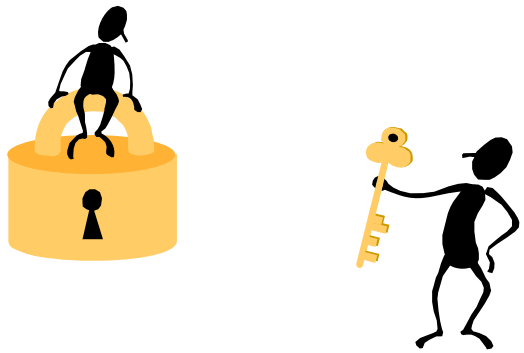
Šifrirni algoritmi

- Klasično šifriranje
  - transpozicijska in substitucijska šifra
  - pretočno in blokovno šifriranje
- Simetrični šifrirni algoritmi
  - DES
  - AES
  - ostali simetrični šifrirni algoritmi



Klasične metode šifriranja

- Pri transpozicijskem šifriranju premešamo znake v sporočilu
  - izberemo tajno "ključno besedo" npr. *blisk* :

geslo →

čistopis:

napad ob šesti uri

b	*l*	*i*	*s*	*k*
1	4	2	5	3
n	a	p	a	d
o	b	š	e	s
t	i	u	r	i

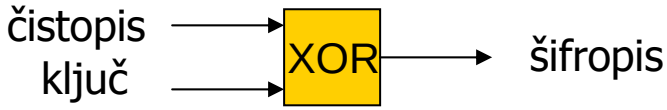
šifropis:

notpšudsiabiaer

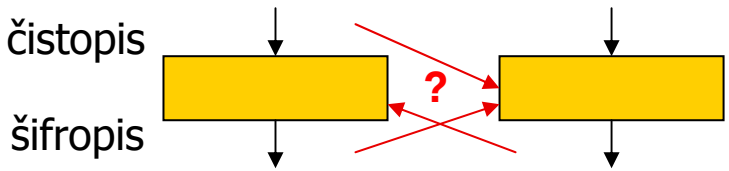
- Pri substitucijskem šifriranju zamenjamo znake v sporočilu
  - zamenjava je lahko s pomočjo tabele ali algoritma
  - Primer je Cezarjeva šifra: C(P)=(P+3) mod 25

Pretočno in blokovno šifriranje

- Glede na dolžino sporočila, ki ga naenkrat šifriramo ločimo:
  - Pretočno šifriranje preslika sproti vsak znak ali zelo majhno število znakov, primer je substitucijsko šifriranje.
  - Blokovno šifriranje, kjer veliko število znakov čistopisa šifriramo v blok znakov šifropisa, primer je transpozicijsko šifriranje.
- Pretočno šifriranje je mnogo hitrejše od blokovnega.
  - Primer zelo hitrega pretočnega šifriranja je množenje bitnega zaporedja čistopisa z naključno izbranim ključem po modulu 2.

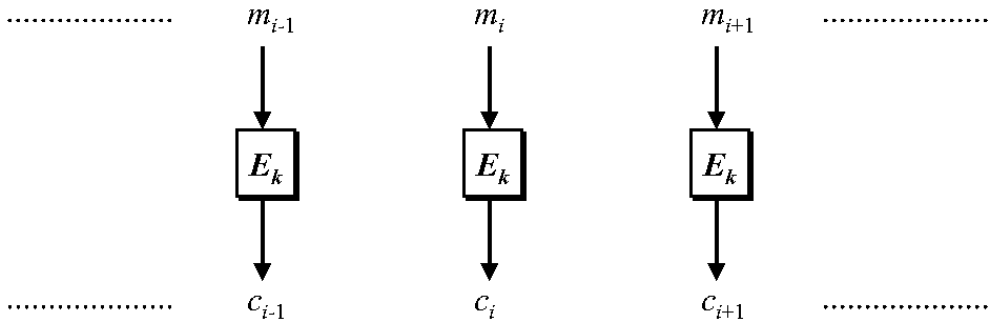


- Blokovno šifriranje je tipično z dolžino 64 bitov (primer: DES). Glede na soodvisnosti čistopisov in šifropisov med bloki ločimo več načinov blokovnega šifriranja (ECB, CBC, CFB, OFB).



Načini blokovnega šifriranja

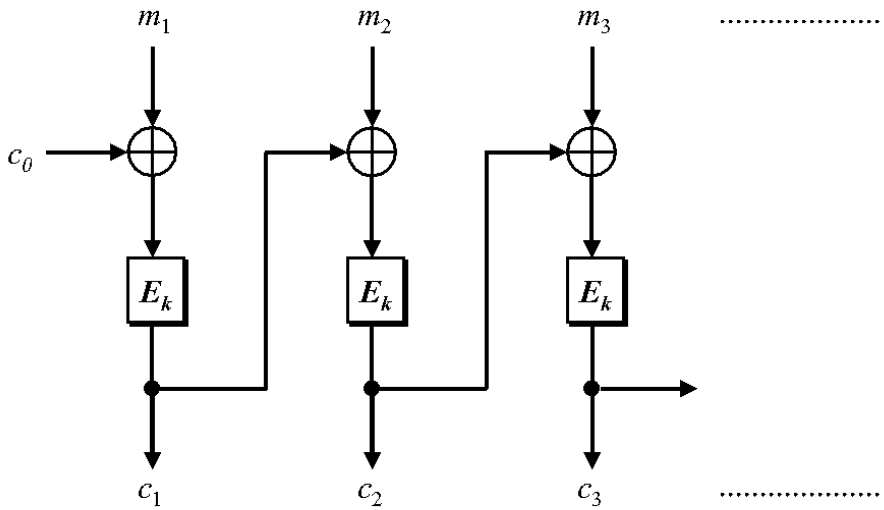
- ECB = Electronic Code Book



- Med bloki ni povezav, vsak blok šifriramo ločeno z 64 bitnim ključem
- Slabost: pri ponavljajočih blokih čistopisa dobimo tudi ponavljajoči vzorec v šifropisu.

Načini blokovnega šifriranja

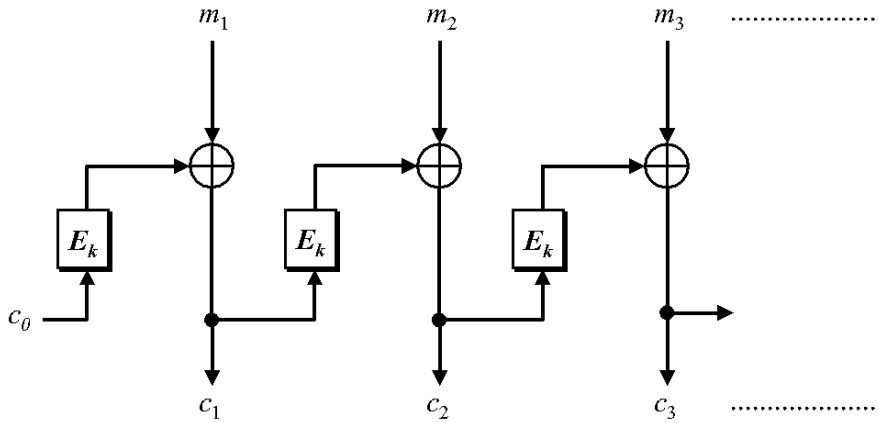
- CBC = Cipher Block Chaining



- Bloki so verižno povezani tako, da vedno šifriramo mešani (XOR) čistopis bloka in šifropis predhodnega bloka.
- Veriženje preprečuje pojav ponavljajočih vzorce v šifropisu.
- Začetno stanje določa inicializacijski vektor c_0

Način blokovnega šifriranja

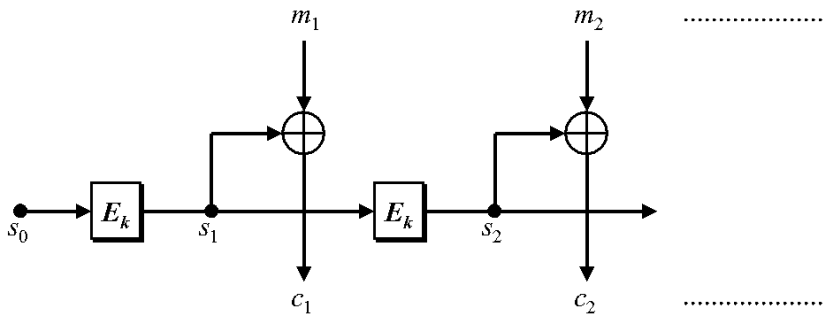
- CFB = Cipher Feedback Mode



- Šifropis bloka dobimo z mešanjem (XOR) čistopisa in šifropisa predhodnega bloka.
- Začetno stanje določa inicializacijski vektor c_0 .

Načini blokovnega šifriranja

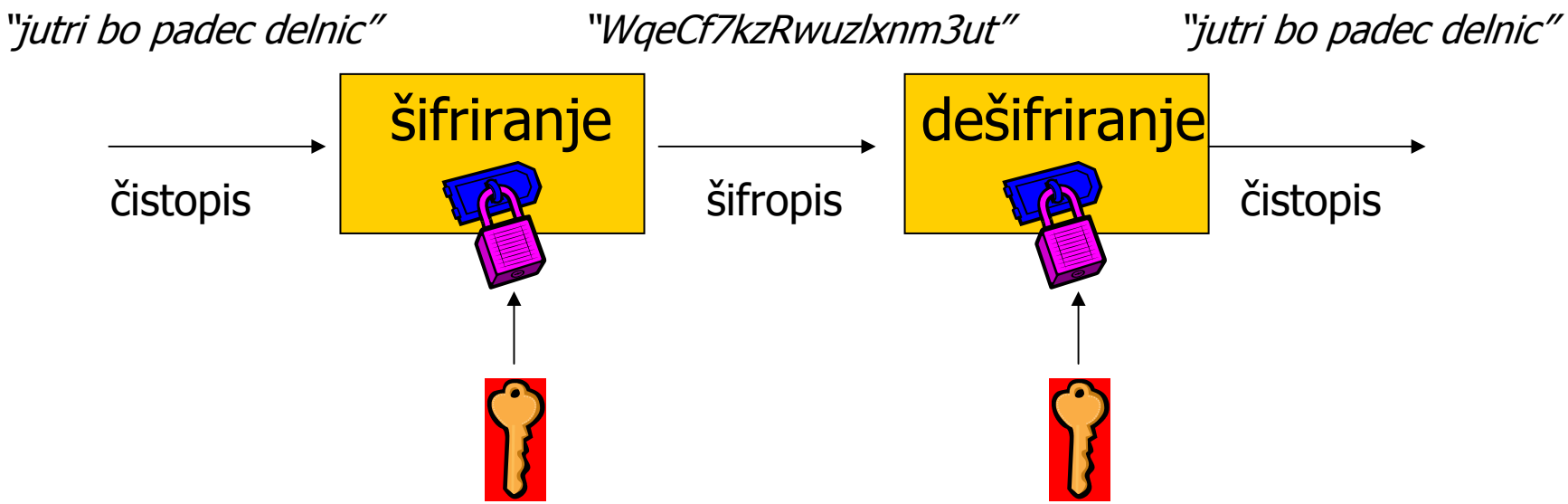
- OFB = Output Feedback Mode



- Šifropis bloka dobimo z mešanjem (XOR) čistopisa in zaporednega stanja s_k .
- Zaporedja podatkovnih blokov s_k dobimo s šifriranjem predhodnih blokov s_{k-1}
- Začetno stanje s_0 je naključno število

Simetrično šifriranje

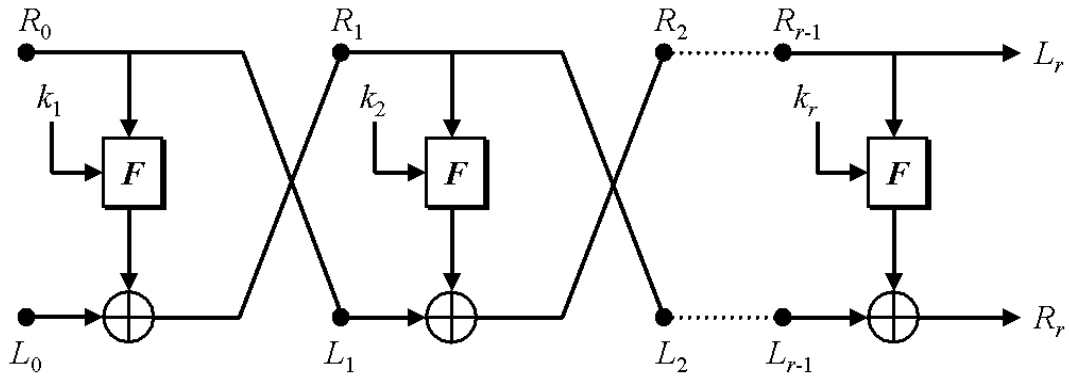
- Za šifriranje in dešifriranje uporabimo isti ključ:



- Pošiljatelj in prejemnik morata uporabiti enak tajni ključ !

Blokovni šifrirni postopek s ponavljanjem

- Proces blokovnega šifriranja lahko poteka v več krogih z enako transformacijsko funkcijo in različnimi ključi. Nabor ključev v tem primeru izhaja iz istega tajnega ključa. Varnost algoritma se povečuje s številom krogov, žal pa tudi računska kompleksnost.
- Feistel - ovo šifriranje je večkrožno blokovno šifriranje, kjer podatkovni blok razpolovimo na levi in desni del:



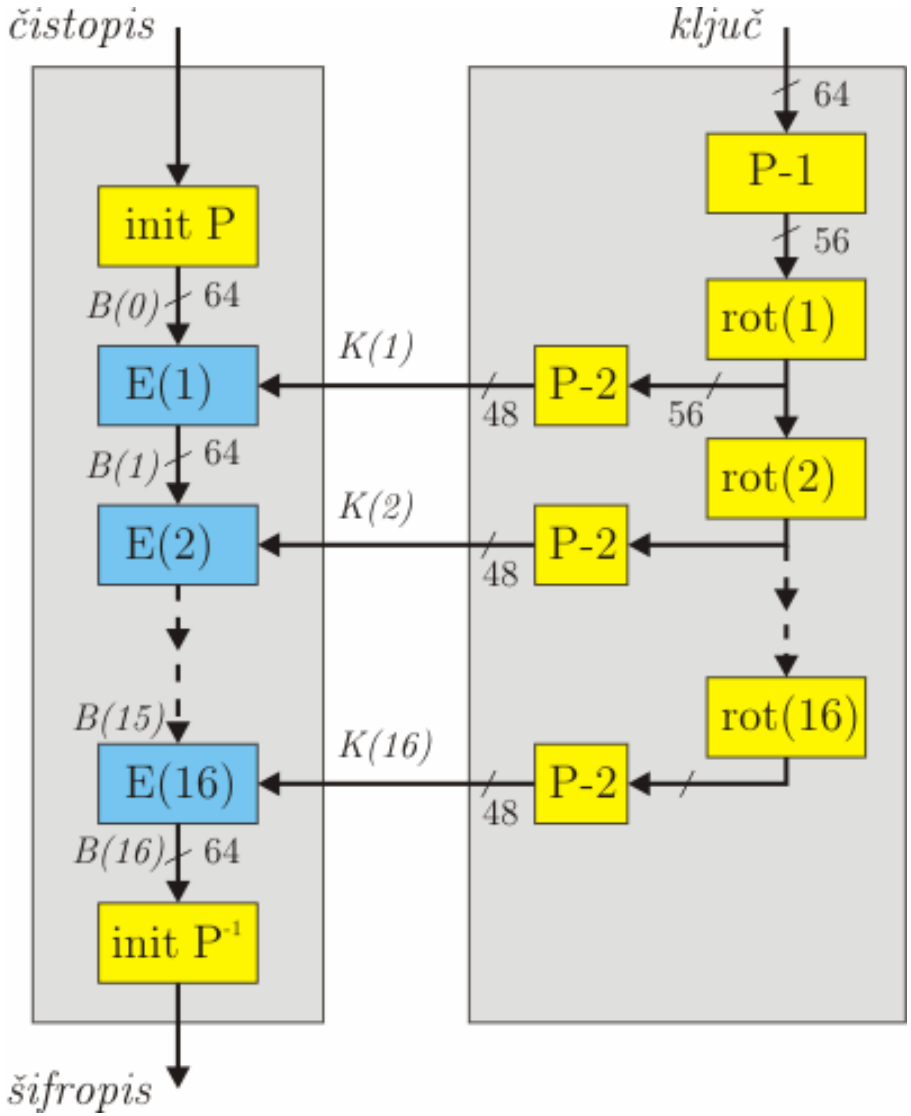
- Šifriranje se izvaja samo nad polovico podatkovnega bloka, druga polovica pa se diagonalno prepisuje v naslednji krog.
- Dešifriranje poteka na enak način, vendar s ključi v nasprotnem vrstnem redu (kr, ...k2,k1)

Simetrični šifrirni algoritem DES

- DES = Data Encryption Standard
  - prvič je objavljen 1977, vlada ZDA ga je izbrala kot standard za podatkovne komunikacije,
  - ključ ima dolžino 56 bitov, dolžina bloka je 64 bitov,
  - največkrat se uporablja CBC način bločnega šifriranja, možni pa so tudi vsi ostali načini (CFB in OFB).
  - s poskušanjem (brute force) je mogoče z zelo dobro opremo dešifrirati DES v razmeroma kratkem času, vseeno pa zadošča za običajno civilno uporabo
- Triple-DES (3 DES) : trikrat šifrira 64 bitni blok podatkov z DES algoritmom z različnimi ključi. Obstajajo tri verzije 3 DES:
  - E(K1, E(K2), E(K3, P))) , 3 ključi,
  - E(K1, E(K2, E(K1, P)), 2 ključa,
  - E(K1, D(K2, E(K1, P)), 2 ključa,
  - vse tri verzije so enako varne (efektivni 112 bitni ključ)

Šifrirni algoritem DES

- Po začetni permutaciji poteka šifriranje v 16 krogih
- na osnovi 56 bitnega sejnega ključa generiramo 16 podključev K(r)
- jedro DES algoritma je enkripcijski modul E(1) - E(16)
- zadnja operacija nad blokom šifriranih podatkov je inverzna začetna permutacija



Permutacije bitov

- blok N bitov preslikamo tako, da zamenjamo lego bitov v bloku
- takšni preslikavi sta permutaciji bloka podatkov IP in IP^{-1} pri DES algoritmu:

44 -> 35

Bit	0	1	2	3	4	5	6	7
1	40	8	48	16	56	24	64	32
9	39	7	47	15	55	23	63	31
17	38	6	46	14	54	22	62	30
25	37	5	45	13	53	21	61	29
33	36	4	44	12	52	20	60	28
41	35	3	43	11	51	19	59	27
49	34	2	42	10	50	18	58	26
57	33	1	41	9	49	17	57	25

35 -> 44

Bit	0	1	2	3	4	5	6	7
1	58	50	42	34	26	18	10	2
9	60	52	44	36	28	20	12	4
17	62	54	46	38	30	22	14	6
25	64	56	48	40	32	24	16	8
33	57	49	41	33	25	17	9	1
41	59	51	43	35	27	19	11	3
49	61	53	45	37	29	21	13	5
57	63	55	47	39	31	23	15	7

Permutacije bitov v manjše ali večje bloke

- Blok N bitov preslikamo z zamenjavo lege v manjši blok bitov. Primer redukcije pri DES algoritmu je permutacija bitov po tabeli P-2:

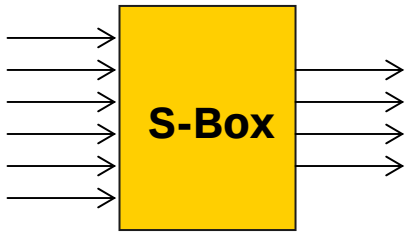
Bit	0	1	2	3	4	5
1	14	17	11	24	1	5
7	3	28	15	6	21	10
13	23	19	12	4	26	8
19	16	7	27	20	13	2
25	41	52	31	37	47	55
31	30	40	51	45	33	48
37	44	49	39	56	34	53
43	46	42	50	36	29	32

- Blok N bitov preslikamo z zamenjavo lege v večji blok bitov. Primer ekspanzije pri DES algoritmu je permutacija bitov po tabeli E:

Bit	0	1	2	3	4	5
1	32	1	2	3	4	5
7	4	5	6	7	8	9
13	8	9	10	11	12	13
19	12	13	14	15	16	17
25	16	17	18	19	20	21
31	20	21	22	23	24	25
37	24	25	26	27	28	29
43	28	29	30	31	32	1

Substitucijsko šifriranje

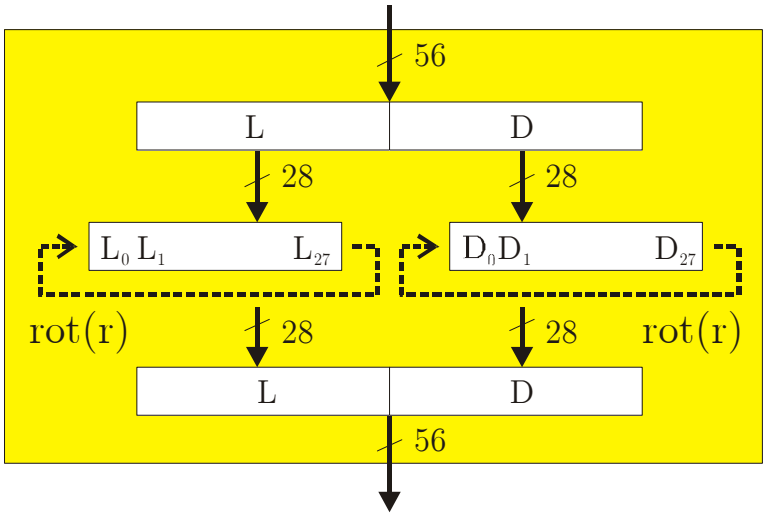
- Blok N bitov preslikamo v nov blok z zamenjavami. Primer substitucijskega kodiranja pri DES algoritmu so S- škatle
- S_1 do S_8 pretvarjajo 6-bitne bloke v 4-bitne bloke.
- Zgornji in spodnji bit določata vrstico v tabeli, srednji štirje biti pa določajo stolpec v tabeli:

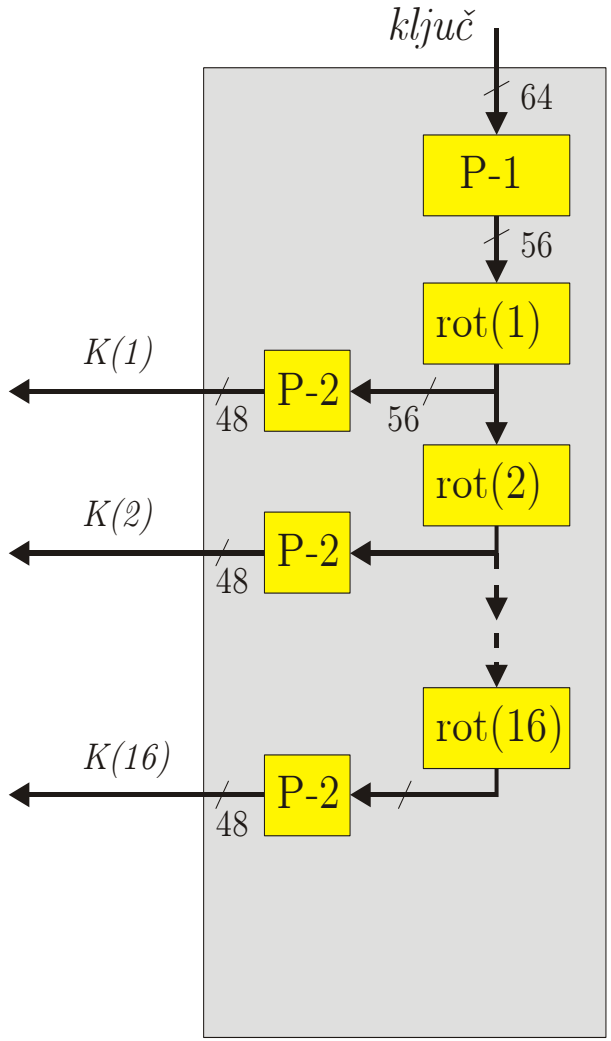


Row / Column	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6

Generacija nabora 16 ključev

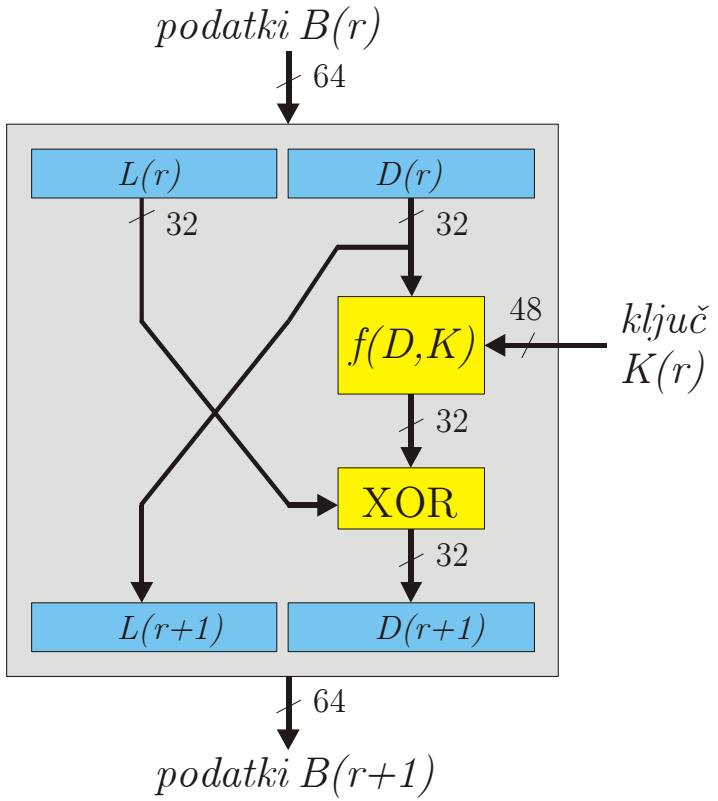
- P-1 preslika 64-bitni ključ v 56-bitni ključ
- P-2 je zamenjava bitov z redukcijo bloka iz 56 v 48 bitov
- rotacija ali krožna preslikava leve in desne polovice 56- bitnega ključa se ponavlja z različnim številom premikov (1 ali 2)

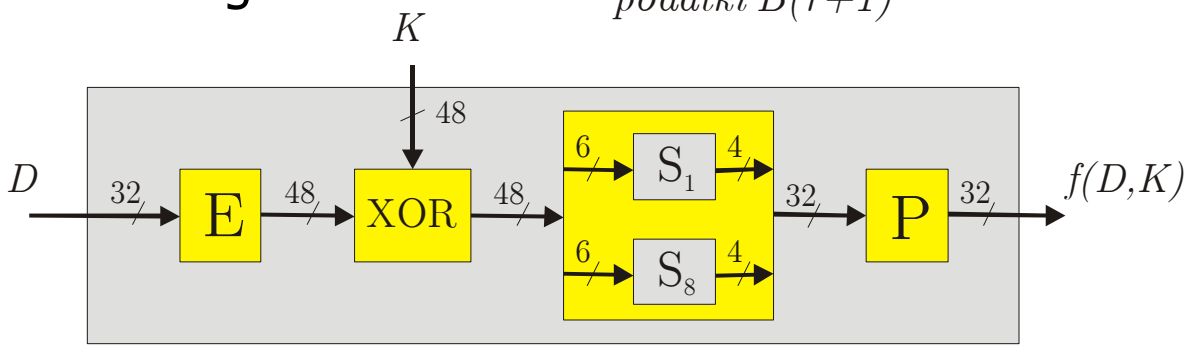




Jedro DES algoritma

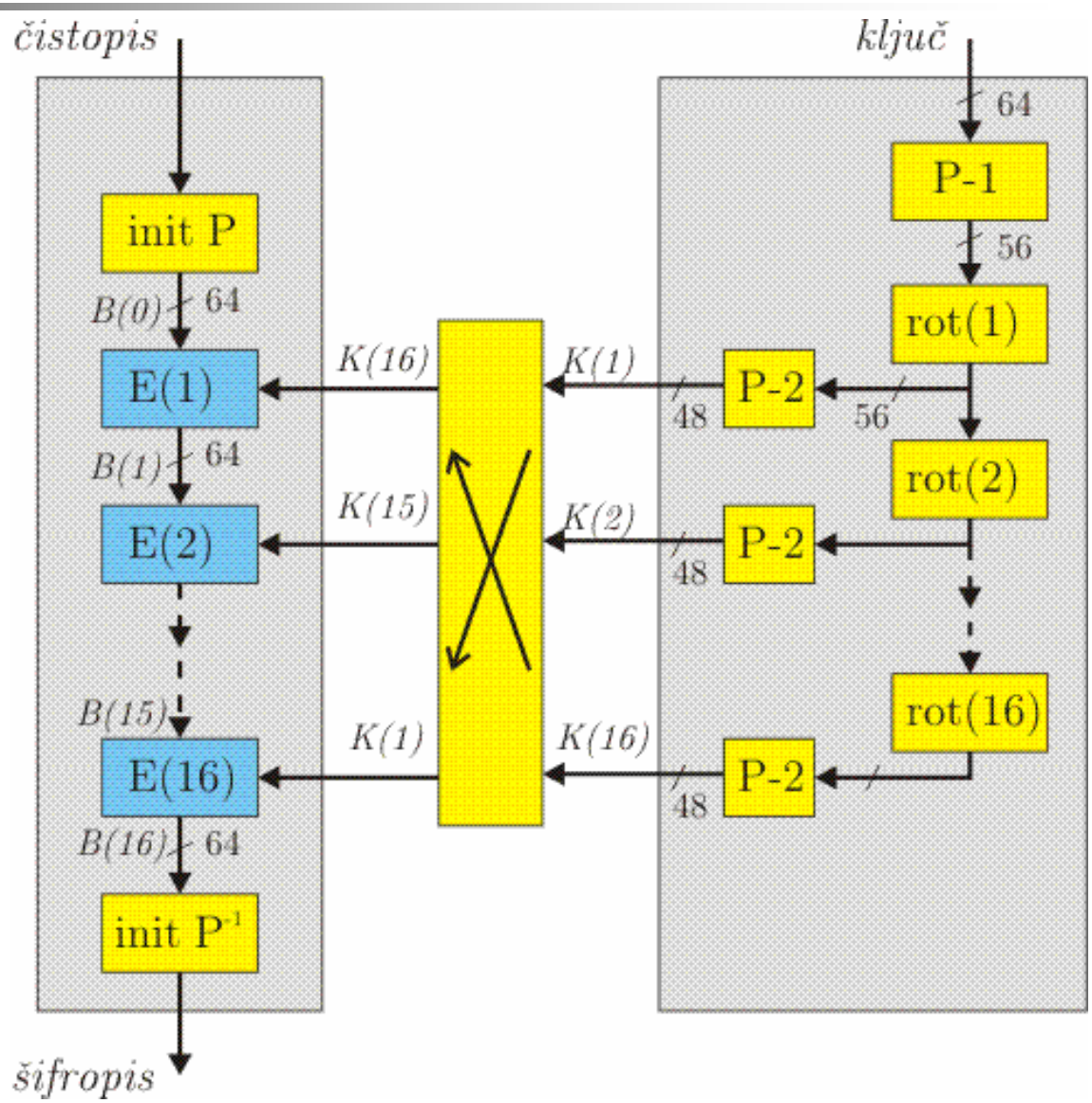
- postopek šifriranja 64-bitnega bloka podatkov ponavljamo z različnimi ključi *K(1)...K(16)*
- blok razdelimo na levo in desno polovico *L(r)* in *D(r)*
- leva polovica v novem bloku *L(r+1)* je enaka desni polovici predhodnega bloka
- desna polovica v novem bloku *D(r+1)* je odvisna od ključa in celotne vsebine predhodnega bloka:





Dešifrirni algoritem DES

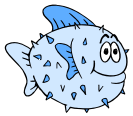
- DES je simetrični šifrirni postopek
- algoritem za dešifriranje je enak kot za šifriranje,
- Pri dešifriranju se zamenja le vrstni red pri uporabi podključev:
  - K(16),
  - K(15) ..
  - K(1)



AES = Advanced Encryption Standard

- AES nudi najbolj zanesljiv simetrični šifrirni postopek in služi kot zamenjava za zastareli DES in 3DES
- NIST je v natečaju za AES leta 1997 postavil zahtevo za javni simetrični blokovni algoritem, ki deluje z 128-bitnimi blokom in uporablja tri dolžine ključa: 128, 192 in 256 bitov.
- RIJNDAEL algoritem izpolnjuje postavljene zahteve z najboljšo oceno analiz v času javnega ocenjevanja (do 2000). Izbiramo lahko med devetimi kombinacijami parov dolžine bloka in dolžine ključa (128, 192 in 256). Ime algoritma izhaja iz priimkov avtorjev iz Belgije: Rijmen in Daemen.
- RIJNDAEL je ponavljajoč (večkrožni) blokovni algoritem, število krogov šifriranja (od 10 do 14) pa je odvisno od dolžine bloka in dolžine ključa. V vsakem krogu šifriranja se izvaja štiri različne matematične operacije (ByteSub, ShiftRow, MixColumn, AddRoundKey).

Ostali simetrični šifrirni postopki



- IDEA - International Data Encryption Algorithm uporablja 128 bitni ključ, ki ga razdelimo na 52 ključev dolžine 16 bitov.
- Blowfish algoritem uporablja različno dolge ključe od 32 do 448 bitov,
- Skipjack algoritem uporablja 80-bitni ključ. Implementiran je v šifrirnih napravah Clipper, zato je bil zelo dolgo tajen,
- CAST uporablja ključ z dolžino od 40-128 bitov,
- Kot finalni kandidati natečaja za AES (1997-98) so poleg zmagovalca RIJNDAEL nastopili še:
  - MARS (IBM)
  - RC6 (RSA Security)
  - TWOFISH (Counterpane Systems)
  - SERPENT