

שיעור 9

צפנים בלוקים ו-DES

9.1 רשת החלפה-תמורה

הגדרה 9.1 רשת החלפה-תמורה

נתון טקסט גלוי $x = \{0, 1\}^n$ כרצף סיביות. מחלקים x ל- m קבוצות של אורך ℓ :

$$x = x_{<1>} || x_{<2>} || \cdots || x_{<m>}$$

כאשר

$$x_{<1>} = x_1 x_2 \cdots x_\ell, \quad x_{<2>} = x_{\ell+1} x_{\ell+2} \cdots x_{2\ell}, \quad x_{<m>} = x_{(m-1)\ell+1} x_{(m-1)\ell+2} \cdots x_{m\ell}.$$

ברשת החלפה-תמורה יש 4 מרכיבים:

- החלפה של אורך m , שנסמן $\pi_S : \{0, 1\}^\ell \rightarrow \{0, 1\}^\ell$
- תמורה של אורך $n = \ell m$ שנסמן $\pi_P : \{1, \dots, \ell m\} \rightarrow \{1, \dots, \ell m\}$
- מפתח התחלתי k .
- תזמון המפתחות (k^1, \dots, k^{N+1}) , אחד לכל שלב של ההצפנה.

האלגוריתם של ההצפנה הוא כמפורט להלן:

(1) מגדירים $w^0 = x$.

(2) מחשבים $u^1 = w^0 \oplus k^1$ כאשר \oplus האופרטור XOR.

(3) מבצעים את ההחלפה π_S על כל תת-קבוצה $u_{<i>}^1$ לכל $1 \leq i \leq m$: $v_{<i>}^1 = \pi_S(u_{<i>}^1)$

(4) מבצעים את התמורה π_P על תת-קבוצה v^1 : $w_i^1 = v_{\pi_P(i)}^1$

כעת חוזרים על שלבים (2)-(4):

(2') מחשבים $u^2 = w^1 \oplus k^2$ כאשר \oplus האופרטור XOR.

(3') מבצעים את ההחלפה π_S על כל תת-קבוצה $u_{<i>}^2$ לכל $1 \leq i \leq m$: $v_{<i>}^2 = \pi_S(u_{<i>}^2)$

(4') מבצעים את התמורה π_P על תת-קבוצה v^2 : $w_i^2 = v_{\pi_P(i)}^2$

התהליך ממשיך עד שמגיעים לסוף שלב ה- N -ית. בשלב N לא משחבים את w^N אלא מקבלים את הטקסט מוצפן לפי

$$y = v^N \oplus k^{N+1}.$$

דוגמה 9.1

נתון הטקסט גלוי

$x = 00100110$.

נתונה ההחלפה $\pi_S : \{0, 1\}^4 \rightarrow \{0, 1\}^4$ שמוגדרת

z	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$\pi_S(z)$	D	4	3	1	2	F	B	8	3	A	6	C	5	9	0	7

נתונה התמורה $\pi_P\{1, \dots, 8\} \rightarrow \{1, \dots, 8\}$ שמוגדרת

z	1	2	3	4	5	6	7	8
$\pi_P(z)$	8	5	4	2	3	6	1	7

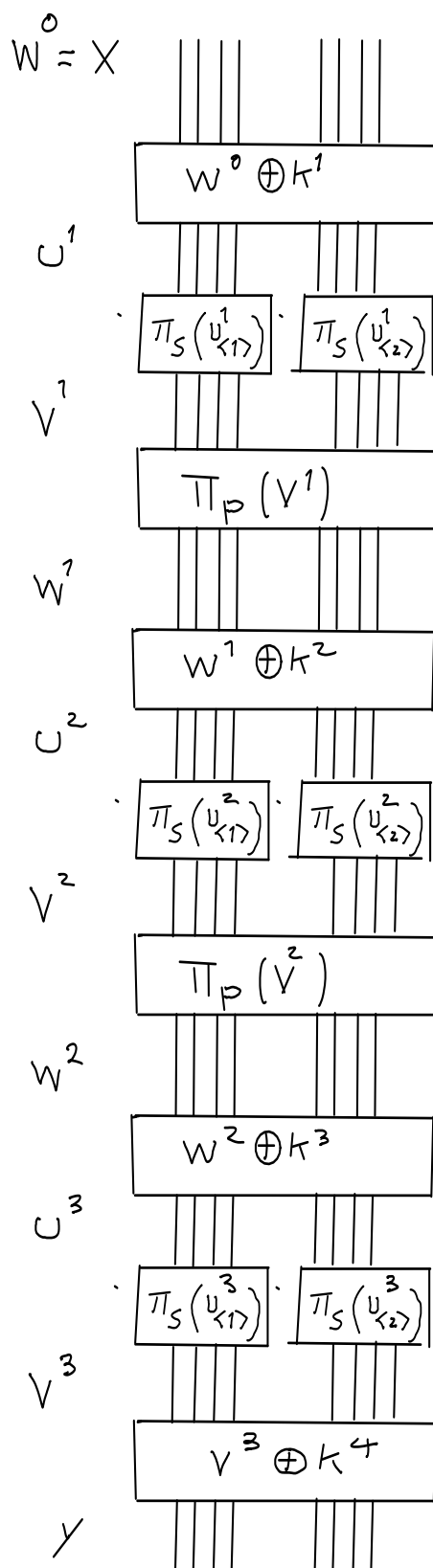
או בסימון מחזורי

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

ונתון מפתח התחלתי

$k = 0011\ 1010\ 1001\ 0100\ 1111$.

מספר השלבים בהצפנה הוא $N + 1$ כאשר $N = 2$. נגדיר תזמון המפתחות (k^1, k^2, k^3) כאשר המפתח k^i רצף סיביות של אורך 8 אשר מתחיל עם הסיבית ה- $(4i - 3)$ ית של k . מצטו את הטקסט מוצפן.



פתרון:

המפתחות של כל שלב של ההצפנה הם

$$k^1 = 0011 \ 1010 ,$$

$$k^2 = 1010 \ 1001 ,$$

$$k^3 = 1001 \ 0100 ,$$

$$k^4 = 0100 \ 1111 .$$

שלב (1)

$$w^0 = 0010 \ 0110$$

$$k^1 = 0011 \ 1010$$

$$u^1 = w^0 \oplus k^1 = 0001 \ 1100$$

$$u^1 = u_{<1>} || u_{<2>} = 0001 || 1100$$

בבסיס הקסדצימלי:

$$u^1 = u_{<1>} || u_{<2>} = 1 || C$$

$$v^1 = \pi_S(u_{<1>}) || \pi_S(u_{<2>}) = \pi_S(1) || \pi_S(C) = 4 || 5$$

בבסיס בינארי:

$$v^1 = 0100 || 0101$$

$$w^1 = \pi_P(0100 \ 0101) = 1001 \ 0100$$

שלב (2)

$$w^1 = 1001 \ 0100$$

$$k^2 = 1010 \ 1001$$

$$u^2 = w^1 \oplus k^2 = 0011 \ 1101$$

$$u^2 = u_{<1>}^2 || u_{<2>}^2 = 0011 || 1101$$

בבסיס הקסדצימלי:

$$u^2 = u_{<1>}^2 || u_{<2>}^2 = 3 || D$$

$$v^2 = \pi_S(u_{<2>}^2) || \pi_S(u_{<2>}^2) = \pi_S(3) || \pi_S(D) = 1 || 9$$

בבסיס בינארי:

$$v^2 = 0001 || 1001$$

$$w^2 = \pi_P(0001 \ 1001) = 1110 \ 0000$$

שלב (3)

$$\begin{aligned}
 w^2 &= 1110 \ 0000 \\
 k^3 &= 1001 \ 0100 \\
 u^3 &= w^2 \oplus k^3 = 0111 \ 0100 \\
 u^3 &= u_{<1>}^3 || u_{<2>}^3 = 0111 || 0100
 \end{aligned}$$

בבסיס הקסדצימלי:

$$u^3 = u_{<1>}^3 || u_{<2>}^3 = 7 || 4$$

$$v^3 = \pi_S(u_{<2>}^3) || \pi_S(u_{<1>}^3) = \pi_S(7) || \pi_S(4) = 8 || 2$$

בבסיס בינארי:

$$v^3 = 1000 || 0010$$

$$\begin{aligned}
 v^3 &= 1000 \ 0010 \\
 k^4 &= 0100 \ 1111 \\
 y &= v^3 \oplus k^4 = 1100 \ 1101
 \end{aligned}$$

9.2 רשת פייסטל

הגדרה 9.2 רשת פייסטל (Feistel)

נתון טקסט גלוי $x = \{0, 1\}^{2n}$ כרצף סיביות.מחלקים את x לשני חצאים שנסמן L_0 ו- R_0 :

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

ברשת פייסטל יש 4 מרכיבים:

- מספר שלם N אשר קובע את המספר השלבים בתהליך הצפנה.
- מפתח התחלתי k .
- מערכת של N תת-מפתחות (k_1, \dots, k_N) , אחד לכל שלב של התהליך הצפנה.
- פונקציית ליבה $f: \{0, 1\}^n \rightarrow \{0, 1\}^n$.

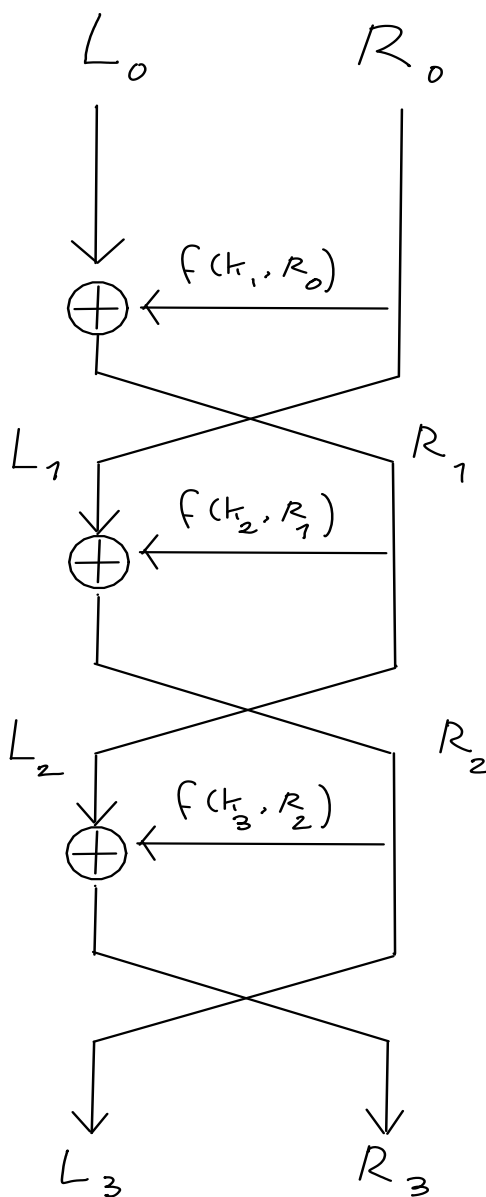
$$(1) \text{ מגדירים } R_0 = x_n \dots x_{2n}, L_0 = x_1 \dots x_n$$

$$(2) \text{ בשלב ה- } i \text{ ית } (1 \leq i \leq N): R_i = L_{i-1}, L_i = L_{i-1} \oplus f(R_{i-1}, k_i)$$

$$(3) \text{ בשלב ה- } N \text{ נקבל את הטקסט מוצפן לפי } y = R_N L_N$$

לדוגמה, עבור תהליך הצפנה עם $N = 3$ שלבים:

$$\begin{aligned} L_1 &= R_0, & L_2 &= R_1, & L_3 &= R_2, \\ R_1 &= L_0 \oplus f(R_0, k_1), & R_2 &= L_1 \oplus f(R_1, k_2), & R_3 &= L_2 \oplus f(R_2, k_3). \end{aligned}$$



9.2 דוגמה

נתון צופן פייסטל שמוגדר עם הפונקציית ליבה $f(x_1x_2x_3x_4x_5, \pi) = x_{\pi(1)}x_{\pi(2)}x_{\pi(3)}x_{\pi(4)}x_{\pi(5)}$ המפתח ההתחלתי הוא התמורה $(135)(24)$. כל תת-מפתח k_i הוא התמורה המתקבלת על ידי לבצע i פעמים את התמורה π . מצאו את טקסט מוצפן של הטקסט גלוי 0010111001.

פתרון:

$L_0 = 00101$ ו- $R_0 = 11001$. התת מפתחות הם

$$k_1 = (135)(24), \quad k_2 = (153)(2)(4), \quad k_3 = (1)(3)(5)(24).$$

מכאן

$$\begin{aligned} L_1 &= R_0 = 11001 . \\ R_1 &= L_0 \oplus f(R_0, k_1) = 00101 \oplus 00111 = 00010 . \\ L_2 &= R_1 = 00010 . \\ R_2 &= L_1 \oplus f(R_1, k_2) = 11001 \oplus 00010 = 11011 . \\ L_3 &= R_2 = 11011 . \\ R_3 &= L_2 \oplus f(R_2, k_3) = 00010 \oplus 11011 = 11001 . \\ y &= R_3 L_3 = 1100111011 \end{aligned}$$

משפט 9.1 משוואות פייסטל

משוואות פייסטל להצפנה:

נתון טקסט גלוי $x = L_0 R_0$ לכל $1 \leq i \leq N$:

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

משוואות פייסטל לפענוח:

נתון טקסט גלוי $y = R_N L_N$ לכל $1 \leq i \leq N$:

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

דוגמה 9.3 פענוח של צופן פייסטל

טקסט גלוי של 10 bit היה מוצפן באמצעות צופן פייסטל עם מפתח התחלתי $k = (124)(35)$. כל תת מפתח k_i מתקבל על ידי לבצע התמורה ההתחלתית i פעמים. הטקסט מוצפן הוא 1100001010. מצאו את הטקסט גלוי.

פתרון:

התת מפתחות הם:

$$k_1 = (124)(35) , \quad k_2 = (142)(3)(5) , \quad k_3 = (1)(2)(4)(35) .$$

הטקסט מוצפן התקבל על ידי להפוך את השני חצאים, $L_3 = 01010$, $R_3 = 11000$. לכן, השלב 1 הוא:

$$R_2 = L_3 = 01010$$

-1

$$L_2 = R_3 \oplus f(R_2, k_3) = 11000 \oplus 01010 = 10010 .$$

שלב 2:

$$R_1 = L_2 = 10010 .$$

$$L_1 = R_2 \oplus f(R_1, k_2) = 01010 \oplus 11000 = 10010$$

שלב 3:

$$R_0 = L_1 = 10010 .$$

$$L_0 = R_1 \oplus f(R_0, k_1) = 10010 \oplus 01010 = 11000$$

לכן הטקסט גלוי הוא

$$X = L_0 R_0 = 1100010010 .$$

■

9.3 תקן הצפנת מידע (DES)

התקן הצפנת מידע, באנגלית Data Encryption Standard (DES), הוא צופן בלוקים סימטרי שפותח ב-1974 במרכז המחקר של IBM בשיתוף פעולה עם הסוכנות לביטחון לאומי של ממשלת ארצות הברית.

שלב (1) נתון טקסט גלוי $x = x_1 \dots x_{64}$ כרצף סיביות של 64 ביטים. בונים רצף סיביות x_0 באמצעות תמורה של הביטים של x לפי תמורה סטטית הנקראת IP (initial permutation):

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

ז"א, לפי הטבלה,

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

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

שלב (2) מחלקים $x_0 = IP(x)$ לשני חצאים:

$$x_0 = IP(x) = L_0 R_0 ,$$

כאשר L_0 ה-32 ביטים הראשונים של x_0 ו- R_0 ה-32 ביטים 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) מבצעים 16 מחזורים של אלגוריתם פייסטל מסוים. מחשבים את L_i, R_i $1 \leq i \leq 16$ לפי הכלל

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

כאשר \oplus מסמן XOR ו- k_1, \dots, k_{16} התת-מפתחות שבנויים מרצפי סיביות, כל אחד של אורך 48 שמתקבלים ממפתח התחלתי k .

שלב (4) בסוף מפעילים התמורה ההופכית IP^{-1} על הרצף סיביות $R_{16}L_{16}$ כדי לקבל הטקסט מוצפן הסופי y . ז"א

$$y = IP^{-1}(R_{16}L_{16}).$$

כאשר

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

הפונקציית ליבה של DES

בכל מחזור של DES מבצעים את הפונקציית ליבה

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

f מקבלת ארגומנט ראשון A אשר הוא רצף סיביות של אורך 32, וארגומנט שני J אשר רצף סיביות של אורך 48, ומחזירה רצף סיביות של אורך 32.

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

שלב (1) ראשית הפונקציית ליבה f הופכת A לרצף סיביות של אורך 48 באמצעות הפונקציה

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

$E(A)$ היא תמורה של הסיביות של A עבורה 16 ספרות מופיעות פעמיים.

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

שלב (2) מחשבים $E(A) \oplus J$ ורושמים התוצאה כשירשור של שמונה רצפי סיביות של 6 ביטים

$$B = B_1B_2B_3B_4B_5B_6B_7B_8.$$

שלב (3) בשלב זה משתמשים בקופסאות ההחלפות $S_1, S_2, S_3, S_4, S_5, S_6, S_7, S_8$.

כל S_i היא מטריצה 4×16 אשר איבריה הם שלמים $0, 1, \dots, 15$.

כל S_i עובדת כפונקציה

$$S_j : \{0, 1\}^2 \times \{0, 1\}^4 \rightarrow \{0, 1\}^4 .$$

ספציפי, נתון רצף סיביות של אורך 6, $B_j = b_1 b_2 b_3 b_4 b_5 b_6$, אז

$$S_j(B_j) = S_j(r, c)$$

כאשר $S_j(r, c)$ הוא האיבר בשורה ה- r ועמודה ה- c של המטריצה S_j .

הביטים $b_1 b_6$ קובעים את היצוג הבינארי של שורה r של S_j , והביטים $b_2 b_3 b_4 b_5$ קובעים את היצוג הבינארי של עמודה c של S_j .

מגדירים

$$C_j = S_j(B_j) , \quad 1 \leq j \leq 8 .$$

שלב (4) מבצעים תמורה הסטטי P על הרצף $C = C_1 C_2 C_3 C_4 C_5 C_6 C_7 C_8$ כאשר התמורה P נתונה בטבלה למטה:

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

הרצף סיביות המתקבל $P(C)$ מוגדר להיות $f(A, J)$.

התזמון המפתח של DES

נתון מפתח התחלתי k של 64 ביטים. משתמשים ב- 56 סיביות של k בהרכב התת-מפתחות k_1 .

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

$$PC_1(k) = C_0 D_0$$

כאשר C_0 ה- 28 סיביות הראשונות ו- D_0 ה- 28 סיביות האחרונות.

שלב (3) לכל $1 \leq i \leq 16$, מחשבים

$$C_i = LS_i(C_{i-1}) , \quad D_i = LS_i(D_{i-1}) .$$

ו-

$$k_i = PC_2(C_i D_i) .$$

LS_i הוא הזזה של מקום אחד או שתי מקומות שמאולה:

$$LS_i = \begin{cases} \text{הזזה מקום אחת שמאולה} & i = 1, 2, 9, 16, \\ \text{הזזה שתי מקומות שמאולה} & i = 3, 4, 5, 6, 7, 8, 10, 11, 12, 13, 14, 15 . \end{cases}$$

התמורה PC_2 היא

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

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

דוגמאות

9.4 דוגמה

בצעו את האלגוריתם ליצירת תת-מפתחות לחשב k_1 מהמפתח ההתחלתי

$$k = 133457799BBCDFF1$$

פתרון:

hex	1	3	3	4	5	7	7	9
binary	0001	0011	0011	0100	0101	0111	0111	1001

hex	9	B	B	C	D	F	F	1
binary	1001	1011	1011	1100	1101	1111	1111	0001

מכאן

$$k = 0001 \ 0011 \ 0011 \ 0100 \ 0101 \ 0111 \ 0111 \ 1001 \\ 1001 \ 1011 \ 1011 \ 1100 \ 1101 \ 1111 \ 1111 \ 0001 .$$

$$PC_1(k) = C_0 D_0$$

כאשר

$$C_0 = 1111 \ 0000 \ 1100 \ 1100 \ 1010 \ 1010 \ 1111$$

$$D_0 = 0101 \ 0101 \ 0110 \ 0110 \ 0111 \ 1000 \ 1111 .$$

נבצע הזזה של ספרה אחד לשמאל לקבל

$$C_1 = 111 \ 0000 \ 1100 \ 1100 \ 1010 \ 1010 \ 1111 \ 1$$

$$D_1 = 101 \ 0101 \ 0110 \ 0110 \ 0111 \ 1000 \ 1111 \ 0 .$$

$$PC_2(C_1 D_1) = k_1 = 0001 \ 1011 \ 0000 \ 0010 \ 1110 \ 1111 \ 1111 \ 1100 \ 0111 \ 0000 \ 0111 \ 0010 .$$

■

9.5 דוגמה

מצאו את ההצפנה אחרי מחזור אחד של קריפטו-מערכת DES של הטקסט גלוי

0123456789ABCDEF

עם מפתח התחלתי

133457799BBCDF1

פתרון:

תחילה נרשום את הטקסט מוצפן בסיביות:

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

אנחנו כבר חישבנו את התת-מפתח k_1 בדוגמה 9.4:

$$k_1 = 0001 \ 1011 \ 0000 \ 0010 \ 1110 \ 1111 \ 1111 \ 1100 \ 0111 \ 0000 \ 0111 \ 0010 .$$

נפעיל תמורה הסטטית IP על הרצף סיביות 64 ביטים ונקבל

$$IP(x) = L_0 R_0$$

כאשר

$$L_0 = 1100 \ 1100 \ 0000 \ 0000 \ 1100 \ 1100 \ 1111 \ 1111 ,$$

ו-

$$R_0 = 1111 \ 0000 \ 1010 \ 1010 \ 1111 \ 0000 \ 1010 \ 1010 ,$$

כעת נחשב את $f(R_0, k_1)$:

(1) שלב

$$E(R_0) = 0111 \ 1010 \ 0001 \ 0101 \ 0101 \ 0101 \ 0111 \ 1010 \ 0001 \ 0101 \ 0101 \ 0101 ,$$

(2) שלב

$$E(R_0) \oplus k_1 = 011000 \ 010001 \ 011110 \ 111010 \ 100001 \ 100110 \ 010100 \ 100111 ,$$

שלב (3) בעזרת הקופסאות S_i נחליף כל רצף 6- ביטים אם רצף 4- ביטים.

שלב (4) עבור הרצף 6- ביטים הראשון:

$$b_1 b_2 b_3 b_4 b_5 b_6 = 011000 ,$$

נקח שורה $b_1 b_6 = 00$ ועמודה $b_2 b_3 b_4 b_5 = 1100$ של הקופסה S_2 . זוהי 5, אשר הוא 0101 בבסיס בינארי. חוזרים ומבצעים אותו חישוב על כל רצף 6 - ביטים של $E(R_0) \oplus k_1$ כדי לקבל הרצף 32- ביטים:

$$C = 0101 \ 1100 \ 1000 \ 0010 \ 1011 \ 0101 \ 1001 \ 0111$$

שלב (5) מפעילים התמורה P על C :

$$f(R_0, k_1) = P(C) = 0010 \ 0011 \ 0100 \ 1010 \ 1010 \ 1001 \ 1011 \ 1011$$

בסוף $L_1 = R_0$ ו-

$$R_1 = L_0 \oplus f(R_0, k_1) = 1110 \ 1111 \ 0100 \ 1010 \ 0110 \ 0101 \ 0100 \ 0100$$

■

דוגמה 9.6

נתון הטקסט גלוי

02468ACE13579BDF ,

נתון המפתח ההתחלתי

$$k = 010145458989\text{CDCD},$$

ונתון כי התת-מפתח הראשון של קריפטו-מערכת DES הוא

$$k_1 = 0000 \ 1011 \ 0000 \ 0010 \ 0100 \ 0011 \ 1001 \ 1001 \ 0100 \ 1000 \ 0010 \ 0100.$$

בצעו את המחזור הראשון של הצפנת DES.

פתרון:

hex	0	2	4	6	8	A	C	E
binary	0000	0010	0100	0110	1000	1010	1100	1110
hex	1	3	5	7	9	B	D	F
binary	0001	0011	0101	0111	1001	1011	1101	1111

$$IP(x) = L_0 R_0 \text{ כאשר}$$

$$L_0 = 1010 \ 1010 \ 1111 \ 0000 \ 1010 \ 1010 \ 1111 \ 0000$$

$$R_0 = 1100 \ 1100 \ 0000 \ 0000 \ 1100 \ 1100 \ 1111 \ 1111$$

כדי

להשתמש במשוואות פייסטל נצטרך לחשב את הפונקציית ליבה $f(R_0, k_1)$. תחילה משחבים את

$$E(R_0) = 1111 \ 1111 \ 0111 \ 1001 \ 0101 \ 0110 \ 0001 \ 0000 \ 0000 \ 1000 \ 0101 \ 1110.$$

מבצעים XOR של $E(R_0)$ עם k_1 ורושמים את התוצאה בקבוצות של 6 ביטים:

$$E(R_0) \oplus k_1 = 111011 \ 101000 \ 001001 \ 000010 \ 111111 \ 001101 \ 111111 \ 011011.$$

קופסה החלפה S1 שורה 11, עמודה 1101, ומקבלים את האיבר 0.

קופסה החלפה S2 שורה 10, עמודה 0100, ומקבלים את האיבר 10.

קופסה החלפה S3 שורה 01, עמודה 0100, ומקבלים את האיבר 3.

קופסה החלפה S4 שורה 00, עמודה 0001, ומקבלים את האיבר 13.

קופסה החלפה S5 שורה 11, עמודה 1111, ומקבלים את האיבר 3.

קופסה החלפה S6 שורה 01, עמודה 0110, ומקבלים את האיבר 9.

קופסה החלפה S7 שורה 11, עמודה 1111, ומקבלים את האיבר 12.

קופסה החלפה S8 שורה 01, עמודה 1101, ומקבלים את האיבר 14.

לכן

$$C = 0000 \ 1010 \ 0011 \ 1101 \ 0011 \ 1001 \ 1100 \ 1110$$

מבצעים את התמורה הסטטית C :

$$P(C) = f(R_0, k_1) = 1111 \ 1100 \ 0001 \ 1010 \ 0011 \ 0000 \ 1110 \ 0101$$

לבסוף אנחנו מקבלים

$$L_1 = R_0 = 1100 \ 1100 \ 0000 \ 0000 \ 1100 \ 1100 \ 1111 \ 1111$$

$$R_1 = L_0 \oplus f(R_0, k_1) = 0101 \ 0110 \ 1110 \ 1010 \ 1001 \ 1010 \ 0001 \ 0101$$

■

IDEA 9.4

הגדרה 9.3 פעולות בינאריות של IDEA

\oplus	או מוציא XOR
\boxplus	חיבור מודולו 2^n כאשר n שלם השווה לאורך של הבלוקים
\odot	כפל מודולו $2^n + 1$

9.7 דוגמה

$$0110 \oplus 1011 = 1101 .$$

9.8 דוגמה

$$0110 \boxplus 1011 \xrightarrow{\text{ספרות דצימליות}} 6 \boxplus 11 = 6 + 11 \mod 2^4 = 1 \xrightarrow{\text{סיביות}} 0001 .$$

9.9 דוגמה

$$0110 \odot 1011 \xrightarrow{\text{ספרות דצימליות}} 6 \odot 11 = 6 \cdot 11 \mod 2^4 + 1 = 66 \mod 17 = 15 \xrightarrow{\text{סיביות}} 1111 .$$

9.10 דוגמה

$$0000 \odot 1011 \xrightarrow{\text{ספרות דצימליות}} 2^4 \odot 11 = 16 \cdot 11 \mod 2^4 + 1 = 176 \mod 17 = 6 \xrightarrow{\text{סיביות}} 0110 .$$

תת מפתחות של IDEA

נתון מפתח התחלתי k של IDEA של אורך 128 ביטים. כל הצפנה משתמשת ב-6 תת מפתחות, וכל תפוקה משתמשת ב-4 תת מפתחות. התת מפתחות מסומנות ב- $k_i^{(r)}$, $1 \leq i \leq 4$, $1 \leq r \leq 8$, ו- $k_i^{(9)}$, $1 \leq i \leq 4$. התת מפתחות מתקבלים על ידי לחלק k לשמונה תת-מפתחות, כל אחד של אורך 16 ביטים, ואחר כך להזיז k 25 מקומות שמאלה. התת מפתחות המתקבלים מתוארים בטבלה למטה.

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 ההצפנה

• נתון טקסט גלוי P של אורך 64 ביטים.

• מחלקים X לארבע בלוקים, כל אחד של אורך 16 ביטים:

$$P = P_1 P_2 P_3 P_4 .$$

• בתחילה של מחזור ה- r , $1 \leq r \leq 9$, נסמן את הטקסט מוצפן המתקבל ממחזור הקודם (מחזור $r-1$) ב- $C^{(r)}$, מלבד מ- $C^{(1)} = P$.

• כל מחזור r מורכב מהשלבים הבאים:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

הערכים Y_i נקראים הערכים הביניים. התפוקות $C_i^{(r)}$, $1 \leq i \leq 4$ נקראות הטקסטים מוצפנים הביניים.

• בכדי לקבל את הטקסט מוצפן הסופי, אחרי השלבים של כל מחזור r מבצעים את השלב התפוקה:

$$C_1 = C_1^{(9)} \odot k_1^{(9)} = C_1^{(9)} \cdot k_1^{(9)} \mod 2^{16} + 1 \quad [1]$$

$$C_2 = C_3^{(9)} \boxplus k_2^{(9)} = C_3^{(9)} + k_2^{(9)} \mod 2^{16} \quad [2]$$

$$C_3 = C_2^{(9)} \boxplus k_3^{(9)} = C_2^{(9)} + k_3^{(9)} \bmod 2^{16} \quad [3]$$

$$C_4 = C_4^{(9)} \odot k_4^{(9)} = C_4^{(9)} \cdot k_4^{(9)} \bmod 2^{16} + 1 \quad [4]$$

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

$$C = C_1 C_2 C_3 C_4 .$$

דוגמאות

דוגמה 9.11

נתון מפתח התחלתי

$$k = 01010303030301010123cdef00110011$$

בצעו את המחזור הראשון של הצפנת IDEA על הטקסט גלוי

$$P = 000f11111111000f$$

פתרון:

רושמים את המפתח במונחי סיביות:

hex	0	1	0	1	0	3	0	3
binary	0000	0001	0000	0001	0000	0011	0000	0011
hex	0	3	0	3	0	1	0	1
binary	0000	0011	0000	0011	0000	0001	0000	0001
hex	0	1	2	3	c	d	e	f
binary	0000	0001	0010	0011	1100	1101	1110	1111
hex	0	0	1	1	0	0	1	1
binary	0000	0000	0001	0001	0000	0000	0001	0001

יוצרים את התת מתחות למחזור הראשון:

$$k_1^{(1)} = 0000000100000001 = 257$$

$$k_2^{(1)} = 0000001100000011 = 771$$

$$k_3^{(1)} = 0000001100000011 = 771$$

$$k_4^{(1)} = 0000000100000001 = 257$$

$$k_5^{(1)} = 0000000100100011 = 291$$

$$k_6^{(1)} = 1100110111101111 = 52719$$

רושמים את הטקסט גלוי במונחי סיביות:

hex	0	0	0	f	1	1	1	1
binary	0000	0000	0000	1111	0001	0001	0001	0001
hex	1	1	1	1	0	0	0	f
binary	0001	0001	0001	0001	0000	0000	0000	1111

מבצעים מחזור ראשון של ההצפנה:

$$\begin{aligned}
P_1 = C_1^{(1)} &= 00000000000001111 = 15, \\
P_2 = C_2^{(1)} &= 0001000100010001 = 4369, \\
P_3 = C_3^{(1)} &= 0001000100010001 = 4369, \\
P_4 = C_4^{(1)} &= 00000000000001111 = 15,
\end{aligned}$$

$$\begin{aligned}
Y_1 = C_1^{(1)} \odot k_1^{(1)} &= 15 \cdot 257 \mod 65537 = 3855 \Rightarrow Y_1 = 0000 \ 1111 \ 0000 \ 1111, \\
Y_2 = C_2^{(1)} \boxplus k_2^{(1)} &= 4369 + 771 \mod 65536 = 5140 \Rightarrow Y_2 = 0001 \ 0100 \ 0001 \ 0100, \\
Y_3 = C_3^{(1)} \boxplus k_3^{(1)} &= 4369 + 771 \mod 65536 = 5140 \Rightarrow Y_3 = 0001 \ 0100 \ 0001 \ 0100, \\
Y_4 = C_4^{(1)} \odot k_4^{(1)} &= 15 \cdot 257 \mod 65537 = 3855 \Rightarrow Y_4 = 0000 \ 1111 \ 0000 \ 1111, \\
Y_5 = Y_1 \oplus Y_3 &= 0001 \ 1011 \ 0001 \ 1011 = 6939, \\
Y_6 = Y_2 \oplus Y_4 &= 0001 \ 1011 \ 0001 \ 1011 = 6939, \\
Y_7 = Y_5 \odot k_5^{(1)} &= 6939 \cdot 291 \mod 65537 = 53139 \Rightarrow Y_7 = 1100 \ 1111 \ 1001 \ 0011, \\
Y_8 = Y_6 \boxplus Y_7 &= 6939 + 53139 \mod 65536 = 60078 \Rightarrow Y_8 = 1110 \ 1010 \ 1010 \ 1110, \\
Y_9 = Y_8 \odot k_6^{(1)} &= 60078 \cdot 52719 \mod 65537 = 45483 \Rightarrow Y_9 = 1011 \ 0001 \ 1010 \ 1011, \\
Y_{10} = Y_7 \boxplus Y_9 &= 53139 + 45483 \mod 65536 = 33086 \Rightarrow Y_{10} = 1000 \ 0001 \ 0011 \ 1101.
\end{aligned}$$

התפוקה של מחזור הראשון הינה

$$\begin{aligned}
C_1^{(2)} = Y_1 \oplus Y_9 &= 1011111010100100 \\
C_2^{(2)} = Y_3 \oplus Y_9 &= 1010010110111111 \\
C_3^{(2)} = Y_2 \oplus Y_{10} &= 1001010100101010 \\
C_4^{(2)} = Y_4 \oplus Y_{10} &= 1000111000110001
\end{aligned}$$

דוגמה 9.12

מצאו את המפתחות פענוח של המחזור הראשון של פענוח IDEA בעזרת המפתח ההתחלתי

$$k = 00112233445566778899aabbccddeeff.$$

פתרון:

המפתחות לפענוח הם

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

hex	0	0	1	1	2	2	3	3	4	4	5
binary	0000	0000	0001	0001	0010	0010	0011	0011	0100	0100	0101

hex	5	6	6	7	7	8	8	9	9	a	a
binary	0101	0110	0110	0111	0111	1000	1000	1001	1001	1010	1010

hex	b	b	c	c	d	d	e	e	f	f
binary	1011	1011	1100	1100	1101	1101	1110	1110	1111	1111

$$k_1^{(9)} = 0100\ 0110\ 0110\ 1000 = 18024 . \quad \text{ביטים } 22 - 37$$

$$k_2^{(9)} = 1000\ 1010\ 1010\ 1100 = 35500 . \quad \text{ביטים } 38 - 53$$

$$k_3^{(9)} = 1100\ 1110\ 1111\ 0001 = 52977 . \quad \text{ביטים } 54 - 69$$

$$k_4^{(9)} = 0001\ 0011\ 0011\ 0101 = 4917 . \quad \text{ביטים } 70 - 85$$

$$k_5^{(8)} = 1011\ 1100\ 1100\ 1101 . \quad \text{ביטים } 93 - 108$$

$$k_6^{(8)} = 1101\ 1110\ 1110\ 1111 . \quad \text{ביטים } 109 - 124$$

$$DK_1^{(1)} = \left(K_1^{(9)}\right)^{-1} = (18024)^{-1} \bmod 65537 = 45753 = 1011\ 0010\ 1011\ 1001 ,$$

$$DK_2^{(1)} = -\left(K_2^{(9)}\right) = -35500 \bmod 65536 = 30036 = 0111\ 0101\ 0101\ 0100 .$$

$$DK_3^{(1)} = -\left(K_3^{(9)}\right) = -52977 \bmod 65536 = 12559 = 0011\ 0001\ 0000\ 1111 .$$

$$DK_4^{(1)} = \left(K_4^{(9)}\right)^{-1} = (4917)^{-1} \bmod 65537 = 18047 = 0100\ 0110\ 0111\ 1111 .$$

$$DK_5^{(1)} = K_5^{(8)} = 1011\ 1100\ 1100\ 1101 .$$

$$DK_6^{(1)} = K_6^{(8)} = 1101\ 1110\ 1110\ 1111 .$$

■