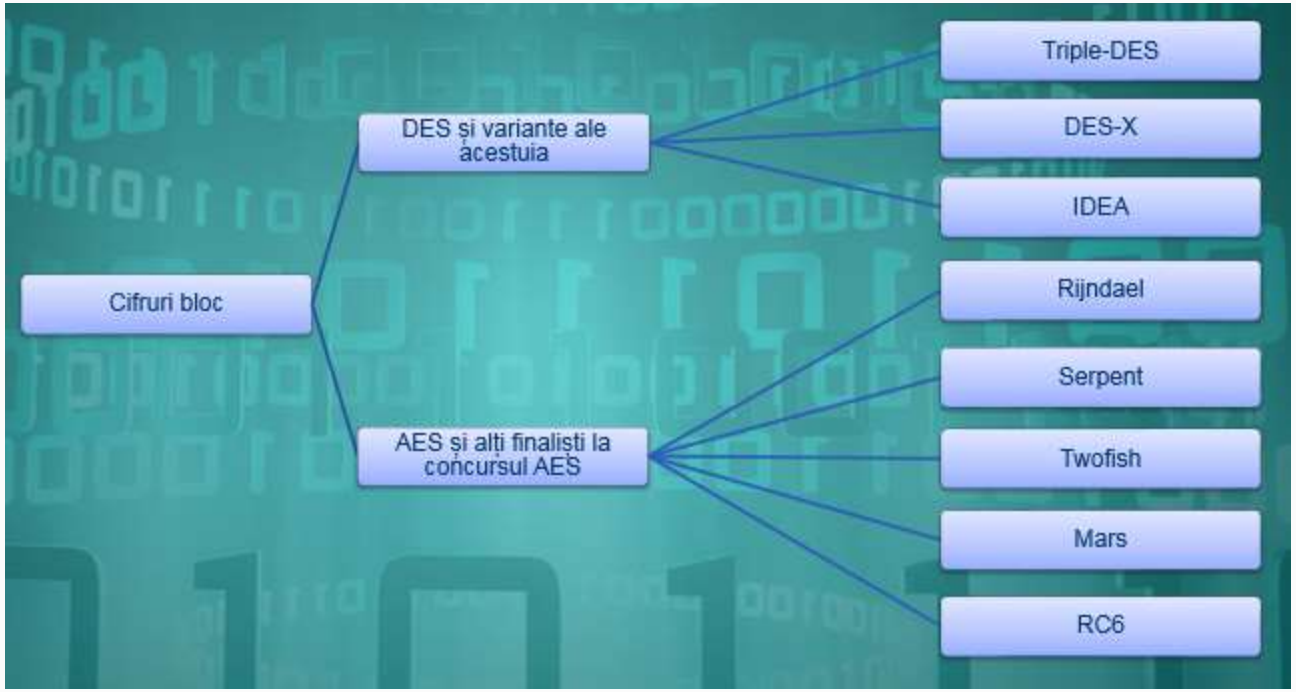
METODE CRIPTOGRAFICE DE PROTECȚIE A INFORMAȚIEI

Tema: Cifruri bloc moderne

CELE MAI POPULARE CIFRURI BLOC



SISTEMUL DE CRIPTARE DES

În această secțiune vom examina ex-standardul de criptare simetrică bloc DES. Principalele obiective ale acestei subsecțiuni sunt următoarele:

- A prezenta istoria apariției DES;
- A descrie modul în care DES folosește rețeaua Feistel pentru a realiza transformările de permutare și de substituție;
- A expune detalii privind elementele DES;
- A descrie procedura de generare a cheilor de rundă DES.

SISTEMUL DE CRIPTARE DES

În anul 1973 Biroul Național de Standardizare al SUA a lansat un apel în Registrul Federal (jurnalul oficial al guvernului SUA) privind construirea unui sistem de criptare oficial, care să se numească Data Encryption Standard (prescurtat DES). Firma IBM a fost cea care a construit acest sistem, publicat în Registrul Federal în anul 1975, modificând sistemul Lucifer, pe care deja îl testa. După dezbateri publice, la 17 ianuarie 1977 DES a fost adoptat în calitate de standard de criptare. De atunci, DES a fost reevaluat la fiecare 5 ani, devenind primul cifru bloc recunoscut internațional, detaliile de implementare ale căruia au fost complet specificate în standardul FIPS 46-2. Ultima versiune a standardului (a patra) ce reglementează DES este FIPS 46-3, în care se recomandă utilizarea unei versiuni mai sigure a lui DES – Triplu DES, varianta simplă DES fiind acceptată pentru utilizare doar pe sistemele vechi.

SISTEMUL DE CRIPTARE DES

În prezent DES este considerat ca fiind nesigur pentru utilizare în cadrul aplicațiilor. Spargerea sa în 1998 a fost realizată în 56 de ore de către supercalculatorul EFF DES Cracker, construit de firma RSA Laboratory. Mai târziu, au apărut și rezultate analitice care au confirmat prezența vulnerabilităților în algoritmul DES. Cu toate că în anul 2005 NIST a retras standardul FIPS 46-3 (ce specifica și recomanda algoritmul DES), DES a fost unul din sistemele de criptare cu cele mai multe implementări. Pe parcursul anilor generații de criptografi au examinat cifrul DES, iar bazele teoretice ale acestuia au contribuit la înțelegerea aspectelor moderne ale cifrurilor bloc și a metodelor de criptanaliză ale acestora.

2.3.3.1 Descrierea sistemului de criptare DES

2.3.3.1.1 Prezentarea generală a sistemului DES

La baza algoritmului DES stă o rețea Feistel, care procesează blocuri de text clar pe $n = 64$ biți și generează blocuri de text criptat tot pe 64 biți (a se vedea Figura 2.3.5). Algoritmul implică atât transformări liniare (permutările E, IP, IP^{-1}), cât și neliniare (S-boxe).

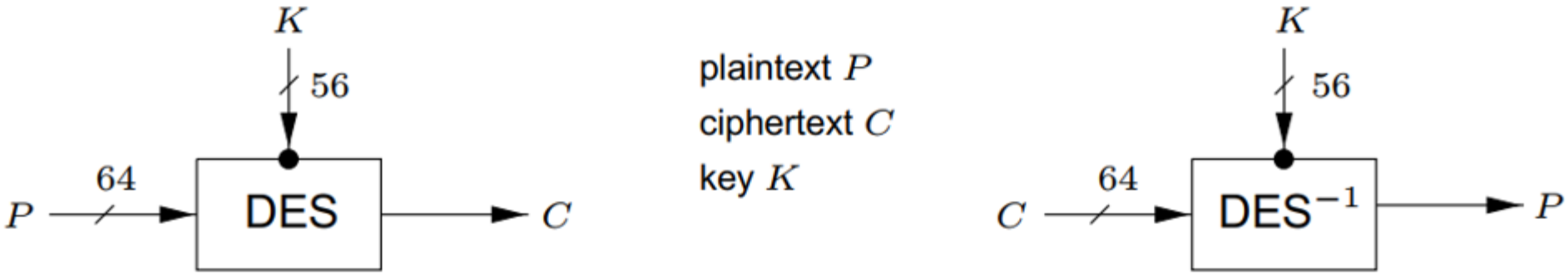


Figura 2.3.5. Datele de intrare pentru criptarea și decriptarea DES

SISTEMUL DE CRIPTARE DES

Cheia secretă K este specificată pe 64 biți, dintre care 8 biți (mai exact, biții 8,16,...,64) sunt utilizați pentru testarea parității. Astfel, bitul 8 al cheii este XOR-ul biților 1,2,...,7; bitul 16 – XOR-ul biților 9,10,..., 15 ș.a.m.d. Prin urmare, dimensiunea efectivă a cheii secrete K este de $k = 56$ biți. Cele 2^{56} chei posibile implementează cel mult 2^{56} din $2^{64}!$ bijecții posibile pe blocuri de 64 biți. O convingere larg răspândită este că biții de paritate au fost introduși pentru a reduce dimensiunea efectivă a cheii de la 64 la 56 biți, intenționat scăzând costul de căutare exhaustivă a cheii printr-un factor de 256.

SISTEMUL DE CRIPTARE DES

Procedura de criptare este construită în baza următoarelor transformări: o permutare inițială, 16 runde de transformări Feistel și o permutare finală (a se vedea Figura 2.3.6). În baza cheii secrete K sunt generate, prin procedura de expandare, 16 subchei de rundă K_i pe 48 biți fiecare, câte una pentru fiecare rundă.

Înainte de prima rundă, în blocul de text clar inițial pe 64 biți, este efectuată o permutare inițială de biți IP, iar șirul rezultat este divizat în două jumătăți pe 32 biți, L_0 (formată din primii 32 biți) și R_0.

SISTEMUL DE CRIPTARE DES

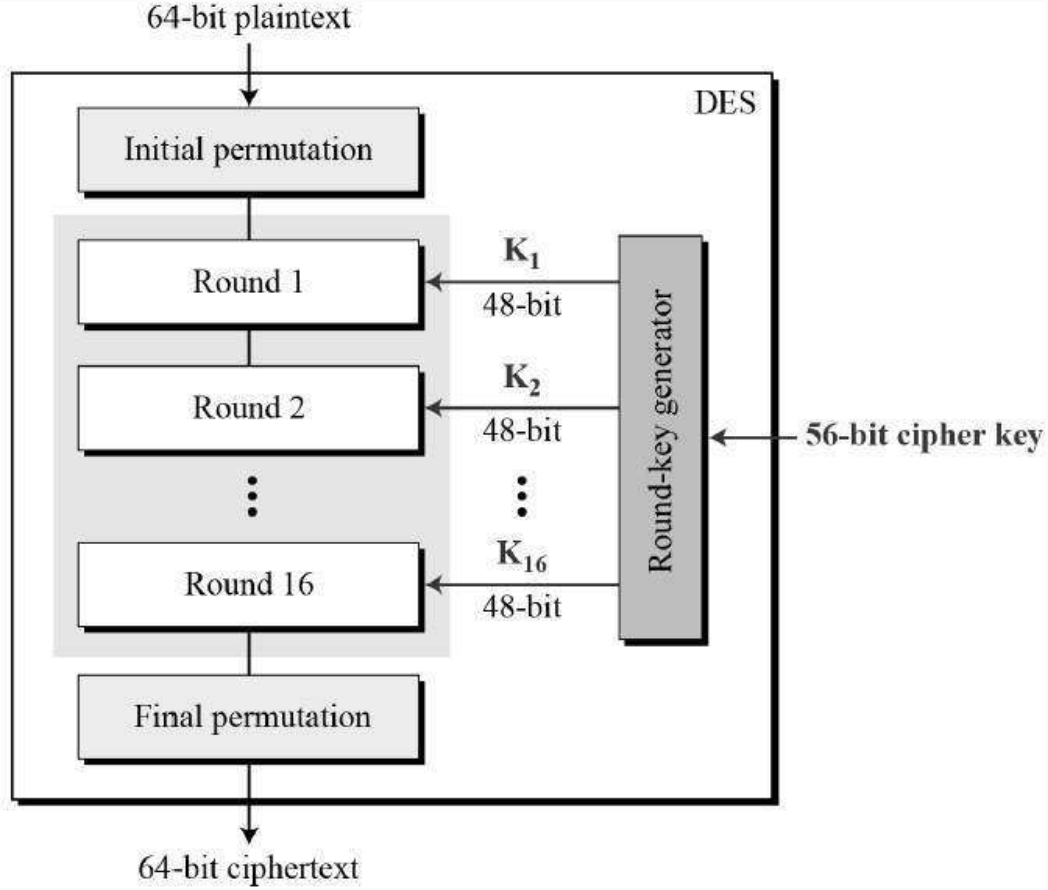
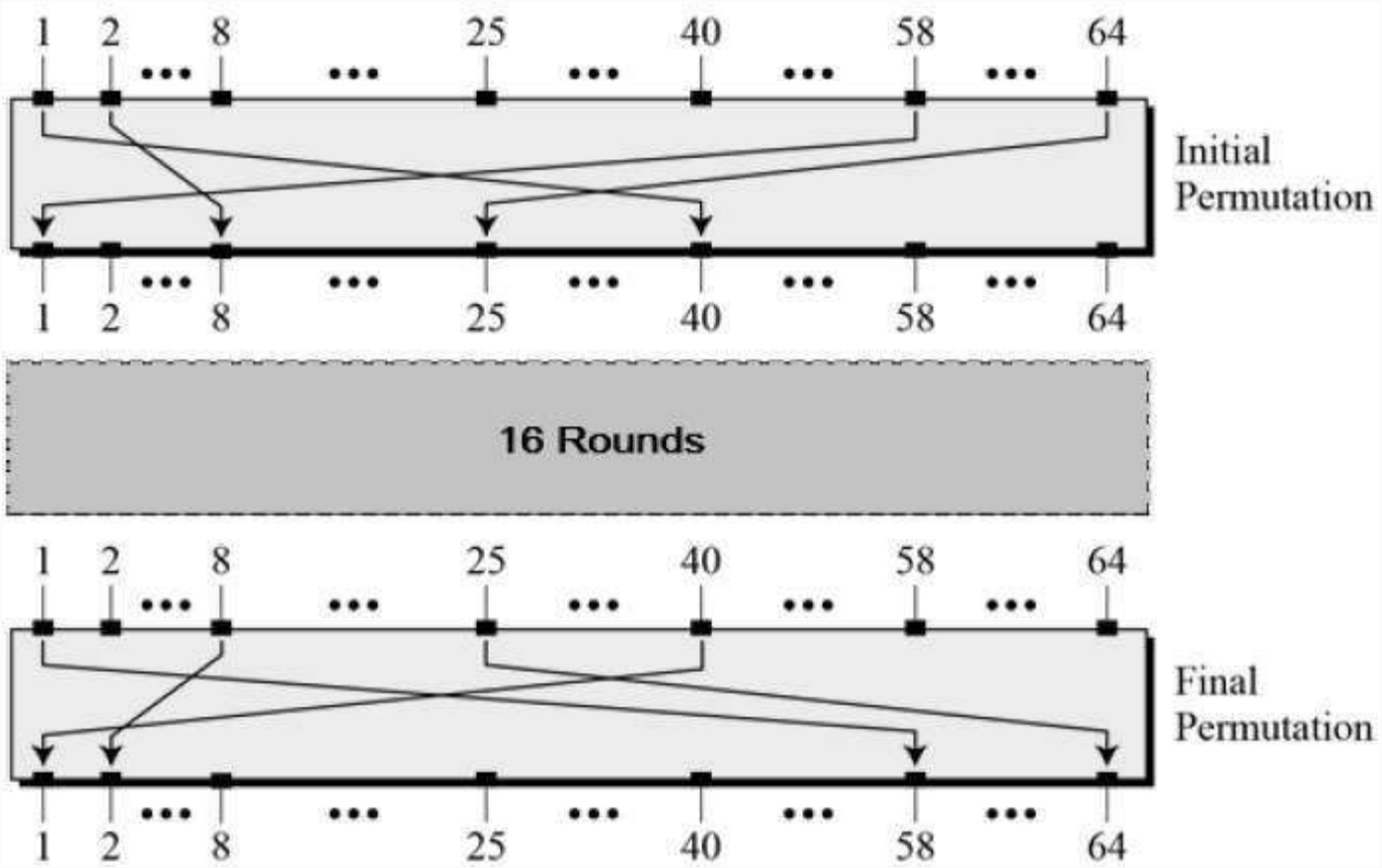


Figura 2.3.6. Structura generală a algoritmului DES

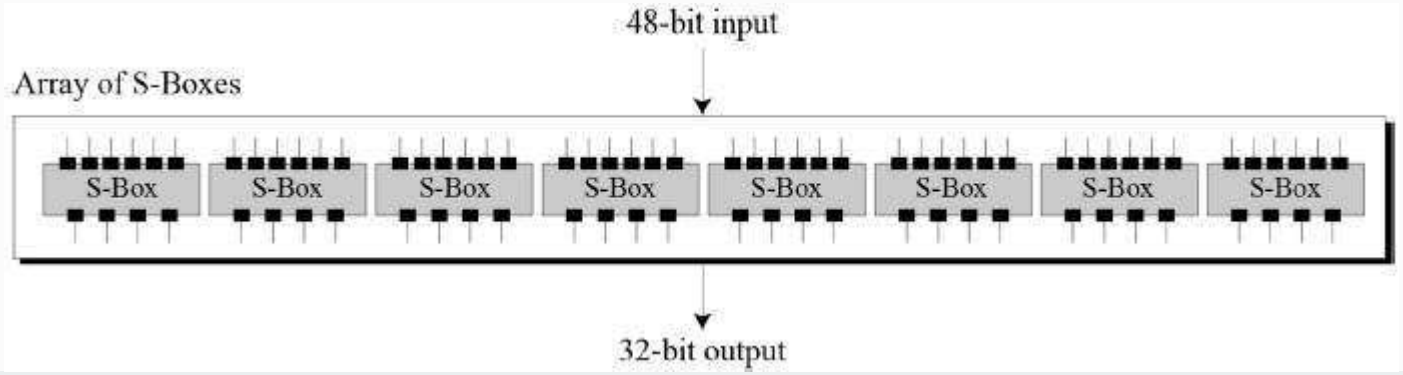
SISTEMUL DE CRIPTARE DES



Permutările inițială și finală

SISTEMUL DE CRIPTARE DES

În cadrul fiecărei runde sunt efectuate același tip de operații. Astfel, la runda i jumătatea de dreapta R_{i-1} este extinsă de la 32 la 48 biți (toți biții lui R_{i-1} sunt folosiți cel puțin o dată și doar unii biți – de două ori), folosind funcția de expansiune E, după care șirul de 48 biți rezultat este combinat prin XOR cu subcheia de rundă K_i. Șirul rezultat este divizat în 8 subșiruri de câte 8 biți, care servesc ca intrări pentru 8 transformări de substituție fixate S_j, $j = \overline{1,8}$ (S-boxe), notate colectiv prin S. La intrarea în fiecare S-boxă avem 6 biți, iar la ieșire – 4 biți. Cele 8 subșiruri de la ieșirile din S-boxe sunt concatenate în unul pe 32 biți, la care se aplică transformarea de permutare fixă P.



SISTEMUL DE CRIPTARE DES

În cadrul rundei i, $i = \overline{1,16}$, se preiau șirurile pe 32 biți L_{i-1} și R_{i-1}, obținute la runda precedentă, și se generează șirurile L_i și R_i pe 32 biți în modul următor:

$$L_i := R_{i-1},$$
$$R_i := L_{i-1} \oplus f\left(R_{i-1}, K_i\right),\ f\left(R_{i-1}, K_i\right) := P\left(S\left(E\left(R_{i-1}\right) \oplus K_i\right)\right).$$

Astfel, jumătățile rezultate în cadrul fiecărei runde sunt interschimbate (a se vedea Figura 2.3.7).

Jumătățile șirului $L_{16}R_{16}$, obținut după efectuarea rundei 16, sunt interschimbate. Textul criptat final este obținut prin aplicarea permutării inverse IP^{-1} la șirul rezultat $R_{16}L_{16}$.

SISTEMUL DE CRIPTARE DES

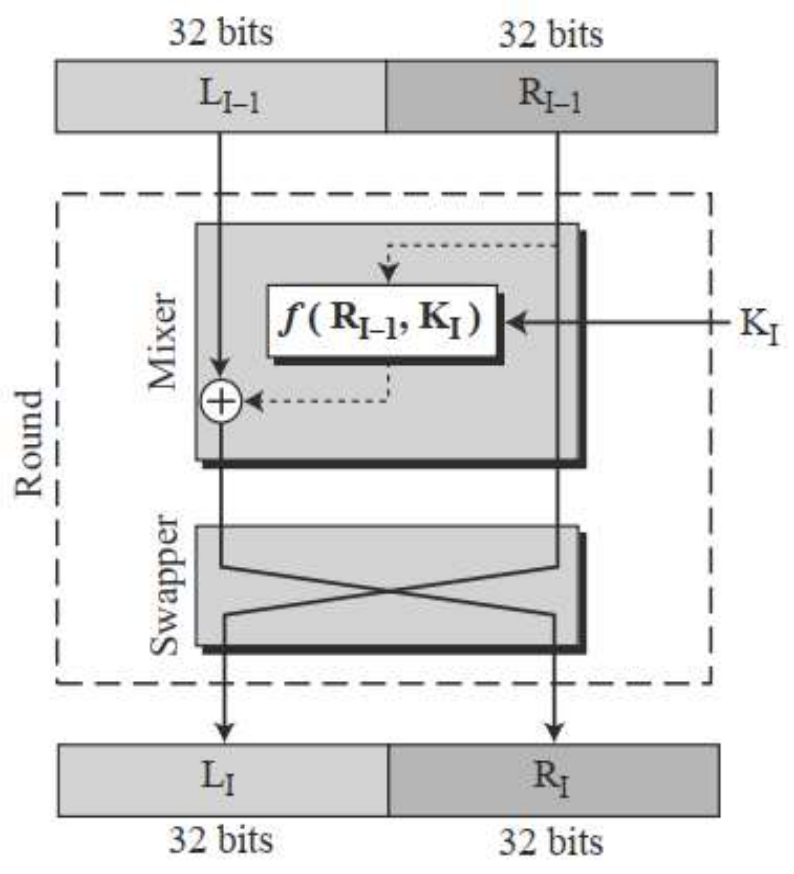


Figura 2.3.7. Ilustrarea unei runde de criptare DES

SISTEMUL DE CRIPTARE DES

Decriptarea implică aceleași cheie și algoritm, doar că subcheile sunt utilizate în ordine inversă pe parcursul rundelor intermediare.

Algoritmul de expandare (de diversificare) a cheii DES specifică modul de generare a subcheilor de rundă K_i, fiecare dintre care conține 48 de biți ai lui K. Algoritmul implică tabelele de permutare $PC1$ (Permuted Choice 1) și $PC2$ (Permuted Choice 2) din Tabelul 2.3.4. Inițial, permutarea $PC1$ elimină 8 biți $(k_8, k_{16}, ..., k_{64})$ ai lui K. Cei 56 de biți rămași sunt permutați și scriși în două variabile C și D pe 28 biți fiecare, apoi, pe parcursul a 16 iterații, șirurile din variabilele C și D sunt supuse unei rotații ciclice cu 1 sau cu 2 biți, iar din rezultatul obținut prin concatenare, sunt selectați 48 de biți (K_i).

SISTEMUL DE CRIPTARE DES

2.3.3.1.2 Algoritmul de criptare DES

Detalii privind cifrul bloc DES sunt prezentate în *Algoritmul de criptare DES* și Figura 2.3.7.

Algoritmul de criptare DES
Date de intrare: $m_1 \ldots m_{64}$ - bloc de text clar pe 64 biți $K = k_1 \ldots k_{64}$ - cheia secretă pe 64 biți, care include 8 biți de paritate *Date de ieșire:* $C = c_1 \ldots c_{64}$ - bloc de text criptat pe 64 biți

SISTEMUL DE CRIPTARE DES

Pașii algoritmului:

1. Expandarea cheii: Pornind de la cheia K, se aplică *Algoritmul de expandare a cheii DES* (prezentat separat în algoritmul de la 2.3.3.1.3), determinând astfel 16 subchei de rundă K_i pe 48 biți fiecare.
2. Permutarea inițială. Se va utiliza tabelul de permutare IP (a se vedea **Tabelul 2.3.1**) pentru a permuta biții blocului de text clar. Rezultatul este divizat în două jumătăți pe 32 biți

$$L_0 = m_{58}m_{50}m_{42}m_{34}m_{26}m_{18}m_{10}m_2m_{60}m_{52}...m_8,\ R_0 = m_{57}m_{49}m_{41}m_{33}m_{25}m_{17}m_9m_1m_{59}m_{51}...m_7$$

astfel încât $(L_0, R_0) := IP(m_1...m_{64})$.

SISTEMUL DE CRIPTARE DES

3. Efectuarea a 16 runde:

Pentru $i := \overline{1,16}$ *execută*

{

Se calculează L_i și R_i în baza relațiilor:

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

Valoarea funcției de rundă f se determină în baza relației $f(R_{i-1}, K_i) := P(S(E(R_{i-1}) \oplus K_i))$, în care R_{i-1} reprezintă un șir de 32 biți, iar K_i - șir de 48 biți. Rezultatul este un șir de 32 biți. Etapele de calcul ale valorii funcției de rundă sunt următoarele (a se vedea **Figura 2.3.8**) :

SISTEMUL DE CRIPTARE DES

a) *Expansiune*. Se extinde argumentul $R_{i-1} = r_1 \ldots r_{32}$ de la 32 la 48 biți, folosind funcția de expansiune E din Tabelul 2.3.2: $T := E(R_{i-1})$. Tabloul T cuprinde biții lui R_{i-1} așezați într-o anumită ordine, unii biți fiind scriși de două ori, $T := r_{32} r_1 r_2 \ldots r_{31} r_{32} r_1$ (a se vedea Tabelul 2.3.2).

b) *Mixare prin XOR*. Se calculează $T' := T \oplus K_i$. După combinarea prin XOR cu subcheia K_i, blocul obținut T' este divizat în 8 părți B_i de câte 6 biți fiecare: $(B_1, \ldots, B_8) := T'$.

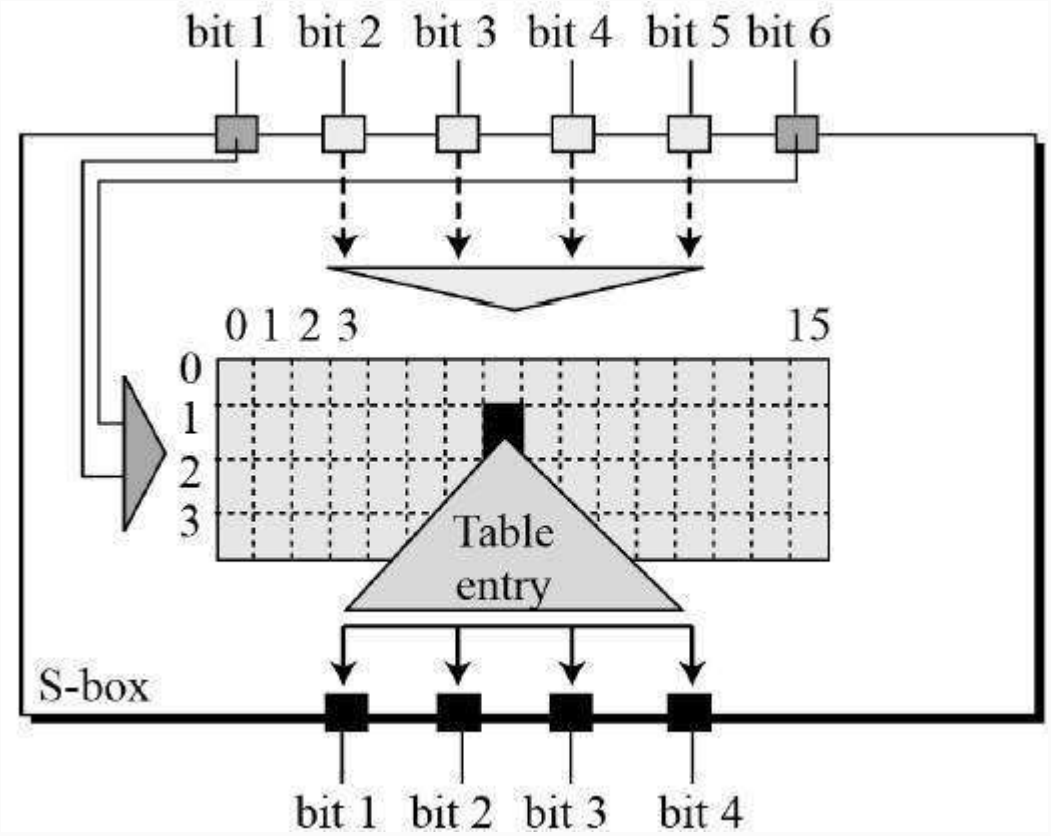
SISTEMUL DE CRIPTARE DES

c) *Substituție*. Fiecare din cele 8 S-boxe S_j (tablou de dimensiuni 4×16) înlocuiește cei 6 biți de intrare ai lui B_i cu 4 biți, conform unei transformări neliniare, date sub forma unui tabel: $T'' := \left(S_1(B_1),...,S_8(B_8)\right)$. În relația anterioară $S_i(B_i)$ aplică $B_i = b_1...b_6$ într-un șir de 4 biți astfel: pornind de la $b_1...b_6$ se determină linia r și coloana c a S-boxei S_i din Tabelul 2.3.3, în care $r = 2b_1 + b_6$, iar șirul $b_2b_3b_4b_5$ dă reprezentarea binară a indicelui unei coloane $c \in [0,15]$ din tablou. Deci $S_1(011011)$ implică $r = 1, c = 13$ și ieșirea 5, adică binarul 0101.

d) Permutare. Este utilizată permutarea P din **Tabelul 2.3.2** cu scopul de a rearanja 32 de biți ai lui $T'' = t_1...t_{32}$, ceea ce conduce la $t_{16}t_7..t_{25}$ (a se vedea **Tabelul 2.3.2**). Avem $T''' := P(T'')$.

}

SISTEMUL DE CRIPTARE DES



Regula de transformare neliniară prin S-boxe

SISTEMUL DE CRIPTARE DES

4. Permutarea finală. Se interschimbă blocurile finale L_{16}, R_{16}. Avem $b_1 \ldots b_{64} := (R_{16}, L_{16})$.
5. Se aplică permutarea IP^{-1} definită în Tabelul 2.3.1. Avem $C := IP^{-1}(b_1 \ldots b_{64}) = b_{40} b_8 \ldots b_{25}$.

SISTEMUL DE CRIPTARE DES

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

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

Tabelul 2.3.1. Permutarea inițială DES și inversa acesteia

SISTEMUL DE CRIPTARE DES

E

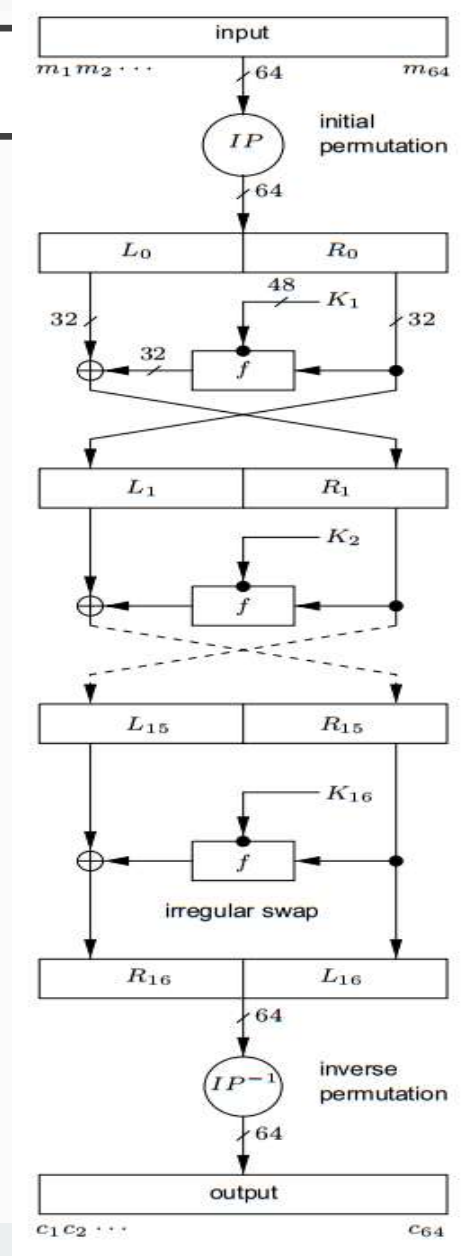
32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

P

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

Tabelul 2.3.2. Funcții DES utilizate la fiecare rundă: expansiunea E și permutarea P

SISTEMUL DE CRIPTARE DES



SISTEMUL DE CRIPTARE DES

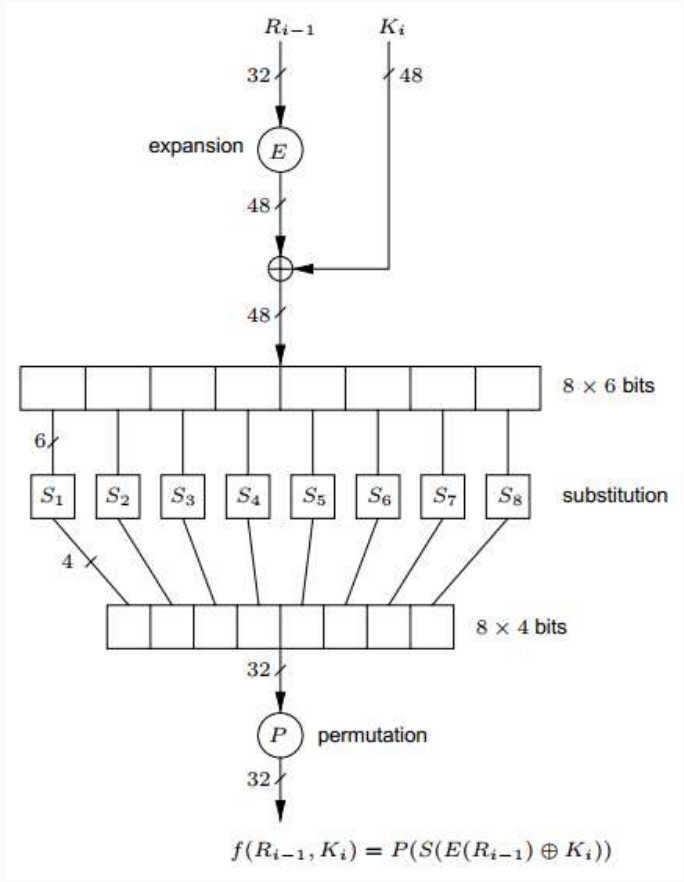


Figura 2.3.8. Funcția de rundă f a algoritmului DES

SISTEMUL DE CRIPTARE DES

Rând	Numărul coloanei															
	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]	[11]	[12]	[13]	[14]	[15]
S_1																
[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
S_2																
[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

SISTEMUL DE CRIPTARE DES

S_3																
[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
S_4																
[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

SISTEMUL DE CRIPTARE DES

S_5																
[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
S_6																
[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

SISTEMUL DE CRIPTARE DES

S_7																
[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
S_8																
[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

Tabelul 2.3.3. S-boxele din algoritmul DES

SISTEMUL DE CRIPTARE DES

2.3.3.1.3 Algoritmul de expandare a cheii DES

Algoritmul de expandare (diversificare) a cheii DES
Date de intrare: $K = k_1 \ldots k_{64}$ - cheia secretă pe 64 biți, care include 8 biți de paritate Date de ieșire: $K_i, i = \overline{1,16}$ - 16 subchei de rundă pe 48 biți

SISTEMUL DE CRIPTARE DES

Pașii algoritmului:

1. Se definesc valorile $v_i, i=\overline{1,16}$, după cum urmează: $v_i=1$ pentru $i\in\{1,2,9,16\}$; $v_i=2$ în caz contrar. Acestea sunt valorile pentru deplasările la stânga în cadrul rotațiilor ciclice pe 28 biți.
2. Se determină $T:=PC1(K)$ și se reprezintă șirul T ca două subșiruri (C_0,D_0) pe 28 de biți. În acest sens, pentru a selecta biții din K, se folosește permutarea $PC1$ din Tabelul 2.3.4: $C_0=k_{57}k_{49}...k_{36}$, $D_0=k_{63}k_{55}...k_4$.

SISTEMUL DE CRIPTARE DES

3.

Pentru $i := \overline{1,16}$ *execută*

{

Se calculează K_i în baza relațiilor:

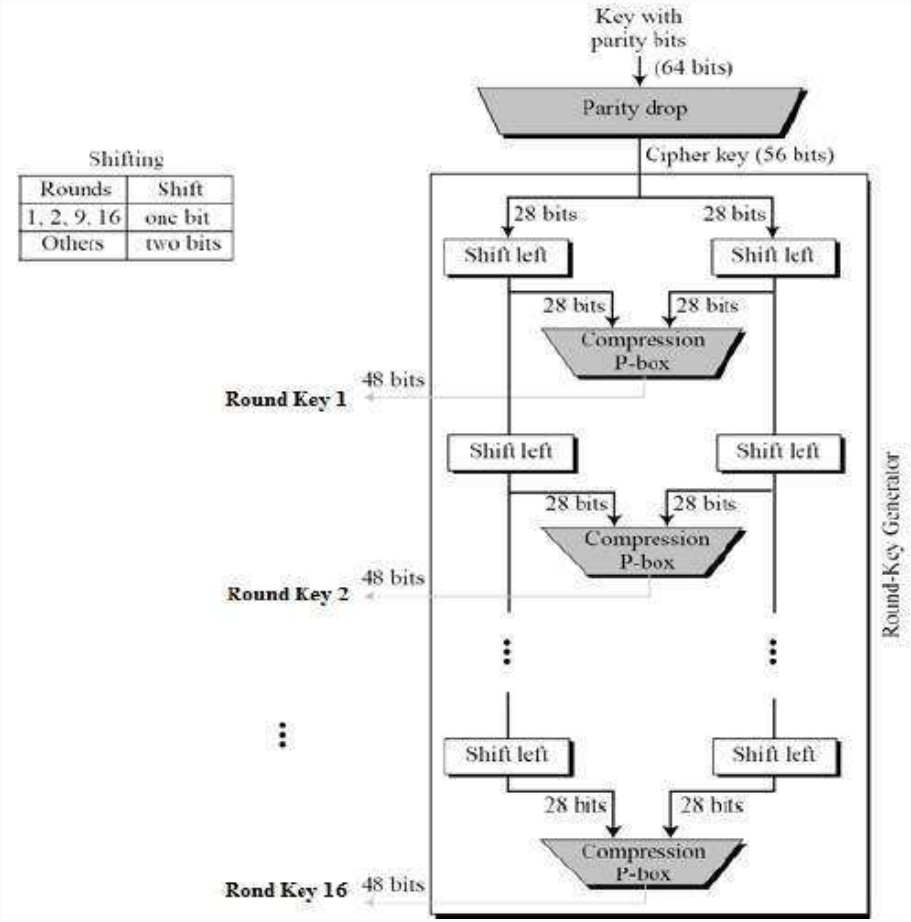
$$C_i := rol(C_{i-1}, v_i),\ D_i := rol(D_{i-1}, v_i),\ K_i := PC2(C_i, D_i),$$

unde *rol* este operația de rotație ciclică la stânga cu v_i poziții.

Se folosește permutarea $PC2$ din **Tabelul 2.3.4** pentru a selecta 48 de biți din șirul $b_1 ... b_{56}$, obținut prin concatenarea lui C_i și D_i: $K_i = b_{14} b_{17} ... b_{32}$.

}

SISTEMUL DE CRIPTARE DES



Procedura de expandare a cheii

SISTEMUL DE CRIPTARE DES

*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
de sus pentru C_i ; de jos pentru D_i						
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

*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

Tabelul 2.3.4. Permutările pentru selectarea biților în algoritmul de expandare a cheii DES

2.3.3.1.4 Algoritmul de decriptare DES

Decriptarea DES este realizată, pornind de la textul criptat și, aplicând algoritmul de criptare cu aceeași cheie secretă, dar cu subcheile de rundă implicate în ordine inversă $K_{16}, K_{15}, ..., K_1$. Subcheile pot fi generate cu algoritmul de expandare a cheii, după care să fie utilizate în ordine inversă, dar pot fi generate și direct în ordine inversă. Aceasta se poate realiza dacă în *Algoritmul de expandare a cheii* se efectuează următoarele modificări: rotațiile la stânga se înlocuiesc prin rotații la dreapta, iar valoarea v_1 se modifică în 0.

SISTEMUL DE CRIPTARE DES

Efectul permutării inverse IP^{-1} este anulat de transformarea IP, rezultând șirul (R_{16}, L_{16}).

Deoarece avem $L_{16} = R_{15}$, $R_{16} = L_{15} \oplus f(R_{15}, K_{16})$, rezultă

$$R_{16} \oplus f(L_{16}, K_{16}) = L_{15} \oplus f(R_{15}, K_{16}) \oplus f(R_{15}, K_{16}) = L_{15}.$$

Astfel, la decriptare după runda întâi se obține perechea (R_{15}, L_{15}), adică argumentul de la intrarea în runda 16 a algoritmului de criptare. La runda $i = \overline{16,1}$, subșirurile L_{i-1} și R_{i-1} pe 32 biți sunt determinate în baza formulelor:

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