

## תוכן העניינים

4	1	תורת המספרים
6	2	חוגים
7	3	כפni בסיסים
8	4	צופן RSA
9	5	צופן ElGamal
9	6	צופן אינגרה
11	7	תורת שאנו וסודיות מושלמות
12	8	צופן פיסטול
13	9	צופן IDEA
14	10	DES

## 1 תורת המספרים

$a \equiv b \pmod{m}$   $\iff m | a - b \iff a = qm + b$  אם ורק אם קיימים שלם  $q$  כך ש  $a = qm$  ו  $r$  ש  $m | a - qb$  ו  $0 \leq r < |b|$ .  
 קיימים שלם  $q$  כך ש:  $a = qb + r$ ,  $0 \leq r < |b|$ .

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

$$x = a \bmod b \quad \text{ו-} \quad q = \left\lfloor \frac{a}{b} \right\rfloor.$$

**האלגוריתם של אוקלידס:** לכל זוג שלמים חיוביים  $a, b$  עבורם  $a \geq b$  האלגוריתם הבא נותן את  $\gcd(a, b)$ .

### האלגוריתם של אוקלידס 1

```

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

```

שלב	$q_n$	$r_n$
$n = 1$	$q_1 = \left\lfloor \frac{r_0}{r_1} \right\rfloor$	$r_2 = r_0 - q_1 r_1$
$n = 2$	$q_2 = \left\lfloor \frac{r_1}{r_2} \right\rfloor$	$r_3 = r_1 - q_2 r_2$
$\vdots$		
$n - 1$	$q_{n-1} = \left\lfloor \frac{r_{n-2}}{r_{n-1}} \right\rfloor$	$r_n = r_{n-2} - q_{n-1} r_{n-1}$
$n$	$q_n = \left\lfloor \frac{r_{n-1}}{r_n} \right\rfloor$	$r_{n+1} = r_{n-1} - q_n r_n$

**משפט ב'ו:** לכל זוג שלמים  $a, b$  קיימים שלמים  $s, t$  כך ש:  
 $sa + tb = d$ ,  $d = \gcd(a, b)$ .

בהתנן  $0 \leq b \leq a$  האלגוריתם המוכלל של אוקלידס נותן את השלמים  $(s, t, d)$  בפרק (s, t, d) באופן הבא:

### האלגוריתם המוכלל של אוקלידס 2

```

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

```

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

שני מספרים שלמים  $a, b$  נקראים **מספרים זרים** אם  $\gcd(a, b) = 1$

**משפט הפירוק הראשוניים:**

לכל שלם חייבי  $m$  קיים מספרים ראשוניים  $p_1, p_2, \dots, p_n$  ושלם אי-שליליים  $e_1, \dots, e_n$  כך שניתן לרשום  $m$  כפирוק לראשוניים בצורה הבאה:

$$m = p_1^{e_1} \times p_2^{e_2} \dots p_n^{e_n}.$$

**פונקציית אוילר:**

אם הפירוק לראשוניים של מספר שלם  $m$  הוא  $m = \prod_{i=1}^n p_i^{e_i}$ , אז המספר של שלים אשר זרים ביחס ל-  $m$  וקטן ממנו ניתן על ידי הנוסחה

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

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

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

$$\phi(s \cdot t) = \phi(s)\phi(t).$$

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

אם  $p$  מספר ראשוני אז:אם  $p$  מספר ראשוני אז:אם  $s, t$  שלמים זרים (כלומר  $\gcd(s, t) = 1$ ) אז:אם  $p$  ו-  $q$  מספרים ראשוניים שונים אז:**משפט הקטן של פרמה:**אם  $p$  מספר ראשוני אז לכל  $a$  שלם התנאים הבאים מתקיימים:

$$a^p \equiv a \pmod{p}, \quad a^{p-1} \equiv 1 \pmod{p}, \quad a^{-1} \equiv a^{p-2} \pmod{p}.$$

.  $a^{-1} \equiv a^{\phi(n)-1} \pmod{n}$  וגם  $a^{\phi(n)} \equiv 1 \pmod{n}$  וגם  $\gcd(a, n) = 1$   $a \in \mathbb{Z}_n$  ו-  $a$  שלם חיובי ו-**משפט השארות הסיני:** יהי  $m_1, \dots, m_r$  שלמים זרים בזוגות ו-  $a_1, \dots, a_r$  שלמים. אז למערכת

$$x \equiv a_1 \pmod{m_1}$$

$$x \equiv a_2 \pmod{m_2}$$

⋮

$$x \equiv a_r \pmod{m_r}$$

קיים פתרון ייחיד מודולו  $M = m_1 m_2 \dots m_r$  שהוא

$$x \equiv \sum_{i=1}^r a_i M_i y_i \pmod{M}$$

$$\text{כאשר } 1 \leq i \leq r \text{ ו- } y_i = M_i^{-1} \pmod{m_i} \text{ ו- } M_i = \frac{M}{m_i}$$

**2 חוגים**

$\mathbb{Z}_m \triangleq \{0, 1, \dots, m-1\}$  החוג  $\mathbb{Z}_m$  מוגדר כך:  $a \equiv b \pmod{m}$  לכל שלם  $b$  נתאים איבר  $a \in \mathbb{Z}_m$  לפי התנאי:

**איבר הופכי של איבר חוג:**

לכל  $a \in \mathbb{Z}_m$  אם קיים שלם  $x$  כך ש:  $ax \equiv 1 \pmod{m}$  אז אומרים כי  $x$  האיבר הופכי של  $a$  ב-  $\mathbb{Z}_m$ . מסומן  $a^{-1} \in \mathbb{Z}_m$ .

תנאי לקיים איבר הופכי בחוג: נתון  $a \in \mathbb{Z}_m$  קיים איבר הופכי  $a^{-1}$  אם ורק אם  $\gcd(a, m) = 1$ .

הקובקטור ה-  $j$  של מטריצה  $A$  שווה ל determinant המטריצה המתכת אחריו מהיקת שורת  $i$  ועומודת:

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1j} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2j} & \dots & a_{2n} \\ \vdots & \vdots & & \vdots & & \vdots \\ a_{i1} & a_{i2} & \dots & a_{ij} & \dots & a_{in} \\ \vdots & \vdots & & \vdots & & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nj} & \dots & a_{nn} \end{pmatrix} \Rightarrow C_{ij} = (-1)^{i+j} \begin{vmatrix} a_{11} & a_{12} & \dots & a_{1j} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2j} & \dots & a_{2n} \\ \vdots & \vdots & & \vdots & & \vdots \\ a_{i1} & a_{i2} & \dots & a_{ij} & \dots & a_{in} \\ \vdots & \vdots & & \vdots & & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nj} & \dots & a_{nn} \end{vmatrix}$$

מטריצת הקופקטוריים של מטריצה  $A$  היא המטריצה שבהרכיב ה-  $ij$  הוא הקופקטור ה-  $ij$  של  $A$ :

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

$$A^{-1} = (\det A)^{-1} C^t$$

איברים הפיכים ב-  $\mathbb{Z}_{26}$ :

$a$	1	3	5	7	9	11	15	17	19	21	23	25
$a^{-1}$	1	9	21	15	3	19	7	23	11	5	17	25

**3 צפני בסיסיים**

ערכים הקריפטוגרפיים של האותיות:

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

לוח הכפל של:

$m$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$26 \times m$	26	52	78	104	130	156	182	208	234	260	286	312	338	364	390
$m$	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
$26 \times m$	416	442	468	494	520	546	572	598	624	650	676	702	728	754	780

## כפניות בסיסיות:

מפתח	כלל מפענה	כלל מצפין	צופן
$k \in \mathbb{Z}_{26}$	$d_k(x) = x - k \bmod 26$	$e_k(x) = x + k \bmod 26$	קיסר
$m$ תמורה של אורך $\pi$	$d_\pi(y_1 \dots y_m) = y_{\pi^{-1}(1)} \dots y_{\pi^{-1}(m)} \bmod 26$	$e_\pi(x_1 \dots x_m) = x_{\pi(1)} \dots x_{\pi(m)} \bmod 26$	תמורה
26 תמורה של אורך $\pi$	$d_\pi(y) = \pi^{-1}(y) \bmod 26$	$e_\pi(x) = \pi(x) \bmod 26$	החלפה
$k = (a, b)$ , $\gcd(a, 26) = 1$ .	$d_k(y) = a^{-1}(y - b) \bmod 26$	$e_k(x) = (ax + b) \bmod 26$	אפיינית
$k = (k_1, \dots, k_m) \in \mathbb{Z}_{26}^m$	$d_k(y_1, \dots, y_m) = (y_1 - k_1, \dots, y_m - k_m) \bmod 26$	$e_k(x_1, \dots, x_m) = (x_1 + k_1, \dots, x_m + k_m) \bmod 26$	ויז'ור
$k \in \mathbb{Z}_{26}^{m \times m}$ $\gcd(\det(k), 26) = 1$ .	$d_k(y_1 \dots y_m) = (y_1 \dots y_m) \cdot k^{-1} \bmod 26$	$e_k(x_1 \dots x_m) = (x_1 \dots x_m) \cdot k \bmod 26$	היל

## 4 צופן RSA

- מפתח ציבורי:  $(b, n)$  כאשר  $pq = n$  כאשר  $p, q$  מספרים ראשוניים שונים.
- מפתח סודי:  $(a, p, q)$  כאשר  $(a, p, q) \equiv b^{-1} \pmod{\phi(n)}$  כאשר  $\phi(n)$  הפונקציה אוילר של  $n$ .
- $\phi(n) = \phi(pq) = (p-1)(q-1)$  כאשר  $p, q$  מספרים שלמים אז  $a \equiv b^{-1} \pmod{(p-1)(q-1)}$  לכן:  $a \equiv b^{-1} \pmod{(p-1)(q-1)}$
- כלל מצפין:  $e_k(x) = x^b \bmod n$  לכל מספר שלם  $x$ .
- כלל מפענה:  $d_k(y) = y^a \bmod n$  לכל מספר שלם  $y$ .

שיטת הריבועים לחישוב חזקה מודולרית:  
בහינתו  $n$  המקיימים  $y = x^b \bmod n$  יי'  $y = x^b \bmod p$  ו  $y = x^b \bmod q$ . אז קיים אלגוריתם הנקרא שיטת הריבועים לשונון ערך של  $y$  באופן הבא:

## האלגוריתם שיטת הריבועים 3

```

1: Input: Integers  $x, b_0, \dots, b_k, n$  .
2:  $i \leftarrow 1$ 
3:  $z_0 \leftarrow x$ 
4: while  $i \leq k$  do
5:    $z_i \leftarrow z_{i-1}^2 \bmod n$ 
6: end while
7:  $i \leftarrow 0$ 
8:  $y \leftarrow 1$ 
9: while  $i \leq k$  do
10:  if  $b_i = 1$  then
11:     $y \leftarrow z_i y \bmod n$ 
12:  end if
13: end while
14: return:  $y$             $\triangleright y = x^b \bmod n$ 

```

האלגוריתם פונCTION צופן RSA :

האלגוריתם הבא נותן את הפתרון  $x$  של הכלל מפענה  $x = y^a \bmod n$  לפי השלבים הבאים:

$$x_1 = (y \bmod p)^{a \bmod (p-1)} \bmod p.$$

שלב [1] מחשבים  $a \bmod (p-1)$  ו-  $y \bmod p$  ואז מחשבים

$$x_2 = (y \bmod q)^{a \bmod (q-1)} \bmod q.$$

שלב [2] מחשבים  $a \bmod (q-1)$  ו-  $y \bmod q$  ואז מחשבים

$$\begin{cases} x = x_1 \bmod p \\ x = x_2 \bmod q \end{cases}$$

שלב [3] בעזרת המשפט השאריות והסני פותרים את המערכת

## 5 צופן ElGamal

- המפתח הוא  $k = (p, a, \alpha, d)$  כאשר:
  - $p$  מספר ראשוני
  - $a, d, \alpha$  מספרים שלמים חיוביים עבורם  $2 \leq a, d, \alpha \leq p-2$
  - $\beta \equiv \alpha^a \pmod{p}$
- כלל מצפין:  $y_1 = \alpha^d \pmod{p}$ ,  $y_2 = x\beta^d \pmod{p}$  לכל  $x$ שלם חיובי.
- כלל מפענה:  $x = (y_1^a)^{-1} y_2 \pmod{p}$  לכל שלמים חיוביים  $y_1, y_2$

## 6 צופן אניגמה

- תמורה על קבוצה סופית  $\Sigma = \{x_1, \dots, x_n\}$  היא פונקציה  $\pi: \Sigma \rightarrow \Sigma$  חד-חד ערכית ו"על"  $\Sigma$ .
- על  $\Sigma$ : לכל  $y \in \Sigma$  קיים  $x \in \Sigma$  כך ש:  $y = \pi(x)$
  - חד-חד-ערכית: לכל  $x, y \in \Sigma$  מתקיים  $x \neq y \Rightarrow \pi(x) \neq \pi(y)$ .

התמורה הזזה מסומנת  $\Sigma \rightarrow \Sigma$  :  $\text{id}(x) = x$  :  $x \in \Sigma$  ומודדרת כך לכל  $\pi$  תמורה הופכית  $\Sigma \rightarrow \Sigma$  על הקבוצה  $\Sigma$ , התמורה ההופכית מסומנת  $\pi^{-1}$  מקיימת את התנאי:  
 $\forall x \in \Sigma \quad \pi\pi^{-1}(x) = x = \pi^{-1}\pi(x)$ .

תמורה  $\Sigma \rightarrow \Sigma$  היא **תמורה משקפת** אם התנאי הזה מתקיים:  
 $\forall x, y \in \Sigma : \rho(x) = y \iff \rho(y) = x$ .

**הgelglis ומשקף הקבוצה של צופן אניגמה:**

$x$	$A$	$B$	$C$	$D$	$E$	$F$	$G$	$H$	$I$	$J$	$K$	$L$	$M$	$N$	$O$	$P$	$Q$	$R$	$S$	$T$	$U$	$V$	$W$	$X$	$Y$	$Z$
$\alpha_1(x)$	$E$	$K$	$M$	$F$	$L$	$G$	$D$	$Q$	$V$	$Z$	$N$	$T$	$O$	$W$	$Y$	$H$	$X$	$U$	$S$	$P$	$A$	$I$	$B$	$R$	$C$	$J$
$\alpha_2(x)$	$A$	$J$	$D$	$K$	$S$	$I$	$R$	$U$	$X$	$B$	$L$	$H$	$W$	$T$	$M$	$C$	$Q$	$G$	$Z$	$N$	$P$	$Y$	$F$	$V$	$O$	$E$
$\alpha_3(x)$	$B$	$D$	$F$	$H$	$J$	$L$	$C$	$P$	$R$	$T$	$X$	$V$	$Z$	$N$	$Y$	$E$	$I$	$W$	$G$	$A$	$K$	$M$	$U$	$S$	$Q$	$O$
$\rho(x)$	$Y$	$R$	$U$	$H$	$Q$	$S$	$L$	$D$	$P$	$X$	$N$	$G$	$O$	$K$	$M$	$I$	$E$	$B$	$F$	$Z$	$C$	$W$	$V$	$J$	$A$	$T$

**כל מצפין וכל מפענה של צופן אניגמה:**

- בහינתן מילה  $x_1x_2 \dots x_k$  של טקסט גלי, הכלל מצפין של האות  $-i$  הוא:  
 $e(x_i) = \Delta_i(x_i)$  כאשר  $\Delta_i$  היא התמורה כתובה למורה.

- בහינתן מילה  $y_1y_2 \dots y_k$  של טקסט מופען הכלל מפענה של האות  $-i$  הוא:  
 $d(y_i) = \Delta_i(y_i)$  כאשר  $\Delta_i$  מפענה של צופן אניגמה.

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

כאשר

- היא התמורה המשקפת הקבואה של צופן אניגמה,

•

$$\tau_i = \sigma_{-i} \alpha_3 \sigma_i \alpha_2 \alpha_1 \pi , \quad \tau_i^{-1} = \pi \alpha_1^{-1} \alpha_2^{-1} \sigma_{-i} \alpha_3^{-1} \sigma_i$$

כאשר  $\alpha_1, \alpha_2, \alpha_3$  הן התמורות של הgelglis של צופן אניגמה הנחות בטבלה לעיל,  $\pi$  היא התמורה המשקפת המותנה,

- היא התמורה ה- $i$  אותיות קדימה באלבפתית:  
 $\sigma_i(x) = x + i \bmod 26$
- היא התמורה ה- $i$  אותיות אחריה באלבפתית:  
 $\sigma_{-i}(x) = x - i \bmod 26$

**מילה משוכפלת** היא מילה סימטרית של טקסט גלי באורך 6 אותיות מהצורה:

$$xyzxyz .$$

**מילה אופיינית** היא ההצפנה של מילה משוכפלת "xyzxyz" צופן אניגמה:

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

**משפט ריבסקי I:** יהי  $\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5\sigma_6$  מילה אופיינית של צופן האניגמה. אז:

$$\sigma_4 = \Delta_4\Delta_1(\sigma_1) , \quad \sigma_5 = \Delta_5\Delta_2(\sigma_2) , \quad \sigma_6 = \Delta_6\Delta_3(\sigma_3) .$$

**משפט ריבסקי II:**

עבור כל אחת של התמורות  $\Delta_6\Delta_3, \Delta_5\Delta_2, \Delta_4\Delta_1$  של צופן אניגמה, קיים סידור של הפירוק לראשונים שנקרה סדר ריבסקי כך שהתנאים הבאים מתקיימים:

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

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

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

## 7 תורת שאנו וסודות מושלמת

הסתברויות של האותיות:

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

קבוצות תדיירות של האותיות בטקסט:

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

זוגות האותיות הנפוצים ביותר:

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

שלשות של אותיות הנפוצים ביותר:

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

$$I_X(x) = -\log_2(P_X(x)) .$$

$$H[X] = -\sum_{i=1}^N P_X(x_i) \log_2(P_X(x_i)) .$$

מידע של מ"מ בדיד  $X$ :

אנטロפייה של מ"מ בדיד  $X$ :

נטוחת ביביס:

$$P(X=x|Y=y)P(Y=y) = P(X=x \cap Y=y) = P(Y=y|X=x)P(X=x) .$$

סודיות:  
נתונה קרייטו-מערכת בעלת קבוצת טקסט גלי  $X$ , קבוצת טקסט מופען  $Y$  וקבוצת מפתחות  $K$ , כל מצפין  $.x = d_k(y) = e_k(x)$

$$P(Y = y) = \sum_{k \in K} P(K = k) P(X = d_k(y)) ,$$

$$P(Y = y|X = x) = \sum_{\substack{k \in K \\ x = d_k(y)}} P(K = k) ,$$

$$P(X = x) \sum_{\substack{k \in K \\ x = d_k(y)}} P(K = k)$$

$$P(X = x|Y = y) = \frac{P(X = x) \sum_{\substack{k \in K \\ x = d_k(y)}} P(K = k)}{\sum_{k \in K} P(K = k) P(X = d_k(y))} .$$

**סודיות מושלמת:** לкриpto-מערכת יש סודיות מושלמת אם התנאי הבא מתקיים:

$$P(X = x|Y = y) = P(X = x) \iff P(Y = y|X = x) = P(Y = y) .$$

אנטropy מותנית:

$$H(X|Y = y) = - \sum_{x \in X} P(X = x|Y = y) \log_2 P(X = x|Y = y) ,$$

$$H(X|Y) = - \sum_{y \in Y} \sum_{x \in X} P(Y = y) P(X = x|Y = y) \log_2 P(X = x|Y = y) ,$$

$$H(X, Y) = H(Y) + H(X|Y) , \quad H(X|Y) \leq H(X) .$$

**משפט האנטרופיה לкриpto-מערכת:**

$$H(K|C) = H(K) + H(P) - H(C) .$$

טבלת אמת:

$p$	$q$	$p \wedge q$	$p \vee q$	$\sim p$	$p \oplus q$
1	1	1	1	0	0
1	0	0	1	0	1
0	1	0	1	1	1
0	0	0	0	1	0

## 8 צופן פיסטול

**ספרות הקסדצימליות:**

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

**משוואות פיסטול להצפנה:**

נתון טקסט גליי  $x = L_0 R_0$  לכל  $1 \leq i \leq N$ .

$$L_i = R_{i-1} , \quad R_i = L_{i-1} \oplus f(R_{i-1}, k_i) , \quad y = R_N L_N .$$

$$\begin{aligned} \text{משוואות פיסטול לפענוח:} \\ \text{נתון טקסט גליי } y = R_N L_N . \text{ לכל } 1 \leq i \leq N . \\ R_i = L_{i+1} , \quad L_i = R_{i+1} \oplus f(R_i, k_{i+1}) , \quad x = L_0 R_0 . \end{aligned}$$

## 9 צופן IDEA

זמן מפתח של IDEA

$r$	$k_1$	$k_2$	$k_3$	$k_4$	$k_5$	$k_6$
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 הצפנה IDEA

- נתון טקסט גליי  $P \in \{0, 1\}^{64}$ . של אורך 64 ביטים.
- מחלקיים  $P$  ארבע בלוקים  $P_i \in \{0, 1\}^{16}$ :  $P = P_1 P_2 P_3 P_4$
- בתחלת מחזור ה-  $r$  ( $1 \leq r \leq 9$ ) מסמנים את הטקסט מוצפן מותקבל ממחזור הקודם (מחזור  $r-1$ ) ב-  $C^{(1)} = X$ , מלבד מ-

כל מחזור  $r$  מורכב מהשלבים הבאים:

$$Y_1 = C_1^{(r)} \odot k_1^{(r)} = C_1^{(r)} \cdot k_1^{(r)} \pmod{(2^{16} + 1)} \quad [1]$$

$$Y_2 = C_2^{(r)} \boxplus k_2^{(r)} = C_2^{(r)} + k_2^{(r)} \pmod{2^{16}} \quad [2]$$

$$Y_3 = C_3^{(r)} \boxplus k_3^{(r)} = C_3^{(r)} + k_3^{(r)} \pmod{2^{16}} \quad [3]$$

$$Y_4 = C_4^{(r)} \odot k_4^{(r)} = C_4^{(r)} \cdot k_4^{(r)} \pmod{(2^{16} + 1)} \quad [4]$$

$$Y_5 = Y_1 \oplus Y_3 \quad [5]$$

$$Y_6 = Y_2 \oplus Y_4 \quad [6]$$

$$Y_7 = Y_5 \odot k_5^{(r)} = Y_5 \cdot k_5^{(r)} \pmod{(2^{16} + 1)} \quad [7]$$

$$Y_8 = Y_6 \boxplus Y_7 = Y_6 + Y_7 \pmod{2^{16}} \quad [8]$$

$$Y_9 = Y_8 \odot k_6^{(r)} = Y_8 \cdot k_6^{(r)} \pmod{2^{16} + 1} \quad [9]$$

$$Y_{10} = Y_7 \boxplus Y_9 = Y_7 + Y_9 \pmod{2^{16}} \quad [10]$$

$$C_1^{(r+1)} = Y_1 \oplus Y_9 \quad [11]$$

$$C_2^{(r+1)} = Y_3 \oplus Y_9 \quad [12]$$

$$C_3^{(r+1)} = Y_2 \oplus Y_{10} \quad [13]$$

$$C_4^{(r+1)} = Y_4 \oplus Y_{10} \quad [14]$$

- בכדי לקבל את הטקסט מוצפן הסופי, אחרי ביצוע של כל המוחזרים  $r$  מבצעים את השלב התפקיד:

$$C_1 = C_1^{(9)} \odot k_1^{(9)} = C_1^{(9)} \cdot k_1^{(9)} \pmod{2^{16} + 1}$$

[1]

$$C_2 = C_3^{(9)} \boxplus k_2^{(9)} = C_3^{(9)} + k_2^{(9)} \pmod{2^{16}}$$

[2]

$$C_3 = C_2^{(9)} \boxplus k_3^{(9)} = C_2^{(9)} + k_3^{(9)} \pmod{2^{16}}$$

[3]

$$C_4 = C_4^{(9)} \odot k_4^{(9)} = C_4^{(9)} \cdot k_4^{(9)} \pmod{2^{16} + 1}$$

[4]

- לבסוף הטקסט מוצפן -64 ביטים מתקבל מהארבע בלוקים 16- ביטים

$$.C = C_1 C_2 C_3 C_4$$

### מפתחות פענו של IDEA

$$\begin{aligned} DK_1^{(1)} &= \left(K_1^{(9)}\right)^{-1}, & DK_2^{(1)} &= -\left(K_2^{(9)}\right), & DK_3^{(1)} &= -\left(K_3^{(9)}\right), & DK_4^{(1)} &= \left(K_4^{(9)}\right)^{-1}, \\ DK_5^{(1)} &= K_5^{(8)}, & DK_6^{(1)} &= K_6^{(8)}. \end{aligned}$$

## 10 צופן DES

**אלגוריתם הצפנה DES :** נתון טקסט גלי 64 ביטים

**שלב [1] מוצעים IP** כאשר IP( $x_1, x_2, \dots, x_{64}$ ) התמורה התחלה:

$$IP = \begin{pmatrix} 58 & 50 & 42 & 34 & 26 & 18 & 10 & 2 & 60 & 52 & 44 & 36 & 28 & 20 & 12 & 4 \\ 62 & 54 & 46 & 38 & 30 & 22 & 14 & 6 & 64 & 56 & 48 & 40 & 32 & 24 & 16 & 8 \\ 57 & 49 & 41 & 33 & 25 & 17 & 9 & 1 & 59 & 51 & 43 & 35 & 27 & 19 & 11 & 3 \\ 61 & 53 & 45 & 37 & 29 & 21 & 13 & 5 & 63 & 55 & 47 & 39 & 31 & 23 & 15 & 7 \end{pmatrix}$$

**שלב [2] מחלקים IP(x) לשניים.** כאשר  $L_0 = IP(x)$  ביטים הראשוניים של  $x_0$  ו- 32 האחרונים:

$$\begin{aligned} L_0 &= x_{58}, x_{50}, x_{42}, x_{34}, x_{26}, x_{18}, x_{10}, x_2, x_{60}, x_{52}, x_{44}, x_{36}, x_{28}, x_{20}, x_{12}, x_4 \\ &\quad x_{62}, x_{54}, x_{46}, x_{38}, x_{30}, x_{22}, x_{14}, x_6, x_{64}, x_{56}, x_{48}, x_{40}, x_{32}, x_{24}, x_{16}, x_8, , \end{aligned}$$

$$\begin{aligned} R_0 &= x_{57}, x_{49}, x_{41}, x_{33}, x_{25}, x_{17}, x_9, x_1, x_{59}, x_{51}, x_{43}, x_{35}, x_{27}, x_{19}, x_{11}, x_3 \\ &\quad x_{61}, x_{53}, x_{45}, x_{37}, x_{29}, x_{21}, x_{13}, x_5, x_{63}, x_{55}, x_{47}, x_{39}, x_{31}, x_{23}, x_{15}, x_7 . \end{aligned}$$

**שלב [3] מוצעים 16 מוחזרים של אלגוריתם פיסטל:**

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

כאשר  $k_1, \dots, k_{16}$  תת-מפתחות כל אחד 48 ביטים שmotkbelim מפתחת התחלה:  $.k$

**שלב [4] IP<sup>-1</sup>** IP( $R_{16}L_{16}$ ) כאשר IP<sup>-1</sup>( $R_{16}L_{16}$ ) התמורה ההפוכה:

$$IP^{-1} = \begin{pmatrix} 40 & 8 & 48 & 16 & 56 & 24 & 64 & 32 & 39 & 7 & 47 & 15 & 55 & 23 & 63 & 31 \\ 38 & 6 & 46 & 14 & 54 & 22 & 62 & 30 & 37 & 5 & 45 & 13 & 53 & 21 & 61 & 29 \\ 36 & 4 & 44 & 12 & 53 & 20 & 60 & 28 & 35 & 3 & 43 & 11 & 51 & 19 & 59 & 27 \\ 34 & 2 & 42 & 10 & 50 & 18 & 58 & 26 & 33 & 1 & 41 & 9 & 49 & 17 & 57 & 25 \end{pmatrix}$$

### הפונקציית ליבנה של DES

$$f : \{0,1\}^{32} \times \{0,1\}^{48} \rightarrow \{0,1\}^{32}.$$

נסמן הארוגומנטים של  $f$  ב-  $J \in \{0,1\}^{48}, A \in \{0,1\}^{32}$  כאשר  $f(A, J)$  מותוארת על ידי האלגוריתם הבא:

$$E = \begin{pmatrix} 32 & 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 6 & 7 & 8 & 9 \\ 8 & 9 & 10 & 11 & 12 & 13 \\ 12 & 13 & 14 & 15 & 16 & 17 \\ 16 & 17 & 18 & 19 & 20 & 21 \\ 20 & 21 & 22 & 23 & 24 & 25 \\ 24 & 25 & 26 & 27 & 28 & 29 \\ 28 & 29 & 30 & 31 & 32 & 1 \end{pmatrix}$$

**שלב [1]** מדילים  $A$  לרץ 48 ביטים באמצעות התמורה והגדלה  
שלב [2] מחשבים  $E(A) \oplus J$  ורושמים התשובה כシリור של שמונה רצפים 6 ביטים:  
 $B = B_1 B_2 B_3 B_4 B_5 B_6 B_7 B_8$ ,  $B_j \in \{0,1\}^6$ .

**שלב [3]** רושמים  $B_j = b_1 b_2 b_3 b_4 b_5 b_6$  כאשר

**שלב [4]** בשלב זה משתמשים החחלפות  $S_1, \dots, S_8$ . כל  $S_j$  היא מטריצה מסדר  $4 \times 16$  שנותן למטה. לכל  $1 \leq j \leq 8$ :

$$C_j = (S_j(r, c))_2, \quad r = (b_1 b_6)_{10}, \quad c = (b_2 b_3 b_4 b_5)_{10}$$

כאשר  $r$  בספרות דצמליות,  $c$  בספרות דצמליות, ו-  $S_j(r, c)$  החיבור בשורה  $r$  ועומודה  $c$  של המטריצה  $S_j$ . לבסוף מmirים  $C_j$  בספרות ביניאריות.

$$.P = \begin{pmatrix} 16 & 7 & 20 & 21 \\ 29 & 12 & 28 & 17 \\ 1 & 15 & 23 & 26 \\ 5 & 18 & 31 & 10 \\ 2 & 8 & 24 & 14 \\ 32 & 27 & 3 & 9 \\ 19 & 13 & 30 & 6 \\ 22 & 11 & 4 & 25 \end{pmatrix}$$

**שלב [5]** כאשר  $P$  התמורה  $f(A, J) = P(C_1 C_2 C_3 C_4 C_5 C_6 C_7 C_8)$

**התזמון המפתח של DES:** נתון מפתח התחaltı ביטים  $.k$ .

$$PC_1 = \begin{pmatrix} 57 & 49 & 41 & 33 & 25 & 17 & 9 \\ 1 & 58 & 50 & 42 & 34 & 26 & 18 \\ 10 & 2 & 59 & 51 & 43 & 35 & 27 \\ 19 & 11 & 3 & 60 & 52 & 44 & 36 \\ 63 & 55 & 47 & 39 & 31 & 23 & 15 \\ 7 & 62 & 54 & 46 & 38 & 30 & 22 \\ 14 & 6 & 61 & 53 & 45 & 37 & 29 \\ 21 & 13 & 5 & 28 & 20 & 12 & 4 \end{pmatrix}$$

**שלב [1]** מוצעים התמורה  $PC_1(k) = C_0 D_0$  כאשר  $C_0$  הראשונים ו-  $D_0$  האחרונים.

**שלב [2]** נסמן  $PC_1(k) = C_0 D_0$  כאשר  $PC_1(k) = C_0 D_0$  כאשר  $C_i = LS_i(C_{i-1})$ ,  $D_i = LS_i(D_{i-1})$ ,  $k_i = PC_2(C_i D_i)$ .

**שלב [3]** לכל  $1 \leq i \leq 16$ , מחשבים

הזהה מקום אחד שמאלה  $i = 1, 2, 9, 16$ , והזהה שני מקומות שמאליה  $i = 3, 4, 5, 6, 7, 8, 10, 11, 12, 13, 14, 15$ ,

$$PC_2 = \begin{pmatrix} 14 & 17 & 11 & 24 & 1 & 5 \\ 3 & 28 & 15 & 6 & 21 & 10 \\ 23 & 19 & 12 & 4 & 26 & 8 \\ 16 & 7 & 27 & 20 & 13 & 2 \\ 41 & 52 & 31 & 37 & 47 & 55 \\ 30 & 40 & 51 & 45 & 33 & 48 \\ 44 & 49 & 39 & 56 & 34 & 53 \\ 46 & 42 & 50 & 36 & 29 & 32 \end{pmatrix}.$$

**הבלוקים של החלפות של DES**

$S_1$	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13
$S_2$	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9
$S_3$	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12
$S_4$	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14
$S_5$	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3
$S_6$	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13
$S_7$	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12
$S_8$	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11