(1) $p \in \mathbb{N}$ prime. Let $x \in \mathbb{Z}$ s.t. $p \nmid x$.

$x = \underbrace{x_1 \cdots x_n}_{L_0} \underbrace{x_{n+1} \cdots x_{2n}}_{R_0}$ $\quad L_0 = x_1 \cdots x_n,\ R_0 = x_{n+1} \cdots x_{2n}$

(2) $n \geq 3$ odd $p \nmid n!$

(3) $(k_1, \ldots, k_n)$ n-cycle in S_n $p \nmid k_1 \cdots k_n$.

---

(1) Fermat's little theorem: $p \in \mathbb{N}$ prime, $a \in \mathbb{Z}$, $p \nmid a$ then $a^{p-1} \equiv 1 \pmod p$

Proof: Let $X = \{1, \ldots, p\}^{\mathbb{Z}/p\mathbb{Z}}$ and $\sigma \in S_p$.

$|X| = p^p$, $\{1, \ldots, p\} = X^{\sigma}$ σ of order p.

$\mathbb{Z}/p\mathbb{Z} \curvearrowright X$ by $(k \cdot x)_i = x_{i+k}$

(2) $\mathbb{Z}/4\mathbb{Z}$

(3) D_{12}

ולד סוף סוף (1M נ)

$X = x_1 \cdots x_n \; x_{n+1} \cdots x_{2n}$

$L_0 = x_1 \cdots x_n \;,\quad R_0 = x_{n+1} \cdots x_{2n}.$

$L_1 = R_0 \;,\quad R_1 = L_0 \oplus f(R_0, k_1)$ — עבור $i=1$

k_1 ו־R_0 הם קלט של f בסיבוב הראשון (עם $i=1$).

$L_2 = R_1, \quad R_2 = L_1 \oplus f(R_1, k_2)$ — עבור $i=2$

$L_3 = R_2, \quad R_3 = L_2 \oplus f(R_2, k_3)$ — עבור $i=3$

סעיף ג (1 נק') נתון $N = p \cdot q$ כאשר p, q ראשוניים שונים ו־$N > 21$. נתון גם $\varphi(N) = 72$. מצא את p ו־q.

$\varphi(N) = (p-1)(q-1) = N - p - q + 1$

$p + q = N - \varphi(N) + 1 = 21 - 72 + 1 = -50$

p, q הם שורשי המשוואה $x^2 + 50x + 21 = 0$

$\Delta = 2500 - 84 = 2416$

$\sqrt{2416} = 4\sqrt{151}$

$p = \frac{-50 + 4\sqrt{151}}{2} = -25 + 2\sqrt{151}$

$q = -25 - 2\sqrt{151}$

(4) סעיף ד (2 נק') $N = 33$ ו־$e = 7$. הצפן $M = 2$. מצא את d ואת C.

$\varphi(N) = 20$

$d \equiv 7^{-1} \pmod{20}$

$7 \cdot 3 = 21 \equiv 1 \pmod{20}$

$d = 3$

$C = 2^7 \bmod 33$

$2^5 = 32 \equiv -1 \pmod{33}$

$2^7 = 2^5 \cdot 2^2 \equiv -4 \equiv 29 \pmod{33}$

$C = 29$

(5) סעיף ה (1 נק') נתון N כלשהו. הסבר מדוע $\varphi(N)$ חייב להיות זוגי.

p, q ראשוניים שונים, $N = pq$.

$\varphi(N) = (p-1)(q-1)$

$p-1$ ו־$q-1$ הם מספרים זוגיים (כי p, q אי־זוגיים).

מכפלה של שני מספרים זוגיים היא זוגית.

אחרי $N=3$ שלבים אנחנו מקבלים את הטקס מוצפן

$Y = R_3 L_3$.

דוגמה

נתון | טקסט גלוי $X = 0010111011$.

נתונה פונקציית [illegible]

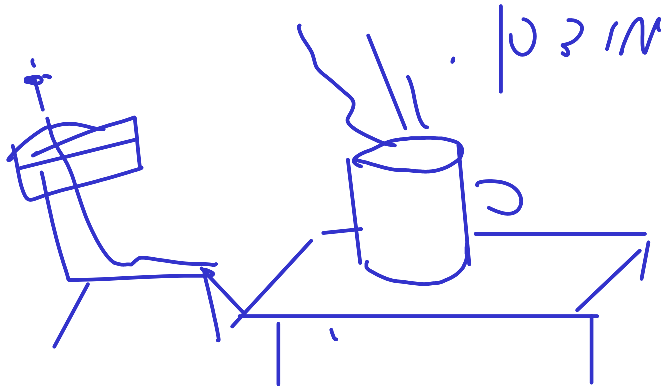
מחרוזת של 5 תווים

$$f(x_1 x_2 x_3 x_4 x_5, \pi) = x_{\pi(1)} x_{\pi(2)} x_{\pi(3)} x_{\pi(4)} x_{\pi(5)}$$

כאשר π התמורה [illegible] $\pi = (1\,3\,5)(2\,4)$.

התזמון מפתחות מוגדר כך: $k_i = \pi^i$ $(i=1,2,3)$.

חשבו את הטקסט מוצפן.



פתרון: שלב 0:

שלב 1: בניית תזמון מפתחות.

יש $N=3$ שלבים. ועבור כל שלב נבנה מפתח.

על פי ההגדרה [illegible]

שלב $i=1$: $k_1 = \pi^1 = \pi$

שלב $i=2$: $k_2 = \pi^2 = \pi \circ \pi$ ← הרכבה של 2 תמורות

$$\pi^2(1)=\pi\circ\pi(1)=\pi(3)=5$$

(#1)

$$\pi^2(1)=\pi(3)=5 \quad \overset{\#1}{=\!=} \quad \pi^2(5)=\pi(1)=3$$
$$\pi^2(2)=\pi(4)=2 \quad \overset{\#1}{=\!=} \quad \pi^2(4)=\pi(2)=4$$
$$\pi^2(3)=\pi(5)=1 \quad \overset{\#1}{=\!=} \quad \pi^2(1)=\pi(3)=5$$

(#2)

$$\pi(1)=3$$
$$\pi(2)=4$$
$$\pi(3)=5$$
$$\pi(4)=2$$
$$\pi(5)=1$$

(#1)

$$\pi = (1\,3\,5)\,(2\,4)$$

i	1	2	3	4	5
$\pi(i)$	3	4	5	2	1

π היא $\quad$ $\pi^3 = \pi\circ\pi\circ\pi = id$ $\quad\leftarrow$ $\quad$ 3 מחזור באורך $\quad$ $i=3$ $\quad$ id

π^4	5	2	1	4	3
7	2	5	4	3	11
5	4	3	2	1	10

$$\pi^3(10) = \pi \circ \pi \circ \pi(10) = \pi(\pi^2(\pi^2(10))) = \pi(\pi^2(5)) = \pi^3(5) = 11$$

$$\pi^3(9) = \pi(\pi^2(\pi^2(9))) = \pi(\pi^2(4)) = \pi^3(4) = 6$$

$$\pi^3(8) = \pi(\pi^2(\pi^2(8))) = \pi(\pi^2(3)) = \pi^3(3) = 10$$

$$\pi^3(7) = \pi(\pi^2(\pi^2(7))) = \pi(\pi^2(2)) = \pi^3(2) = 9$$

$$\pi^3(6) = \pi(\pi^2(\pi^2(6))) = \pi(\pi^2(1)) = \pi^3(1) = 8$$

$$\pi^3(5) = \pi(\pi^2(\pi^2(5))) = \pi(\pi^2(11)) = \pi^3(11) = 1$$

$$\pi^3(4) = \pi(\pi^2(\pi^2(4))) = \pi(\pi^2(6)) = \pi^3(6) = 4$$

$$\pi^3(3) = \pi(\pi^2(\pi^2(3))) = \pi(\pi^2(10)) = \pi^3(10) = 2$$

$$\pi^3(2) = \pi(\pi^2(\pi^2(2))) = \pi(\pi^2(9)) = \pi^3(9) = 7$$

$$\pi^3(1) = \pi(\pi^2(\pi^2(1))) = \pi(\pi^2(7)) = \pi^3(7) = 11$$

$$f_3 = \pi^3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 2 & 5 \end{pmatrix}$$

$$f_2 = \pi^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 1 & 4 & 3 \end{pmatrix}$$

$$f_1 = \pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix} : \text{ص د}$$

$$\boxed{\rho(1) > 0 \quad \text{د}}$$

$$\pi^3(1) = \pi \circ \pi \circ \pi(1) \qquad \text{ا ل ح ل}$$

בכל שלב i אנחנו מבצעים

נוסחאות [illegible] של [illegible] / [illegible]. ←

$$L_i = R_{i-1}$$
$$R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$$

כאשר $f(R_{i-1}, K_i)$ מסמן התמורה של K_i [illegible] R_{i-1}.

שלב $i=1$

$$L_1 = R_0 = 11011$$

$$R_1 = L_0 \oplus f(R_0, K_1)$$

אם $R_0 = 11011$, $K_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix}^{-1}$ אז

$$\begin{matrix} & 1 & 2 & 3 & 4 & 5 \\ R_0 = & 1 & 1 & 0 & 1 & 1 \end{matrix}$$

$$\begin{matrix} & 3 & 4 & 5 & 2 & 1 \\ f(R_0, K_1) = & 0 & 1 & 1 & 1 & 1 \end{matrix}$$

$$R_1 = L_0 \oplus f(R_0, K_1) = (00101) \oplus (01111) = 01010$$

$$L_1 = 11011$$
$$R_1 = 01010$$

שלב $i=2$

$L_2 = R_1$ $\qquad R_2 = L_1 \oplus f(R_1, k_2)$

$L_2 = 01010$

$R_1 = \overset{1}{0}\ \overset{2}{1}\ \overset{3}{0}\ \overset{4}{1}\ \overset{5}{0}$

$k_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 1 & 4 & 3 \end{pmatrix}$

$f(R_1, k_2) = \overset{5}{0}\ \overset{2}{1}\ \overset{1}{0}\ \overset{4}{1}\ \overset{3}{0}$

$R_2 = L_1 \oplus f(R_1, k_2) = (1\ 1\ 0\ 1\ 1) \oplus (0\ 1\ 0\ 1\ 0)$

$= 10001$

$L_2 = 01010$ $\qquad R_2 = 10001$

$i = 3$ אז

$L_3 = R_2 = 10001$ $\qquad R_3 = L_2 \oplus f(R_2, k_3)$

$k_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 2 & 5 \end{pmatrix}$

$R_2 = \overset{1}{1}\ \overset{2}{0}\ \overset{3}{0}\ \overset{4}{0}\ \overset{5}{1}$

$f(R_2, k_3) = \overset{1}{1}\ \overset{4}{0}\ \overset{3}{0}\ \overset{2}{0}\ \overset{5}{1}$

$R_3 = L_2 \oplus f(R_2, k_3) = 01010 \oplus 10001$

$= 11011$ $\qquad L_3 = 10001$ $\qquad R_3 = 11011$

$y = R_3 L_3 = 1101110001$:אז הפלט

!	١	٢	٣	٤	٥
٦	٣	٤	٥	٢	٦
٤٦	٥	٢	١	٤	٣
٦٣	١	٤	٣	٢	٥

$$H_3 = \pi^3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 2 & 5 \end{pmatrix}$$

$$H_2 = \pi^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 1 & 4 & 3 \end{pmatrix}$$

$$H_1 = \pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix} : \text{כך}$$

תרגיל בית 4 / שאלה 1

א. יהי $\pi = (1\ 3\ 5)(2\ 4) \in S_5$. מצאו את π^{-1}, π^2, π^3.

ב. הוכיחו כי π הוא מחזור מאורך 6 ב-S_7, ומצאו את π^{-1}.

שאלה 2 (15 נק')

הוכיחו כי $\mathbb{Z}_{12} \cong \mathbb{Z}_4 \oplus \mathbb{Z}_3$.

$$\varphi(a) = (a \bmod 4,\ a \bmod 3)$$

$$\varphi(0) = (0,0),\ \varphi(1) = (1,1),\ \varphi(2) = (2,2),\ \varphi(3) = (3,0)$$

$$\varphi(4) = (0,1),\ \varphi(5) = (1,2),\ \varphi(6) = (2,0),\ \varphi(7) = (3,1)$$

$$\varphi(8) = (0,2),\ \varphi(9) = (1,0),\ \varphi(10) = (2,1),\ \varphi(11) = (3,2)$$

φ חח"ע ועל, ושומרת פעולה, לכן איזומורפיזם.

$$\mathbb{Z}_{12} \cong \mathbb{Z}_4 \oplus \mathbb{Z}_3$$

$Y = 1101110001$

$R_3 = 11011 \quad L_3 = 10001$

(i = 3 ere Je) : FIN

$R_2 = L_3 = 10001$

$L_2 = R_3 \oplus f(R_2, k_3)$

i = 2 ere Je

$k_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 2 & 5 \end{pmatrix}$

$R_2 = \begin{matrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 0 & 0 & 0 & 1 \\ 1 & 4 & 3 & 2 & 5 \end{matrix}$

$f(R_2, k_3) = 10001$

$L_2 = R_3 \oplus f(R_2, k_3) = 10011 \oplus 10001 = 01010$

$L_2 = 01010 \qquad R_2 = 10001$

i = 1 ere Je

$R_1 = L_2 = 01010 \qquad L_1 = R_2 \oplus f(R_1, k_2)$

$k_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 1 & 4 & 3 \end{pmatrix}$

$R_1 = \begin{matrix} 1 & 2 & 3 & 4 & 5 \\ 0 & 1 & 0 & 1 & 0 \\ 5 & 2 & 1 & 4 & 3 \end{matrix}$

$f(R_1, k_2) = 01010$

$L_1 = R_2 \oplus f(R_1, k_2) = 10001 \oplus 01010 = 11011$

$R_0 = L_1 = 1\ 1\ 0\ 1\ 1$

$L_0 = R_1 \oplus f(R_0, k_1)$

$i = 0$; de

$k_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix}$

$$\begin{array}{rccccc} & 1 & 2 & 3 & 4 & 5 \\ R_0 = & 1 & 1 & 0 & 1 & 1 \\ & 3 & 4 & 5 & 2 & 1 \end{array}$$

$f(R_0, k_1) = 0\ 1\ 1\ 1\ 1$

$L_0 = R_1 \oplus f(R_0, k_1) = 0\ 1\ 0\ 1\ 0 \oplus 0\ 1\ 1\ 1\ 1 = 0\ 0\ 1\ 0\ 1$

$X = L_0 R_0 = 0\ 0\ 1\ 0\ 1\ 1\ 1\ 0\ 1\ 1$

תרגיל בית 5

שאלה 1 (20 נק')

סעיף א' (10 נק')

הוכיחו או הפריכו: קיים $n \in \mathbb{N}$ כך ש-$\varphi(n) = 2^{2025}$.

סעיף ב' (10 נק')

הוכיחו או הפריכו: קיים $n \in \mathbb{N}$ כך ש-$\varphi(n) = n - 2025$.

שאלה 2 (20 נק')

סעיף א' (10 נק')

הוכיחו או הפריכו: קיים $n \in \mathbb{N}$ כך ש-$\varphi(n) = 2^{2025}$.

סעיף ב' (10 נק')

הוכיחו או הפריכו: קיים $n \in \mathbb{N}$ כך ש-$\varphi(n) = n - 2025$.

שאלה 3 (20 נק')

סעיף א' (10 נק')

הוכיחו או הפריכו: קיים $n \in \mathbb{N}$ כך ש-$\varphi(n) = 2^{2025}$.

סעיף ב' (10 נק')

הוכיחו או הפריכו: קיים $n \in \mathbb{N}$ כך ש-$\varphi(n) = n - 2025$.

שאלה 4 (20 נק')

סעיף א' (10 נק')

הוכיחו או הפריכו: קיים $n \in \mathbb{N}$ כך ש-$\varphi(n) = 2^{2025}$.

סעיף ב' (10 נק')

הוכיחו או הפריכו: קיים $n \in \mathbb{N}$ כך ש-$\varphi(n) = n - 2025$.

שאלה 5 (20 נק')

סעיף א' (10 נק')

הוכיחו או הפריכו: קיים $n \in \mathbb{N}$ כך ש-$\varphi(n) = 2^{2025}$.

סעיף ב' (10 נק')

הוכיחו או הפריכו: קיים $n \in \mathbb{N}$ כך ש-$\varphi(n) = n - 2025$.

שאלה 6 (20 נק')

סעיף א' (10 נק')

הוכיחו או הפריכו: קיים $n \in \mathbb{N}$ כך ש-$\varphi(n) = 2^{2025}$.

סעיף ב' (10 נק')

הוכיחו או הפריכו: קיים $n \in \mathbb{N}$ כך ש-$\varphi(n) = n - 2025$.

שאלה 7 (20 נק')

סעיף א' (10 נק')

הוכיחו או הפריכו: קיים $n \in \mathbb{N}$ כך ש-$\varphi(n) = 2^{2025}$.

סעיף ב' (10 נק')

הוכיחו או הפריכו: קיים $n \in \mathbb{N}$ כך ש-$\varphi(n) = n - 2025$.

שאלה 8 (20 נק')

סעיף א' (10 נק')

הוכיחו או הפריכו: קיים $n \in \mathbb{N}$ כך ש-$\varphi(n) = 2^{2025}$.

סעיף ב' (10 נק')

הוכיחו או הפריכו: קיים $n \in \mathbb{N}$ כך ש-$\varphi(n) = n - 2025$.

נשווה בין (*1) לבין (*2) ונקבל כי

$$\phi(pn) = (p-1)\cdot\phi(n).$$

<u>מקרה 2:</u>

אם $p|n$, אזי p מופיע בפירוק לראשוניים של n.

נניח אם $n=p_1^{e_1}p_2^{e_2}p_3^{e_3}\cdots p_k^{e_k}$ אז קיים p_i $(1\le i\le k)$ כך ש $p_i=p$.

ללא הגבלת הכלליות כי $p=p_1$. אזי

$$n=p^{e_1}p_2^{e_2}\cdots p_k^{e_k} \Rightarrow \phi(n)=\left(p^{e_1}-p^{e_1-1}\right)\left(p_2^{e_2}-p_2^{e_2-1}\right)\cdots\left(p_k^{e_k}-p_k^{e_k-1}\right) \text{ —— } (*3)$$

לכן

$$n\cdot p=p^{e_1+1}p_2^{e_2}\cdots p_k^{e_k}$$

$$\Rightarrow \phi(np)=\left(p^{e_1+1}-p^{e_1}\right)\left(p_2^{e_2}-p_2^{e_2-1}\right)\cdots\left(p_k^{e_k}-p_k^{e_k-1}\right)$$

$$=p\left(p^{e_1}-p^{e_1-1}\right)\left(p_2^{e_2}-p_2^{e_2-1}\right)\cdots\left(p_k^{e_k}-p_k^{e_k-1}\right) \text{ —— } (*4)$$

נשווה בין (*3) ו- (*4) ונקבל

$$\phi(np)=p\phi(n).$$

מש"ל