KRIPTOGRAFIJA

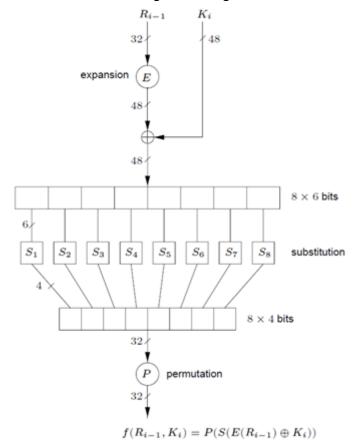
14. Data Encryption Standard (DES) - Supstitucione kutije

Sigurnost DES algoritma počiva na S-kutijama.

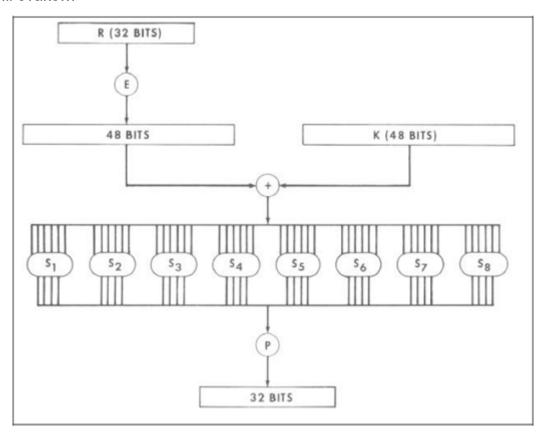
DES S-kutije (S-boxes)

- Supstitucione (zamenske) tabele
- Ulaz dužine 6 bita generiše izlaz dužine 4 bita
- Supstitucija zavisi od vrednosti ulaza (bitova ulaza)
- S-kutije su implementirane kao "lookup" tabele
- Postoji 8 S-kutija
- Svaka od 8 S-kutija ima 64 polja
- Svako polje određuje 4-bitni izlaz

Jedna runda DES algoritma izgleda ovako:



Ili ovako...



Permuatacija proširenja DES-a (E):

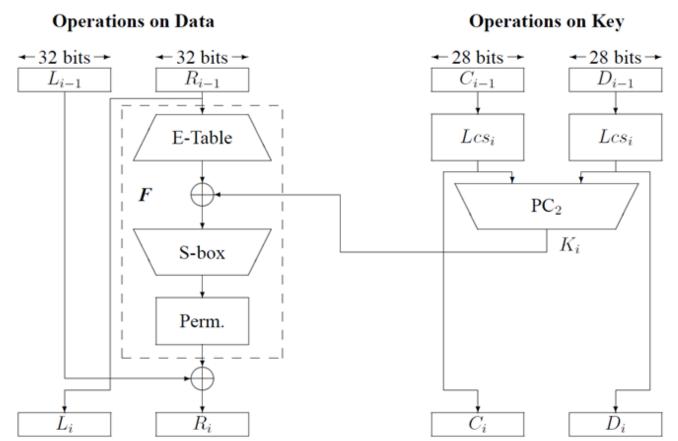
E BIT-SELECTION TABLE

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

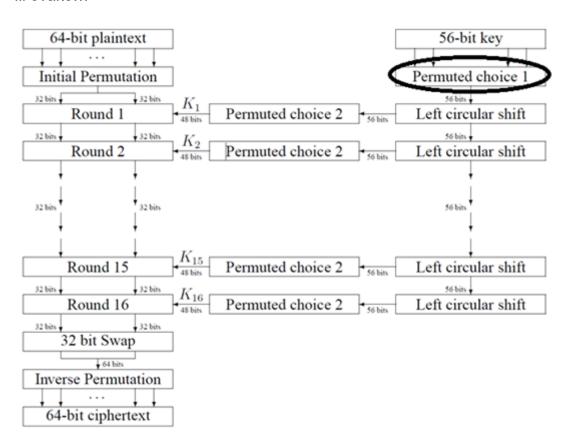
Obična permutacija DES-a (**P**):

	<u> </u>	-	
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

Šta se dešava sa ključem?



Ili ovako...



DES PC1 izbacuje bitove parnosti:

(a) Input 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
57	58	59	60	61	62	63	64

(b) Permuted Choice One (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

DES PC2 ne izbacuje bitove, već ostavlja dužinu od 48 bitova:

(c) Permuted Choice Two (PC-2)

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

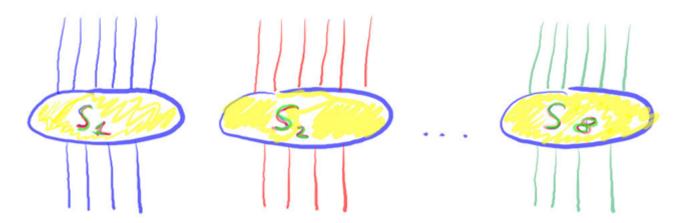
DES Left Circular Shift, odnosno šift left nad levim i desnim delom ključa, definisan je na sledeći način:

(d) Schedule of Left Shifts

Round number	1	2	3	4	5	6	7	8	9	10	11	12	13	14	1.5	16
Bits rotated	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

S-kutije (S-boxes)

Rezultat XOR operatora dužine 48 bita ulazi u supstitucione kutije, tako da svaka kutija prima 6 bitova (68 = 48), a kao rezultat daje 4 bita, odnosno ukupno 32 bita (48 = 32).



DES S kutije:

	14	- 4	13	- 1	2	15	1.1	8	3	10	- 6	12	5	9	0	7
s_1	0	1.5	7	4	1.4	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
	15	- 1	8	14	- 6	11	3	-4	9	7	2	13	12	0	5	10
S_2	3	13	4	7	1.5	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
	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
s_3	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
	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	1.5
s_4	13	8	-11	5	6	15	0	3	4	7	2	12	1	10	14	9
1990	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
	- 3	1.5	0	6	10	- 1	13	8	9	4	5	11	12	7	2	14
	_															
	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
S ₅	14	11	2	12	4	7	13	1	5	0	15	10	13	9	8	6
s_5	14	11 2	2	12	4 10	7 13	13 7	1 8	5 15	9	15 12	10 5	3 6	9	8	6 14
s_5	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
s ₅	14 4 11	11 2 8	1 12	12 11 7	4 10 1	7 13 14	13 7 2	1 8 13	5 15 6	0 9 15	15 12 0	10 5 9	3 6 10	9 3 4	8 0 5	6 14 3
	14 4 11	11 2 8	1 12 10	12 11 7	4 10 1	7 13 14	13 7 2	1 8 13	5 15 6	0 9 15	15 12 0	10 5 9	3 6 10	9 3 4	8 0 5	6 14 3
s ₅	14 4 11 12 10	11 2 8	1 12 10 4	12 11 7	4 10 1 9 7	7 13 14 2 12	13 7 2 6 9	1 8 13 8 5	5 15 6	0 9 15	15 12 0 3 13	10 5 9 4 14	3 6 10 14 0	9 3 4 7 11	8 0 5 5	6 14 3
	14 4 11 12 10 9	11 2 8 1 15 14	1 12 10 4 15	12 11 7 15 2 5	4 10 1 9 7 2	7 13 14 2 12 8	13 7 2 6 9	1 8 13 8 5 3	5 15 6 0 6 7	0 9 15	15 12 0 3 13 4	10 5 9 4 14 10	3 6 10 14 0	9 3 4 7 11 13	8 0 5 5 3 11	6 14 3
	14 4 11 12 10	11 2 8	1 12 10 4	12 11 7	4 10 1 9 7	7 13 14 2 12	13 7 2 6 9	1 8 13 8 5	5 15 6	0 9 15	15 12 0 3 13	10 5 9 4 14	3 6 10 14 0	9 3 4 7 11	8 0 5 5	6 14 3
	14 4 11 12 10 9 4	11 2 8 1 15 14 3	1 12 10 4 15 2	12 11 7 15 2 5 12	4 10 1 9 7 2 9	7 13 14 2 12 8 5	13 7 2 6 9 12 15	1 8 13 8 5 3 10	5 15 6 0 6 7 11	0 9 15 13 1 0 14	15 12 0 3 13 4 1	10 5 9 4 14 10 7	3 6 10 14 0 1 6	9 3 4 7 11 13 0	8 0 5 3 11 8	6 14 3 11 8 6 13
s_6	14 4 11 12 10 9 4	11 2 8 1 15 14 3	1 12 10 4 15 2	12 11 7 15 2 5 12	4 10 1 9 7 2 9	7 13 14 2 12 8 5	13 7 2 6 9 12 15	1 8 13 8 5 3 10	5 15 6 0 6 7 11	0 9 15 13 1 0 14	15 12 0 3 13 4 1	10 5 9 4 14 10 7	3 6 10 14 0 1 6	9 3 4 7 11 13 0	8 0 5 3 11 8	11 8 6 13
	14 4 11 12 10 9 4 13	11 2 8 1 15 14 3	1 12 10 4 15 2	12 11 7 15 2 5 12	4 10 1 9 7 2 9	7 13 14 2 12 8 5	13 7 2 6 9 12 15	1 8 13 8 5 3 10	5 15 6 0 6 7 11	0 9 15 13 1 0 14	15 12 0 3 13 4 1	10 5 9 4 14 10 7	3 6 10 14 0 1 6	9 3 4 7 11 13 0	8 0 5 3 11 8	11 8 6 13
s_6	14 4 11 12 10 9 4 13 1	11 2 8 1 15 14 3 11 0 4	10 4 15 2 11 11	12 11 7 15 2 5 12 14 7 13	4 10 1 9 7 2 9 15 4 12	7 13 14 2 12 8 5	13 7 2 6 9 12 15	1 8 13 8 5 3 10 13 10 14	5 15 6 0 6 7 11 3 14 10	0 9 15 13 1 0 14 12 3 15	15 12 0 3 13 4 1	10 5 9 4 14 10 7 7 12 8	3 6 10 14 0 1 6	9 3 4 7 11 13 0	8 0 5 3 11 8 6 8	11 8 6 13
s_6	14 4 11 12 10 9 4 13	11 2 8 1 15 14 3	1 12 10 4 15 2	12 11 7 15 2 5 12	4 10 1 9 7 2 9	7 13 14 2 12 8 5	13 7 2 6 9 12 15	1 8 13 8 5 3 10	5 15 6 0 6 7 11	0 9 15 13 1 0 14	15 12 0 3 13 4 1	10 5 9 4 14 10 7	3 6 10 14 0 1 6	9 3 4 7 11 13 0	8 0 5 3 11 8	11 8 6 13
s_6	14 4 11 12 10 9 4 13 1 6	11 2 8 1 15 14 3 11 0 4 11	1 12 10 4 15 2 11 11 13	12 11 7 15 2 5 12 14 7 13 8	4 10 1 9 7 2 9 15 4 12 1	7 13 14 2 12 8 5 0 9 3 4	13 7 2 6 9 12 15 8 1 7	1 8 13 8 5 3 10 13 10 14 7	5 15 6 0 6 7 11 3 14 10 9	0 9 15 13 1 0 14 12 3 15 5	15 12 0 3 13 4 1	10 5 9 4 14 10 7 7 12 8 15	3 6 10 14 0 1 6 5 2 0 14	9 3 4 7 11 13 0 10 15 5 2	8 0 5 3 11 8 6 8 9 3	6 14 3 11 8 6 13
s ₆	14 4 11 12 10 9 4 13 1	11 2 8 1 15 14 3 11 0 4 11	1 12 10 4 15 2 11 11 13	12 11 7 15 2 5 12 14 7 13	4 10 1 9 7 2 9 15 4 12	7 13 14 2 12 8 5 0 9 3 4	13 7 2 6 9 12 15 8 1 7 10	1 8 13 8 5 3 10 13 10 14	5 15 6 0 6 7 11 3 14 10 9	0 9 15 13 1 0 14 12 3 15 5	15 12 0 3 13 4 1	10 5 9 4 14 10 7 12 8 15	3 6 10 14 0 1 6	9 3 4 7 11 13 0	8 0 5 3 11 8 6 8 9 3	6 14 3 11 8 6 13 1 6 2 12
s_6	14 4 11 12 10 9 4 13 1 6	11 2 8 1 15 14 3 11 0 4 11	2 1 12 10 4 15 2 11 11 13 8 13	12 11 7 15 2 5 12 14 7 13 8	4 10 1 9 7 2 9 15 4 12 1	7 13 14 2 12 8 5 0 9 3 4	13 7 2 6 9 12 15 8 1 7 10	1 8 13 8 5 3 10 13 10 14 7	5 15 6 0 6 7 11 3 14 10 9	0 9 15 13 1 0 14 12 3 15 5	3 13 4 1 9 5 6 0	10 5 9 4 14 10 7 7 12 8 15	3 6 10 14 0 1 6 5 2 0 14	9 3 4 7 11 13 0 10 15 5 2	8 0 5 3 11 8 6 8 9 3	6 14 3 11 8 6 13 1 6 2 12
s ₆	14 4 11 12 10 9 4 13 1 6	11 2 8 1 15 14 3 11 0 4 11	1 12 10 4 15 2 11 11 13	12 11 7 15 2 5 12 14 7 13 8	4 10 1 9 7 2 9 15 4 12 1	7 13 14 2 12 8 5 0 9 3 4	13 7 2 6 9 12 15 8 1 7 10	1 8 13 8 5 3 10 13 10 14 7	5 15 6 0 6 7 11 3 14 10 9	0 9 15 13 1 0 14 12 3 15 5	15 12 0 3 13 4 1 9 5 6 0	10 5 9 4 14 10 7 12 8 15	3 6 10 14 0 1 6 5 2 0 14	9 3 4 7 11 13 0 15 5 2	8 0 5 3 11 8 6 8 9 3	6 14 3 11 8 6 13 1 6 2 12

																	_
	14	4	13	- 1	2	15	11	8	3	10	6	12	5	9	0	7]
s_1	0	1.5	7	4	14	2	13	1	10	6	12	11	9	5	3	8	bitovi od 1 do 6
	-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]
	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10	l
s_2	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5	bitovi od 7 do 12
	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	1.5	Ditovi od 7 do 12
	13	8	10	- 1	3	15	4	2	-11	6	7	12	0	5	14	9	J
	10	-	-			-		-				-			-		1
	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8	l
s_3	13	7	0	9	3	4	6	10	2	8	5	14	12	11	1.5	1	l
	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	J
	7	13	14	3	0	- 6	9	10	- 1	2	8	5	-11	12	4	15	1
S_4	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9	
-4																	l
	10	15	9	6	12	11	7	13	15	4	5	14	5	7	8	14	l
	3	15	0	0	10	- 1	13	8	- 4	4	- 5	- 11	12	- 1	- 4	14	ı
	2	12	4	- 1	7	10	11	6	8	5	3	15	13	0	14	9	1
S_5	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	
																	•
	12	1	10	15	9	2	- 6	8	0	13	3	4	14	7	.5	11	1
s_6	10	1.5	-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]
	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	- 1	
S ₇	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]
	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7	
s_8	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2	bitovi od 43 do 48
	7	11	4	1	9	12	14	2	0	6	10	13	1.5	3	5	8	
	-3	1	1.4	7	4	10	8	13	15	12	0	0	- 3	- 5	6	11	I

Kako funkcionišu S kutije?

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

Na ulazu u S kutiju je 6 bitova: $b_1 \ b_2 \ b_3 \ b_4 \ b_5 \ b_6$.

Bitovi b_1 i b_6 se kombinuju i formiraju 2 bitni broj (od 0 do 3) koji određije vrstu tabele. Bitovi b_2 b_3 b_4 b_5 se kombijuju i formiraju 4 bitni broj (od 0 do 15) koji određuje kolonu tabele.

Broj koji se nalazi u izabranoj ćeliji se pretvara u binarni zapis i kao takav čini izlaz S kutije.

Primer.

b ₁	b ₂	b ₃	b ₄	b₅	b ₆
1	1	0	0	1	1

 $b_1b_6 = (11)_2 = (3)_{10}$. Odabrana je vrsta 3 S – kutije.

 $b_2b_3b_4b_5 = (1001)_2 = (9)_{10}$. Odabrana je kolona 9 S – kutije.

$$S1[3,9] = (11)_{10} = (1011)_2.$$

Na ulazu S1 – kutije je: 110011, a na izlazu će biti: 1011.

Na ovaj način je ulaz u 8 S kutija, koji je dužine 48 bita, transformisan u izlaz dužine 32 bita.