בוקר טוב

תוכנית:

① צופן פייסטל — הצפנה, פענוח

② DES

③ חזרה

הגדרה: צופן פייסטל

נתון טקסט גלוי $X=\{0,1\}^{2n}$, n שלם.

הצפנת פייסטל היא לפי אלגוריתם הבא: טקסט גלוי

① רושמים X בצורה Left ו-Right:

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

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

② בוחרים שלם $N \geq 3$.

③ מגדירים תזמון מפתחות $(K_1, \dots, K_N)$

על פי סדרה של תמורות.

④ בשלב ה- i, לכל $1 \le i \le N$ (בדרך כלל $N=3$)

מבצעים החישוב

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

כאשר f פונקצית הליבה של ההצפנה.

⑤ לאחר N שלבים, מקבלים את הטקסט מוצפן:

$$Y = R_N L_N .$$

למשל: עבור $N=3$ התהליך ההצפנה של טקסט גלוי בינארי הוא כמוסבר למטה:

נתון טקסט גלוי

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

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

<u>שלב $i=1$</u>

$$L_1 = R_0 , \qquad R_1 = L_0 \oplus f(R_0, k_1)$$

כאשר $f(R_0, k_1)$ היא תמורה של התווים של R_0 ע"י התמורה k_1.

<u>שלב $i=2$</u>

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

<u>שלב $i=3$</u>

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

אחרי $N=3$ שלבים אנחנו מקבלים את הטקס

מוצפן

$$Y = R_3 L_3 .$$

דוגמה

נתון טקסט גלוי $X = 0010111011$.

נתונה פונקציית ערבול

מחרוזת של 5 תווים

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

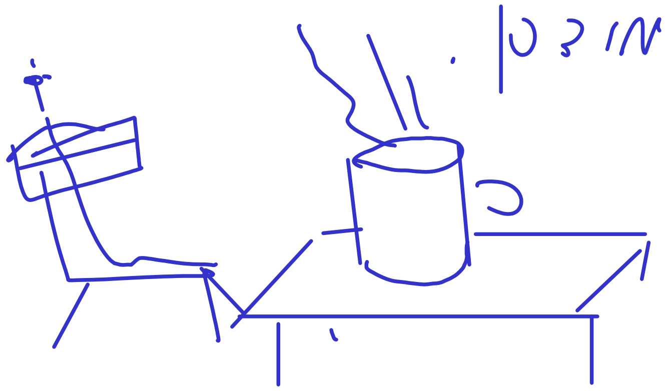
כאשר π היא תמורה [illegible] [illegible] . $\pi = (1\,3\,5)(2\,4)$

ותזמין מפתחות [illegible]: $k_i = \pi^i$ $(i=1,2,3)$.

חשבו את הטקסט מוצפן.

פתרון:

שלב 0:



שלב 1: בניית תזמין מפתחות.

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

על כן והגדרנו

שלב $i=1$ $\quad k_1 = \pi^1 = \pi$

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

לכן $i=3$ $\quad \rho_3 = \pi^3 = \pi \circ \pi \circ \pi$ ← (הרכבה של 3 תמורות

$$\pi = (1\ 3\ 5)(2\ 4)$$: (התמורה ההתחלתית נתונה
נתונה בסימון מעגלי.

נרשום π בסימון שתי-שורות:

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

ל"כ

$$(\#1) \quad \begin{cases} \pi(1) = 3 \\ \pi(2) = 4 \\ \pi(3) = 5 \\ \pi(4) = 2 \\ \pi(5) = 1 \end{cases}$$

נבנה $\pi^2(i) = \pi \circ \pi(i)$

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

נבנה $\pi^3(i)=\pi\circ\pi\circ\pi(i)$

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

לסיכום

i	1	2	3	4	5
π	3	4	5	2	1
π^2	5	2	1	4	3
π^3	1	4	3	2	5

לכן:

$$K_1=\pi=\begin{pmatrix}1&2&3&4&5\\3&4&5&2&1\end{pmatrix}$$
$$K_2=\pi^2=\begin{pmatrix}1&2&3&4&5\\5&2&1&4&3\end{pmatrix}$$
$$K_3=\pi^3=\begin{pmatrix}1&2&3&4&5\\1&4&3&2&5\end{pmatrix}$$

שלב 2 נבצע את השלבים של ההצפנה.

[illegible]

שלב $i=0$

$$X=\underbrace{00101}_{L_0}\underbrace{11011}_{R_0}$$

$L_0=00101$ $\quad$ $R_0=11011$

בכל שלב i אנחנו מבצעים

$$\boxed{\begin{aligned} L_i &= R_{i-1} \\ R_i &= L_{i-1} \oplus f(R_{i-1}, k_i) \end{aligned}}$$

← נוסחאות כלליות של צעד / סיבוב.

כאשר $f(R_{i-1}, k_i)$ מסמן התמורה של k_i המופעלת על R_{i-1}.

<u>שלב $i=1$</u>

$$L_1 = R_0 = 11011$$

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

אם $R_0 = 11011$ $\quad k_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix}^{-1}$ אז

$$\begin{array}{c} \; 1\;2\;3\;4\;5 \\ R_0 = 1\;1\;0\;1\;1 \\ \; 3\;4\;5\;2\;1 \end{array}$$

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

$$R_1 = L_0 \oplus f(R_0, k_1) = (00101) \oplus (01111) = 01010$$

$$L_1 = 11011$$

$$R_1 = 01010$$

<u>שלב $i=2$</u>

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

$L_2 = 01010$

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

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

$$\begin{array}{ccccccc} & & 5 & 2 & 1 & 4 & 3 \\ f(R_1, k_2) & = & 0 & 1 & 0 & 1 & 0 \end{array}$$

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

$$= 1\,0\,0\,0\,1$$

$L_2 = 01010 \qquad R_2 = 10001$

שלב $i = 3$

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

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

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

$$\begin{array}{ccccccc} & & 1 & 4 & 3 & 2 & 5 \\ f(R_2, k_3) & = & 1 & 0 & 0 & 0 & 1 \end{array}$$

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

$$= 11011$$

$L_3 = 10001 \qquad R_3 = 11011$

$Y = R_3 L_3 = 11011\ 10001$ תשובה סופית:

דוגמה: נתון הטקסט מוצפן $Y = 1101110001$

ונתון התזמון מפתחות

$K_1 = \pi$

$K_2 = \pi^2$

$K_3 = \pi^3$

כאשר המפתח ההתחלתי הוא $\pi = (1\ 3\ 5)(2\ 4)$.

חשבו את הטקסט הגלוי.

פתרון

הנוסחאות של פענוח של צופן פייסטל:

$$\boxed{\begin{aligned} R_i &= L_{i+1} \\ L_i &= R_{i+1} \oplus f(R_i, K_{i+1}) \end{aligned}}$$

בפענוח [illegible] מתחילים בשלב $N=3$ ועוברים הפוך.

והתזמון מפתחות כבר בנינו בקודמו

[illegible]:

תזמון מפתחות

i	1	2	3	4	5
π	3	4	5	2	1
π^2	5	2	1	4	3
π^3	1	4	3	2	5

לכן:

$K_1 = \pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix}$

$K_2 = \pi^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 1 & 4 & 3 \end{pmatrix}$

$K_3 = \pi^3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 2 & 5 \end{pmatrix}$

פענוח: (של $i=3$)

$$\cancel{\boxed{Y = \underbrace{11011}_{}\underbrace{10001}_{} \quad L_3 = 11011 \quad R_3 = 10001}}$$

לא נכון

$$\boxed{Y = \underbrace{11011}_{}\underbrace{10001}_{} \quad R_3 = 11011 \quad L_3 = 10001}$$

נכון

של $i=2$

$R_2 = L_3 = 10001$

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

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

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

$f(R_2, k_3) = 10001$

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

$L_2 = 01010 \qquad R_2 = 10001$

של $i=1$

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

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

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

$f(R_1, k_2) = 01010$

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

$i = 0 \Rightarrow$ de

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

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

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

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

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

$L_0 = R_1 \oplus f(R_0, k_1) = 01010 \oplus 01111 = 00101$

$$\boxed{X = L_0 R_0 = 0010111011}$$

תרגול.

תרגיל: (הוכחה)

אם ϕ היא פונקציית אוילר, n מספר שלם ו-p מספר ראשוני. $p>n$. אז:

$$\phi(pn) = \begin{cases} (p-1)\phi(n) & \text{אם } p \nmid n \\ p\,\phi(n) & \text{אם } p \mid n \end{cases}$$

תזכורת: ϕ היא פונקציית אוילר שמוגדרת

$\phi(a) =$ "מספר השלמים $1 \le b < a$ כך ש $\gcd(a,b)=1$".

נוסחה ל $\phi(a)$

אם הפירוק לראשוניים של a הוא: $a = p_1^{e_1} \cdot p_2^{e_2} \cdots p_k^{e_k}$

אז $\phi(a) = (p_1^{e_1} - p_1^{e_1-1})(p_2^{e_2} - p_2^{e_2-1}) \cdots (p_k^{e_k} - p_k^{e_k-1})$

מקרה 1: נניח $p \nmid n$. אם הפירוק לראשוניים של n הוא

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k} \Rightarrow \phi(n) = (p_1^{e_1} - p_1^{e_1-1}) \cdots (p_k^{e_k} - p_k^{e_k-1})$$

אז הפירוק לראשוניים של pn הוא

$$pn = p \cdot p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}.$$

$$= p^1 p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k} \Rightarrow \phi(pn) = (p^1 - p^0)(p_1^{e_1} - p_1^{e_1-1}) \cdots (p_k^{e_k} - p_k^{e_k-1})$$

$$\Rightarrow \phi(pn) = (p-1)\,\phi(n)$$

מקרה 2: אם $p|n$, אז p מופיע בפירוק לגורמים של n.

$$n = p_1^{e_1} p_2^{e_2} p_3^{e_3} \cdots p_k^{e_k} \Rightarrow \phi(n) = \left(p_1^{e_1} - p_1^{e_1-1}\right)\cdots\left(p_k^{e_k} - p_k^{e_k-1}\right)$$

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

$$\Rightarrow p\cdot n = p\cdot p_1^{e_1} p_2^{e_2} p_3^{e_3} \cdots p_k^{e_k}$$

כיוון ש $p|n$ אז $p=p_i$ בפירוק לגורמים של n.

ללא הגבלת הכלליות, נניח ש $p=p_1$,

$$p\cdot n = p_1^{e_1+1} p_2^{e_2} p_3^{e_3} \cdots p_k^{e_k}$$

$$\begin{aligned}
\phi(pn) &= \left(p_1^{e_1+1} - p_1^{e_1}\right)\left(p_2^{e_2} - p_2^{e_2-1}\right)\cdots\left(p_k^{e_k} - p_k^{e_k-1}\right)\\
&= p_1\left(p_1^{e_1} - p_1^{e_1-1}\right)\left(p_2^{e_2} - p_2^{e_2-1}\right)\cdots\left(p_k^{e_k} - p_k^{e_k-1}\right)\\
&= p_1\,\phi(n)\\
&= p\,\phi(n).
\end{aligned}$$

$$\phi(pn) = (p^1 - p^0)\underbrace{(p_1^{e_1} - p_1^{e_1 - 1})(p_2^{e_2} - p_2^{e_2 - 1})\cdots(p_k^{e_k} - p_k^{e_k - 1})}_{\phi(n)}$$

$$= (p-1)\,\phi(n)$$