $r-1$) ב- $C^{(r)}$, מלבד מ- $C^{(1)} = P$.
- כל מחזור r מורכב מהשלבים הבאים:

[1] $$Y_1 = C_1^{(r)} \odot k_1^{(r)} = C_1^{(r)} \cdot k_1^{(r)} \mod (2^{16}+1)$$

[2] $$Y_2 = C_2^{(r)} \boxplus k_2^{(r)} = C_2^{(r)} + k_2^{(r)} \mod 2^{16}$$

[3] $$Y_3 = C_3^{(r)} \boxplus k_3^{(r)} = C_3^{(r)} + k_3^{(r)} \mod 2^{16}$$

[4] $$Y_4 = C_4^{(r)} \odot k_4^{(r)} = C_4^{(r)} \cdot k_4^{(r)} \mod (2^{16}+1)$$

[5] $$Y_5 = Y_1 \oplus Y_3$$

[6] $$Y_6 = Y_2 \oplus Y_4$$

[7] $$Y_7 = Y_5 \odot k_5^{(r)} = Y_5 \cdot k_5^{(r)} \mod (2^{16}+1)$$

[8] $$Y_8 = Y_6 \boxplus Y_7 = Y_6 + Y_7 \mod 2^{16}$$

[9] $$Y_9 = Y_8 \odot k_6^{(r)} = Y_8 \cdot k_6^{(r)} \mod 2^{16}+1$$

[10] $$Y_{10} = Y_7 \boxplus Y_9 = Y_7 + Y_9 \mod 2^{16}$$

[11] $$C_1^{(r+1)} = Y_1 \oplus Y_9$$

[12] $$C_2^{(r+1)} = Y_3 \oplus Y_9$$

[13] $$C_3^{(r+1)} = Y_2 \oplus Y_{10}$$

[14] $$C_4^{(r+1)} = Y_4 \oplus Y_{10}$$

הערכים Y_i נקראים הערכים הביניים. התפוקות $C_i^{(r)}$ $1 \leq i \leq 4$ נקראות הטקסטים מוצפנים הביניים.

- בכדי לקבל את הטקסט מוצפן הסופי, אחרי השלבים של כל מחזור r מבצעים את השלב התפוקה:

[1] $$C_1 = C_1^{(9)} \odot k_1^{(9)} = C_1^{(9)} \cdot k_1^{(9)} \mod 2^{16}+1$$

[2] $$C_2 = C_3^{(9)} \boxplus k_2^{(9)} = C_3^{(9)} + k_2^{(9)} \mod 2^{16}$$

$$C_3 = C_2^{(9)} \boxplus k_3^{(9)} = C_2^{(9)} + k_3^{(9)} \mod 2^{16} \qquad [3]$$

$$C_4 = C_4^{(9)} \odot k_4^{(9)} = C_4^{(9)} \cdot k_4^{(9)} \mod 2^{16} + 1 \qquad [4]$$

- 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

$$k = \texttt{01010303030301010123cdef00110011}$$

בצעו את המחזור הראשון של הצפנת IDEA על הטקסט גלוי

$$P = \texttt{000f11111111000f}$$

פתרון:

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

יוצרים את התת מתחות למחזור הראשון:

$$k_1^{(1)} = 0000000100000001 \quad = 257$$
$$k_2^{(1)} = 0000001100000011 \quad = 771$$
$$k_3^{(1)} = 0000001100000011 \quad = 771$$
$$k_4^{(1)} = 0000000100000001 \quad = 257$$
$$k_5^{(1)} = 0000000100100011 \quad = 291$$
$$k_6^{(1)} = 1100110111101111 \quad = 52719$$

רושמים את הטקסט גלוי 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

מבצעים מחזור ראשון של ההצפנה:

$$
\begin{aligned}
P_1 = C_1^{(1)} &= 0000000000001111 \quad = 15 \ , \\
P_2 = C_2^{(1)} &= 0001000100010001 \quad = 4369 \ , \\
P_3 = C_3^{(1)} &= 0001000100010001 \quad = 4369 \ , \\
P_4 = C_4^{(1)} &= 0000000000001111 \quad = 15 \ ,
\end{aligned}
$$

$$
\begin{array}{llllll}
Y_1 = C_1^{(1)} \odot k_1^{(1)} & = 15 \cdot 257 \mod 65537 & = 3855 & \Rightarrow & Y_1 = 0000\ 1111\ 0000\ 1111 \ , \\
Y_2 = C_2^{(1)} \boxplus k_2^{(1)} & = 4369 + 771 \mod 65536 & = 5140 & \Rightarrow & Y_2 = 0001\ 0100\ 0001\ 0100 \ , \\
Y_3 = C_3^{(1)} \boxplus k_3^{(1)} & = 4369 + 771 \mod 65536 & = 5140 & \Rightarrow & Y_3 = 0001\ 0100\ 0001\ 0100 \ , \\
Y_4 = C_4^{(1)} \odot k_4^{(1)} & = 15 \cdot 257 \mod 65537 & = 3855 & \Rightarrow & Y_4 = 0000\ 1111\ 0000\ 1111 \ , \\
Y_5 = Y_1 \oplus Y_3 & = 0001\ 1011\ 0001\ 1011 & = 6939 \ , & & \\
Y_6 = Y_2 \oplus Y_4 & = 0001\ 1011\ 0001\ 1011 & = 6939 \ , & & \\
Y_7 = Y_5 \odot k_5^{(1)} & = 6939 \cdot 291 \mod 65537 & = 53139 & \Rightarrow & Y_7 = 1100\ 1111\ 1001\ 0011 \ , \\
Y_8 = Y_6 \boxplus Y_7 & = 6939 + 53139 \mod 65536 & = 60078 & \Rightarrow & Y_8 = 1110\ 1010\ 1010\ 1110 \ , \\
Y_9 = Y_8 \odot k_6^{(1)} & = 60078 \cdot 52719 \mod 65537 & = 45483 & \Rightarrow & Y_9 = 1011\ 0001\ 1010\ 1011 \ , \\
Y_{10} = Y_7 \boxplus Y_9 & = 53139 + 45483 \mod 65536 & = 33086 & \Rightarrow & Y_{10} = 1000\ 0001\ 0011\ 1101 \ .
\end{array}
$$

התפוקה של מחזור הראשון הינה

$$
\begin{aligned}
C_1^{(2)} &= Y_1 \oplus Y_9 \quad = 1011111010100100 \\
C_2^{(2)} &= Y_3 \oplus Y_9 \quad = 1010010110111111 \\
C_3^{(2)} &= Y_2 \oplus Y_{10} \quad = 1001010100101010 \\
C_4^{(2)} &= Y_4 \oplus Y_{10} \quad = 1000111000110001
\end{aligned}
$$

■

דוגמה 10.12

מצאו את המפתחות פענוח של המחזור הראשון של פענוח IDEA בעזרת המפתח ההתחלתי

$$k = \texttt{00112233445566778899aabbccddeeff} \ .$$

פתרון:

המפתחות לפענוח הם

$$
\begin{aligned}
DK_1^{(1)} &= \left(K_1^{(9)}\right)^{-1} \ , \\
DK_2^{(1)} &= -\left(K_2^{(9)}\right) \ , \\
DK_3^{(1)} &= -\left(K_3^{(9)}\right) \ , \\
DK_4^{(1)} &= \left(K_4^{(9)}\right)^{-1} \ , \\
DK_5^{(1)} &= K_5^{(8)} \ , \\
DK_6^{(1)} &= K_6^{(8)} \ .
\end{aligned}
$$

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

ביטים $22-37$: $k_1^{(9)} = 0100\ 0110\ 0110\ 1000 = 18024$.

ביטים $38-53$: $k_2^{(9)} = 1000\ 1010\ 1010\ 1100 = 35500$.

ביטים $54-69$: $k_3^{(9)} = 1100\ 1110\ 1111\ 0001 = 52977$.

ביטים $70-85$: $k_4^{(9)} = 0001\ 0011\ 0011\ 0101 = 4917$.

ביטים $93-108$: $k_5^{(8)} = 1011\ 1100\ 1100\ 1101$.

ביטים $109-124$: $k_6^{(8)} = 1101\ 1110\ 1110\ 1111$.

$$\begin{aligned}
DK_1^{(1)} &= \left(K_1^{(9)}\right)^{-1} = (18024)^{-1} \mod 65537 = 45753 = 1011\ 0010\ 1011\ 1001\ ,\\
DK_2^{(1)} &= -\left(K_2^{(9)}\right) = -35500 \mod 65536 = 30036 = 0111\ 0101\ 0101\ 0100\ .\\
DK_3^{(1)} &= -\left(K_3^{(9)}\right) = -52977 \mod 65536 = 12559 = 0011\ 0001\ 0000\ 1111\ .\\
DK_4^{(1)} &= \left(K_4^{(9)}\right)^{-1} = (4917)^{-1} \mod 65537 = 18047 = 0100\ 0110\ 0111\ 1111\ .\\
DK_5^{(1)} &= K_5^{(8)} = 1011\ 1100\ 1100\ 1101\ .\\
DK_6^{(1)} &= K_6^{(8)} = 1101\ 1110\ 1110\ 1111\ .
\end{aligned}$$

■

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 בטיות משיטות חתימה
13.2 שיטות חתימה של אל-גמאל

שיעור 14
סכמות לשיתוף סודות

14.1 סכמת הסף של שמיר

14.2 סכמת סף (t,t) פשוטה