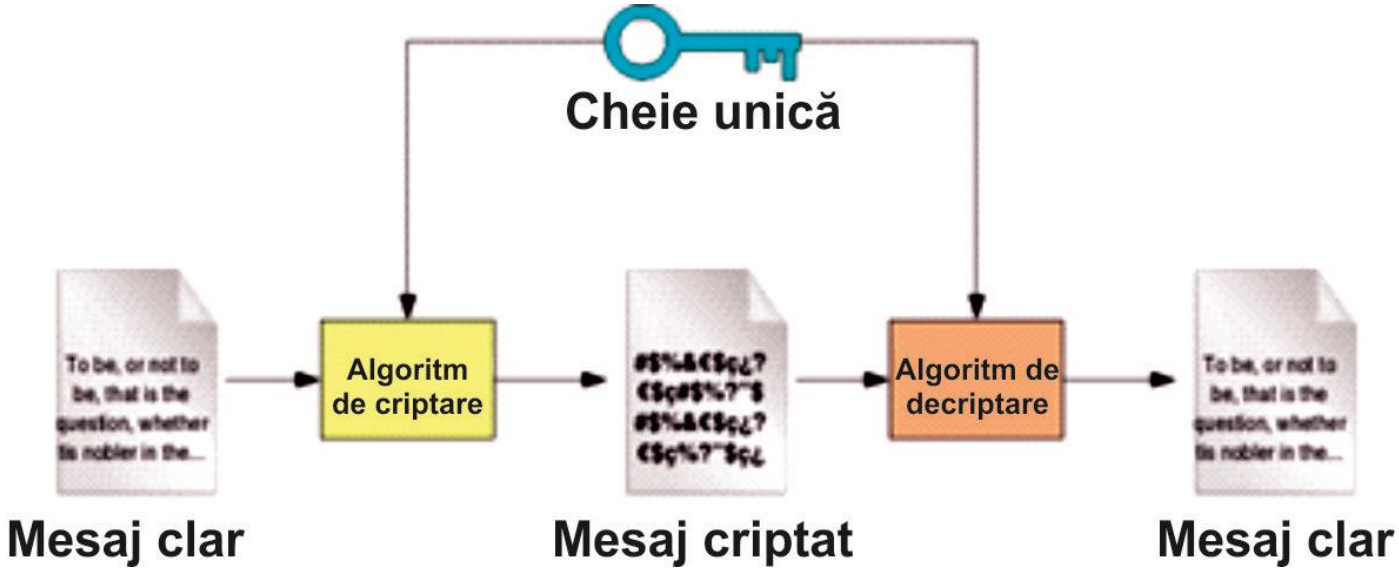
DATA ENCRYPTION STANDARD (DES)

Conf.univ.dr. Ana Cristina Dăscălescu

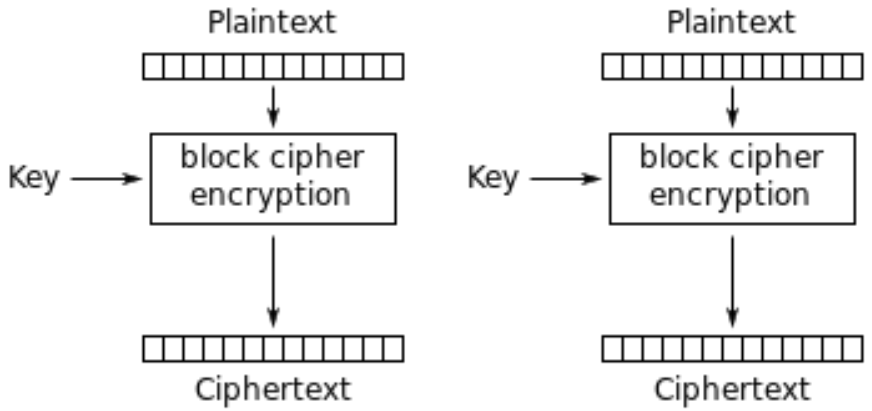
Conf.univ.dr. Radu Boriga

- Utilizează o singură cheie secretă atât pentru procesul de criptare al unui mesaj clar, cât şi pentru procesul de decriptare al unui mesaj criptat.
- Cheia secretă, după ce este în prealabil stabilită şi transmisă pe un canal cu un grad înalt de securitate, va fi folosită în comun atât de către emiţător, cât şi de receptor.



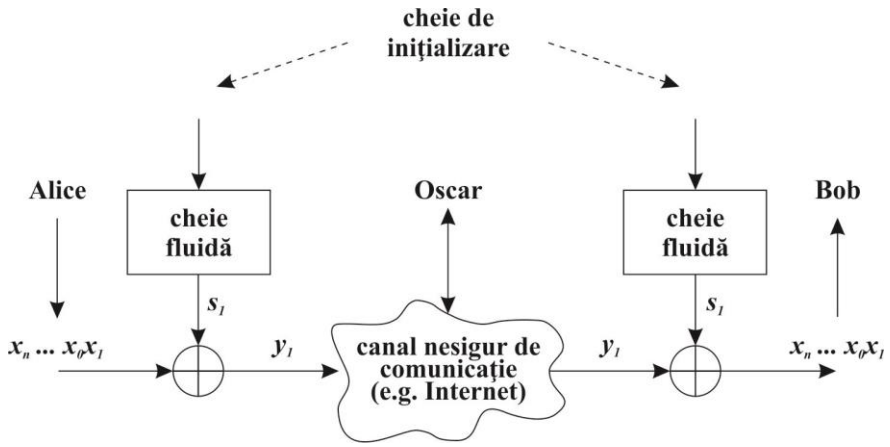
➢ Criptare de tip bloc

- textul este împărţit în blocuri cu aceiaşi dimensiune;
- procesele de criptare/decriptare se realizează prin accesarea bloc cu bloc a textului clar/textului criptat.



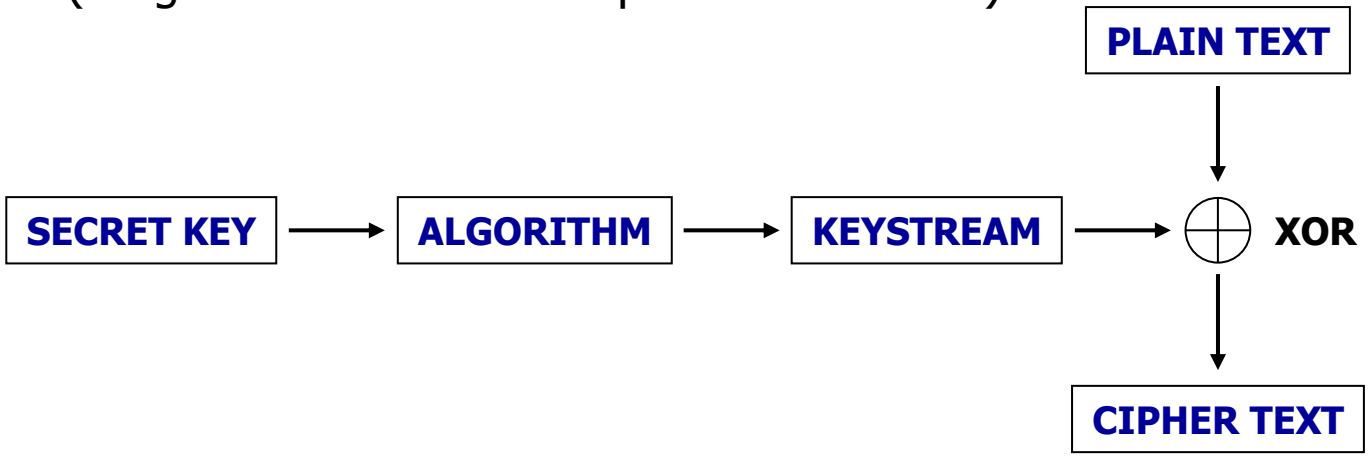
➢ Criptare de tip şir

- textul clar este convertit bit cu bit în text cifrat;
- se utilizează un generator de numere pseudo-aleatoare pentru a obţine o cheie de tip şir;
- se aplică operaţia de XOR între cheia de tip şir şi textul clar/textul criptat.

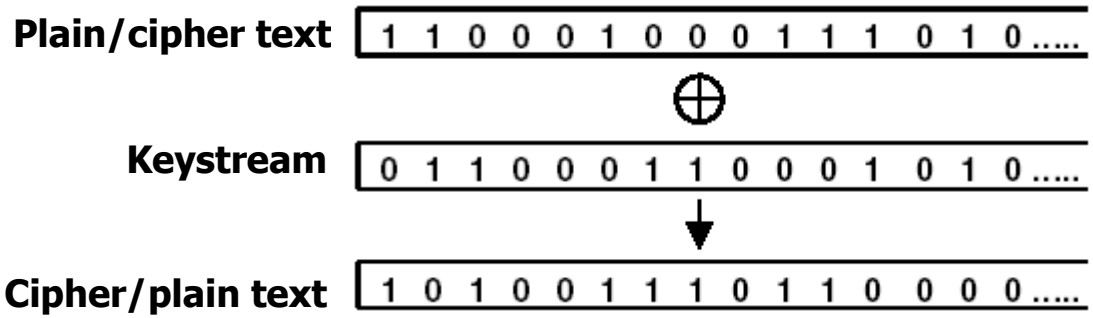


CIFRUL VERNAM

- Criptarea/decriptarea se realizează la nivel de octet, prin XOR-are cu octeți dintr-o cheie fluidă.
- Cheia fluidă se obține dintr-o cheie secretă (de dimensiune mică) folosind un algoritm determinist (un generator de numere pseudo-aleatoare).



- Cifrul de tip Vernam este considerat singurul sistem de criptare complet sigur!



- **Criptare:**

$$C_i = P_i \oplus K_i$$

- **Decriptare:**

$$P_i = C_i \oplus K_i$$

SISTEMUL DE CRIPTARE DES

- **DES (Data Encryption Standard)** a fost dezvoltat de IBM între anii 1972-1976 și adoptat în 1977 de către Biroul Naţional de Standarde, acum Institutul Naţional de Standarde şi Tehnologie (NIST) din SUA, ca standard federal de procesare a informațiilor.

- **DES** este primul standard dedicat protecţiei criptografice a datelor digitale.

- **DES** este un cifru simetric de tip bloc.

- Blocurile au lungimea de **64 biţi** și prelucrate folosind o cheie formată din **56 biţi**.

- Viteza de criptare/decriptare depinde de implementare, în general fiind cuprinsă între **10-20 MB/s**.

- Privit în ansamblu, DES este o combinaţie a două tehnici elementare de criptare, confuzie şi difuziune, implementate folosind **rețele Feistel**.

➢ Principiile lui Claude Shannon:

- Pentru ca un sistem de criptare să fie sigur, trebuie ca el să implementeze următoarele două primitive criptografice:

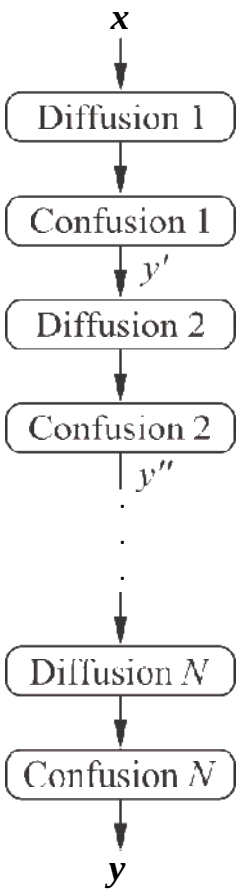
  1. **Confuzia:** Relația dintre textul cifrat și cheia secretă trebuie să fie cât mai complicată.

  2. **Difuzia:** Fiecare bit din textul clar trebuie să influențeze valorile a cât mai multor biți din textul criptat, în scopul de a ascunde proprietățile statistice ale textului clar.

- **Confuzia** este asigurată printr-o operație de substituție!

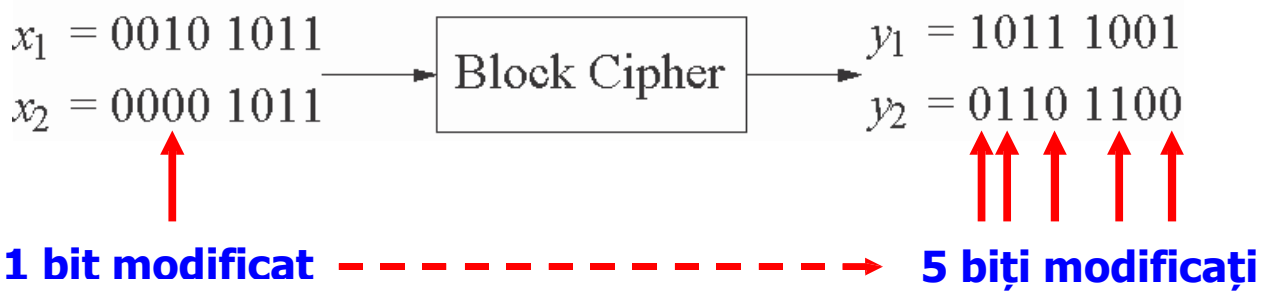
- **Difuzia** este asigurată printr-o operație de permutare!

- Pentru a obține un cifru cu o securitate ridicată, cele două primitive criptografice trebuie combinate într-un **cifru compus**.

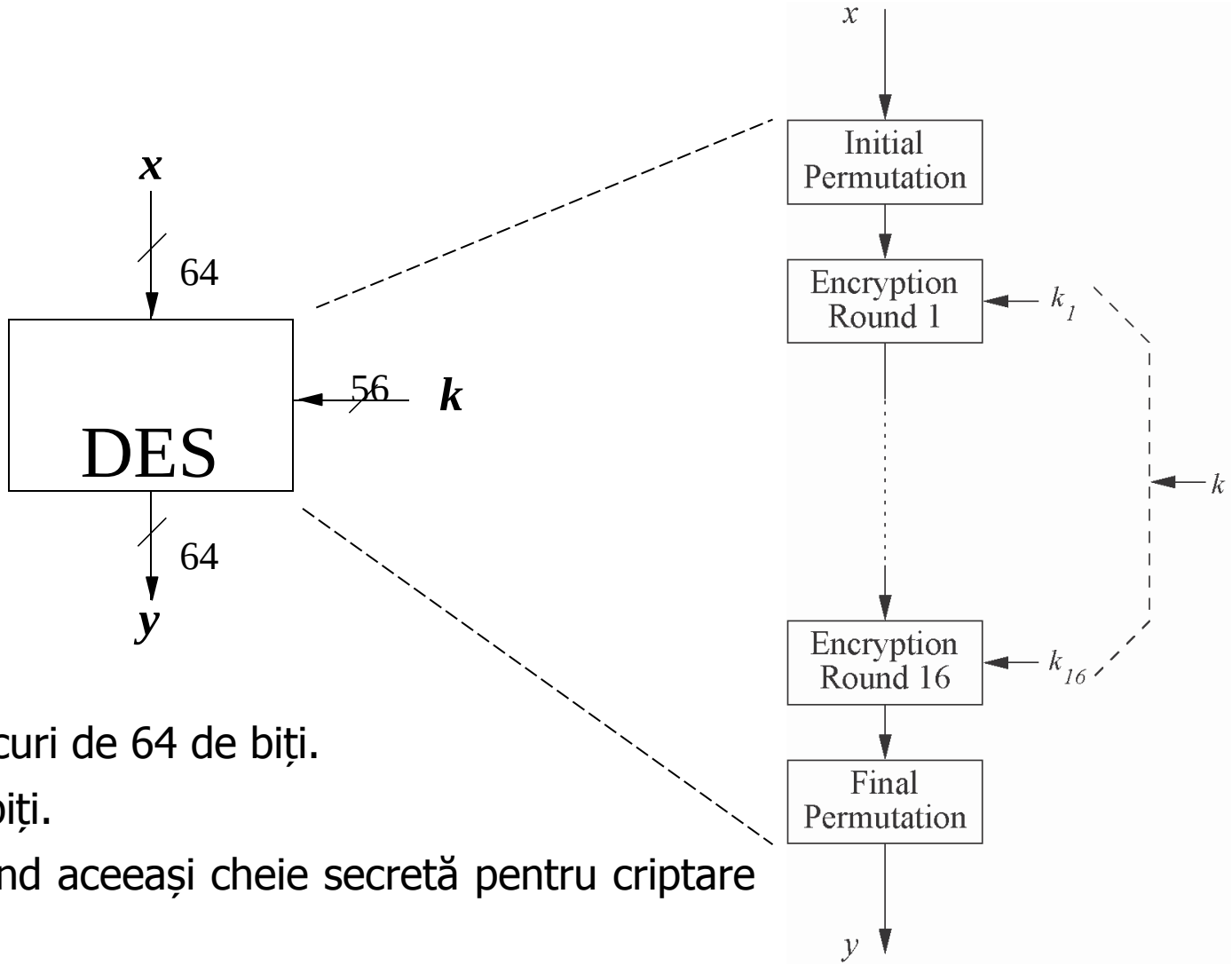


- Majoritatea cifrurilor actuale sunt cifruri compuse, fiind formate din mai multe runde care sunt aplicate în mod repetat asupra textului clar/criptat.

- Cifrurile compuse au o difuzie foarte bună, respectiv modificarea unui singur bit din textul clar conduce la modificarea a mai mult de jumătate din biții textului criptat!



SISTEMUL DE CRIPTARE DES

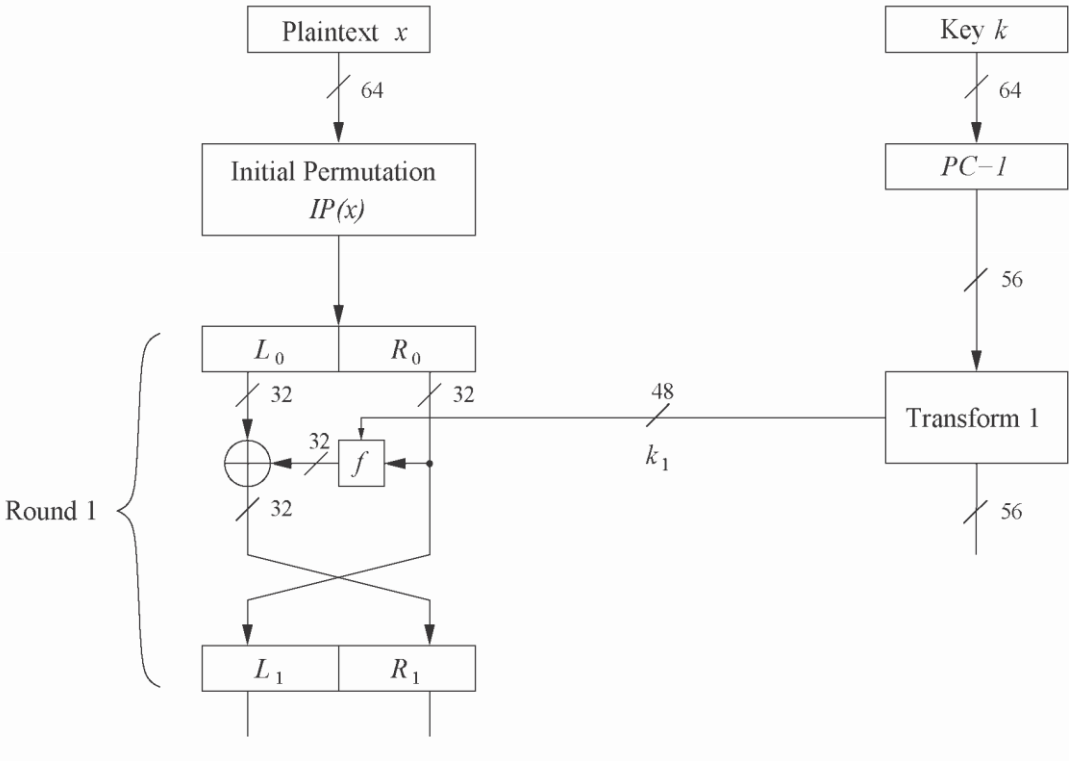


- Criptează/decriptează în blocuri de 64 de biți.
- Folosește o cheie de 56 de biți.
- Este un cifru simetric, folosind aceeași cheie secretă pentru criptare și decriptare.
- Utilizează 16 runde care efectuează toate aceleași operații.
- În fiecare rundă este utilizată o subcheie derivată din cheia secretă.

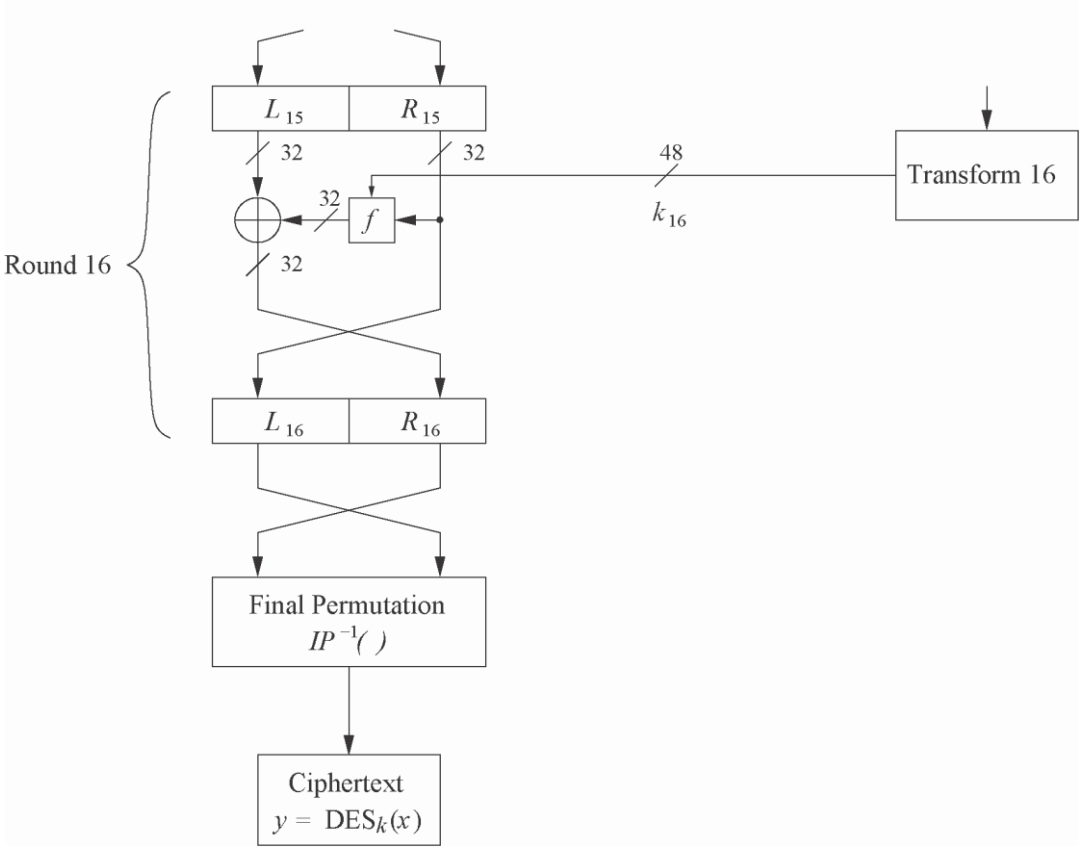
SISTEMUL DE CRIPTARE DES

- DES utilizează rețele Feistel.
- Inițial, se efectuează o permutare a biților textului clar, după care se efectuează 16 runde identice:
  1. Un bloc de 64 de biți este împărțit în două blocuri L_i și R_i, având 32 de biți fiecare
  2. Asupra blocului R_i se aplică funcția f, iar rezultatul obținut este XOR-at cu blocul L_i
  3. Blocurile L_i și R_i sunt interschimbate
- O rundă poate fi exprimată matematic astfel:

$$L_{i+1} = R_i$$
$$R_{i+1} = L_i \oplus f(R_i, K_i)$$



- După cele 16 runde, se mai efectuează o permutare finală a biților, utilizând inversa permutării inițiale.

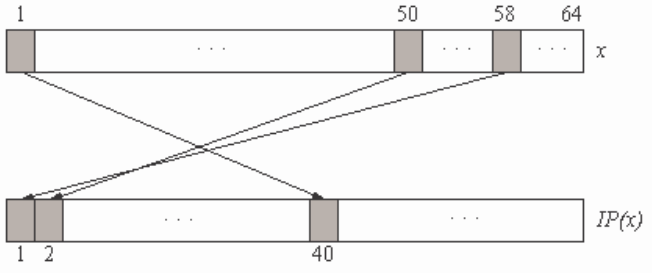


➢ Permutare inițială IP și permutarea finală IP^{-1}

- Sunt permutări la nivel de bit, inverse una celeilalte.

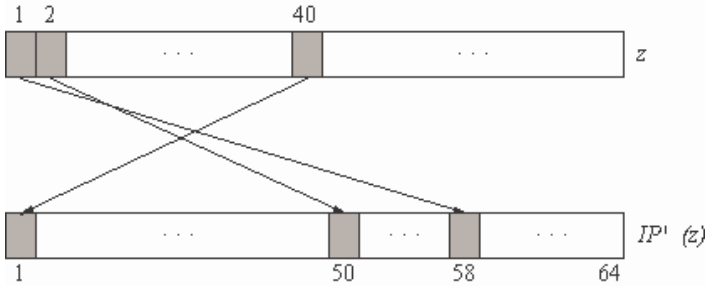
Permutarea inițială IP

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



Permutarea finală IP^{-1}

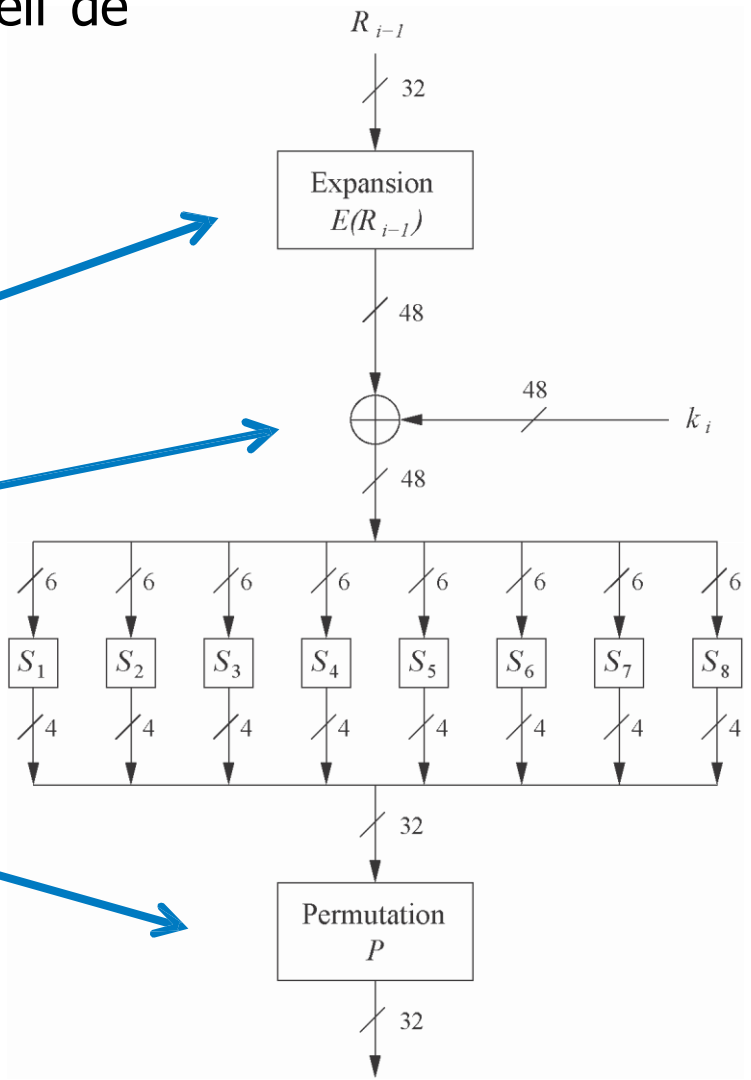
IP^{-1}							
40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25



➢ Funcția f

- Funcția f se aplică asupra blocului R_{i-1} și cheii de rundă K_i, efectuând următoarele 4 operații:

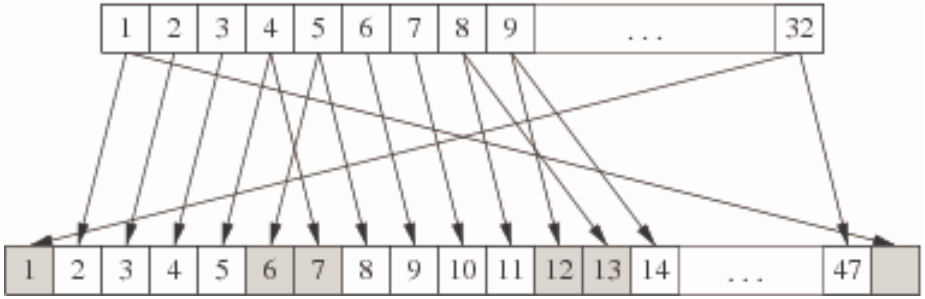
1. **Expansiunea E**
2. **XOR cu cheia de rundă**
3. **Substituția cu S-box-uri**
4. **Permutarea de rundă P**

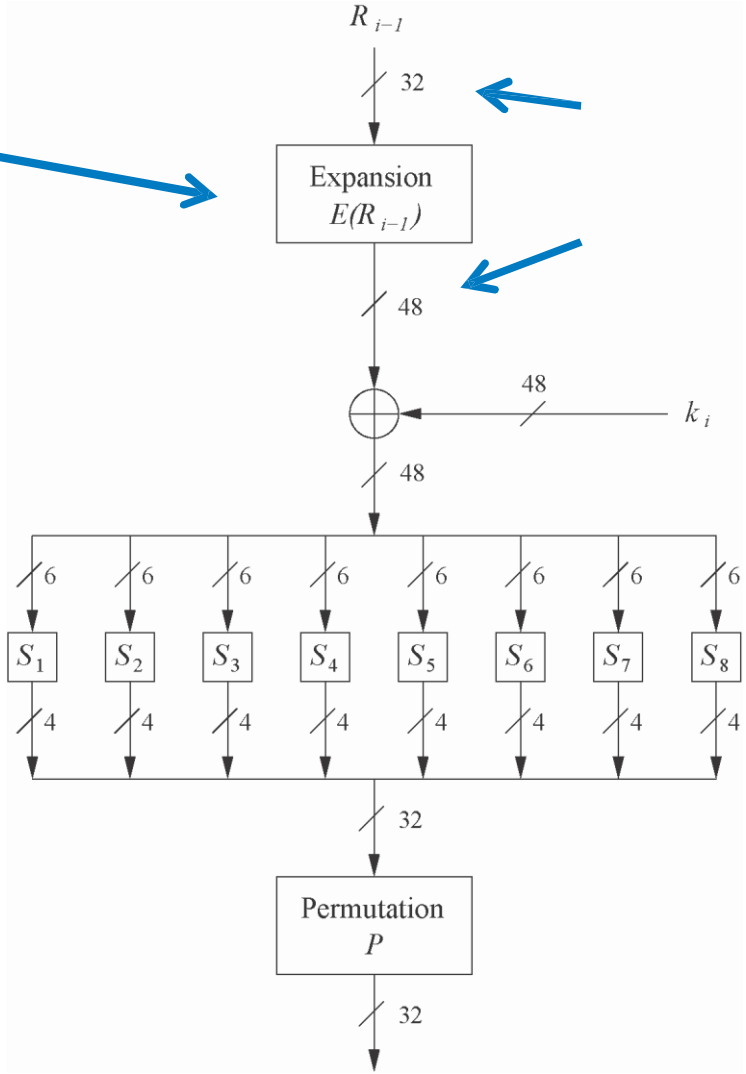


1. Funcția de expansiune E

- Funcția de expansiune E are rolul de a crește difuzia!

E					
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

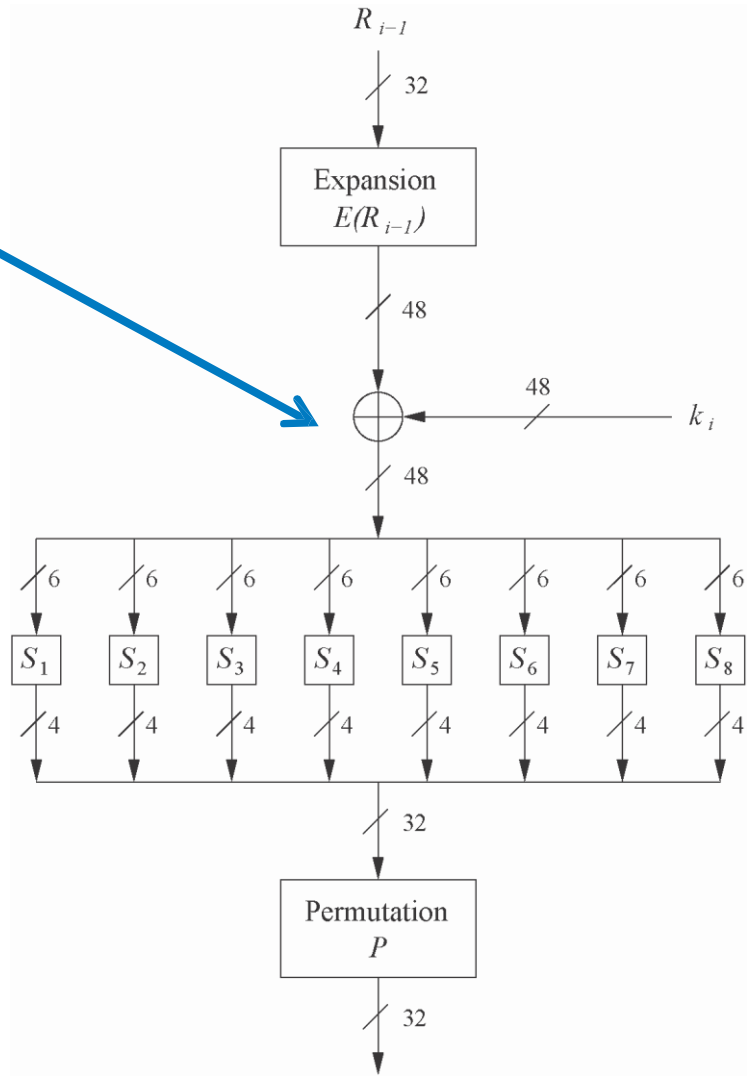




2. XOR cu cheia de rundă

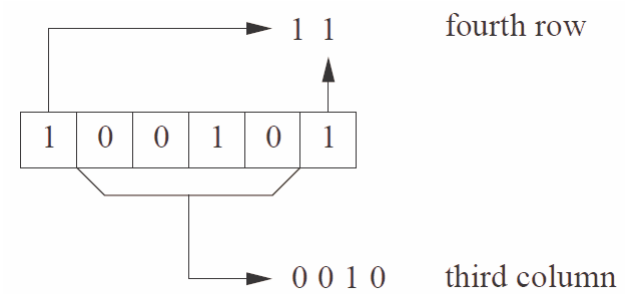
- Se aplică o operație XOR între valoarea obținută la ieșirea funcției de expansiune E și cheia de rundă K_i.

- Cheia de rundă K_i se obține din cheia secretă, folosind un algoritm specific.

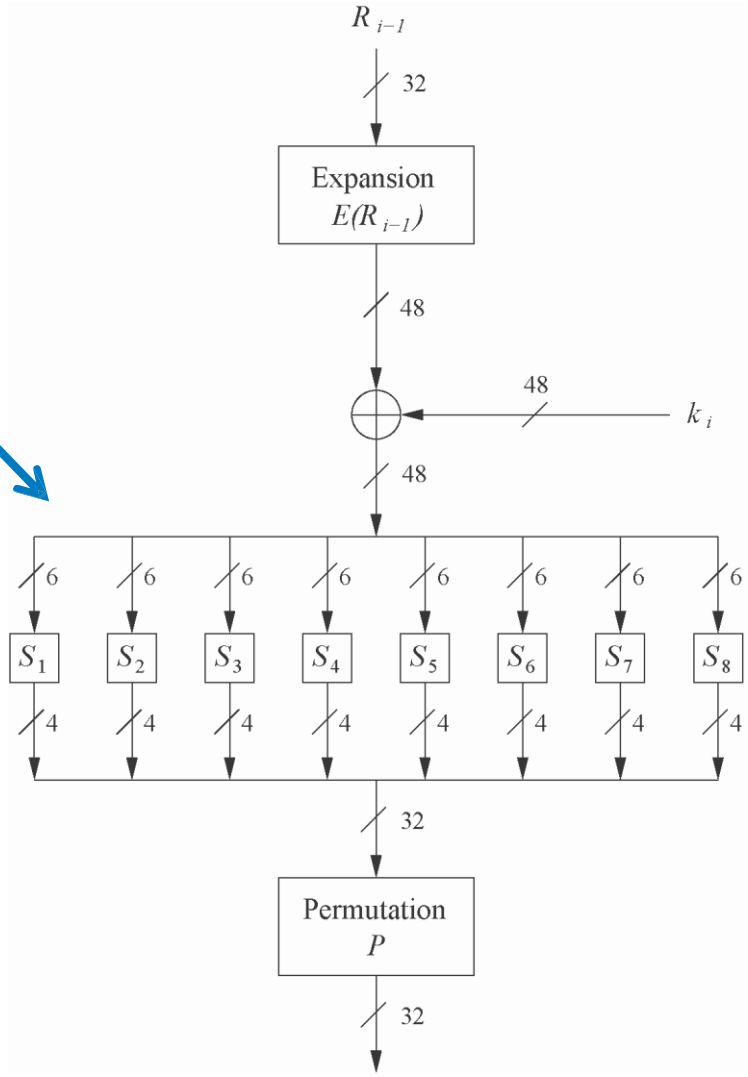


3. Cutiile de substituție

- DES folosește 8 cutii de substituție (S-box).
- O cutie primește la intrare 6 biți și furnizează 4 biți la ieșire.
- Cutiile sunt neliniare și rezistente la criptanaliza diferențială.
- Cutiile induc securitatea DES!



S_1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	04	13	01	02	15	11	08	03	10	06	12	05	09	00	07
1	00	15	07	04	14	02	13	01	10	06	12	11	09	05	03	08
2	04	01	14	08	13	06	02	11	15	12	09	07	03	10	05	00
3	15	12	08	02	04	09	01	07	05	11	03	14	10	00	06	13

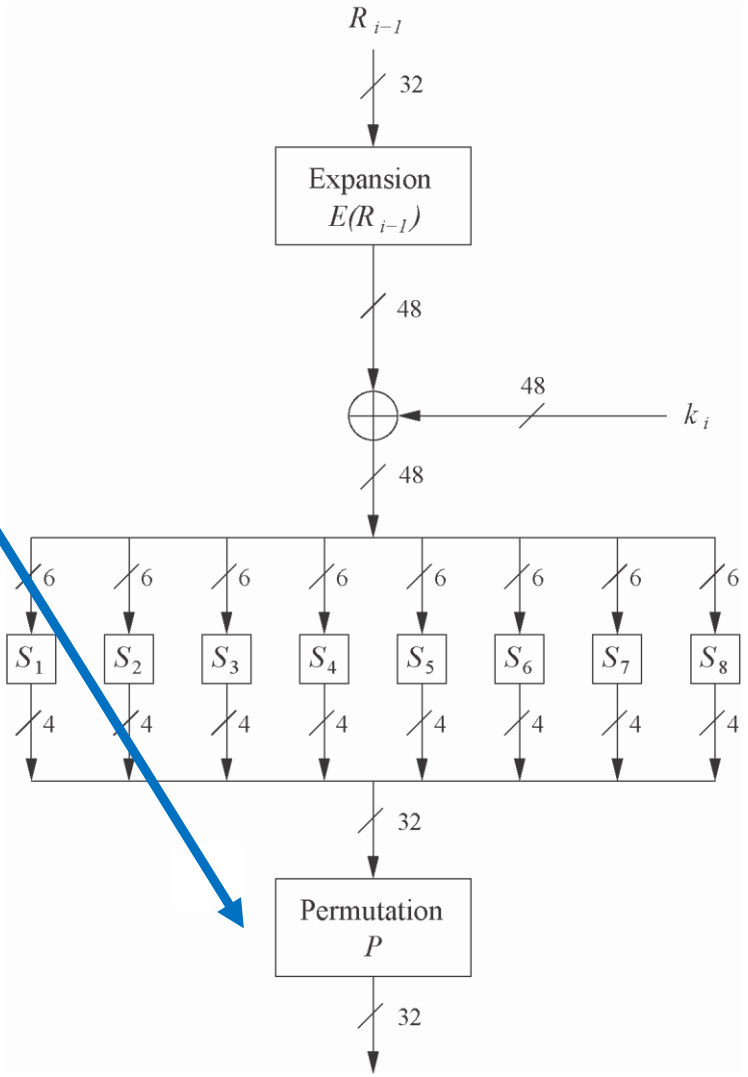


- **Reguli de design ale cutiilor de substituție:**

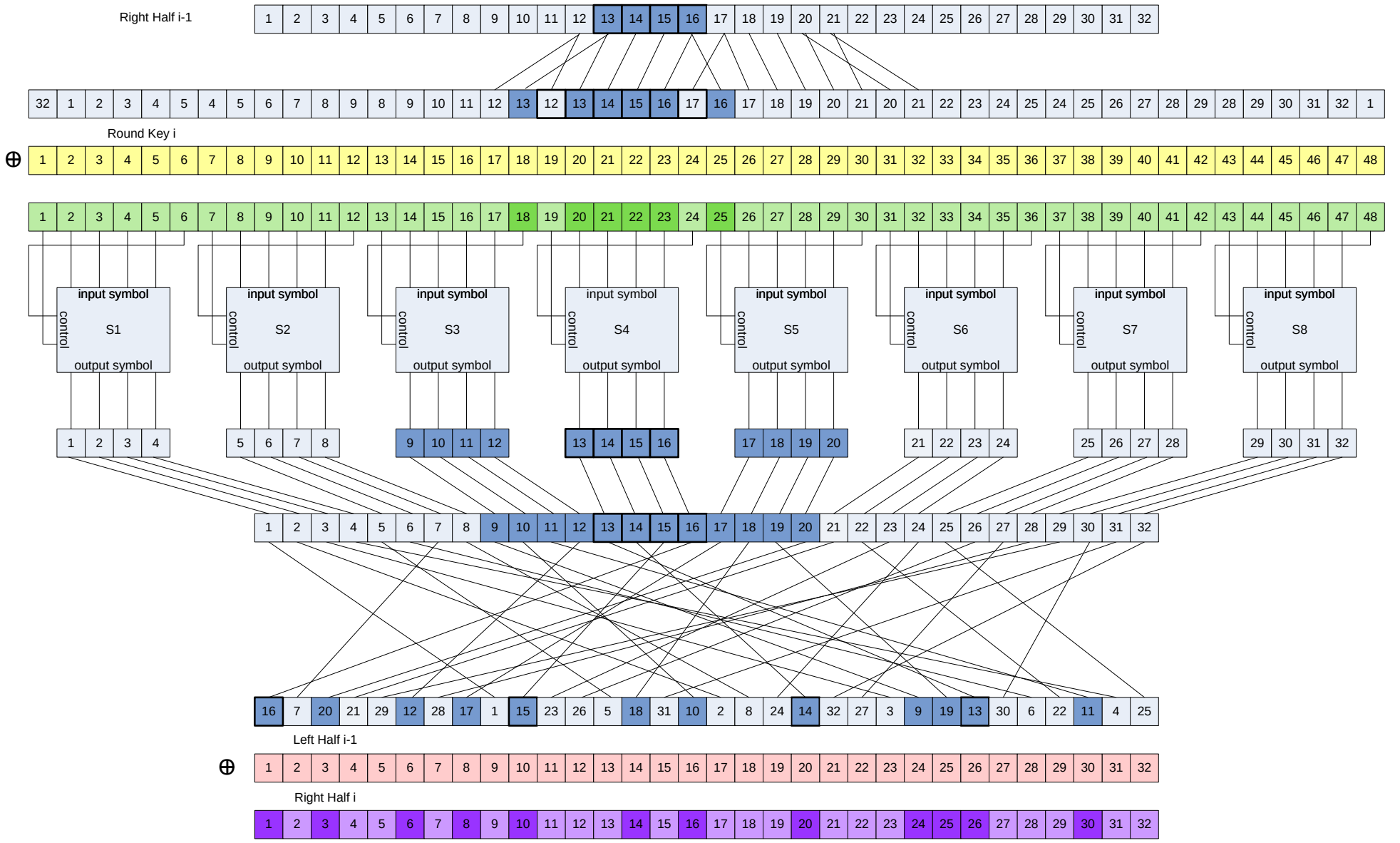
1. Fiecare linie este o permutare a numerelor $0,\ldots,15$.
2. Nici o cutie nu este o funcție liniară sau afină.
3. Modificarea unui bit din operand provoacă modificarea a cel puțin 2 biți din rezultat.
4. Pentru orice cutie S și orice secvență α de lungime 6, $S(\alpha)$ și $S(\alpha \oplus 001100)$ diferă prin cel puțin 2 biți.

4. Permutarea de rundă P

- Este o permutare la nivel de bit, care crește difuzia.
- Practic, după aplicarea permutării P, biții de la ieșirea unei cutii de substituție vor afecta mai multe cutii de substituție în runda următoare.
- Difuzia indusă de funcția de expansiune, cutiile de substituție și permutarea de rundă garantează faptul ca după a cincea rundă fiecare bit din textul criptat depinde de fiecare bit al cheii secrete și de fiecare bit al textului clar!



SISTEMUL DE CRIPTARE DES

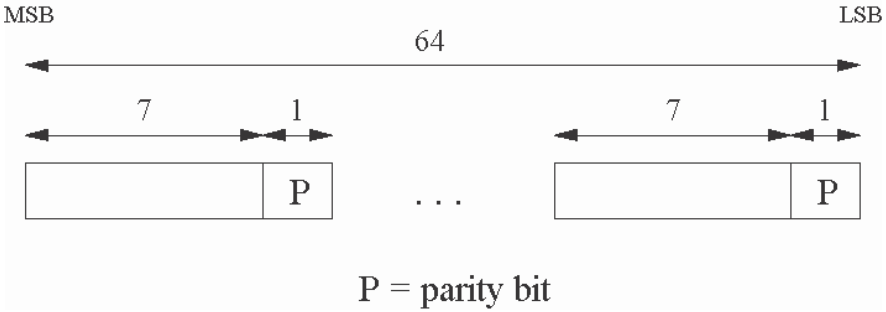


➢ Numărul biților care se modifică în fiecare rundă

(a) Change in Plaintext		(b) Change in Key	
Round	Number of bits that differ	Round	Number of bits that differ
0	1	0	0
1	6	1	2
2	21	2	14
3	35	3	28
4	39	4	32
5	34	5	30
6	32	6	32
7	31	7	35
8	29	8	34
9	42	9	40
10	44	10	38
11	32	11	31
12	30	12	33
13	30	13	28
14	26	14	26
15	29	15	34
16	34	16	35

➢ Generarea cheilor de rundă

- Din cheia secretă, cu lungimea de 56 de biți, sunt derivate 16 chei de rundă K_i, cu lungimea de 48 de biți fiecare.
- Lungimea efectivă a cheii DES este de 64 de biți: 56 de biți pentru cheia secretă și 8 biți de paritate:



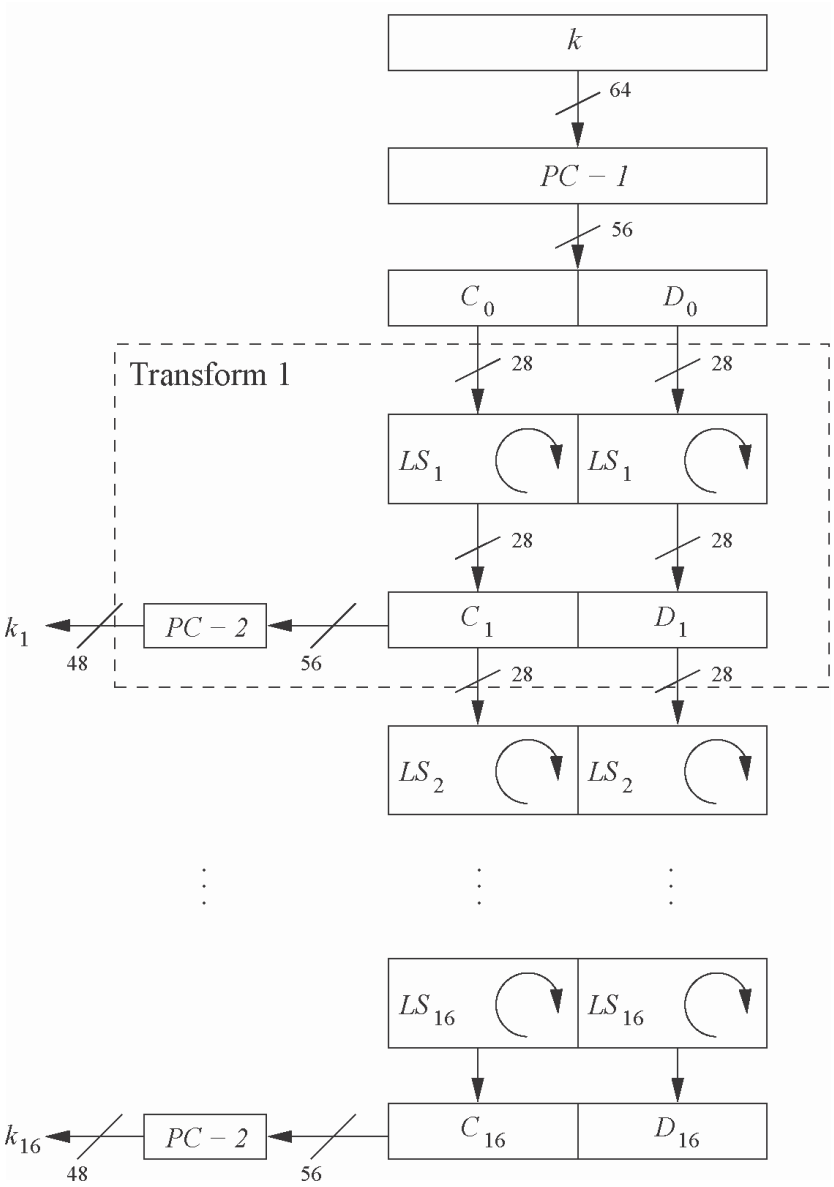
- Biții de paritate sunt eliminați de permutarea PC-1:

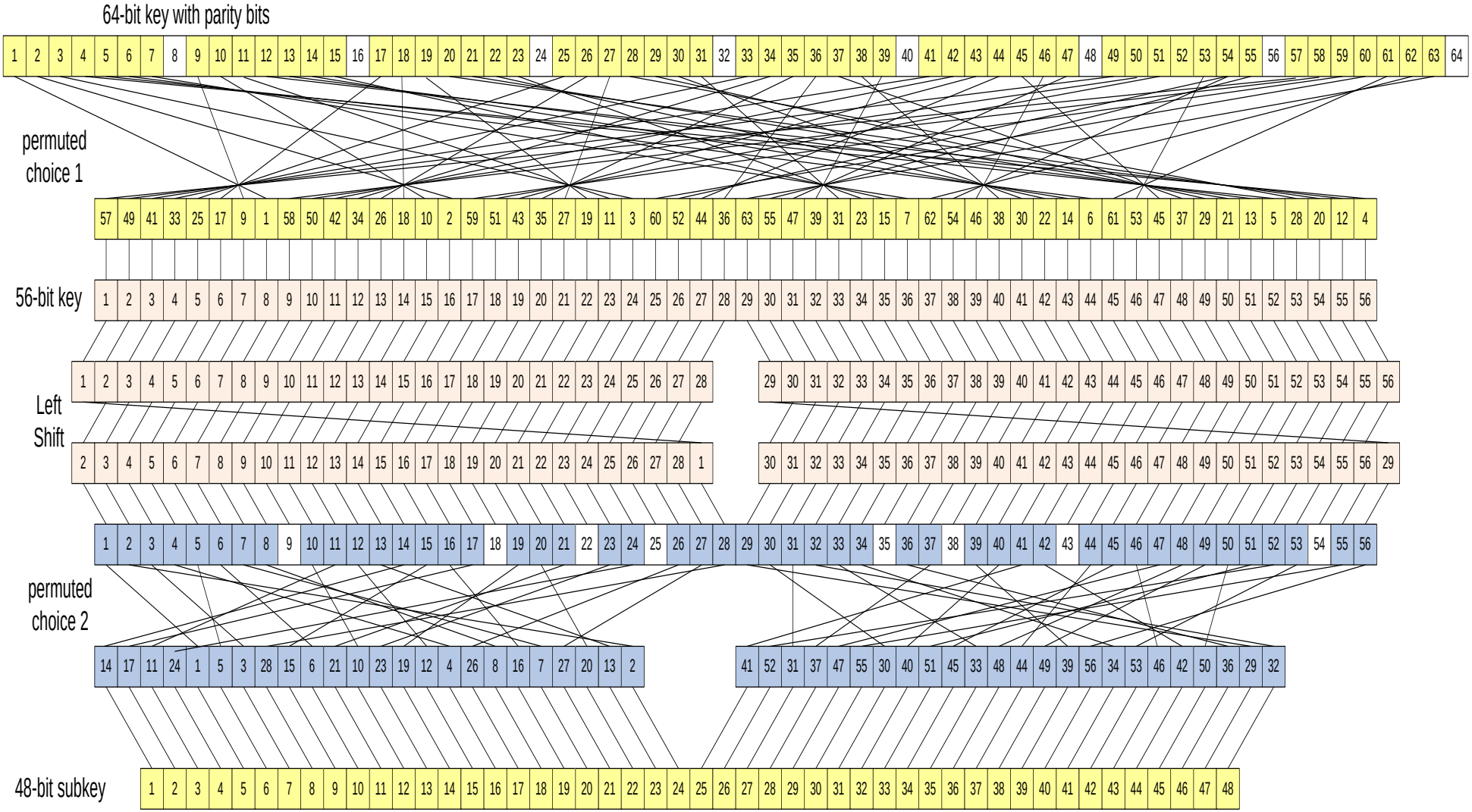
$PC-1$							
57	49	41	33	25	17	9	1
58	50	42	34	26	18	10	2
59	51	43	35	27	19	11	3
60	52	44	36	63	55	47	39
31	23	15	7	62	54	46	38
30	22	14	6	61	53	45	37
29	21	13	5	28	20	12	4

SISTEMUL DE CRIPTARE DES

- Cheia secretă este împărțită în două blocuri C_0 și D_0 de câte 28 de biți fiecare.
- În rundele 1, 2, 9 și 16 ambele blocuri sunt rotite cu un bit spre stânga.
- În toate celelalte runde, cele două blocuri sunt rotite cu 2 biți spre stânga.
- În fiecare rundă, o permutare PC-2 selectează o submulțime de 48 de biți din C_i și D_i pentru a forma cheia de rundă K_i.
- Numărul total al rotațiilor pe biți efectuate este 4 x 1 + 12 x 2 = 28, deci $C_0 = C_{16}$ și $D_0 = D_{16}$!

$PC-2$							
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




64-bit key with parity bits
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 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64
permuted choice 1
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
56-bit key
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 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56
Left Shift
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 26 27 28
29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56
2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 1
30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 29
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 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56
permuted choice 2
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
48-bit subkey
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 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48

➢ Chei slabe

Keys before parities drop (64 bits)	*Actual key (56 bits)*
0101 0101 0101 0101	0000000 0000000
1F1F 1F1F 0E0E 0E0E	0000000 FFFFFFF
E0E0 E0E0 F1F1 F1F1	FFFFFFF 0000000
FEFE FEFE FEFE FEFE	FFFFFFF FFFFFFF

➢ Chei semislabe

First key in the pair	*Second key in the pair*
01FE 01FE 01FE 01FE	FE01 FE01 FE01 FE01
1FE0 1FE0 0EF1 0EF1	E01F E01F F10E F10E
01E0 01E1 01F1 01F1	E001 E001 F101 F101
1FFE 1FFE 0EFE 0EFE	FE1F FE1F FE0E FE0E
011F 011F 010E 010E	1F01 1F01 0E01 0E01
E0FE E0FE F1FE F1FE	FEE0 FEE0 FEF1 FEF1

➢ Criptanaliza DES

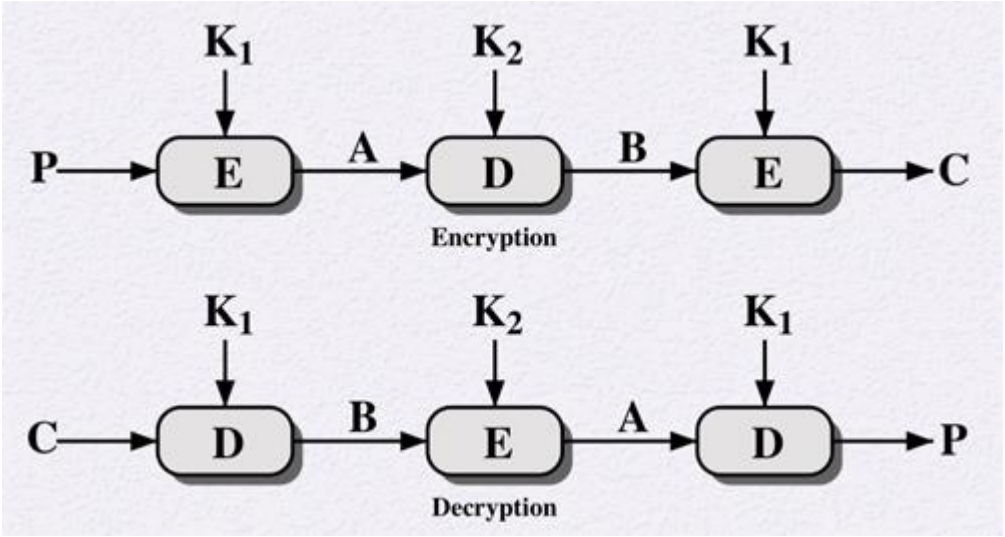
- **Forța brută**
  - cheie de criptare este de 56 de biţi, deci "forța brută" presupune generarea tuturor combinaţiilor posibile (2^{56})
- **Criptanaliză diferențială**
  - a fost propusă de către Adi Shamir și Eli Biham în 1990
  - se analizează influența unei diferențe constante dintre două texte clare asupra diferenței dintre textele criptate corespunzătoare
  - atacul are succes asupra DES dacă se analizează aproximativ 2^{47} perechi de octeți de forma text clar/text criptat
- **Criptanaliză liniară**
  - a fost propusă de către Mitsuru Matsui în 1993
  - urmărește construcția unui sistem de ecuații liniare între biții textului clar, ai textului criptat și ai cheii
  - atacul are succes asupra DES dacă se analizează aproximativ 2^{43} perechi de octeți de forma text clar/text criptat

Year	Proposed/ implemented DES Attack
1977	Diffie & Hellman, (under-)estimate the costs of a key search machine
1990	Biham & Shamir propose differential cryptanalysis (2^{47} chosen ciphertexts)
1993	Mike Wiener proposes design of a very efficient key search machine: Average search requires 36h. Costs: $1.000.000
1993	Matsui proposes linear cryptanalysis (2^{43} chosen ciphertexts)
Jun. 1997	DES Challenge I broken, 4.5 months of distributed search
Feb. 1998	DES Challenge II--1 broken, 39 days (distributed search)
Jul. 1998	DES Challenge II--2 broken, key search machine *Deep Crack* built by the Electronic Frontier Foundation (EFF): 1800 ASICs with 24 search engines each, Costs: $250 000, 15 days average search time (required 56h for the Challenge)
Jan. 1999	DES Challenge III broken in 22h 15min (distributed search assisted by *Deep Crack*)
2006-2008	Reconfigurable key search machine *COPACOBANA* developed at the Universities in Bochum and Kiel (Germany), uses 120 FPGAs to break DES in 6.4 days (avg.) at a cost of $10 000.

➢ Sistemul de criptare 3DES

- Sistemul **3DES** este utilizat pentru a crește dimensiunea cheii DES la 112 biți.

$$C = Enc_{K_3}(Dec_{K_2}(Enc_{K_1}(P)))$$



$$P = Dec_{K_3}(Enc_{K_2}(Dec_{K_1}(P)))$$

➢ Moduri de utilizare 3DES:

- $K_1 \neq K_2 \neq K_3 \Longrightarrow$ cheia are lungimea 168 de biți, dar securitatea este echivalentă cu cea indusă de o cheie de 112 biți
- $K_1 \neq K_2, K_3 = K_1 \Longrightarrow$ cheia are lungimea 112 de biți
- $K_1 = K_2 = K_3 \Longrightarrow$ cheia are lungimea 56 de biți, fiind echivalent cu sistemul DES

➢ Criptanaliza 3DES

- Până în prezent, nu se cunoaște nici un atac criptanalitic care să poată fi efectuat într-un timp util!