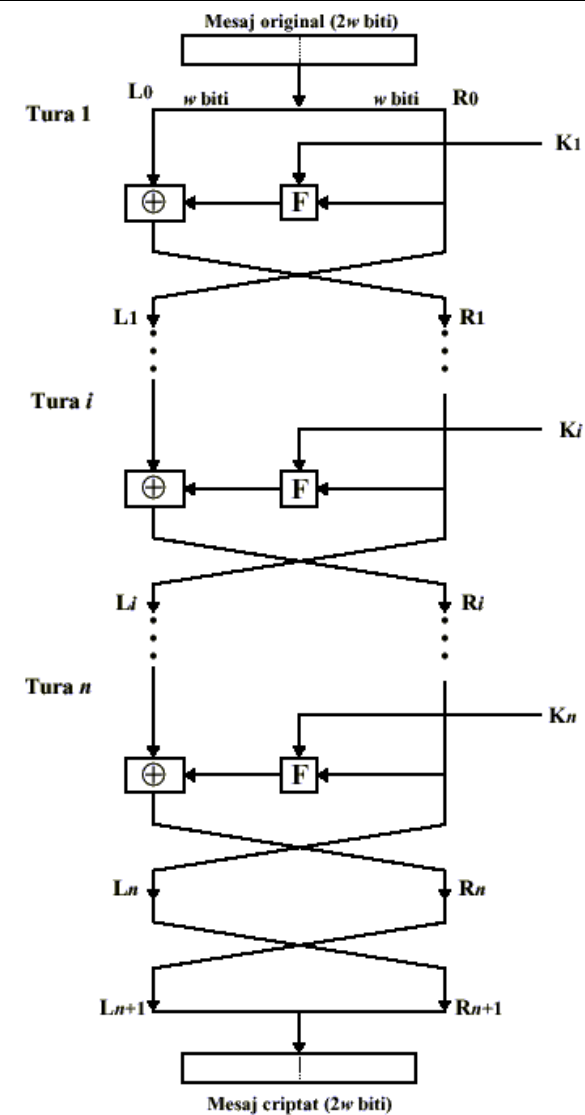


Substituție reversibilă		Substituție ireversibilă	
Original	Criptat	Original	Criptat
00	11	00	11
01	10	01	10
10	00	10	01
11	01	11	01

Tabelul 3.1.

Original		Criptat	
Decimal	Binar	Decimal	Binar
0	0000	14	1110
1	0001	4	0100
2	0010	13	1101
3	0011	1	0001
4	0100	2	0010
5	0101	15	1111
6	0110	11	1011
7	0111	8	1000
8	1000	3	0011
9	1001	11	1010
10	1010	6	0110
11	1011	12	1100
12	1100	5	0101
13	1101	9	1001
14	1110	0	0000
15	1111	7	0111

Tabelul 3.2.

**Figura 3.1.** Rețeaua clasică Feistel

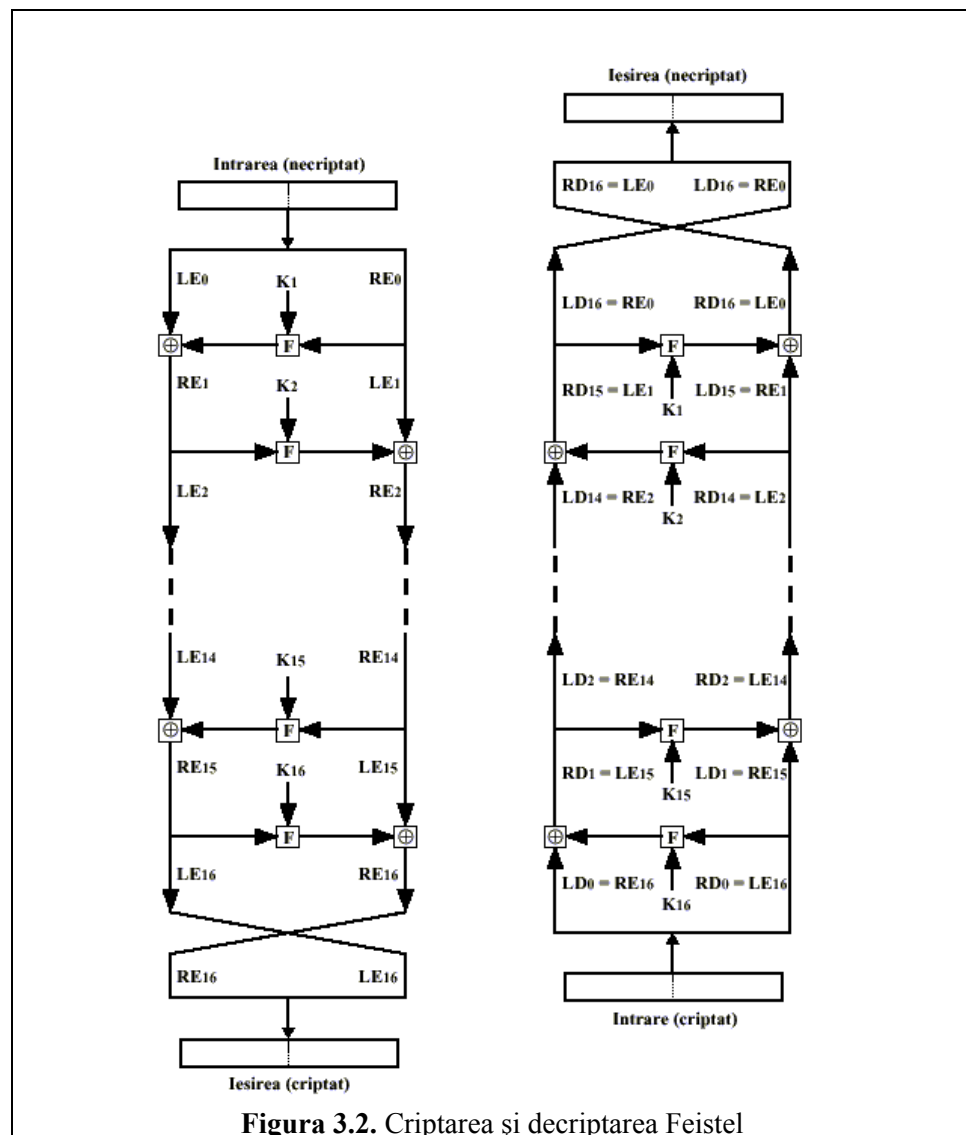


Figura 3.2. Criptarea și decriptarea Feistel

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

Tabelul 3.3. Permutarea inițială

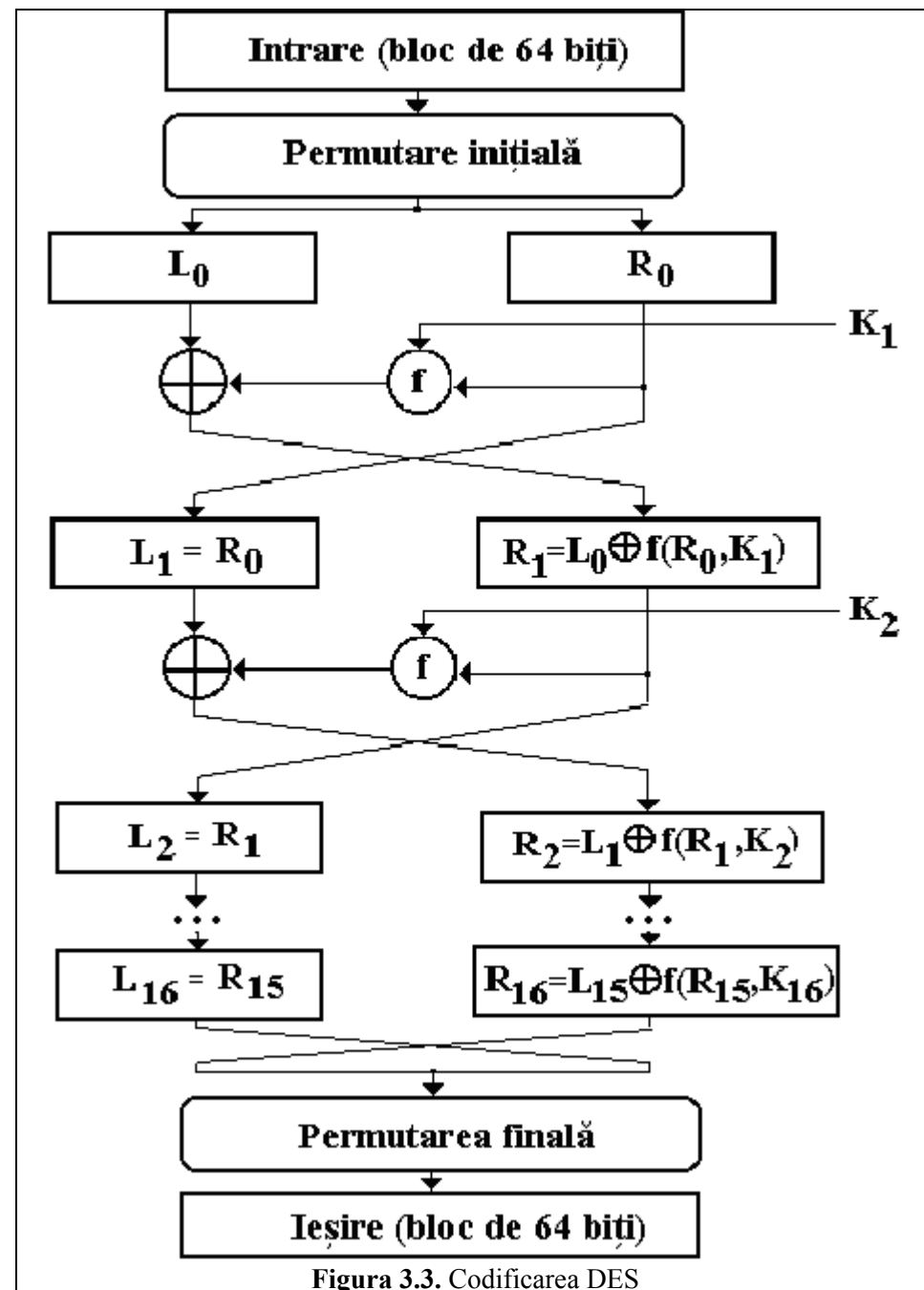


Figura 3.3. Codificarea DES

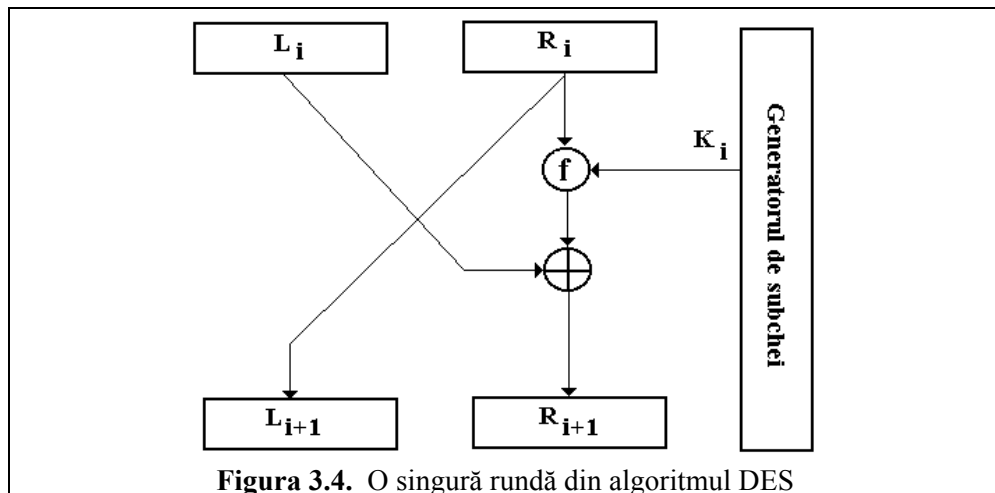


Figura 3.4. O singură rundă din algoritmul DES

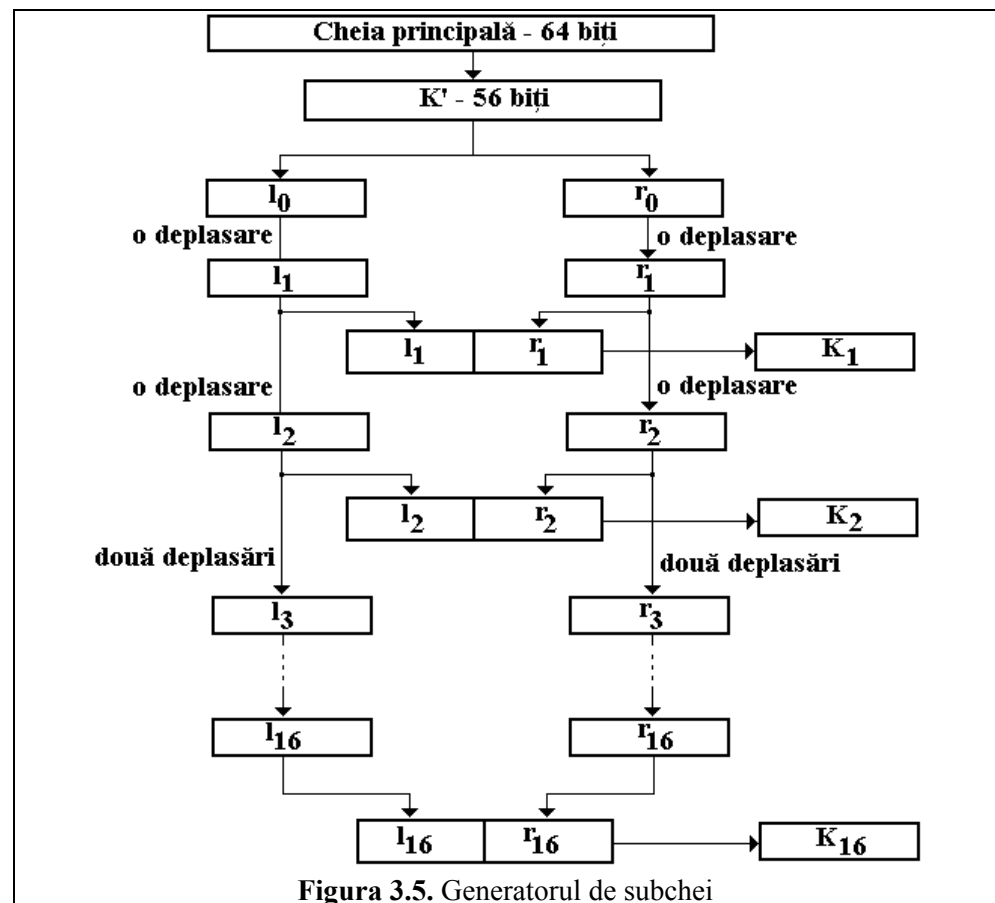
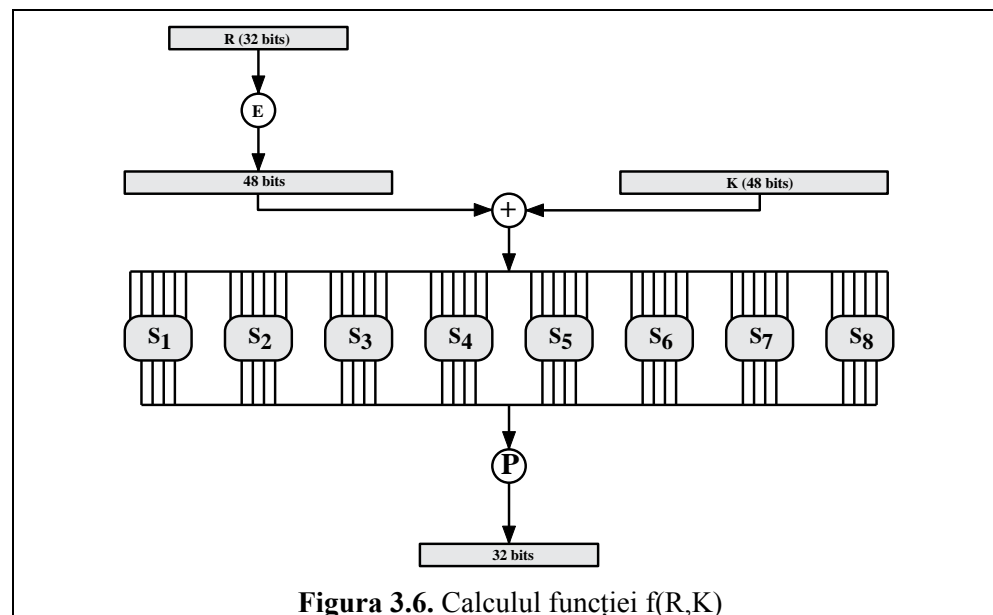


Figura 3.5. Generatorul de subchei

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 3.4. Permutare & Compresie

Figura 3.6. Calculul funcției $f(R,K)$

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

Tabelul 3.5. Permutare & Extindere (E)

S1	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
S2	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	5	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

S3	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
S4	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
S5	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
S6	12	1	10	15	8	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
S7	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
S8	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

Tabelul 3.6. cutiile S

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 3.7. Permutare (P)

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 3.8. Permutarea finală

```

Intrare: .....*
Permutare: .....*
Runda 1: .....*
Runda 2: * * * * .....*
Runda 3: * * * * * * * * * * * * * * * *
Runda 4: * * * * * * * * * * * * * * * *
Runda 5: * * * * * * * * * * * * * * * *
Runda 6: * * * * * * * * * * * * * * * *
Runda 7: * * * * * * * * * * * * * * * *
Runda 8: * * * * * * * * * * * * * * * *
Runda 9: * * * * * * * * * * * * * * * *
Runda 10: * * * * * * * * * * * * * * * *
Runda 11: * * * * * * * * * * * * * * * *
Runda 12: * * * * * * * * * * * * * * * *
Runda 13: * * * * * * * * * * * * * * * *
Runda 14: * * * * * * * * * * * * * * * *
Runda 15: * * * * * * * * * * * * * * * *
Runda 16: * * * * * * * * * * * * * * * *
leșire: .. * * * * * * * * * * * * * * *

```

Figura 3.7.

Schimbări în text				Schimbări în cheie			
Tura	Numărul de schimbări	de	biți	Tura	Numărul de schimbări	de	biți
0	1			0	0		
1	6			1	2		
2	21			2	14		
3	35			3	28		
4	29			4	32		
5	34			5	30		
6	32			6	32		
7	31			7	25		
8	29			8	24		
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		

Tabelul 3.9.

Viteza procesorului Chei testate / sec.	Numărul de procesoare necesare spargerii DES-ului prin căutare exhaustivă			
	An	Lună	Săptămână	Zi
1.000.000	2.300	27.400	119.200	834.000
2.000.000	1.150	13.700	59.600	417.000
4.000.000 (1990)	600	6.850	29.800	208.500
32.000.000 (1995)	75	850	3.700	26.100
256.000.000 (2000)	9	107	500	3.300

Tabelul 3.10. Numărul de procesoare de viteză dată, necesare spargerii DES-ului, prin căutare exhaustivă, într-o perioadă precizată.

CIP		1 Mhz	2 Mhz	4 Mhz	32 Mhz	256 Mhz	Total
1 9 9 0	Preț/buc.	25	250	E/S	N	N	N
	An	2.300	1.150	N	N	N	128.574
	Lună	27.400	13.700	N	N	N	1.531.706
	Săptămână	119.200	59.600	N	N	N	6.663.482
	Zi	834.000	417.000	N	N	N	46.622.017
1 9 9 5	Preț/buc.	E/D	25	250	E/S	N	N
	An	N	1.150	600	N	N	65.670
	Lună	N	13.700	6.850	N	N	765.853
	Săptămână	N	59.600	29.800	N	N	3.331.741
	Zi	N	417.000	208.500	N	N	23.311.009
2 0 0 0	Preț/buc.	E/D	E/D	25	250	E/S	N
	An	N	N	600	75	N	16.771
	Lună	N	N	6.850	850	N	190.763
	Săptămână	N	N	29.800	3.700	N	830.136
	Zi	N	N	208.500	26.100	N	5.831.943

Legendă: E = există, D = depășit, S = prea scump, N = nu e cazul;

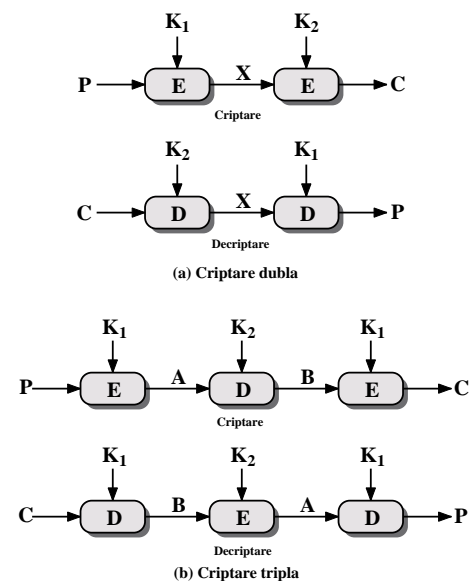
Tabelul 3.11. Costuri investițional-structurale

Anul	An	Lună	Săptămână	Zi
1990	129.000	1.532.000	6.664.000	46.622.000
1995	52.000	600.000	2.611.000	18.265.000
2000	10.300	117.000	510.000	3.580.000

Tabelul 3.12. Investiții necesare spargerii DES-ului prin căutare exhaustivă

Procesor	Viteza/nr.biți	Criptări DES/secundă
8088	4.7 Mhz/8 biți	370
68000	7.6 Mhz/16 biți	900
80286	6.0 Mhz/16 biți	1.100
68020	16 Mhz/32 biți	3.500
68030	16 Mhz/32 biți	3.900
68030	50 Mhz/32 biți	9.600
IBM 3033	Mainframe	15.900
68040	25 Mhz/32 biți	16.000
68040	40 Mhz/32 biți	23.200
IBM 3090	Mainframe	32.000

Tabelul 3.13. Performanțe software în spargerea DES-ului

**Figura 3.8.** Criptare multiplă

X	Y	$X \oplus Y$ adunarea	$X \odot Y$ multiplicarea	$X \oplus Y$ sau-exclusiv
0 00	0 00	0 00	1 01	0 00
0 00	1 01	1 01	0 00	1 01
0 00	2 10	2 10	3 11	2 10
0 00	3 11	3 11	2 10	3 11
1 01	0 00	1 01	0 00	1 01
1 01	1 01	2 10	1 01	0 00
1 01	2 10	3 11	2 10	3 11
1 01	3 11	0 00	3 11	2 10
2 10	0 00	2 10	3 11	2 10
2 10	1 01	3 11	2 10	3 11
2 10	2 10	0 00	0 00	0 00
2 10	3 11	1 01	1 01	1 01
3 11	0 00	3 11	2 10	3 11
3 11	1 01	0 00	3 11	2 10
3 11	2 10	1 01	1 01	1 01
3 11	3 11	2 10	0 00	0 00

Tabelul 3.14.

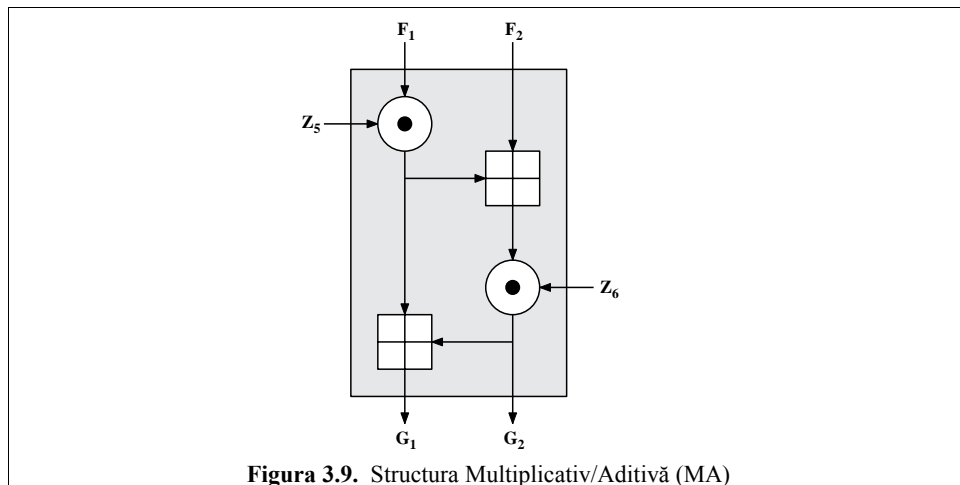


Figura 3.9. Structura Multiplicativ/Aditivă (MA)

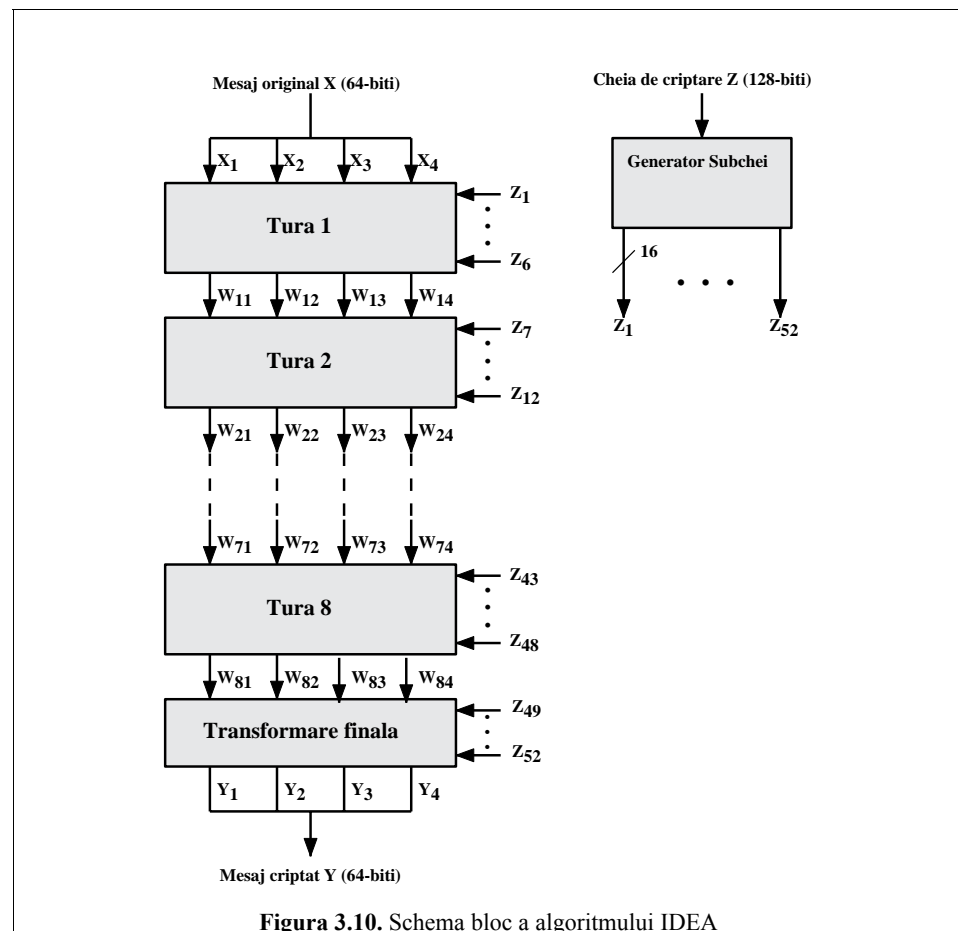


Figura 3.10. Schema bloc a algoritmului IDEA

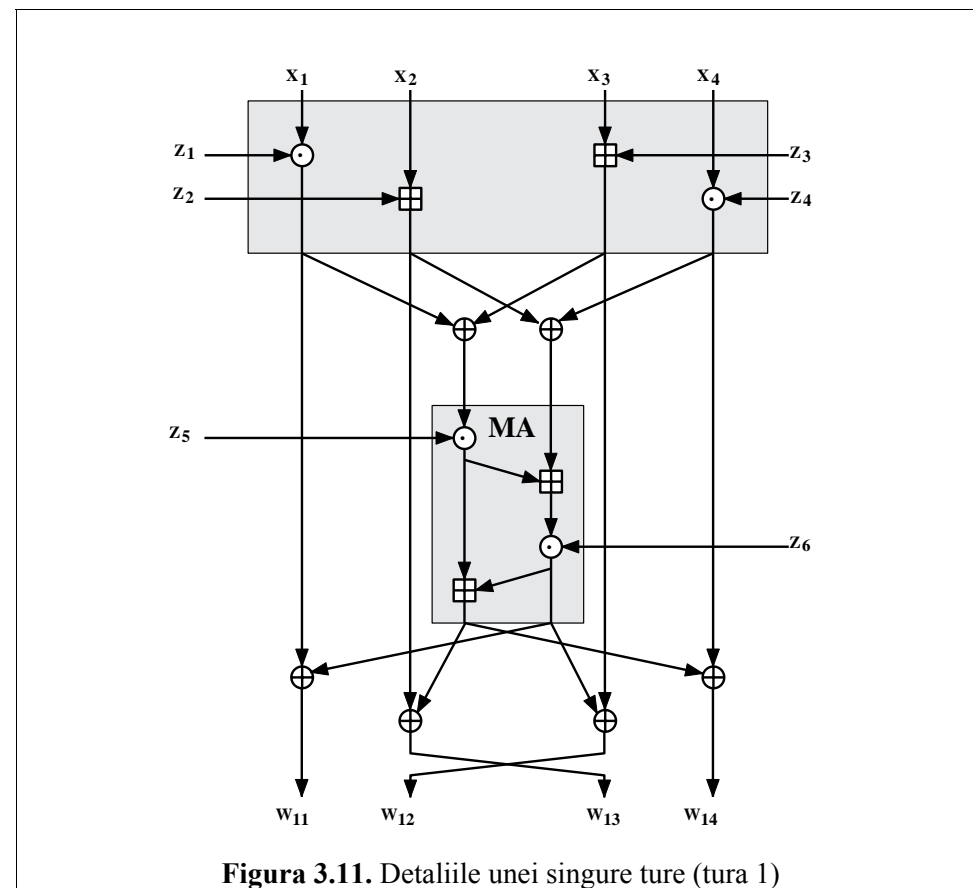


Figura 3.11. Detaliile unei singure ture (tura 1)

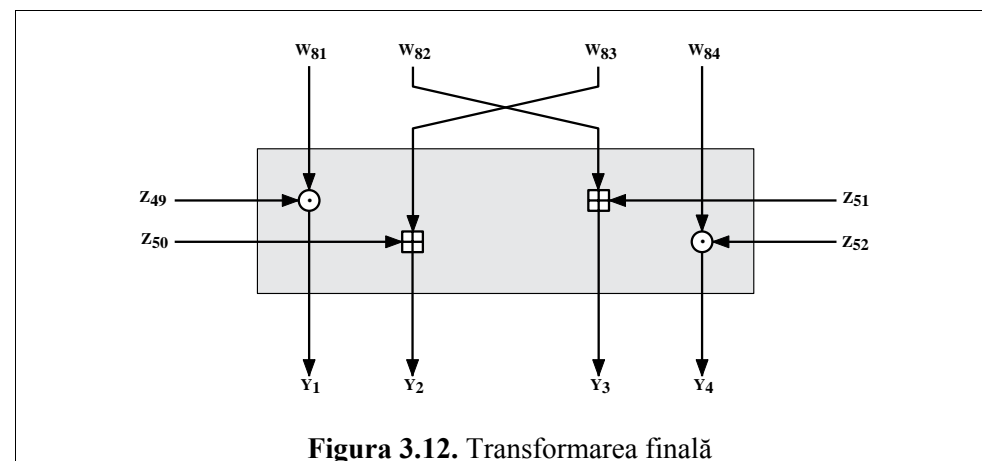
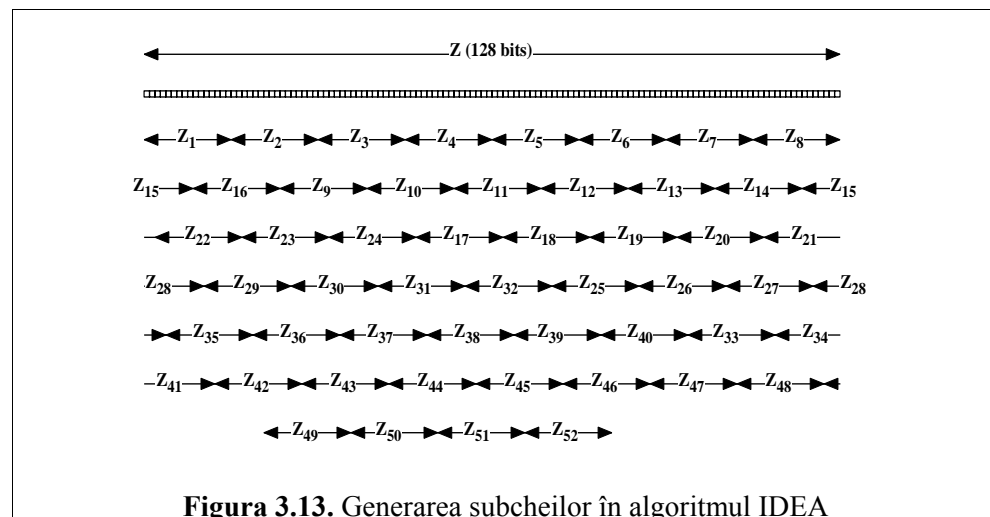
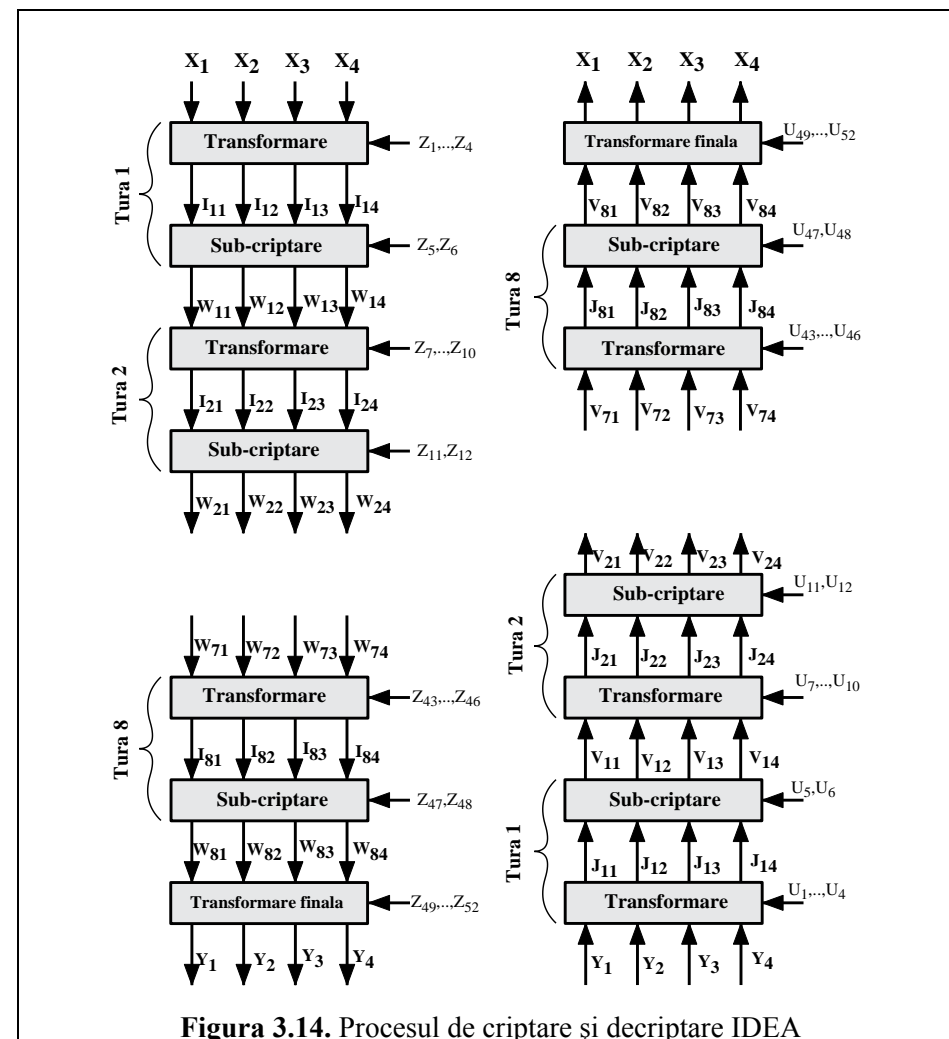


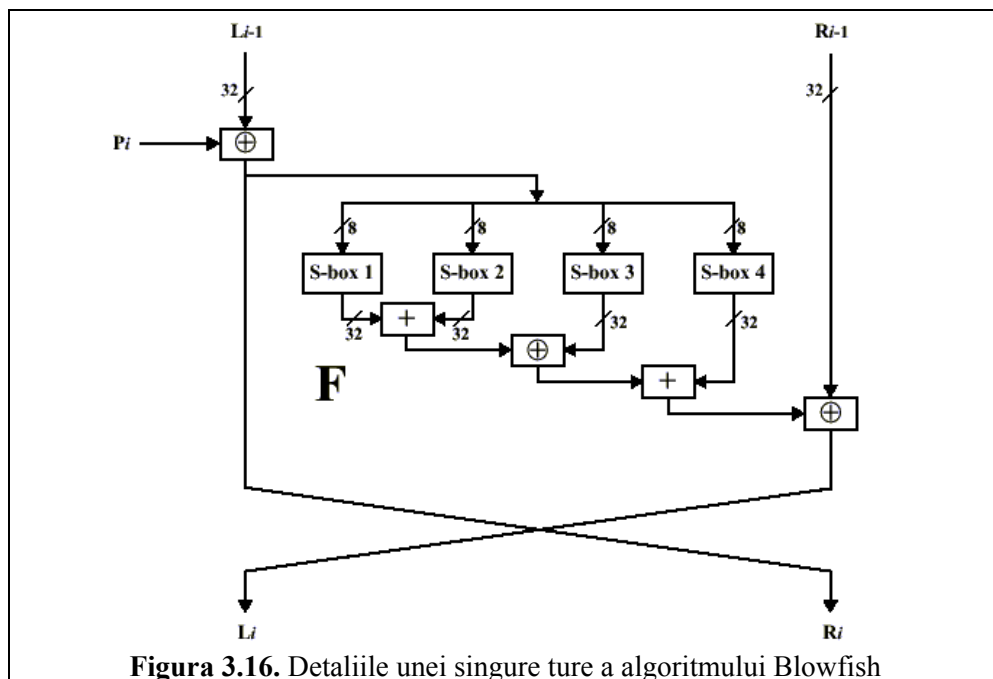
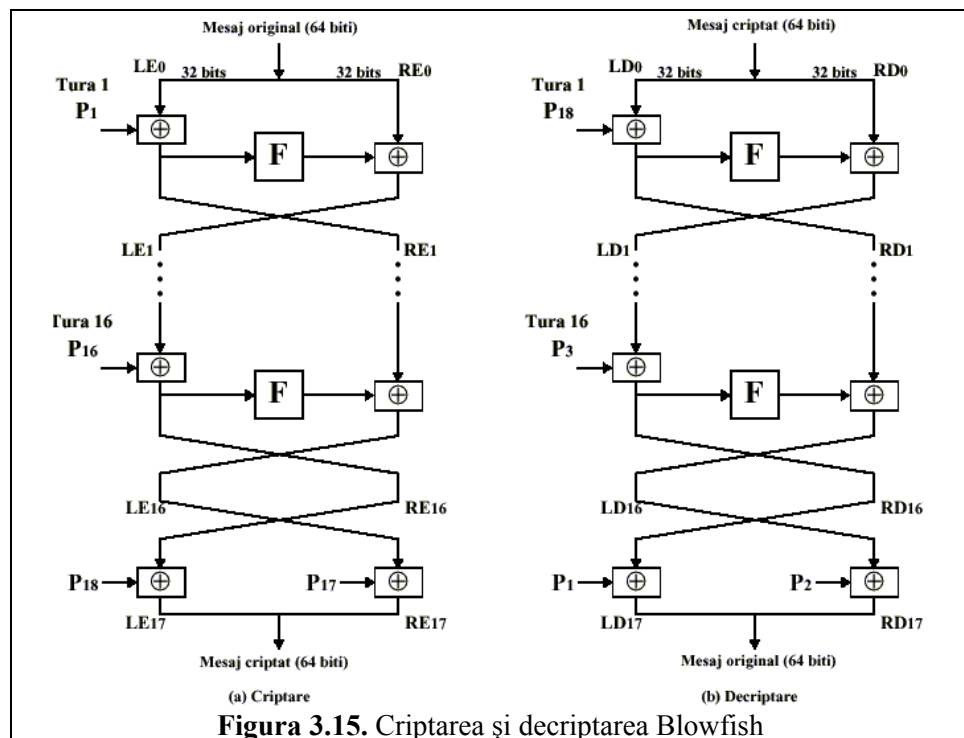
Figura 3.12. Transformarea finală



T u r a	Criptare		Decriptare	
	Șirul subcheilor	Mod de obținere a șirului subcheilor pentru criptare din cheia Z	Șirul subcheilor	Mod de obținere a șirului subcheilor pentru decriptare din subcheile Zi
1	$Z_1 Z_2 Z_3 Z_4 Z_5 Z_6$	$Z[1..96]$	$U_1 U_2 U_3 U_4 U_5 U_6$	$Z_{49}^{-1} Z_{50}^{-1} Z_{51}^{-1} Z_{52}^{-1} Z_{47} Z_{48}$
2	$Z_7 Z_8 Z_9 Z_{10} Z_{11} Z_{12}$	$Z[97..128; 26..89]$	$U_7 U_8 U_9 U_{10} U_{11} U_{12}$	$Z_{43}^{-1} Z_{45}^{-1} Z_{44} Z_{46}^{-1} Z_{41} Z_{42}$
3	$Z_{13} Z_{14} Z_{15} Z_{16} Z_{17} Z_{18}$	$Z[90..128; 1..25; 51..82]$	$U_{13} U_{14} U_{15} U_{16} U_{17} U_{18}$	$Z_{37}^{-1} Z_{39}^{-1} Z_{38} Z_{40}^{-1} Z_{35} Z_{36}$
4	$Z_{19} Z_{20} Z_{21} Z_{22} Z_{23} Z_{24}$	$Z[83..128; 1..50]$	$U_{19} U_{20} U_{21} U_{22} U_{23} U_{24}$	$Z_{31}^{-1} Z_{33}^{-1} Z_{32} Z_{34}^{-1} Z_{29} Z_{30}$
5	$Z_{25} Z_{26} Z_{27} Z_{28} Z_{29} Z_{30}$	$Z[76..128; 1..43]$	$U_{25} U_{26} U_{27} U_{28} U_{29} U_{30}$	$Z_{25}^{-1} Z_{27}^{-1} Z_{26} Z_{28}^{-1} Z_{23} Z_{24}$
6	$Z_{31} Z_{32} Z_{33} Z_{34} Z_{35} Z_{36}$	$Z[44..75; 101..128; 1..36]$	$U_{31} U_{32} U_{33} U_{34} U_{35} U_{36}$	$Z_{19}^{-1} Z_{21}^{-1} Z_{20} Z_{22}^{-1} Z_{17} Z_{18}$
7	$Z_{37} Z_{38} Z_{39} Z_{40} Z_{41} Z_{42}$	$Z[37..100; 126..128; 1..29]$	$U_{37} U_{38} U_{39} U_{40} U_{41} U_{42}$	$Z_{13}^{-1} Z_{15}^{-1} Z_{14} Z_{16}^{-1} Z_{11} Z_{12}$
8	$Z_{43} Z_{44} Z_{45} Z_{46} Z_{47} Z_{48}$	$Z[30..125]$	$U_{43} U_{44} U_{45} U_{46} U_{47} U_{48}$	$Z_7^{-1} Z_9^{-1} Z_8 Z_{10}^{-1} Z_5 Z_6$
9	$Z_{49} Z_{50} Z_{51} Z_{52}$	$Z[23..86]$	$U_{49} U_{50} U_{51} U_{52}$	$Z_1^{-1} Z_2^{-1} Z_3 Z_4^{-1}$

Tabelul 3.15.

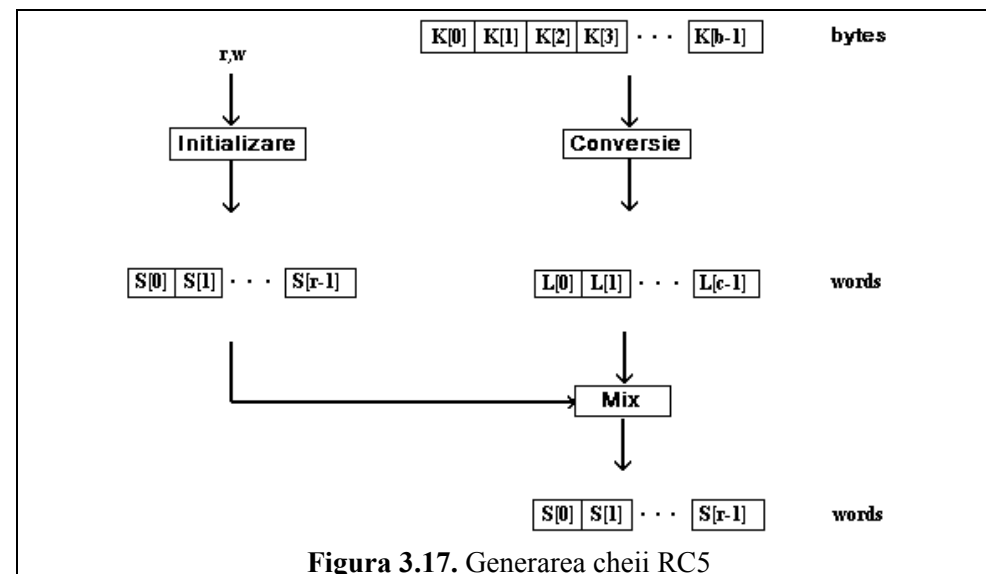


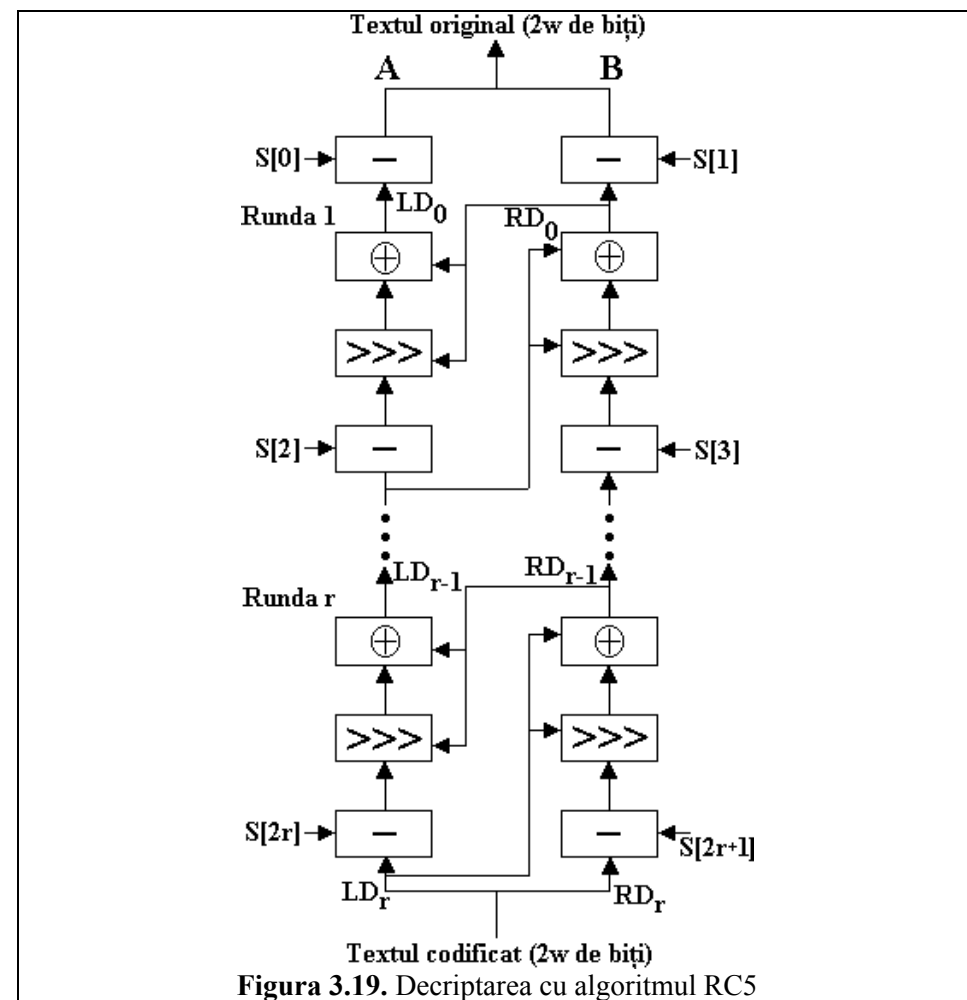
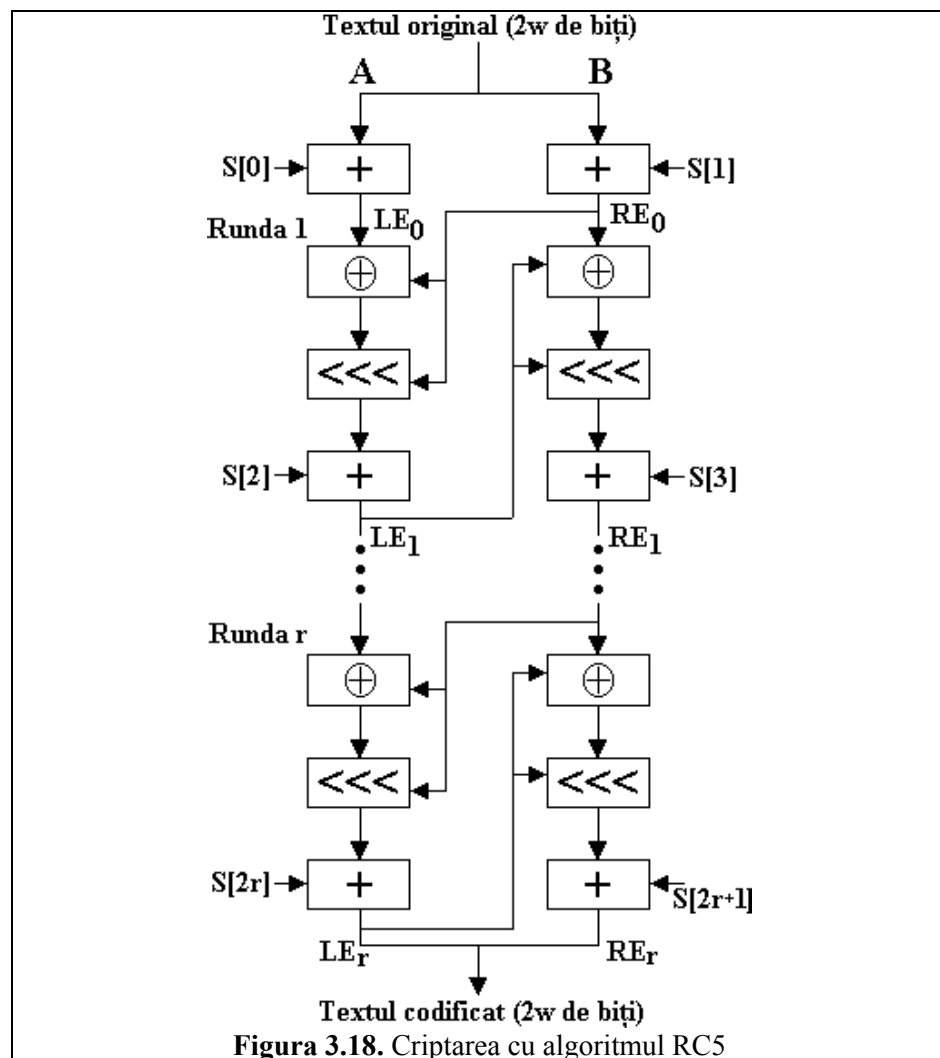


Algoritmul	Ciclii mașină pe o rundă	Numărul rundelor	Numărul ciclurilor de mașină pe un byte codificat
Blowfish	9	16	18
RC5	12	16	23
DES	18	16	45
IDEA	50	8	50

Tabelul 3.16. Comparații de viteză pe un Pentium

Parametru	Definiție	Valori admise
w	Dimensiunea cuvântului. RC5 criptează blocuri de 2 cuvinte	16, 32, 64
r	Numărul de ture (runde)	0, 1, ..., 255
b	Numărul de octeți din cheia secretă K	0, 1, ..., 255

Tabelul 3.17.



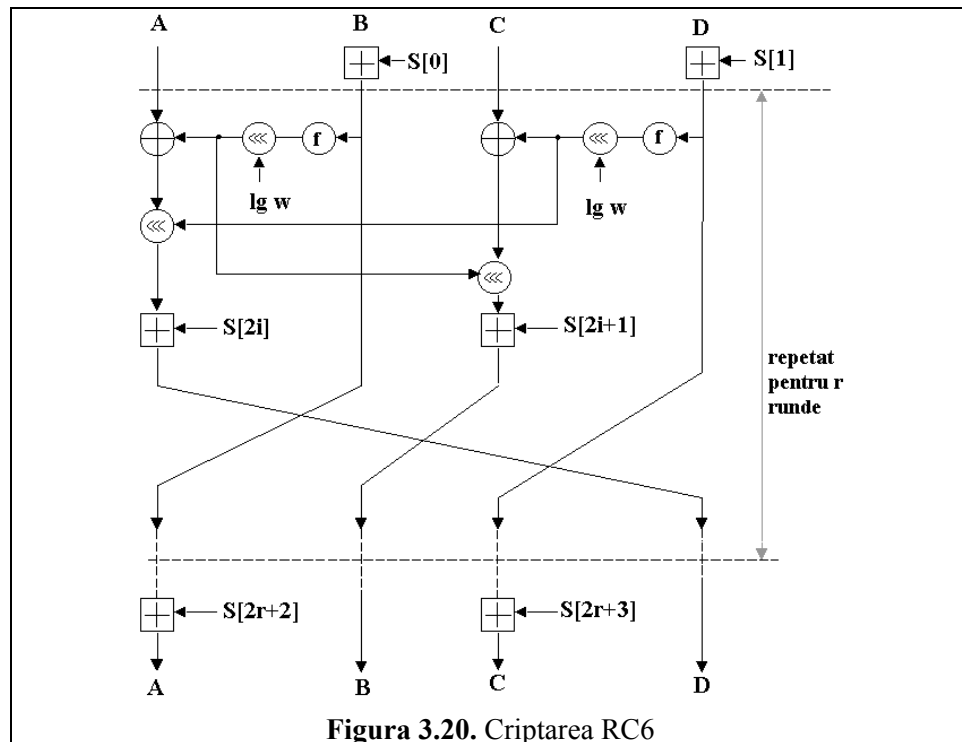


Figura 3.20. Criptarea RC6

0	32	64	96	1	33	65	97	2	34	66	98	3	35	67	99
4	36	68	100	5	37	69	101	6	38	70	102	7	39	71	103
8	40	72	104	9	41	73	105	10	42	74	106	11	43	75	107
12	44	76	108	13	45	77	109	14	46	78	110	15	47	79	111
16	48	80	112	17	49	81	113	18	50	82	114	19	51	83	115
20	52	84	116	21	53	85	117	22	54	86	118	23	55	87	119
24	56	88	120	25	57	89	121	26	58	90	122	27	59	91	123
28	60	92	124	29	61	93	125	30	62	94	126	31	63	95	127

Tabelul 3.18. Permutarea inițială

S0	3	8	15	1	10	6	5	11	14	13	4	2	7	0	9	12
S1	15	12	2	7	9	0	5	10	1	11	14	8	6	13	3	4
S2	8	6	7	9	3	12	10	15	13	1	14	4	0	11	5	2
S3	0	15	11	8	12	9	6	3	13	1	2	4	10	7	5	14
S4	1	15	8	3	12	0	11	6	2	5	4	10	9	14	7	13
S5	15	5	2	11	4	10	9	12	0	3	14	8	13	6	7	1
S6	7	2	12	5	8	4	6	11	14	9	1	15	13	3	10	0
S7	1	13	15	0	14	8	2	11	7	4	12	10	9	3	5	6

Tabelul 3.19. Culiile S (de la S₀ la S₇)

InvS0	13	3	11	0	10	6	5	12	1	14	4	7	15	9	8	2
InvS1	5	8	2	14	15	6	12	3	11	4	7	9	1	13	10	0
InvS2	12	9	15	4	11	14	1	2	0	3	6	13	5	8	10	7
InvS3	0	9	10	7	11	14	6	13	3	5	12	2	4	8	15	1
InvS4	5	0	8	3	10	9	7	14	2	12	11	6	4	15	13	1
InvS5	8	15	2	9	4	1	13	14	11	6	5	3	7	12	10	0
InvS6	15	10	1	13	5	3	6	0	4	9	14	7	2	12	8	11
InvS7	3	0	6	13	9	14	15	8	5	12	11	7	10	1	4	2

Tabelul 3.20. Culiile S inverse folosite pentru decodificare (de la InvS0 la InvS7)

0	4	8	12	16	20	24	28	32	36	40	44	48	52	56	60
64	68	72	76	80	84	88	92	96	100	104	108	112	116	120	124
1	5	9	13	17	21	25	29	33	37	41	45	49	53	57	61
65	69	73	77	81	85	89	93	97	101	105	109	113	117	121	125
2	6	10	14	18	22	26	30	34	38	42	46	50	54	58	62
66	70	74	78	82	86	90	94	98	102	106	110	114	118	122	126
3	7	11	15	19	23	27	31	35	39	43	47	51	55	59	63
67	71	75	79	83	87	91	95	99	103	107	111	115	119	123	127

Tabelul 3.21. Permutarea finală

Variantă AES	Nk	Nb	număr de runde
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

Tabelul 3.22. Variante de implementare AES

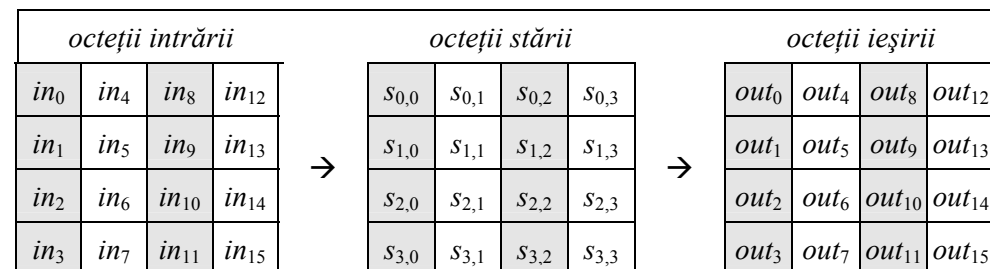


Figura 3.21. Tablourile intrării, stării și ieșirii

```

Cipher (byte in[4*Nb], byte out[4*Nb], word w[Nb*(Nr+1)])
begin
  byte state[4,Nb]
  state = in
  AddRoundKey(state,w)           // vezi 3.12.1.2.4
  for round = 1 step 1 to Nr-1

```

```

SubBytes(state)           // vezi 3.12.1.2.1
ShiftRows(state)          // vezi 3.12.1.2.2
MixColumns(state)         // vezi 3.12.1.2.3
AddRoundKey(state,w+round*Nb)
end for
SubBytes(state)
ShiftRows(state)
AddRoundKey(state,w+Nr*Nb)
out = state
end

```

Figura 3.22. Pseudocodul criptării AES

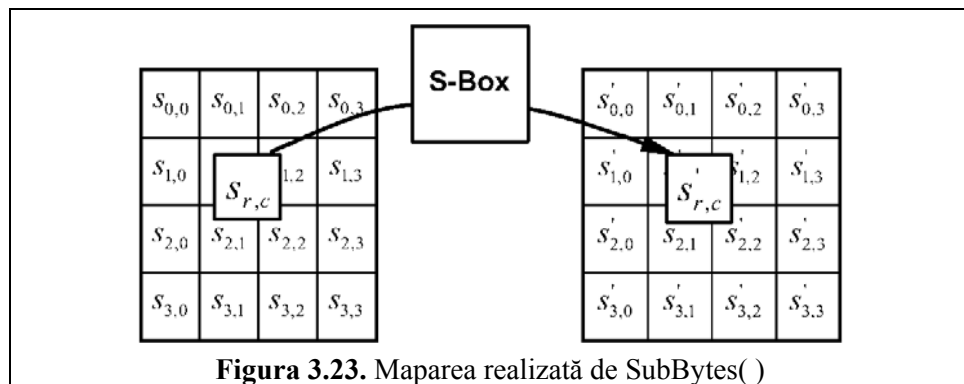


Figura 3.23. Maparea realizată de SubBytes()

		y															
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
x	0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
	1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
	2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
	3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
	4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
	5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
	6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
	7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
	8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
	9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
	a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
	b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
	c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
	d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
	e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
	f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Figura 3.24. Descrierea substituției octetului xy (in hexazecimal) utilizând cutia S

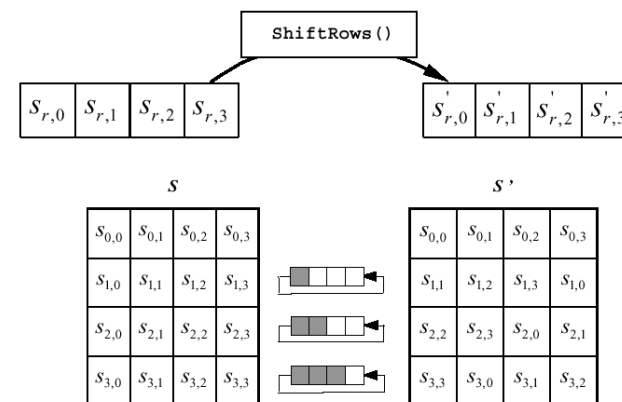


Figura 3.25. Transformarea ShiftRows()

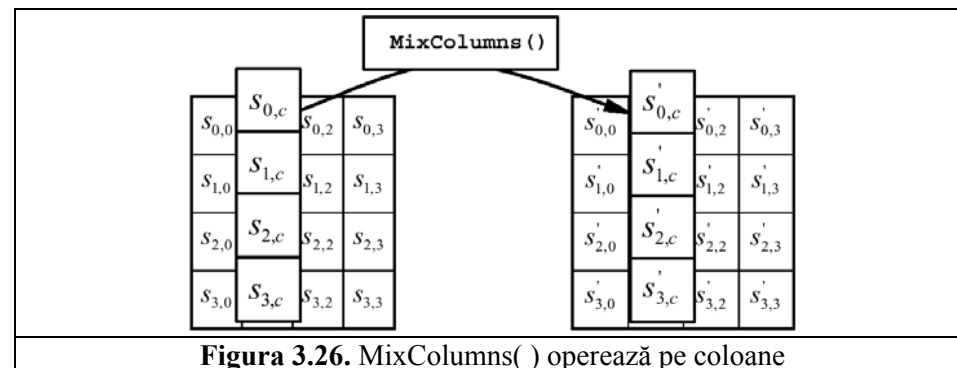


Figura 3.26. MixColumns() operează pe coloane

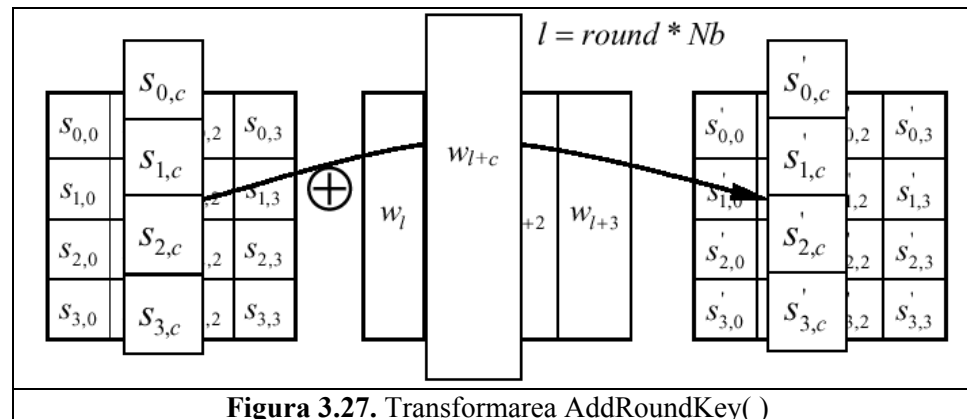


Figura 3.27. Transformarea AddRoundKey()

```

KeyExpansion(byte key[4 * Nk], word w[Nb * (Nr + 1)], Nk)
begin
i=0
while (i < Nk)
w[i] = word[key[4*i],key[4*i+1],key[4*i+2],key[4*i+3]]
i = i + 1
end while
i = Nk
while (i < Nb * (Nr + 1))
word temp = w[i - 1]
if (i mod Nk = 0)
temp = SubWord(RotWord(temp)) xor Rcon[i / Nk]
else if (Nk = 8 and i mod Nk = 4)
temp = SubWord(temp)
end if
w[i] = w[i - Nk] xor temp
i = i + 1
end while
end

```

Figura 3.28. Pseudocodul pentru generarea subcheilor

```

InvCipher(byte in[4 * Nb], byte out[4 * Nb], word w[Nb * (Nr + 1)])
begin
byte state[4,Nb]
state = in
AddRoundKey(state, w + Nr * Nb) // vezi 3.12.1.2.4
for round = Nr - 1 step -1 to 1
InvShiftRows(state) // vezi 3.12.1.4.1
InvSubBytes(state) // vezi 3.12.1.4.2
AddRoundKey(state, w + round * Nb)
InvMixColumns(state) // vezi 3.12.1.4.3
end for
InvShiftRows(state)
InvSubBytes(state)
AddRoundKey(state, w)
out = state
end

```

Figura 3.29. Pseudocodul decriptării AES

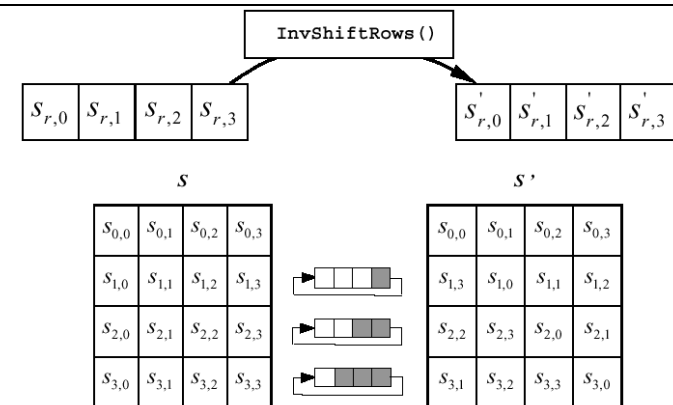


Figura 3.30. Transformarea InvShiftRows()

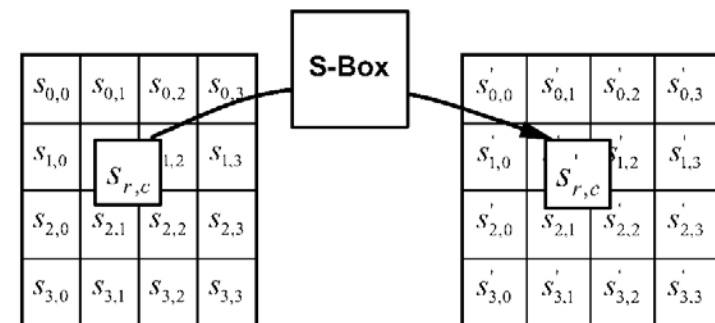


Figura 3.31. Maparea realizată de InvSubBytes()

	y															
	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
x	0	52	09	6a	d5	30	36	a5	38	bf	40	a3	9e	81	f3	db
	1	7c	e3	39	82	9b	2f	ff	87	34	8e	43	44	c4	de	e9
	2	54	7b	94	32	a6	c2	23	3d	ee	4c	95	0b	42	fa	c3
	3	08	2e	a1	66	28	d9	24	b2	76	5b	a2	49	6d	8b	d1
	4	72	f8	f6	64	86	68	98	16	d4	a4	5c	cc	5d	65	b6
	5	6c	70	48	50	fd	ed	b9	da	5e	15	46	57	a7	8d	9d
	6	90	d8	ab	00	8c	bc	d3	0a	f7	e4	58	05	b8	b3	45
	7	d0	2c	1e	8f	ca	3f	0f	02	c1	af	bd	03	01	13	8a
	8	3a	91	11	41	4f	67	dc	ea	97	f2	cf	ce	f0	b4	e6
	9	96	ac	74	22	e7	ad	35	85	e2	f9	37	e8	1c	75	df
	a	47	f1	1a	71	1d	29	c5	89	6f	b7	62	0e	aa	18	be
	b	fc	56	3e	4b	c6	d2	79	20	9a	db	c0	fe	78	cd	5a
	c	1f	dd	a8	33	88	07	c7	31	b1	12	10	59	27	80	ec
	d	60	51	7f	a9	19	b5	4a	0d	2d	e5	7a	9f	93	c9	9c
	e	a0	e0	3b	4d	ae	2a	f5	b0	c8	eb	bb	3c	83	53	99
	f	17	2b	04	7e	ba	77	d6	26	e1	69	14	63	55	21	0c

Figura 3.32. Descrierea substituției octetului xy (in hexazecimal) utilizând cutia inversă S

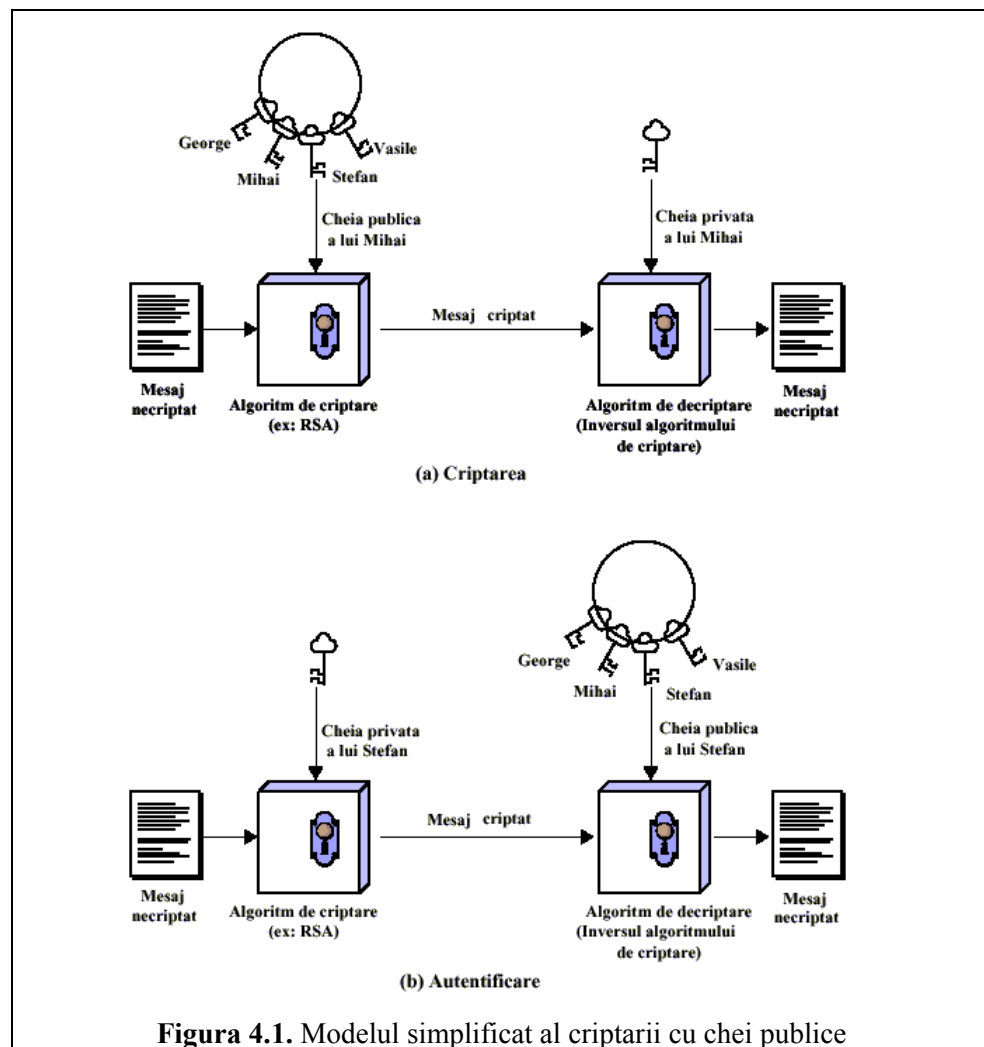


Figura 4.1. Modelul simplificat al criptării cu chei publice

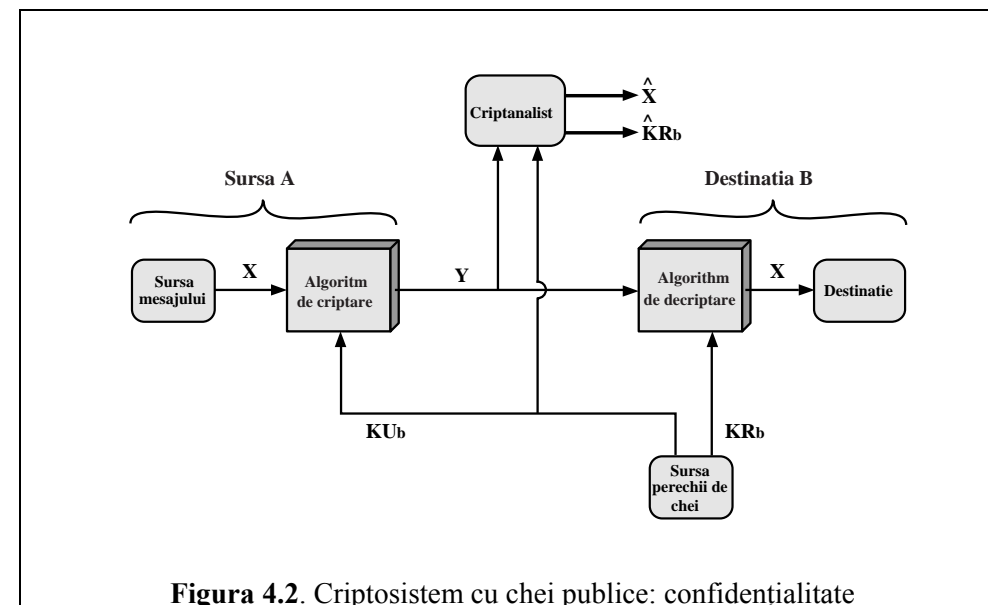


Figura 4.2. Criptosistem cu chei publice: confidențialitate

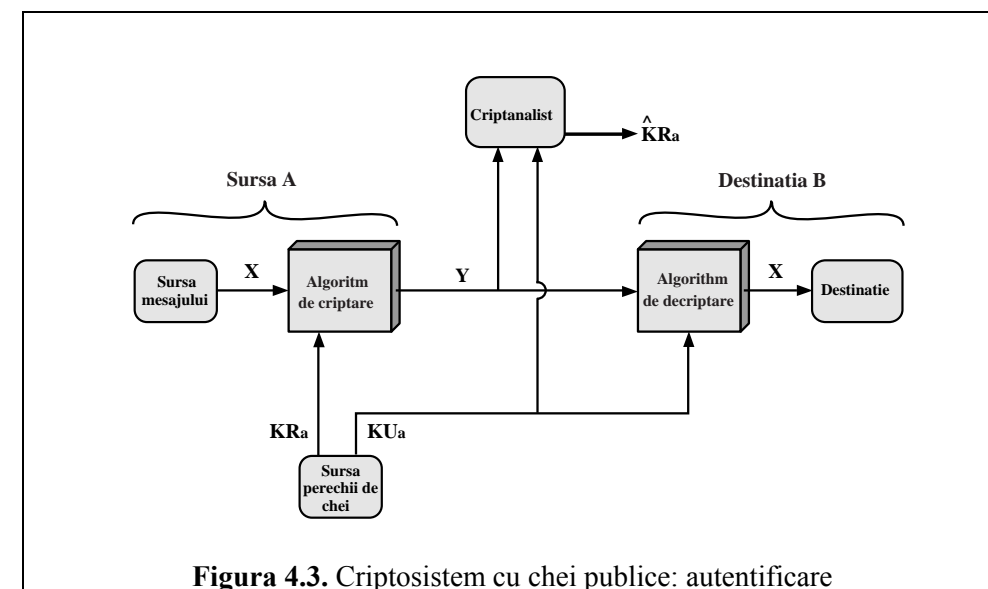
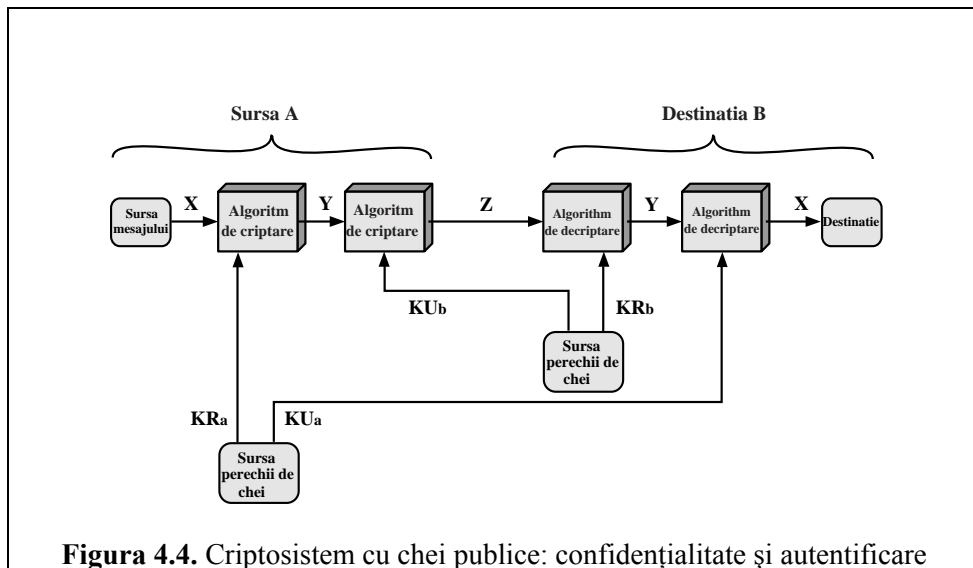


Figura 4.3. Criptosistem cu chei publice: autentificare

**Generarea cheilor**

Alege p, q (p și q sunt numere prime)

Calculează $n = p \cdot q$

Calculează $\phi(n) = (p-1)(q-1)$

Alege întregul e astfel încât $\text{cmmdc}(\phi(n), e) = 1$; $1 < e < \phi(n)$

Calculează d astfel încât $d \cdot e \bmod \phi(n) = 1$

Cheia publică $KU = \{e, n\}$

Cheia privată $KR = \{d, n\}$

Criptare

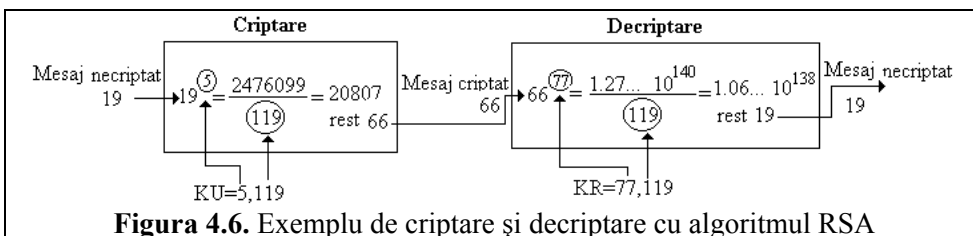
Mesaj necriptat: $M < n$

Mesaj criptat: $C = M^e \bmod n$

Decriptare

Mesaj criptat: C

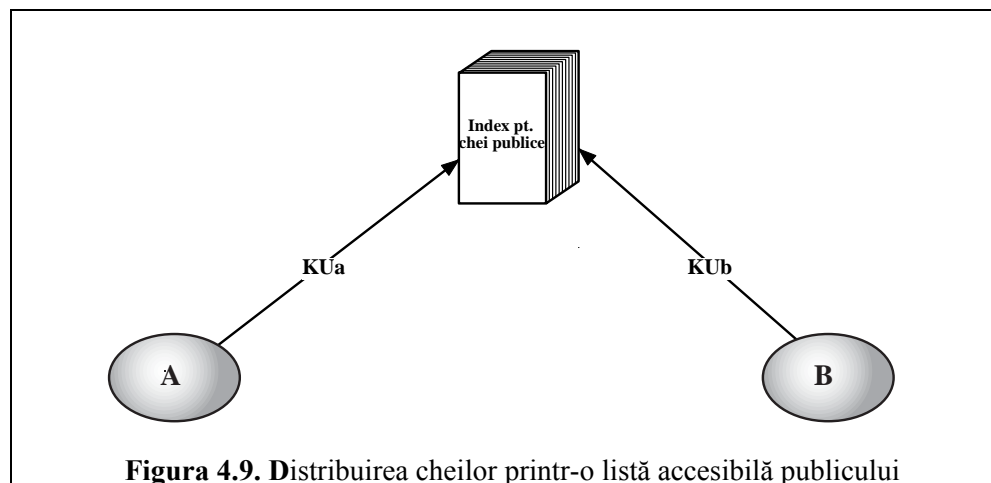
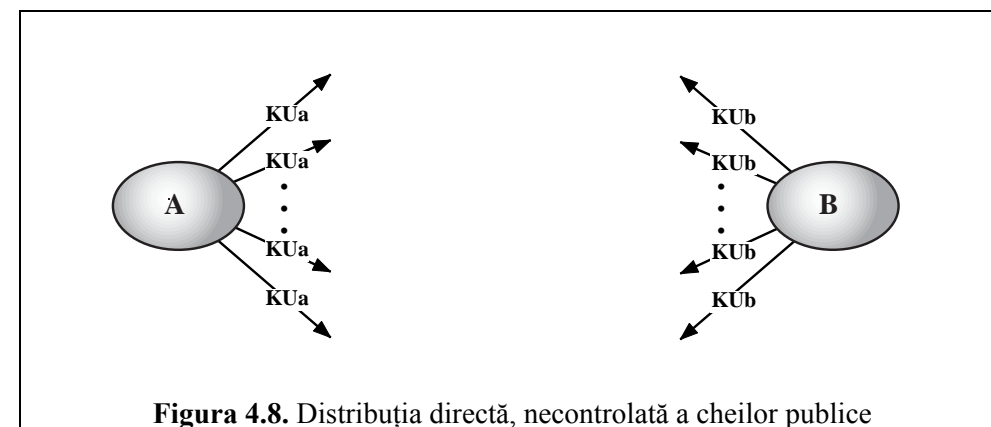
Mesaj necriptat: $M = C^d \bmod n$

Figura 4.5. Algoritmul RSA – prezentare pe scurt

```

c=0;d=1;
for i=k downto 0
do c=2c;
  d=(d·d) mod n;
  if bi=1
  then c=c+1;
    d=(d·a) mod n;
return d;

```

Figura 4.7. Algoritmul pentru calcularea $a^b \bmod n$ 

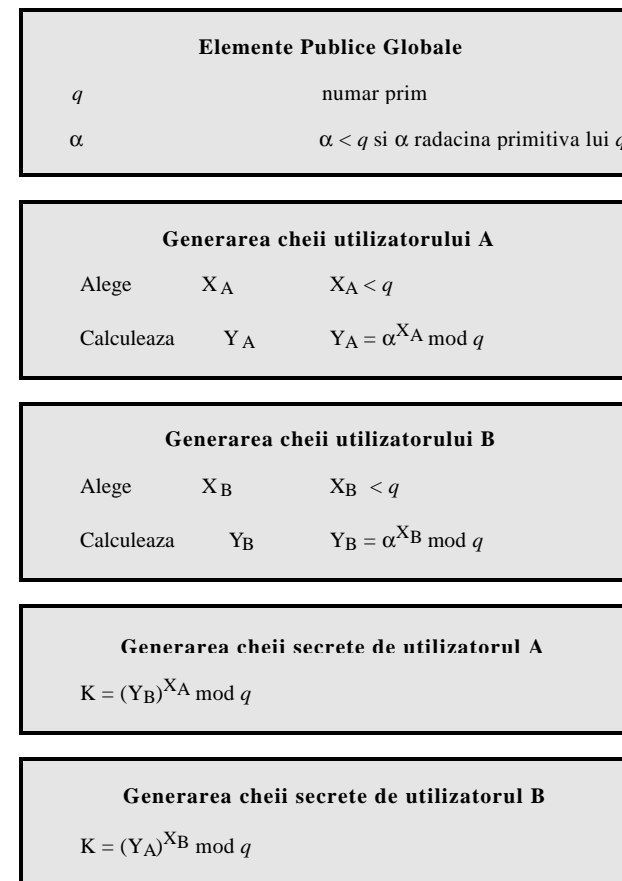
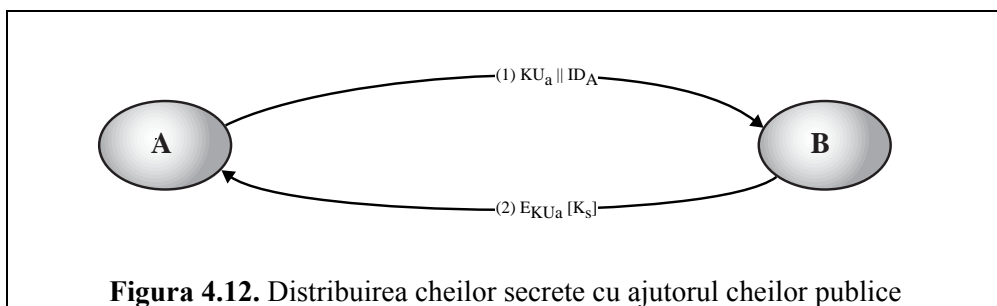
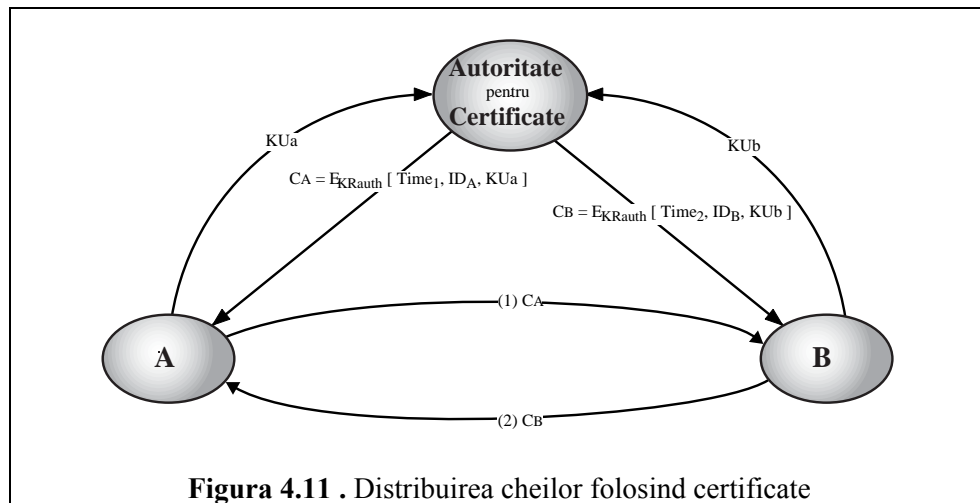
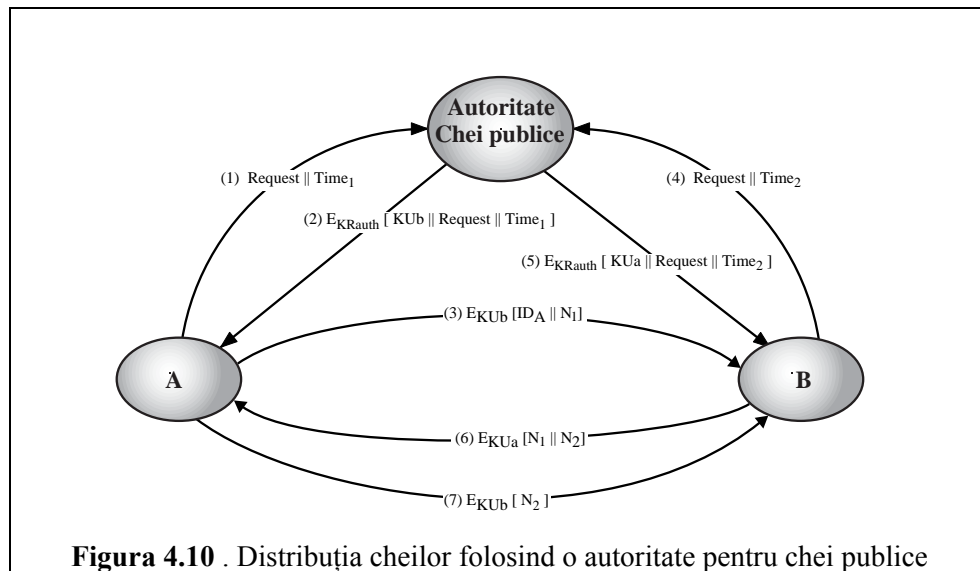


Figura 4.13. Algoritmul Diffie-Hellman