$m \mid a$ אם קיים שלם q כך ש $a = qm$.

$a \equiv b \mod m$ אם $m \mid a - b$, כלומר קיים שלם q כך ש- $a = qm + b$.

השארית של a בחלוקה ב- m מסומנת a % m.

משפט השארית של שלם שלילי: $a \text{ \% } m = a - m\left\lfloor \frac{a}{m} \right\rfloor$, $(-a) \text{ \% } m = m - (a \text{ \% } m) = m\left\lceil \frac{a}{m} \right\rceil - a$.

משפט החילוק של אוקליד: עבור שלמים $a, m \neq 0$ קיימים שלמים q, r כך ש $a = qm + r,$
כאשר m **המודולו,** q נקרא **המנה** ואילו $r = a \text{ \% } m$ **השארית**.

האלגוריתם של אוקליד: נתונים שלמים a, b ($a, b \geq 0$, $a \geq b$). ניתן לחשב את $d = \gcd(a, b)$ לפי האלגוריתם

שלב 1:	$a = bq_1 + r_1$	$0 \leq r_1 \leq b$
שלב 2:	$b = r_1 q_2 + r_2$	$0 \leq r_2 \leq r_1$
שלב 3:	$r_1 = r_2 q_3 + r_3$	$0 \leq r_3 \leq r_2$
	$\vdots$	
שלב n:	$r_{n-2} = r_{n-1} q_n + r_n$	$0 \leq r_n \leq r_{n-1}$
שלב $n+1$:	$r_{n-1} = r_n q_{n+1}$	$(r_{n+1} = 0)$

אלגוריתם אוקליד המוכלל: נתונים שלמים a, b ($a, b \geq 0$, $a \geq b$) ו- $d = \gcd(a, b)$. קיימים שלמים x, y כך ש-

$$ax + by = d \ .$$

ניתן למצוא את הערכים של x ו- y על ידי האלגוריתם הבא. נגדיר את הפרמטרים: $\left\{ \begin{array}{llll} r_0 = & a \ , & r_1 = b \ , \\ s_0 = & 1 \ , & s_1 = 0 \ , \\ t_0 = & 0 \ , & t_1 = 1 \ , \end{array} \right\}$

שלב 1:	$r_2 = r_0 - q_1 r_1$	$s_2 = s_0 - q_1 s_1$	$t_2 = t_0 - q_1 t_1$	$(0 \leq r_2 < \lvert r_1 \rvert)$
שלב 2:	$r_3 = r_1 - q_2 r_2$	$s_3 = s_1 - q_2 s_2$	$t_3 = t_1 - q_2 t_2$	$(0 \leq r_3 < \lvert r_2 \rvert)$
$\vdots$				
שלב i:	$r_{i+1} = r_{i-1} - q_i r_i$	$s_{i+1} = s_{i-1} - q_i s_i$	$t_{i+1} = t_{i-1} - q_i t_i$	$(0 \leq r_{i+1} < \lvert r_i \rvert)$
$\vdots$				
שלב $n-1$:	$r_n = r_{n-2} - q_{n-1} r_{n-1}$	$s_n = s_{n-2} - q_{n-1} s_{n-1}$	$t_n = t_{n-2} - q_{n-1} t_{n-1}$	$(0 \leq r_n < \lvert r_{n-1} \rvert)$
שלב n:	$r_{n+1} = 0$			

$$\gcd(a, b) = r_n \ , \qquad x = s_n \ , \qquad y = t_n \ .$$

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

משפט הפירוק לראשוניים: לכל שלם m קיים ראשוניים $p_1, p_2, \ldots, p_n$ ושלמים $e_1, \ldots, e_n$ כך ש-

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

פונקצית אוילר: אם הפירוק לראשוניים של מספר שלם m הוא $m = \prod_{i=1}^{n} p_i^{e_i}$, אז מספר השלמים הזרים ל- m בין 0 עד $m-1$ ניתן על ידי

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

אם p מספר ראשוני אז $\phi(p) = p - 1$.
אם p מספר ראשוני אז $\phi(p^n) = p^n - p^{n-1}$.
אם s, t שלמים זרים (כלומר $\gcd(s,t) = 1$) אז $\phi(s \cdot t) = \phi(s) \cdot \phi(t)$.
אם p ו- q מספרים ראשוניים שונים אז $\phi(p \cdot q) = (p-1)(q-1)$.

משפט פרמה: אם p מספר ראשוני ו- $a \in \mathbb{Z}_p$. אז התנאים הבאים מתקיימים:

$$a^p \equiv a \mod p\ , \qquad a^{p-1} \equiv 1 \mod p\ , \qquad a^{-1} \equiv a^{p-2} \mod p\ .$$

אם a, n שלמים ו- $\gcd(a,n) = 1$ אז $a^{\phi(n)} \equiv 1 \mod n$.
אם a, n שלמים ו- $\gcd(a,n) = 1$ אז $a^{-1} \equiv a^{\phi(n)-1} \mod n$.

משפט השאריות הסיני: יהיו $m_1, \ldots, m_r$ שלמים זרים בזוגות ו- $a_1, \ldots, a_r$ שלמים. למערכת

$$\left\{\begin{array}{rcl} x = & a_1 & \mod m_1 \\ x = & a_2 & \mod m_2 \\ & \vdots & \\ x = & a_r & \mod m_r \end{array}\right\}$$

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 $M_i = \frac{M}{m_i}$
ו- $y_i = M_i^{-1} \mod m_i$ לכל $1 \le i \le r$.

חוג של אורך m: $\mathbb{Z}_m = \{0, 1, \ldots, m-1\}$.

שני איברים a, b שקולים ב- $\mathbb{Z}_m$ אם $a \equiv b \mod m$.

נתון $a \in \mathbb{Z}_m$. קיים איבר הופכי $a \in \mathbb{Z}_m$ אם ורק אם $\gcd(a,m) = 1$.
הקופקטור ה- ij של מטריצה A שווה לדטרמיננטת המטריצה המתקלת אחרי מחיקת שורת i ועמודת j:

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

מטריצת הקופקטורים של מטריצה A היא מטריצה עבורה הרכיב ij היא הקופקטור ij של A: $C = \begin{pmatrix} C_{11} & \cdots & C_{1n} \\ \vdots & \ddots & \vdots \\ C_{n1} & \cdots & C_{nn} \end{pmatrix}$.

נוסחת קריימר למטריצה הופכית: $A^{-1} = (\det A)^{-1} C^t$.

איברים הפיכים ב- $\mathbb{Z}_{26}$:

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

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 26:

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

צפנים בסיסיים:

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

הסתברויות של האותיות:

אות	הסתברות
a	0.082
b	0.015
c	0.028
d	0.043
e	0.127

אות	הסתברות
f	0.022
g	0.02
h	0.061
i	0.07
j	0.002

אות	הסתברות
k	0.008
l	0.04
m	0.024
n	0.067
o	0.075

אות	הסתברות
p	0.019
q	0.001
r	0.06
s	0.063
t	0.091

אות	הסתברות
u	0.028
v	0.01
w	0.023
x	0.001
y	0.02
z	0.001

קבוצות תדירויות של האותיות בטקסט:

	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	$p < 0.01$

זוגות האותיות הנפוצים ביותר בטקסט:

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 בטקסט:

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

מידע של מ"מ בדיד X: $I(X=x) = \log_2\left(\frac{1}{P(X=x)}\right) = -\log_2(P(X=x))$.

אנטרופיה של מ"מ בדיד X: $H[X] = \sum_{i=1}^{N} P(X=x_i)I(X=x_i) = -\sum_{i=1}^{N} P(X=x_i)\log_2(P(X=x_i))$.

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

סודיות:
נתונה קריפטו-מערכת בעלת קבוצת טקסט גלוי X, קבוצת טקסט מוצפן Y וקבוצת מפתחות K, כלל מצפין $y = e_k(x)$ וכלל מפענח $x = d_k(y)$.

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

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

סודיות מושלמת: לקריפטו-מערכת יש סודיות מושלמת אם:

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

אנטרופיה מותנית:

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

משפט האנטרופיה לקריפו-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

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 פייסטל להצפנה: נתון טקטסט גלוי $x = L_0R_0$. לכל $1 \leq i \leq N$:

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

משוואות פייסטל לפענוח: נתון טקטסט גלוי $y = R_N L_N$. לכל $1 \leq i \leq N$:

$$R_i = L_{i+1} \ , \qquad L_i = R_{i+1} \oplus f(R_i, k_{i+1}) \ , \qquad x = L_0 R_0$$

תזמון 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 הצפנת IDEA

- נתון טקסט גלוי $P \in \{0,1\}^{64}$. של אורך 64 ביטים.
- מחלקים P לארבע בלוקים $P_i \in \{0,1\}^{16}$: $P = P_1P_2P_3P_4$.
- בתחילת מחזור ה- r ($1 \leq r \leq 9$) מסמנים את הטקסט מוצפן המתקבל ממחזור הקודם (מחזור $r-1$) ב- $C^{(r)}$, מלבד מ- $C^{(1)} = X$.
- כל מחזור r מורכב מהשלבים הבאים:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

- בכדי לקבל את הטקסט מוצפן הסופי, אחרי ביצוע של כל המחזורים r מבצעים את השלב התפוקה:

$$C_1 = C_1^{(9)} \odot k_1^{(9)} = C_1^{(9)} \cdot k_1^{(9)} \mod 2^{16}+1 \quad [1]$$
$$C_2 = C_3^{(9)} \boxplus k_2^{(9)} = C_3^{(9)} + k_2^{(9)} \mod 2^{16} \quad [2]$$
$$C_3 = C_2^{(9)} \boxplus k_3^{(9)} = C_2^{(9)} + k_3^{(9)} \mod 2^{16} \quad [3]$$
$$C_4 = C_4^{(9)} \odot k_4^{(9)} = C_4^{(9)} \cdot k_4^{(9)} \mod 2^{16}+1 \quad [4]$$

- לבסוף הטקסט מוצפן 64- ביטים מתקבל מהארבע בלוקים 16- ביטים $C = C_1C_2C_3C_4$.

מפתחות פענוח של IDEA

$$DK_1^{(1)} = \left(K_1^{(9)}\right)^{-1} , \quad DK_2^{(1)} = -\left(K_2^{(9)}\right) , \quad DK_3^{(1)} = -\left(K_3^{(9)}\right) , \quad DK_4^{(1)} = \left(K_4^{(9)}\right)^{-1} ,$$

$$DK_5^{(1)} = K_5^{(8)} , \quad DK_6^{(1)} = K_6^{(8)} .$$

אלגוריתם הצפנת DES : נתון טקסט גלוי 64 ביטים $x = x_1 \dots x_{64}$.

שלב [1] מבצעים $IP(x_1, x_2, \dots, x_{64})$ כאשר IP התמורה הסטטית ההתחלתית:

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

שלב [2] מחלקים $IP(x) = L_0R_0$ לשניים. L_0 כאשר ה-32 ביטים הראשונים של x_0 ו- R_0 ה- 32 האחרונים:

$$\begin{aligned} L_0 =& x_{58}, x_{50}, x_{42}, x_{34}, x_{26}, x_{18}, x_{10}, x_2, x_{60}, x_{52}, x_{44}, x_{36}, x_{28}, x_{20}, x_{12}, x_4 \\ & x_{62}, x_{54}, x_{46}, x_{38}, x_{30}, x_{22}, x_{14}, x_6, x_{64}, x_{56}, x_{48}, x_{40}, x_{32}, x_{24}, x_{16}, x_8 \ , \\ R_0 =& x_{57}, x_{49}, x_{41}, x_{33}, x_{25}, x_{17}, x_9, x_1, x_{59}, x_{51}, x_{43}, x_{35}, x_{27}, x_{19}, x_{11}, x_3 \\ & x_{61}, x_{53}, x_{45}, x_{37}, x_{29}, x_{21}, x_{13}, x_5, x_{63}, x_{55}, x_{47}, x_{39}, x_{31}, x_{23}, x_{15}, x_7 \ . \end{aligned}$$

שלב [3] מבצעים 16 מחזורים של אלגוריתם פייסטל: $L_i = R_{i-1} , \qquad R_i = L_{i-1} \oplus f\left(R_{i-1}, k_i\right).$

כאשר $k_1, \dots, k_{16}$ תת-מפתחות כל אחד 48 ביטים שמתקבלים ממפתח התחלתי k.

שלב [4] $y = IP^{-1}\left(R_{16}L_{16}\right)$ כאשר IP^{-1} התמורה ההופכית:

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

הפונקציית ליבה של DES

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

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

שלב [1] מגדילים A לרצף 48 ביטים באמצעות התמורה ההגדלה $E = \begin{pmatrix} 32 & 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 6 & 7 & 8 & 9 \\ 8 & 9 & 10 & 11 & 12 & 13 \\ 12 & 13 & 14 & 15 & 16 & 17 \\ 16 & 17 & 18 & 19 & 20 & 21 \\ 20 & 21 & 22 & 23 & 24 & 25 \\ 24 & 25 & 26 & 27 & 28 & 29 \\ 28 & 29 & 30 & 31 & 32 & 1 \end{pmatrix}$

שלב [2] מחשבים $E(A) \oplus J$ ורושמים התשובה כשירשור של שמונה רצפים 6 ביטים:

$$B = B_1B_2B_3B_4B_5B_6B_7B_8 \ , \qquad B_j \in \{0,1\}^6 \ .$$

שלב [3] רושמים $B_j = b_1b_2b_3b_4b_5b_6$ כאשר $b_i \in \{0,1\}$.

שלב [4] בשלב זה משתמשים ההחלפות $S_1, \ldots, S_8$. כל S_j היא מטריצה מסדר 4×16 שנתון למטה. לכל $1 \le j \le 8$:

$$C_j = \big(S_j(r,c)\big)_2 \ , \qquad r = (b_1b_6)_{10} \ , \qquad c = (b_2b_3b_4b_5)_{10}$$

כאשר r בספרות דצמליות, c בספרות דצמליות, ו- $S_j(r,c)$ האיבר בשורה r ועמודה c של המטריצה S_j. לבסוף ממירים C_j לספרות ביניאריות.

שלב [5] $f(A,J) = P(C_1C_2C_3C_4C_5C_6C_7C_8)$ כאשר P התמורה $P = \begin{pmatrix} 16 & 7 & 20 & 21 \\ 29 & 12 & 28 & 17 \\ 1 & 15 & 23 & 26 \\ 5 & 18 & 31 & 10 \\ 2 & 8 & 24 & 14 \\ 32 & 27 & 3 & 9 \\ 19 & 13 & 30 & 6 \\ 22 & 11 & 4 & 25 \end{pmatrix}$.

התזמון המפתח של DES: נתון מפתח התחלתי 64 ביטים, k.

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 ביטים הראשונים ו- D_0 ה- 28 ביטים האחרונים.

שלב [3] לכל $1 \le i \le 16$, מחשבים $C_i = LS_i\left(C_{i-1}\right) \ , \qquad D_i = LS_i\left(D_{i-1}\right) \ , \qquad k_i = PC_2\left(C_iD_i\right).$

כאשר $LS_i = \left\{ \begin{array}{ll} \text{הזזה מקום אחת שמאולה} & i = 1,2,9,16, \\ \text{הזזה שתי מקומות שמאלה} & i = 3,4,5,6,7,8,10,11,12,13,14,15 \ , \end{array} \right\}$ ו- PC_2 התמורה

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

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

הצפנת RSA:

לכל מפתח $k=(n,p,q,a,b)$ כאשר $n=pq$, p,q מספרים ראשוניים, ו- a,b שלמים כך ש- $ab=1 \mod \phi(n)$.

נגדיר כלל מצפין $e_k(x)=x^b \mod n$

ונגדיר כלל מפענח $d_k(x)=y^a \mod n$.

(p,q,b) מפתח תיבורי ו- a מפתח סודי.

פענוח RSA:

המשוואת פענוח $x=y^a \mod n$ ניתן לפתור באמצעות האלגוריתם הבא:

שלב [1] מחשבים $y \mod p$ ו- $a \mod (p-1)$ ואז מחשבים $x_1=(y \mod p)^{a \mod (p-1)} \mod p.$

שלב [2] מחשבים $y \mod q$ ו- $a \mod (q-1)$ ואז מחשבים $x_2=(y \mod q)^{a \mod (q-1)} \mod q.$

שלב [3] בעזרת המשפט השאריות הסיני פותרים את המערכת $\left\{\begin{array}{rl} x= & x_1 \mod p \\ x= & x_2 \mod q \end{array}\right\}$.

צופן אל-גמאל: יהי p מספר ראשוני, α יוצר של $\left(\mathbb{Z}_p^*,\times_p\right)$ ו- $a\in\{2,3,\ldots,p-2\}$. יהי $\beta=\alpha^a \mod p$.

נתון מפתח $k=(p,\alpha,a,\beta)$.

נגדיר כלל מצפין $e_k(x,d)=(y_1,y_2)\,,\quad y_1=\alpha^d \mod p\,,\quad y_2=\beta^d x \mod p$,

ונגדיר כלל מפענח $d_k(y_1,y_2)=\left(y_1^a\right)^{-1}y_2 \mod p$.

(p,α,β) מפתח ציבורי ו- a מפתח סודי.