

שיעור 4

תמורות וצופן אניגמה

4.1 תמורות

הגדרה 4.1 תמורה

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

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

תזכורת:

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

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

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

דוגמה 4.1

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

דוגמה 4.2

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

דוגמה 4.3

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

פתרונות:

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

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

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

לכן

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

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

Σ , בסתירה לכך ש: π חד-חד-ערכית. לכן הוכחנו דרך השיליה כי

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

הוכחנו כי π גם $|\pi(\Sigma)| = |\Sigma|$ אז בהכרח

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

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



הגדרה 4.2 הרכבה של תמורה

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

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

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

דוגמה 4.4

נתון הרכבה π ו- σ :

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

אזי ההרבה $\sigma\pi$ היא:

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

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

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

כלומר $\sigma\pi \neq \pi\sigma$.

משפט 4.1 הרכבה של תמורה היא תמורה

תהי Σ קבוצה נוצר סופית ותהינה $\Sigma \rightarrow \Sigma : \pi$ ו- $\Sigma \rightarrow \Sigma : \sigma$ 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 בשיליה כי $\sigma\pi$ לא חח"ע. אזי קיימים $x_1, x_2 \in \Sigma$ כך ש- $(\pi(x_1)) = \sigma(\pi(x_2))$. 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

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

$$\sigma(\pi(x_1)) = \sigma(\pi(x_2))$$

בסתירה לכך ש- $\sigma\pi$ פונקציה חח"ע.

• על

נניח בשלילה כי $\pi \sigma$ לא פונקציה "על". נסמן (Σ) התחמונה של $\pi \sigma$. אז $\sigma \pi(\Sigma) \neq \Sigma$.

ראשית מכיוון ש- (Σ) הוא התחמונה של $\pi \sigma$ אז $\Sigma \subseteq \pi \sigma(\Sigma)$. לכן אם $\Sigma \neq \pi \sigma(\Sigma)$ אז

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

לכן בהכרח קיימים לפחות שני איברים $x_1, x_2 \in \Sigma$ עבורם $\sigma \pi(x_1) = \sigma \pi(x_2)$. זאת בסתיויה כך ש- π חח"ע, שMOVED בסייף הקודם.

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

הגדרה 4.3 תמורהות מתחלפות

תהיינה π, σ תמורהות. אומרים כי π ו- σ מתחלפות אם

$$\pi \sigma = \sigma \pi .$$

הגדרה 4.4 תמורהות מתחלפות

תהי $\Sigma \rightarrow \Sigma$ 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 ונקודת זהה

תהי $\Sigma \rightarrow \Sigma$ תמורה.

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

הגדרה 4.6 תמורה זהה

התמורה זהה מסומנת $\Sigma \rightarrow \Sigma$ לפי ומוגדרת כך שלכל $x \in \Sigma$:

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

במילים אחרות אם $\Sigma \rightarrow \Sigma$ היא התמורה זהה אז כל נקודת $\Sigma \in x$ היא נקודת שבת של id .

משפט 4.2 תמורה ההפכית של תמורה מורכבת

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

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

הוכחה: נוכיח את הטענה באינדוקציה.

שלב הבסיס

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

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

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

שלב האינדוקציה

נניח כי הטענה מתקיימת עבור $t = k > 2$ (זאת היא ההנחה האינדוקציה). אז נראה כי הטענה נכונה גם במקרה $t = k + 1$ באופן הבא. נתבונן על התמורה המורכבת $\pi_k \pi_{k+1} \cdots \pi_1$. נסמן התמורה המורכבת מ- k תמורות כ- σ : $\sigma = \pi_1 \cdots \pi_k$. 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 שלב הבסיס מההפכית היא

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

כעת נזכיר את ההגדרה $\sigma = \pi_1 \cdots \pi_k$ ונשתמש בהנחה 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 בהנחה האינדוקציה.

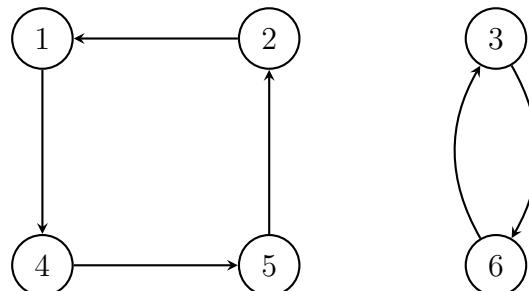
■

4.2 פירוק למחזוריים של תמורה

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

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

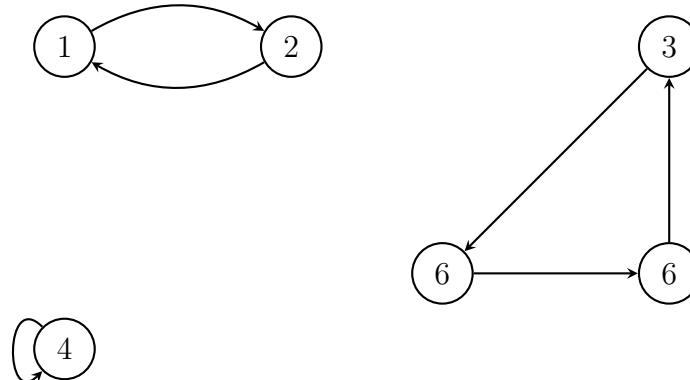
נדיר הgraf המכובן $G_\pi = (V, E)$ כאשר הקבוצת הקודקודים היא $V = \Sigma$, ולכל $x \in \Sigma$ נגידר צלע מ- x ל- $\pi(x)$. א"א $E = \{e_1, e_2, \dots, e_n\}$ כאשר $e_i = x_i \pi(x_i)$ הינה הצלע מקודקוד x_i לקודקוד $\pi(x_i)$. על פי ההגדרה זאת הgraf G_π של התמורה π היא כמתוארת באיור למטה.



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:



בgraf של תמורה, כל קודקוד שיעיר לבדוק מעגל מכוכן אחד (שייתכן הוא עובר דרך קודקוד אחד בלבד).
הרי קיימים התאמות אחת-אחת בין תמורה על Σ לבין graf שמכסה כל המעגלים המכוכנים של Σ . התופעה זו היא המוטיבציה לשימוש מחזוריים של תמורים.

הגדרה 4.7 מחזור

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

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

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

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

משפט 4.3 פירוק למחזוריים של תמורה

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

■ **הוכחה:** שאללה לעובdet הגשה.

דוגמה 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 למחזוריים הוא:

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

משפט 4.4

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

הוכחה:
כיון אם

נניח ש- π מכילה מחזורי באורך k .

$\left(a_1 \ a_2 \ \dots \ \subseteq a_k \right) \in \pi \Leftarrow$ קיימים איברים שונים $a_1, \dots, a_k \in \Sigma$ כך ש:

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

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

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

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

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

$.k$ מכילה מעגל המילטוני באורך k .

כיון רק אם

נניח ש- G_π מכיל מעגל המילטוני באורך k .

\Leftarrow קיימים קבוצות $a_1, \dots, a_k \in \Sigma$ עוברים

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

\Leftarrow מכיוון ש- G_π הוא הגרף של התמורה π איזי

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

\Leftarrow π מכילה מחזורי באורך k :

$\left(a_1 \ a_2 \ \dots \ \subseteq a_k \right) \subseteq \pi$.



הגדרה 4.8 החלוקת של תמורה

תהי $\Sigma \rightarrow \pi$ תמורה. אומרים כי π שיכת לחלוקת $[1^{z_1} 2^{z_2} \dots n^{z_n}]$ אם בפרק למחזורים של π יש לבדוק z_1 מחזורים באורך-1, z_2 מחזורים באורך-2, z_3 מחזורים באורך-3, וכן הלאה.

במילים אחרות:

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

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

דוגמה 4.7

תהי $\Sigma = \{A, B, C, D, E, F\}$

$$\bullet \text{ התמורה } .(A \ B)(C \ D)(E \ F) \in [2^3]$$

• 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 Tamotim Zmodot

תהינה σ, π 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 Tamotim Zmodot

תהינה $\Sigma : \sigma : \Sigma \rightarrow \Sigma$ ו- $\pi : \Sigma \rightarrow \Sigma$ תמורות על הקבוצה סופית Σ . לכל $x, y \in \Sigma$ אם $\sigma(x) = y$ אז $\pi(\sigma(x)) = \pi(y)$.

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

הוכחה: נניח ש: $\sigma(x) = y$. אז

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

משפט 4.6 פירוקים למחזורים של Tamotim Zmodot Shovim

תהינה $\Sigma : \sigma : \Sigma \rightarrow \Sigma$ ו- $\pi : \Sigma \rightarrow \Sigma$ תמורות על הקבוצה סופית Σ . ונניח כי הפירוק למחזורים של σ הוא

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

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

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

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

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

מנובע ממשפט כי לכל מחזור של σ מתקיים:

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

משפט 4.7 חלוקה של Tamotim Zmodot Nshmerat

תהינה $\Sigma : \sigma : \Sigma \rightarrow \Sigma$ ו- $\tau : \tau : \Sigma \rightarrow \Sigma$ תמורות על הקבוצה סופית Σ . τ צמודה ל- σ אם ורק אם $\sigma \circ \tau$ שייכות לאותה חלוקה.

הוכחה:

כיוון אם:

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

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

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

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

ולכן ל- τ ול- σ יש אותו מבנה של מחזורים וכך שיקיות לאוთה מחלוקת.

כיוון רק אם:

■

4.4 צופן אניגמה

הgelgi האתחול של צופן אניגמה הם 3 תמורה קבועות שמוגדרות:

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

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

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

המשקף הקבוע הוא תמורה הבאה:

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

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

הגדרה 4.10 כלל מצפן וככל מפענה של צופן אניגמה

יהי π משקף כלשהו מעל האלפבית $Z = A, \dots, Z$. הבחירה של המשקף מהווה את הלוח התקעים. יהי $x_1 x_2 \dots x_n = w$ מילה של טקסט גלי. לכל $i = 1, \dots, n$ הכלל מצפן והככל מפענה של האות במקומות ה- i -בטקסט הם:

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

כאשר Δ_i היא התמורה המורכבת

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

כאשר

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

אם נגדיר את התמורה המורכבת π נגיד $\tau_i = \sigma_{-i} \alpha_3 \sigma_i \alpha_2 \alpha_1 \pi$ ולכן

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

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

דוגמה 4.8 הצפנה על ידי צופן אניגמה

נתון הטקסט גלי

hello .

נניח כי הלוח התקעים הוא

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

חשבו את הטקסט מוצפן.

פתרונות:

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

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

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

$$\begin{array}{ccccccccc} E & \xrightarrow{\pi} & E & \xrightarrow{\sigma_2} & G & \xrightarrow{\alpha_3} & C & \xrightarrow{\sigma_{-2}} & A \\ & \xrightarrow{\alpha_1^{-1}} & H & \xrightarrow{\alpha_2^{-1}} & L & \xrightarrow{\sigma_2} & N & \xrightarrow{\alpha_3^{-1}} & N \end{array}$$

$$x_3 = L \quad (3)$$

$$\begin{array}{ccccccccc} L & \xrightarrow{\pi} & P & \xrightarrow{\sigma_3} & S & \xrightarrow{\alpha_3} & G & \xrightarrow{\sigma_{-3}} & D \\ & \xrightarrow{\alpha_1^{-1}} & B & \xrightarrow{\alpha_2^{-1}} & J & \xrightarrow{\sigma_3} & M & \xrightarrow{\alpha_3^{-1}} & V \end{array}$$

$$x_4 = S \quad (4)$$

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

 $x_5 = \circ$ (5)

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

לפייך הטקסט מוצפן הוא: EPSAX.

דוגמה 4.9 הצפנה על ידי צופן איניגמה

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

פתרונות: $y_1 = E$ (1)

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

 $y_2 = P$ (2)

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

 $y_3 = S$ (3)

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

 $y_4 = A$ (4)

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

 $y_5 = X$ (5)

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

לפייך הטקסט המקורי הוא: HELLO.

4.5 משפט ריבסקי והתקפה על הצופן האניגמה

הגדרה 4.11 משקף

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

משפט 4.8 תכונות של תמורה משקפת

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

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

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

הוכחה:

כיוון אם

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

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

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

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

כעת נראה שאם $\Sigma \in x$ אז $x \neq \rho(x)$. נניח בשילhouette שקיימות נקודה $\Sigma \in x$ עבורות x ($\rho(x) = x$). אזי ρ מתקיים לפחות אחד באורך 1, בסתריה לכך ρ היא משקף.

כיוון רק אם

נניח כי $\Sigma \rightarrow \Sigma : \rho$ היא תמורה כך שלכל $\Sigma \in x$ מתקיים $\rho(\rho(\Sigma)) = \Sigma$. נוכיח כי ρ היא משקף. נניח בשילhouette כי ρ לא משקף. אזי ρ מכילה לפחות מהJOR אחד באורך $k > 2$. נניח כי קיימים מהJOR באורך 1. אזי קיימת נקודת שבת של ρ , קלומר קיימת $\Sigma \in x$ עבורות x ($\rho(\rho(\Sigma)) = \Sigma$). והגענו לסתירה. מצד שני נניח כי קיימים מהJOR באורך $2 < k$. אזי ניתן לרשום ρ כהרכבה באופן הבא:

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

כאשר $(\dots \ x_1 \ x_2 \ x_3 \ \dots)$ הוא מהJOR באורך k . ז"א ההופכית של ρ היא

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

בסתריה לכך $\rho^{-1} = \rho$.

משפט 4.9 הכלל מצפן של אניגמה הוא משקף על האלפבית האנגלית

הכלל מצפן (והכלל מפענה) של צופן אניגמה הוא משקף על האלפבית האנגלית.

הוכחה: הכלל מצפן והכלל מפענה של צופן אניגמה הם

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

כאשר π הכלל מצפן ו- ρ המשקף הקבוע של צופן אניגמה.

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

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

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

\Leftarrow לפי הדרה 4.11 התמורה Δ_i היא משקף.

משפט 4.10

יהיו ρ_1 ו- ρ_2 משקפים על הקבוצה סופית Σ .
לכל $x \in \Sigma$, $\rho_2\rho_1(y_1) = y_2$ אם $\rho_1(x) = y_1$ ו- $\rho_2(x) = y_2$ אזי $\rho_1(x) = y_1$ ו- $\rho_2(x) = y_2$.

הוכחה: מכיוון ש- ρ_1 משקף ו- ρ_2 אזי $\rho_1(x) = y_1$

$$\rho_1(x) = y_1 \iff \rho_1^{-1}(\rho_1(x)) = \rho_1^{-1}(y_1) \iff x = \rho_1^{-1}(y_1) \iff x = \rho_1(y_1) .$$

ז"א הוכחנו ש- $x = \rho_1(y_1)$. מכאן $\rho_2\rho_1(y_1) = \rho_2(x) = y_2$,

כנדרש.

דוגמה 4.10

נניח שיש לנו טקסט שמוספן ע"י צופן אניגמה שמתחל ב- ICPWLV. איזו אנחנו יודעים שקיים ב- ICPWLV?

כך ש:

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

כאשר Δ_i הוא הכלל מצפן של צופן אניגמה המורכב מהתמורה הנעלוות. מצד שני אנחנו כן יודעים שכל Δ_i הוא משקף על פ"י. לכן, בזכות המשפט, אפשר להסיק כי:

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

משפט 4.11 משפט ריבסקי

יהיו ρ_1 ו- ρ_2 משקפים על הקבוצה סופית Σ . אם המוחזר

$$(a_1 \ a_2 \ \dots \ a_t)$$

מופייע בפרק למחוזרים של התמורה המורכבת $\rho_2 \rho_1$, איזי בהכרח המוחזר

$$(\rho_1(a_t) \quad \rho_1(a_{t-1}) \quad \cdots \quad \rho_1(a_2) \quad \rho_1(a_1))$$

גם מופייע בפרק למחוזרים של התמורה המורכבת $\rho_1 \rho_2$, ובנוסף הוא שונה מהוחזר

$$(a_1 \quad a_2 \quad \cdots \quad a_t)$$

דוגמה 4.11

נניח ש-

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

זה בדיקת הסוג של פירוק למחוזרים הנקבע על ידי משפט ריבסקי: יש זוג מוחוזרים באורך 7, זוג מוחוזרים באורך 5, זוג מוחוזרים באורך 1. מכיוון שיש רק שני מוחוזרים מכל אורך, איזי אנחנו יודעים כיצד להתאים אותם:

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

דוגמה 4.12 קריpto-אנליזה של צופן אניגמה

נתונות התמורות הבאות של צופן אניגמה:

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

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

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

פענוו את הקסט מוצפן

ILBDA

פתרונות:

שלב 1) התמורה $\Delta_4 \Delta_1$

ראשית נסתכל על התמורה $\Delta_4 \Delta_1$.

	$\Delta_4 \Delta_1$	Δ_1	Δ_4
A	C		
B	G		
C	I		
D	O		
E	T		
F	W		
G	P		
H	Q		
I	K		
J	N		
K	E		
L	X		
M	L		
N	V		
O	F		
P	D		
Q	B		
R	Y		
S	Z		
T	M		
U	J		
V	U		
W	H		
X	A		
Y	S		
Z	R		

נתחיל עם הזוג תמורה $(Z R Y S) (J N V U)$. לפי משפט ריבסקי:

$$\Delta_1(U) = Z, \quad \Delta_1(V) = R, \quad \Delta_1(N) = Y, \quad \Delta_1(J) = S.$$

	$\Delta_4 \Delta_1$	Δ_1	Δ_4
A	C		
B	G		
C	I		
D	O		
E	T		
F	W		
G	P		
H	Q		
I	K		
J	N		
K	E		
L	X		
M	L		
N	V		
O	F		
P	D		
Q	B		
R	Y		
S	Z		
T	M		
U	J		
V	U		
W	H		
X	A		
Y	S		
Z	R		

עבור הזוג תמורות (GPDOFWHQB) (ACIKETMLX), לפי משפט ריבסקי:

$$\Delta_1(X) = G, \quad \Delta_1(L) = P, \quad \Delta_1(M) = D, \quad \Delta_1(T) = O, \quad \Delta_1(E) = F,$$

$$\Delta_1(K) = W, \quad \Delta_1(I) = H, \quad \Delta_1(C) = Q, \quad \Delta_1(A) = B.$$

	$\Delta_4 \Delta_1$	Δ_1	Δ_4
A	C	B	
B	G		
C	I	Q	
D	O		
E	T	F	
F	W		
G	P		
H	Q		
I	K	H	
J	N	S	
K	E	W	
L	X	P	
M	L	D	
N	V	Y	
O	F		
P	D		
Q	B		
R	Y		
S	Z		
T	M	O	
U	J	Z	
V	U	R	
W	H		
X	A	G	
Y	S		
Z	R		

בנוסח Δ_1 הוא משקף, לכן, אם למשל $\Delta_1(A) = B$ אז בהכרח $\Delta_1(B) = A$. על פי זה אפשר להשלים את העמודה של Δ_1 של הטבלה:

	$\Delta_4\Delta_1$	Δ_1	Δ_4
A	C	B	
B	G	A	
C	I	Q	
D	O	M	
E	T	F	
F	W	E	
G	P	X	
H	Q	I	
I	K	H	
J	N	S	
K	E	W	
L	X	P	
M	L	D	
N	V	Y	
O	F	T	
P	D	L	
Q	B	C	
R	Y	V	
S	Z	J	
T	M	O	
U	J	Z	
V	U	R	
W	H	K	
X	A	G	
Y	S	N	
Z	R	U	

הערכים של התמורה Δ_4 נתונים ע"י העמודות Δ_1 ו- $\Delta_4\Delta_1$. למשל, לפי השורה הראשונה:

$$\Delta_1(A) = B \quad \text{ו} \quad \Delta_4(\Delta_1(A)) = C \quad \Rightarrow \quad \Delta_4(B) = C .$$

כדוגמה נוספת, לפי השורה השנייה:

$$\Delta_1(B) = A \quad \text{ו} \quad \Delta_4(\Delta_1(B)) = G \quad \Rightarrow \quad \Delta_4(A) = G .$$

לפי השורה השלישית:

$$\Delta_1(C) = Q \quad \text{ו} \quad \Delta_4(\Delta_1(C)) = I \quad \Rightarrow \quad \Delta_4(Q) = I ,$$

וכן הלא. באופן זה אפשר למצוא את כל הערכים של התמורה Δ_4 על האותיות של האלפבית:

	$\Delta_4\Delta_1$	Δ_1	Δ_4
A	C	B	G
B	G	A	C
C	I	Q	B
D	O	M	L
E	T	F	W
F	W	E	T
G	P	X	A
H	Q	I	K
I	K	H	Q
J	N	S	Z
K	E	W	H
L	X	P	D
M	L	D	O
N	V	Y	S
O	F	T	M
P	D	L	X
Q	B	C	I
R	Y	V	U
S	Z	J	N
T	M	O	F
U	J	Z	R
V	U	R	Y
W	H	K	E
X	A	G	P
Y	S	N	V
Z	R	U	J

שלב 2) התמורה $\Delta_5\Delta_2$ כעת נסתכל על התמורה $\Delta_5\Delta_2$:

	$\Delta_5 \Delta_2$	Δ_2	Δ_5
A	I		
B	P		
C	E		
D	O		
E	U		
F	V		
G	Q		
H	J		
I	A		
J	S		
K	G		
L	R		
M	Z		
N	W		
O	D		
P	M		
Q	C		
R	N		
S	T		
T	Y		
U	K		
V	L		
W	F		
X	B		
Y	H		
Z	X		

נתחיל עם הזוג תמורהות (IA) (DO). לפי משפט ריבסקי:

$$\Delta_2(A) = D, \quad \Delta_2(I) = O.$$

עבור הזוג תמורהות (CEUKGQ) (NWFVLR), לפי משפט ריבסקי:

$$\Delta_2(Q) = N, \quad \Delta_2(G) = W, \quad \Delta_2(K) = F, \quad \Delta_2(U) = V, \quad \Delta_2(E) = L, \quad \Delta_2(C) = R.$$

עבור הזוג תמורהות (BPMZX) (STYHJ), לפי משפט ריבסקי:

$$\Delta_2(X) = S, \quad \Delta_2(Z) = T, \quad \Delta_2(M) = Y, \quad \Delta_2(P) = H, \quad \Delta_2(B) = J.$$

	$\Delta_5 \Delta_2$	Δ_2	Δ_5
A	I	D	
B	P	J	
C	E	R	
D	O		
E	U	L	
F	V		
G	Q	W	
H	J		
I	A	O	
J	S		
K	G	F	
L	R		
M	Z	Y	
N	W		
O	D		
P	M		
Q	C	N	
R	N		
S	T		
T	Y		
U	K	V	
V	L		
W	F		
X	B	S	
Y	H		
Z	X	T	

בנוסך Δ_2 הוא משקף, כלומר אם למשל $\Delta_2(A) = D$ אז בהכרח $\Delta_2(D) = A$. על פי זה אפשר להשלים את העמודה של Δ_2 של ה таблицה:

	$\Delta_5 \Delta_2$	Δ_2	Δ_5
A	I	D	
B	P	J	
C	E	R	
D	O	A	
E	U	L	
F	V	K	
G	Q	W	
H	J	P	
I	A	O	
J	S	B	
K	G	F	
L	R	E	
M	Z	Y	
N	W	Q	
O	D	I	
P	M	H	
Q	C	N	
R	N	C	
S	T	X	
T	Y	Z	
U	K	V	
V	L	U	
W	F	G	
X	B	S	
Y	H	M	
Z	X	T	

הערכים של התמורה Δ_5 נתונים ע"י העמודות Δ_2 ו- $\Delta_5 \Delta_2$. למשל, לפי השורה הראשונה:

$$\Delta_2(A) = D \quad \text{ו} \quad \Delta_5(\Delta_2(A)) = I \quad \Rightarrow \quad \Delta_5(D) = I .$$

כדוגמה נוספת, לפי השורה השנייה:

$$\Delta_2(B) = J \quad \text{ו} \quad \Delta_5(\Delta_2(B)) = P \quad \Rightarrow \quad \Delta_5(J) = P .$$

לפי השורה השלישית:

$$\Delta_2(C) = R \quad \text{ו} \quad \Delta_5(\Delta_2(C)) = E \quad \Rightarrow \quad \Delta_5(R) = E ,$$

וכן הלא. באופן זה אפשר למצוא את כל הערכים של התמורה Δ_5 על האותיות של האלפבית:

	$\Delta_5 \Delta_2$	Δ_2	Δ_5
A	I	D	O
B	P	J	S
C	E	R	N
D	O	A	I
E	U	L	R
F	V	K	G
G	Q	W	F
H	J	P	M
I	A	O	D
J	S	B	P
K	G	F	V
L	R	E	U
M	Z	Y	H
N	W	Q	C
O	D	I	A
P	M	H	J
Q	C	N	W
R	N	C	E
S	T	X	B
T	Y	Z	X
U	K	V	L
V	L	U	K
W	F	G	Q
X	B	S	T
Y	H	M	Z
Z	X	T	Y

שלב 3) התמורה $\Delta_6 \Delta_3$

כעת נסתכל על התמורה: $\Delta_6 \Delta_3$:

	$\Delta_6 \Delta_3$	Δ_3	Δ_6
A	G		
B	I		
C	N		
D	H		
E	M		
F	P		
G	L		
H	R		
I	Z		
J	V		
K	C		
L	Y		
M	O		
N	K		
O	E		
P	X		
Q	D		
R	S		
S	U		
T	J		
U	Q		
V	F		
W	B		
X	T		
Y	A		
Z	W		

נתחיל עם הזוג תמורהות (CNK) (MOE). לפי משפט ריבסקי:

$$\Delta_3(K) = M, \quad \Delta_3(N) = O, \quad \Delta_3(C) = E.$$

עבור הזוג תמורהות (AGLY) (WBIQ), לפי משפט ריבסקי:

$$\Delta_3(Y) = W, \quad \Delta_3(L) = B, \quad \Delta_3(G) = I, \quad \Delta_3(A) = Z.$$

עבור הזוג תמורהות (DHRSUQ) (VFPXTJ), לפי משפט ריבסקי:

$$\Delta_3(Q) = V, \quad \Delta_3(U) = F, \quad \Delta_3(S) = P, \quad \Delta_3(R) = X, \quad \Delta_3(H) = T, \quad \Delta_3(D) = J.$$

	$\Delta_6 \Delta_3$	Δ_3	Δ_6
A	G	Z	
B	I		
C	N	E	
D	H	J	
E	M		
F	P		
G	L	I	
H	R	T	
I	Z		
J	V		
K	C	M	
L	Y	B	
M	O		
N	K	O	
O	E		
P	X		
Q	D	V	
R	S	X	
S	U	P	
T	J		
U	Q	F	
V	F		
W	B		
X	T		
Y	A	W	
Z	W		

בנוסך Δ_3 הוא משקף, כלומר אם למשל $Z = \Delta_3(A)$ אז בהכרח $\Delta_3(Z) = A$. על פי זה אפשר להשלים את העמודה של Δ_3 של ה таблицה:

	$\Delta_6 \Delta_3$	Δ_3	Δ_6
A	G	Z	
B	I	L	
C	N	E	
D	H	J	
E	M	C	
F	P	U	
G	L	I	
H	R	T	
I	Z	G	
J	V	D	
K	C	M	
L	Y	B	
M	O	K	
N	K	O	
O	E	N	
P	X	S	
Q	D	V	
R	S	X	
S	U	P	
T	J	H	
U	Q	F	
V	F	Q	
W	B	Y	
X	T	R	
Y	A	W	
Z	W	A	

הערכים של התמורה Δ_6 נתונים ע"י העמודות Δ_3 ו- $\Delta_6 \Delta_3$. למשל, לפי השורה הראשונה:

$$\Delta_3(A) = Z \quad \text{ו} \quad \Delta_6(\Delta_3(A)) = G \quad \Rightarrow \quad \Delta_6(Z) = G .$$

כדוגמה נוספת, לפי השורה השנייה:

$$\Delta_3(B) = L \quad \text{ו} \quad \Delta_6(\Delta_3(B)) = I \quad \Rightarrow \quad \Delta_6(L) = I .$$

לפי השורה השלישית:

$$\Delta_3(C) = E \quad \text{ו} \quad \Delta_6(\Delta_3(C)) = N \quad \Rightarrow \quad \Delta_6(E) = N ,$$

וכן הלא. באופן זה אפשר למצוא את כל הערכים של התמורה Δ_6 על האותיות של האלפבית:

	$\Delta_6 \Delta_3$	Δ_3	Δ_6
A	G	Z	W
B	I	L	Y
C	N	E	M
D	H	J	V
E	M	C	N
F	P	U	Q
G	L	I	Z
H	R	T	J
I	Z	G	L
J	V	D	H
K	C	M	O
L	Y	B	I
M	O	K	C
N	K	O	E
O	E	N	K
P	X	S	U
Q	D	V	F
R	S	X	T
S	U	P	X
T	J	H	R
U	Q	F	P
V	F	Q	D
W	B	Y	A
X	T	R	S
Y	A	W	B
Z	W	A	G

שלב 4) פענוח:

$$\Delta_1(\sigma_1) = I, \quad \Delta_2(\sigma_2) = L, \quad \Delta_3(\sigma_3) = B, \quad \Delta_4(\sigma_4) = D, \quad \Delta_5(\sigma_5) = A.$$

לפיכך:

$$\sigma_1 = \Delta_1(I) = H,$$

$$\sigma_2 = \Delta_2(L) = E,$$

$$\sigma_3 = \Delta_3(B) = L,$$

$$\sigma_4 = \Delta_4(D) = L,$$

$$\sigma_5 = \Delta_5(A) = O.$$

