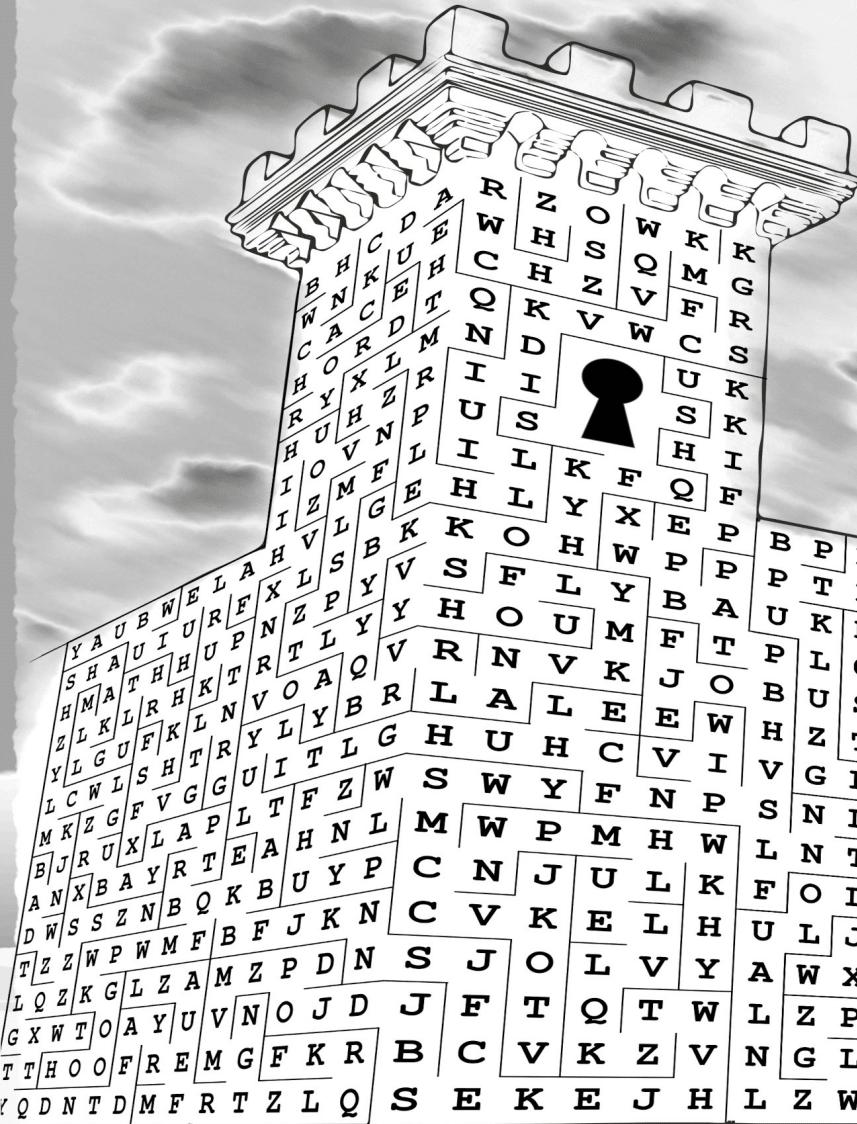


Szimmetrikus kulcsú rendszerek

A DES (Data Encryption Standard)



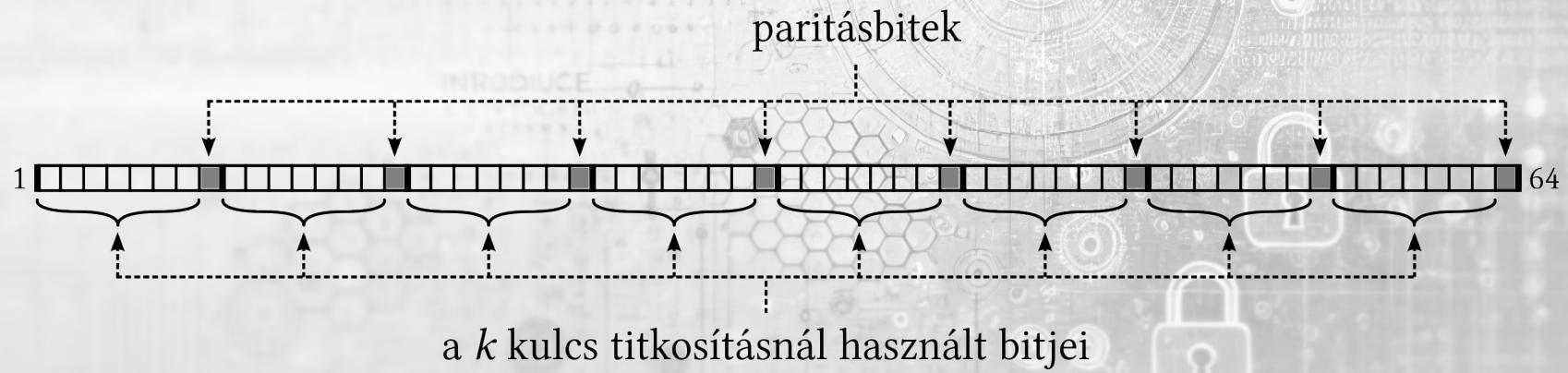
B	P	K	P	U	Q	Z	J	U	P	R	H	U	F	Z	Y	V	E	G	U	R	F	W	C	S	F	M	O	X	P	Q	W	U	I	F	W	O	A	H	T	L	A	H	V	V	B	U	R	C	Z	M	G	Y	J	G	F	D	X	V	T	
P	T	L	U	C	F	I	O	P	R	H	U	F	Z	Y	V	E	G	U	R	F	W	C	S	F	M	O	X	P	Q	W	U	I	F	W	O	A	H	T	L	A	H	V	V	B	U	R	C	Z	M	G	Y	J	G	F	D	X	V	T		
U	K	E	G	V	Y	A	O	P	R	H	U	F	Z	Y	V	E	G	U	R	F	W	C	S	F	M	O	X	P	Q	W	U	I	F	W	O	A	H	T	L	A	H	V	V	B	U	R	C	Z	M	G	Y	J	G	F	D	X	V	T		
L	C	T	G	H	W	A	T	P	R	H	U	F	Z	Y	V	E	G	U	R	F	W	C	S	F	M	O	X	P	Q	W	U	I	F	W	O	A	H	T	L	A	H	V	V	B	U	R	C	Z	M	G	Y	J	G	F	D	X	V	T		
S	F	T	J	L	H	W	X	G	Z	W	L	O	F	W	L	T	W	J	W	N	N	B	L	M	O	I	I	T	N	B	K	L	E	F	S	Z	B	E	R	A	M	P	E	T	V	H	G	V	W	U	J	B	C	X	V	T				
F	T	J	L	H	W	X	G	Z	W	L	O	F	W	L	T	W	J	W	N	N	B	L	M	O	I	I	T	N	B	K	L	E	F	S	Z	B	E	R	A	M	P	E	T	V	H	G	V	W	U	J	B	C	X	V	T					
T	L	H	W	X	G	Z	W	L	O	F	W	L	T	W	J	W	N	N	B	L	M	O	I	I	T	N	B	K	L	E	F	S	Z	B	E	R	A	M	P	E	T	V	H	G	V	W	U	J	B	C	X	V	T							
U	S	K	S	A	F	T	J	L	H	W	X	G	Z	W	L	O	F	W	L	T	W	J	W	N	N	B	L	M	O	I	I	T	N	B	K	L	E	F	S	Z	B	E	R	A	M	P	E	T	V	H	G	V	W	U	J	B	C	X	V	T
G	L	W	N	K	Q	G	M	W	P	S	I	U	A	H	M	H	L	U	B	R	Y	K	T	H	E	Y	T	A	U	P	H	O	V	C	Y	R	V	R	G	L	U	A	I	I	H	V	E	T												
W	N	K	Q	G	M	W	P	S	I	U	A	H	M	H	L	U	B	R	Y	K	T	H	E	Y	T	A	U	P	H	O	V	C	Y	R	V	R	G	L	U	A	I	I	H	V	E	T														
N	L	Z	N	L	Z	N	L	T	H	U	Q	Á	E	E	N	T	R	U	J	I	G	S	K	M	V	R	Z	G	F	W	V	R	U	V	R	H	M	L	T	S	U	P	B	A	T	Y	G	N	S	R	X	A	J	J	Y	E	T			
L	N	T	H	U	Q	Á	E	E	N	T	R	U	J	I	G	S	K	M	V	R	Z	G	F	W	V	R	U	V	R	H	M	L	T	S	U	P	B	A	T	Y	G	N	S	R	X	A	J	J	Y	E	T									
H	R	V	R	H	W	V	U	U	Z	D	R	C	N	J	K	P	H	C	L	F	F	P	A	H	C	Z	A	D	N	F	H	S	I	D	J	C	X	J	H	R	N	X	J	Y	E	T														
R	V	R	H	W	V	U	U	Z	D	R	C	N	J	K	P	H	C	L	F	F	P	A	H	C	Z	A	D	N	F	H	S	I	D	J	C	X	J	H	R	N	X	J	Y	E	T															
V	R	H	W	V	U	U	Z	D	R	C	N	J	K	P	H	C	L	F	F	P	A	H	C	Z	A	D	N	F	H	S	I	D	J	C	X	J	H	R	N	X	J	Y	E	T																
U	U	Z	D	R	C	N	J	K	P	H	C	L	F	F	P	A	H	C	Z	A	D	N	F	H	S	I	D	J	C	X	J	H	R	N	X	J	Y	E	T																					
Z	D	R	C	N	J	K	P	H	C	L	F	F	P	A	H	C	Z	A	D	N	F	H	S	I	D	J	C	X	J	H	R	N	X	J	Y	E	T																							
D	R	C	N	J	K	P	H	C	L	F	F	P	A	H	C	Z	A	D	N	F	H	S	I	D	J	C	X	J	H	R	N	X	J	Y	E	T																								
R	C	N	J	K	P	H	C	L	F	F	P	A	H	C	Z	A	D	N	F	H	S	I	D	J	C	X	J	H	R	N	X	J	Y	E	T																									
C	N	J	K	P	H	C	L	F	F	P	A	H	C	Z	A	D	N	F	H	S	I	D	J	C	X	J	H	R	N	X	J	Y	E	T																										
N	J	K	P	H	C	L	F	F	P	A	H	C	Z	A	D	N	F	H	S	I	D	J	C	X	J	H	R	N	X	J	Y	E	T																											
J	K	P	H	C	L	F	F	P	A	H	C	Z	A	D	N	F	H	S	I	D	J	C	X	J	H	R	N	X	J	Y	E	T																												
K	P	H	C	L	F	F	P	A	H	C	Z	A	D	N	F	H	S	I	D	J	C	X	J	H	R	N	X	J	Y	E	T																													
P	H	C	L	F	F	P	A	H	C	Z	A	D	N	F	H	S	I	D	J	C	X	J	H	R	N	X	J	Y	E	T																														
H	C	L	F	F	P	A	H	C	Z	A	D	N	F	H	S	I	D	J	C	X	J	H	R	N	X	J	Y	E	T																															
C	L	F	F	P	A	H	C	Z	A	D	N	F	H	S	I	D	J	C	X	J	H	R	N	X	J	Y	E	T																																
L	F	F	P	A	H	C	Z	A	D	N	F	H	S	I	D	J	C	X	J	H	R	N	X	J	Y	E	T																																	
F	F	P	A	H	C	Z	A	D	N	F	H	S	I	D	J	C	X	J	H	R	N	X	J	Y	E	T																																		
P	A	H	C	Z	A	D	N	F	H	S	I	D	J	C	X	J	H	R	N	X	J	Y	E	T																																				
A	H	C	Z	A	D	N	F	H	S	I	D	J	C	X	J	H	R	N	X	J	Y	E	T																																					
H	C	Z	A	D	N	F	H	S	I	D	J	C	X	J	H	R	N	X	J	Y	E	T																																						
C	Z	A	D	N	F	H	S	I	D	J	C	X	J	H	R	N	X	J	Y	E	T																																							
Z	A	D	N	F	H	S	I	D	J	C	X	J	H	R	N	X	J	Y	E	T																																								
A	D	N	F	H	S	I	D	J	C	X	J	H	R	N	X	J	Y	E	T																																									
D	N	F	H	S	I	D	J	C	X	J	H	R	N	X	J	Y	E	T																																										
N	F	H	S	I	D	J	C	X	J	H	R	N	X	J	Y	E	T																																											
F	H	S	I	D	J	C	X	J	H	R	N	X	J	Y	E	T																																												
H	S	I	D	J	C	X	J	H	R	N	X	J	Y	E	T																																													
S	I	D	J	C	X	J	H	R	N	X	J	Y	E	T																																														
I	D	J	C	X	J	H	R	N	X	J	Y	E	T																																															
D	J	C	X	J	H	R	N	X	J	Y	E	T																																																
J	C	X	J	H	R	N	X	J	Y	E	T																																																	
C	X	J	H	R	N	X	J	Y	E	T																																																		
X	J	H	R	N	X	J	Y	E	T																																																			
J	H	R	N	X	J	Y	E	T																																																				
H	R	N	X	J	Y	E	T																																																					
R	N	X	J	Y	E	T																																																						
N	X	J	Y	E	T																																																							
X	J	Y	E	T																																																								
J	Y	E	T																																																									
Y	E	T																																																										

DES (Data Encryption Standard)

- 1977-ben vezette be az NBS (National Bureau of Standards, ma NIST): [FIPS-46-3](#)
- 64-bites adatblokkokat titkosít, 56-bites kulccsal
- biztonsága vitatott
- nyilvános információk szerint csak brute-force módszerekkel törhető

DES (Data Encryption Standard)

Kulcs: A k kulcs is egy 64 bites bináris adattömb. Fontos megjegyezni, hogy a lehetséges 2^{64} méretű kulcstér helyett a DES kulcstere csak 2^{56} nagyságú, mivel a kulcs minden egyes bájtjának utolsó bitje hibaellenőrzésre van fenntartva (paritásbit).



DES (Data Encryption Standard)

Kódolás:

Algorithm DES (E_k):

Input: B, k

Output: C

$L_0 \parallel R_0 := IP(B)$ {kulcstól független}

for $n := 1, \dots, 16$ **do**

$K_n := KS(n, k)$

$L_n := R_{n-1}$

$R_n := L_{n-1} \oplus f(R_{n-1}, K_n)$

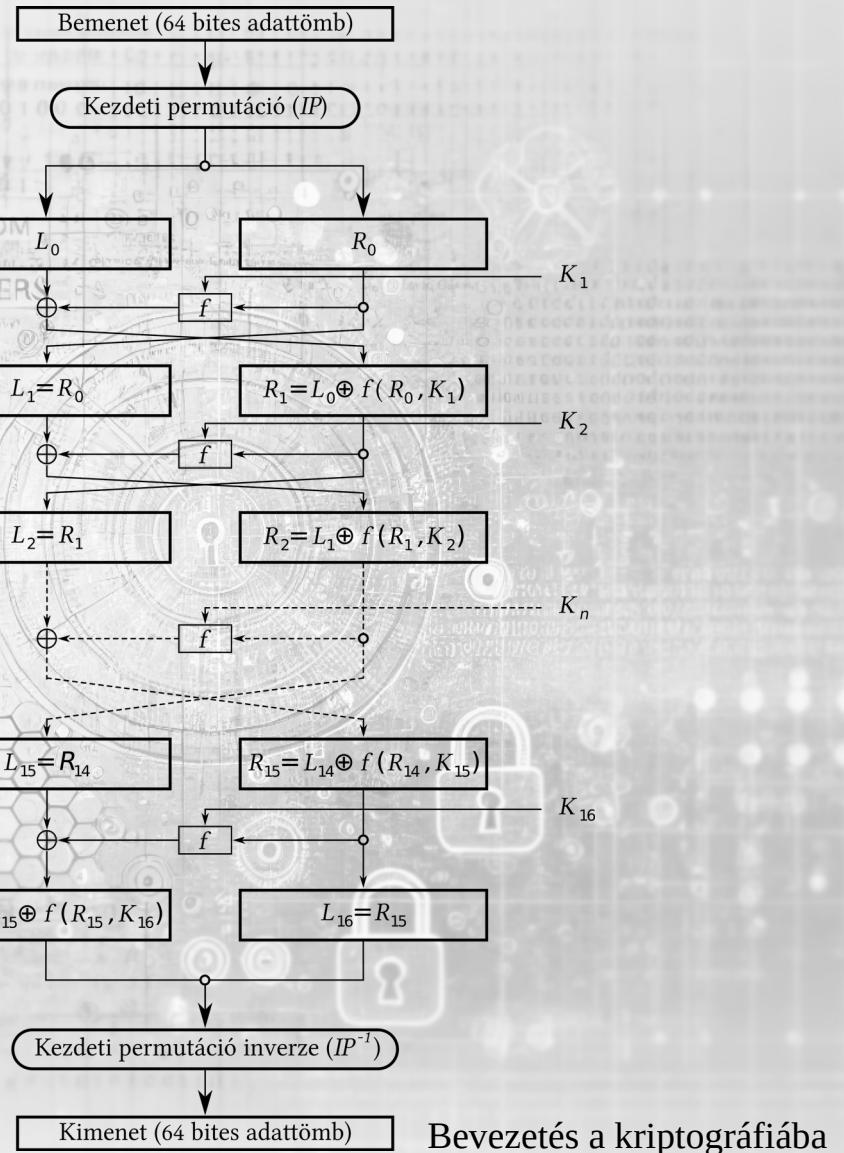
end for

$C' := R_{16} \parallel L_{16}$

$C := IP^{-1}(C')$ {kulcstól független}

return C

end Algorithm



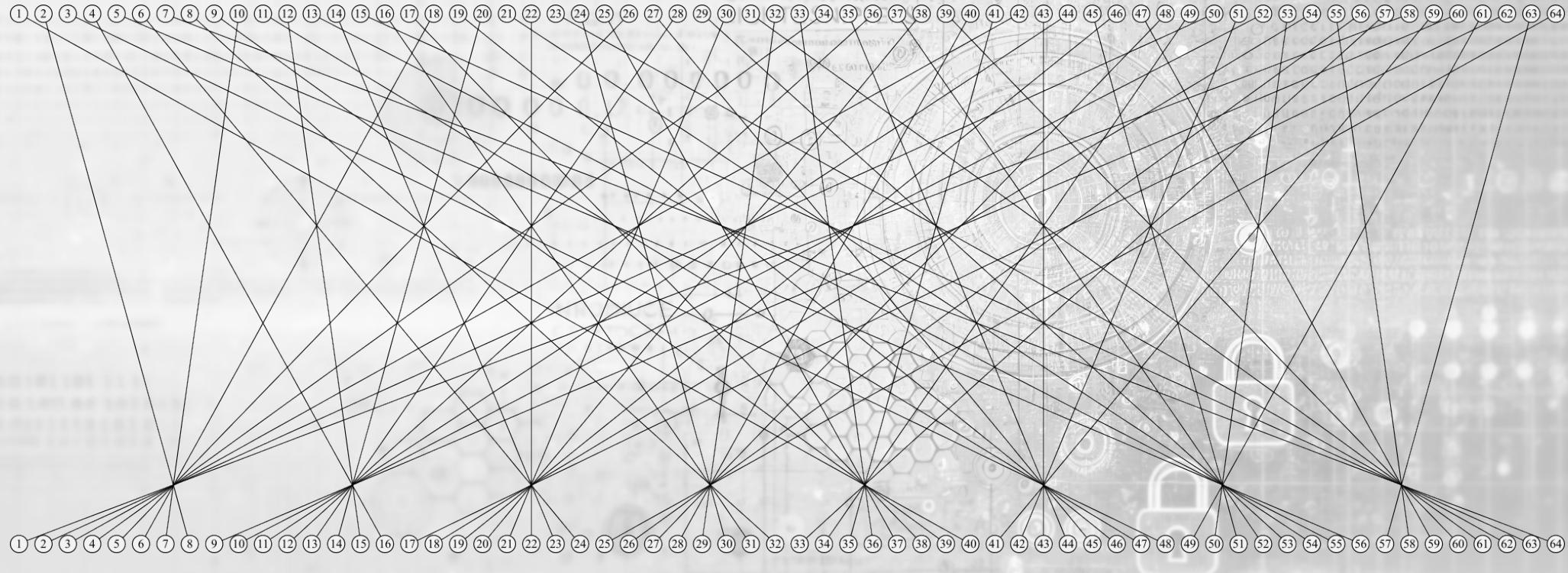
DES (Data Encryption Standard)

- L_n és R_n ($n \in \{0, \dots, 16\}$) egyenként 32 bites adattömbök
- a cikluson belül található a kódoló eljárás kulcstól függő része
- KS a kulcsütemező függvény: attól függően, hogy hányadik az iterációnál tart az algoritmus, kiválaszt 48 bitet a k kulcs titkosításra használt 56 bitje közül
- a KS kimenete egy-egy 48 bites adattömb (K_n segédkulcs)

DES – kezdeti permutáció (*IP*)

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

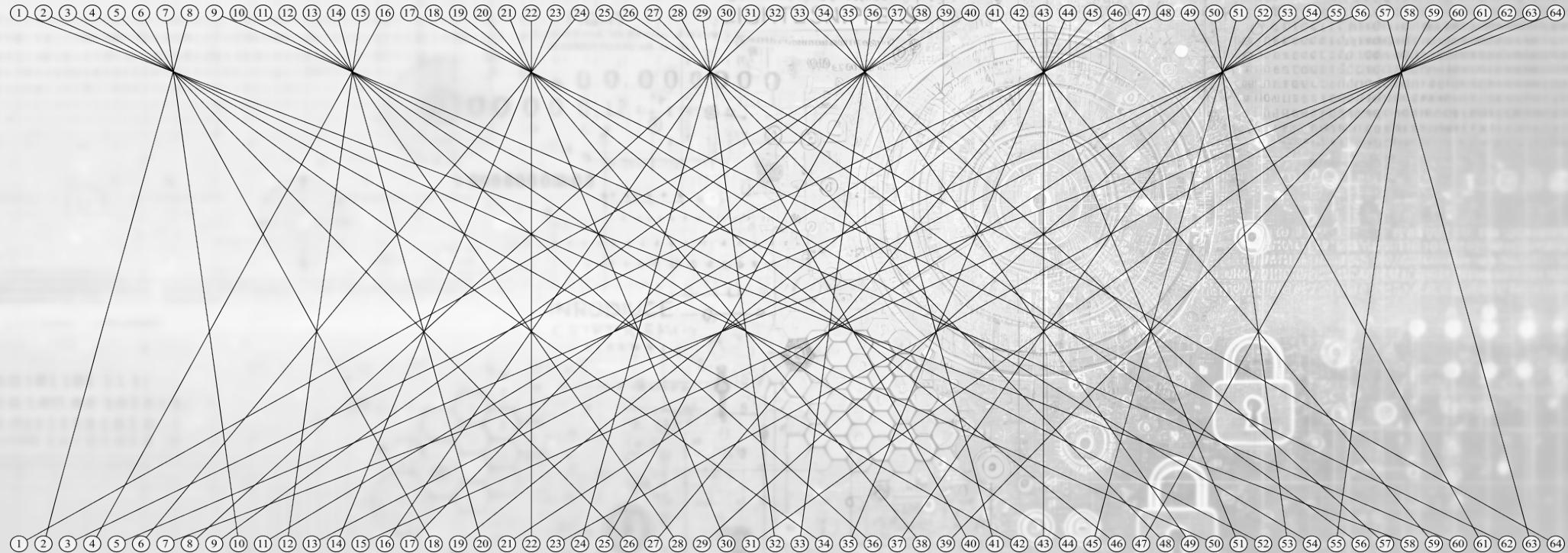
DES – kezdeti permutáció (*IP*)



DES – végső permutáció (IP^{-1})

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	52	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

DES – végső permutáció (IP^{-1})



DES – kulcsütemező függvény (KS)

Algorithm KS:

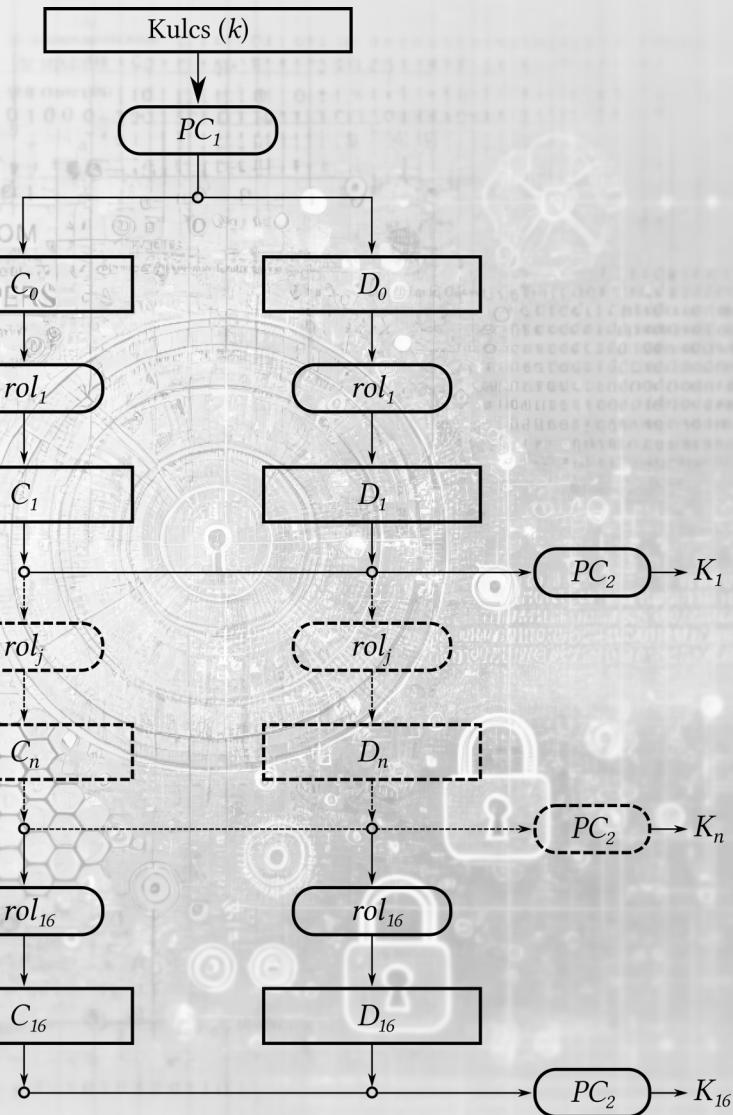
Input: n, k

Output: K_n

```

 $C_0 \parallel D_0 := PC_1(k)$ 
for  $i := 1, \dots, n$  do
    if  $i \in \{1, 2, 9, 16\}$  then
         $j := 1$ 
    else
         $j := 2$ 
    end if
     $C_i := rol(C_{i-1}, j)$ 
     $D_i := rol(D_{i-1}, j)$ 
end for
 $K_n := PC_2(C_n \parallel D_n)$ 
return  $K_n$ 
end Algorithm

```



DES – kulcsütemező függvény (KS)

- a PC_1 (permuted choice) függvény bemenete a k kulcs, kimenete pedig egy 56 bites tömb (kimaradnak a paritásbitek)
- C_n és $D_n(n \in \{0, \dots, 16\})$ egyenként 28 bites adattömbök
- a $rol(X, s)$ eljárás az X tömb bitjeit ciklikusan balra tolja s pozícióval
- a PC_2 függvény bemenete egy 56 bites, kimenete pedig egy 48 bites tömb.

DES – a PC_1 permutáló-kiválasztó függvény

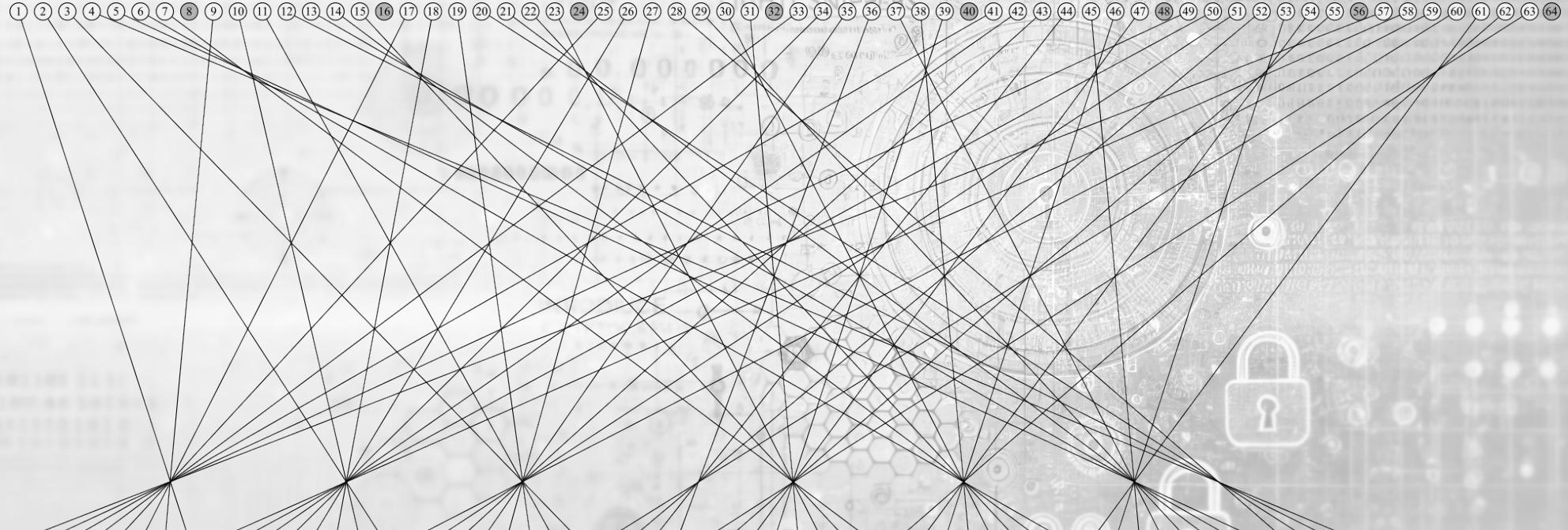
C_0 bitjei:

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

D_0 bitjei:

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

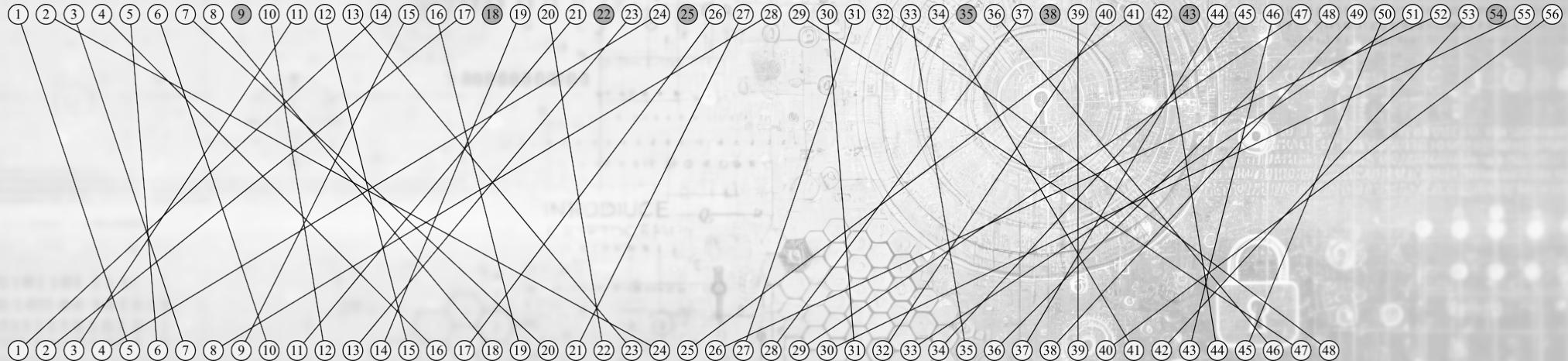
DES – a PC_1 permutáló-kiválasztó függvény



DES – a PC_2 permutáló-kiválasztó függvény

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

DES – a PC_2 permutáló-kiválasztó függvény



DES – az $f(R,K)$ függvény

Algorithm f :

Input: R, K

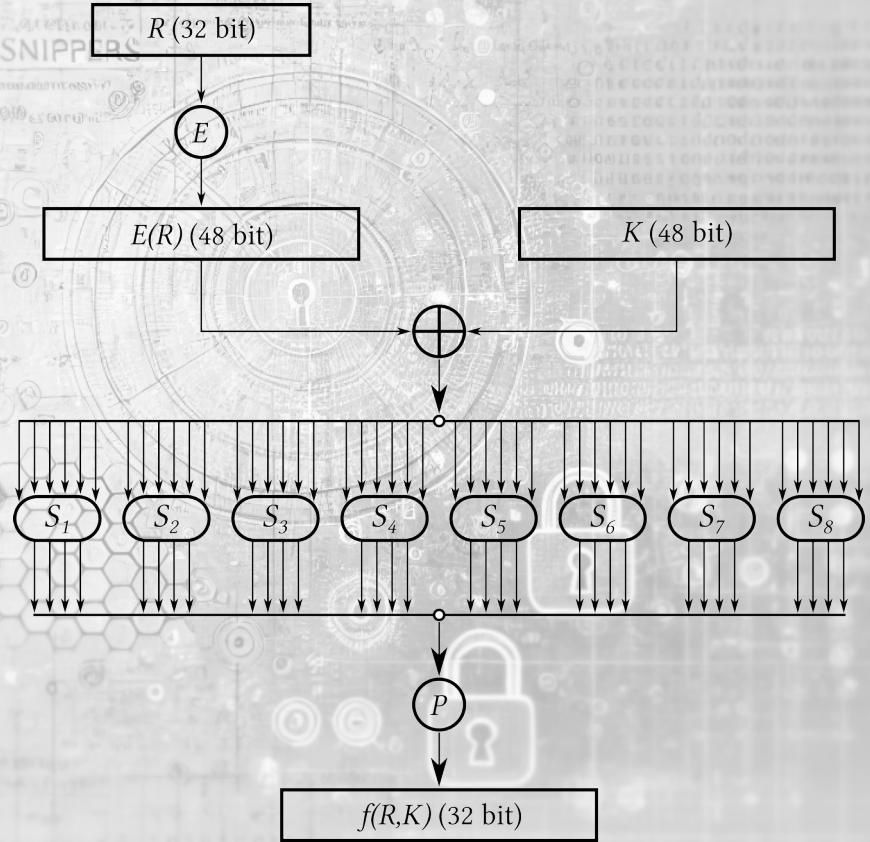
Output: T

$$T_1 \parallel T_2 \parallel T_3 \parallel T_4 \parallel T_5 \parallel T_6 \parallel T_7 \parallel T_8 := K \oplus E(R)$$

$$T := P(S_1(T_1) \parallel S_2(T_2) \parallel \cdots \parallel S_8(T_8))$$

return T

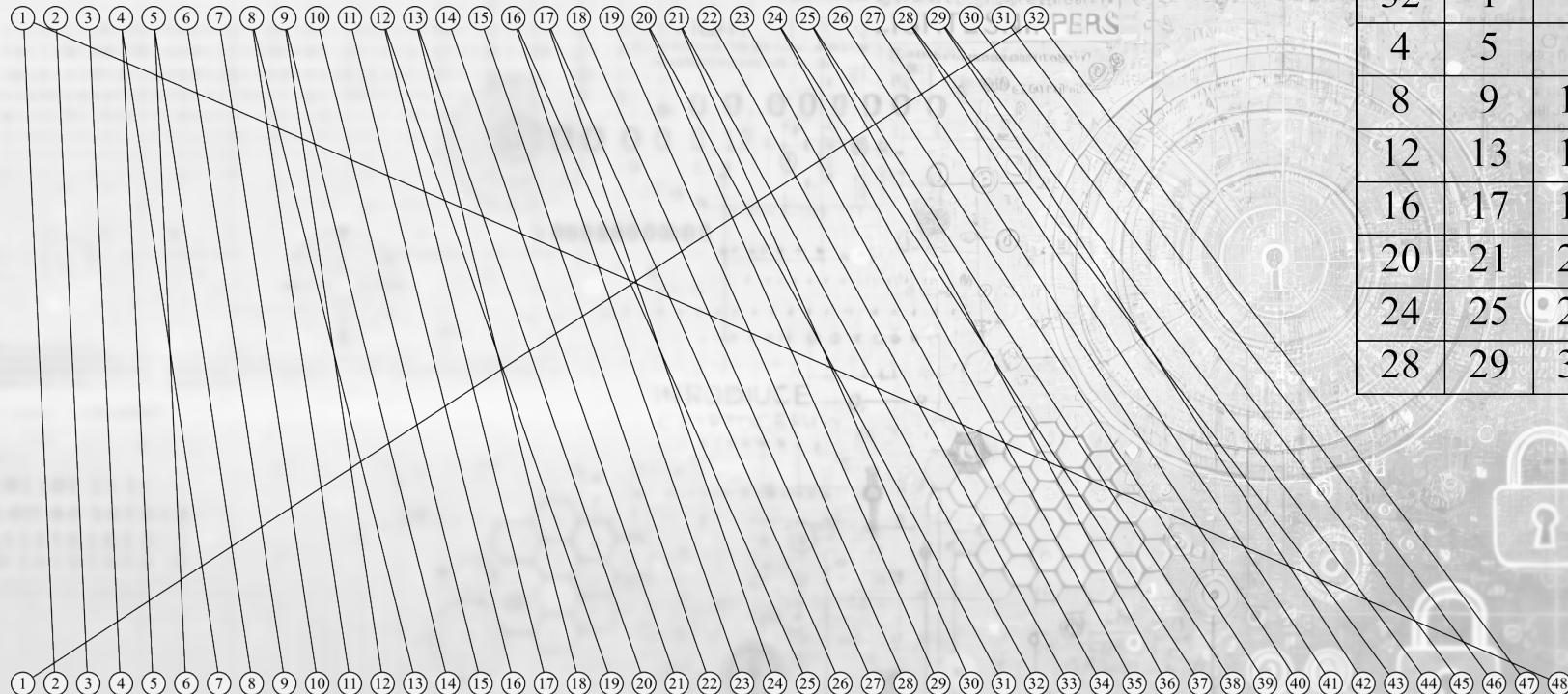
end Algorithm



DES – az $f(R,K)$ függvény

- T_1, T_2, \dots, T_8 egyenként 6 bitesek
- az $f(R,K)$ függvénynek két bemenete van: egy 32 bites tömb (R) és egy 48 bites tömb (K)
- E egy olyan eljárás, ami a 32 bites bemeneti tömb bitjei közül válogatva épít fel egy 48 bites kimenetet (duzzasztófüggvény)
- az S_1, S_2, \dots, S_8 ún. S -dobozok mindegyike 6 bites bemenetből 4 bites kimenetet gyárt

DES – az E duzzasztófüggvény



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

DES – S-dobozok

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
1	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
2	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
3	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
1	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
2	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
3	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
1	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
2	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
3	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
1	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
2	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

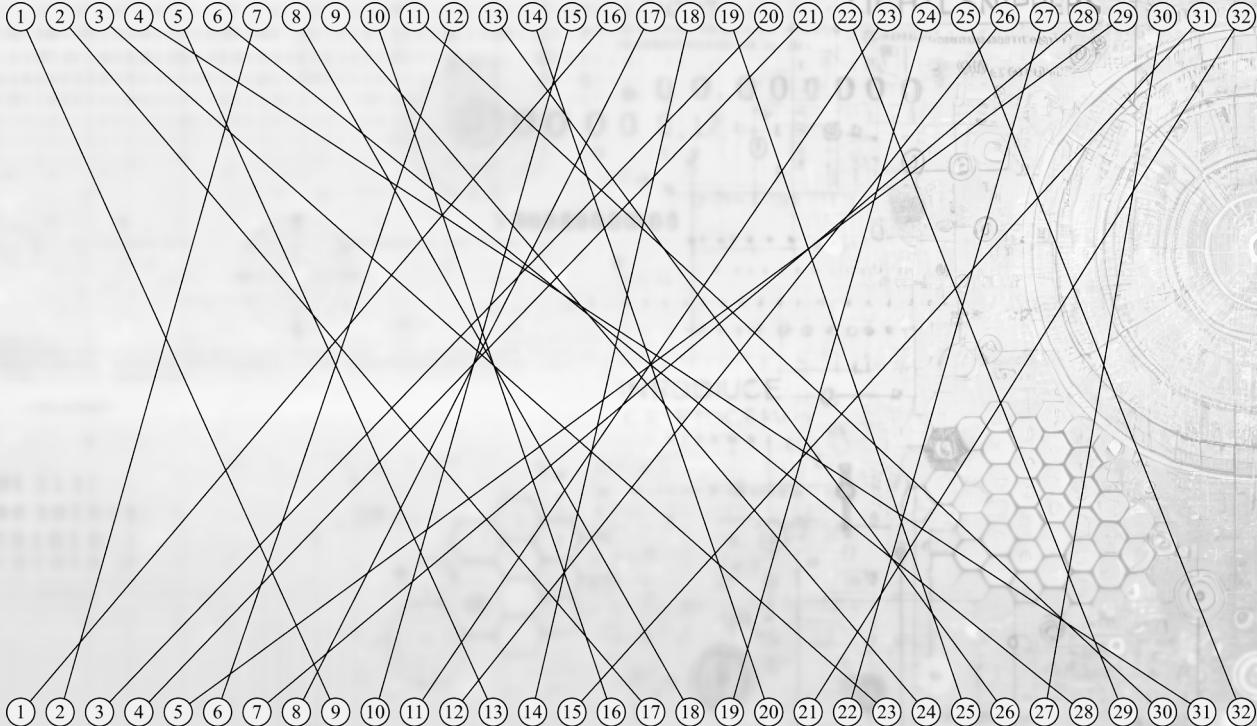
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
1	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
2	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
3	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

DES – S-dobozok

- legyen $\ell \in \{1, \dots, 8\}$ és T az S_ℓ doboz 6 bites bemenete:
 - T első és utolsó bitje kettes számrendszerben meghatároz egy $i \in \{0, 1, 2, 3\}$ számot
 - T középső négy bitje kettes számrendszerben meghatároz egy $j \in \{0, 1, \dots, 15\}$ számot
- megkeressük az S_ℓ táblázatában az i -edik sorban és j -edik oszlopban levő számot – legyen ez $S_\ell[i, j] \in \{0, 1, \dots, 15\}$
- a kimenet az $S_\ell[i, j]$ szám kettes számrendszerben felírásának számjegyeiből áll össze (ha szükséges, akkor ezt nullákkal egészítjük ki balról, hogy az eredmény négy bit hosszú legyen)
- példa: $T = 011011$, $i = (01)_2 = 1$, $j = (1101)_2 = 13$, $S_1(T) = (S_1[1, 13])_2 = 5 = (101)_2 = 0101$

DES – a P permutáció



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

DES (Data Encryption Standard)

Dekódolás:

Algorithm DES (D_k):

Input: C, k

Output: B

$R_{16} \parallel L_{16} := IP(C)$ {kulcstól független}

for $n := 16, \dots, 1$ **do**

$K_n := KS(n, k)$

$R_{n-1} := L_n$

$L_{n-1} := R_n \oplus f(L_n, K_n)$

end for

$B' := L_0 \parallel R_0$

$B := IP^{-1}(B')$ {kulcstól független}

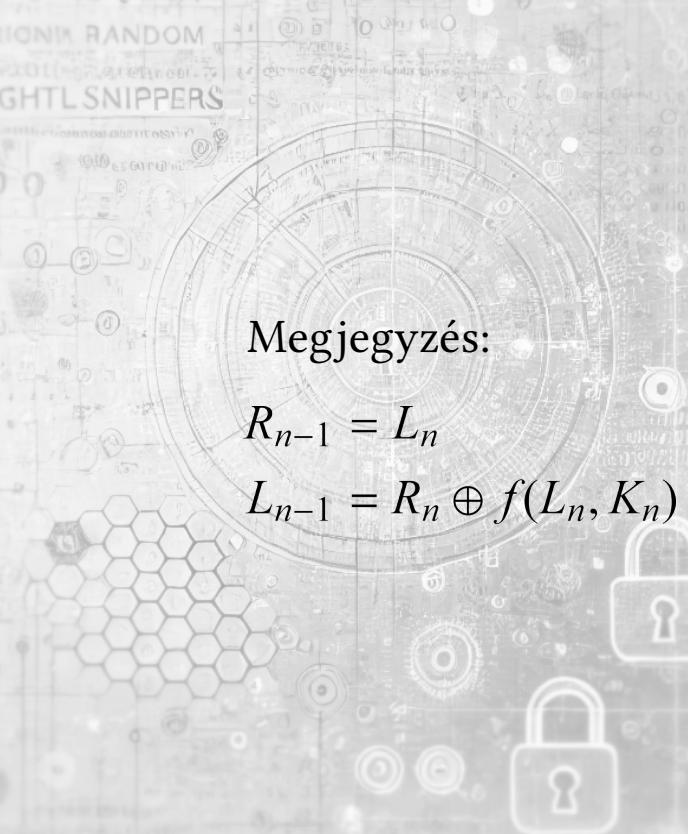
 return B

end Algorithm

Megjegyzés:

$$R_{n-1} = L_n$$

$$L_{n-1} = R_n \oplus f(L_n, K_n)$$



DES (Data Encryption Standard)

Kriptoanalízis:

- Kimerítő kulcskeresés. 1998-ban kimerítő kulcskeresést használva 56 óra alatt találták meg a kulcsot. Hat hónappal később 22 óra alatt sikerült a DES feltörése (100000 személyi számítógéppel)
- Differenciál-kriptoanalízis. A DES úgy volt tervezve, hogy ellenálljon a differenciál-kriptoanalízisnek. Legkevesebb 2^{47} választott üzenet szükséges ahhoz, hogy ez a támadástípus sikeres legyen.
- Lineáris kriptoanalízis. Legkevesebb 2^{43} ismert üzenet szükséges ahhoz, hogy a támadás sikeres legyen.

Lavinahatás a DES esetében

Input:

Permuted:

Round 1:

Round 2:

Round 3:

Round 4:

Round 5:

Round 6:

Round 7:

Round 8:

Round 9:

Round 10:

Round 11:

Round 12:

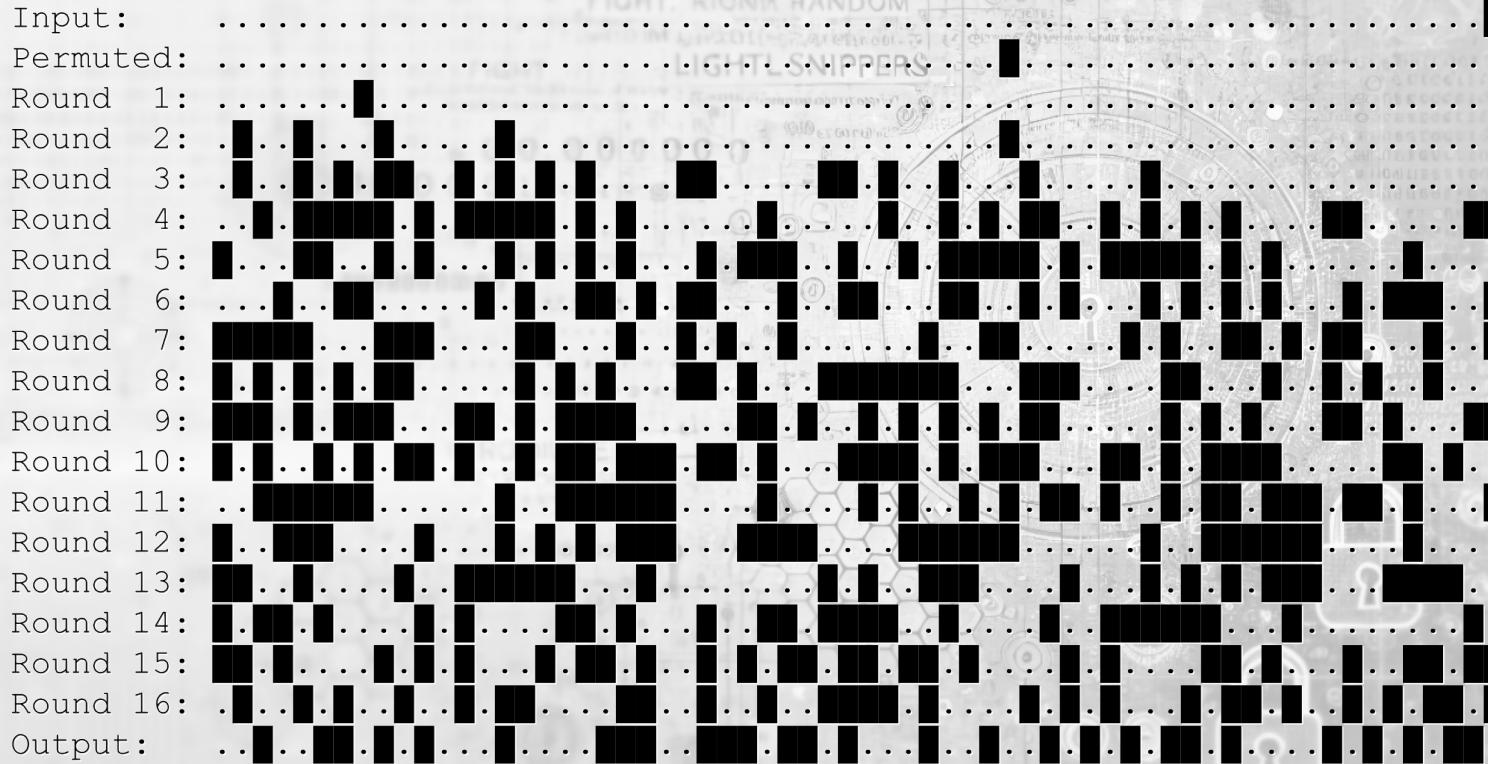
Round 13:

Round 14:

Round 15:

Round 16:

Output:



Megj.: A fekete négyzetek a megváltoztatott biteket jelölik.

TDEA (Triple Data Encryption Algorithm)

- A biztonság növelése érdekében 1999 októberében az amerikai szabványügyi hivatal szabványosítja az úgynévezett tripla-DESt (TDEA).
- ha (k_1, k_2, k_3) három DES-kulcs, akkor:
 - kódolás: $C = E_{k_3}(D_{k_2}(E_{k_1}(P)))$
 - dekódolás: $P = D_{k_1}(E_{k_2}(D_{k_3}(C)))$