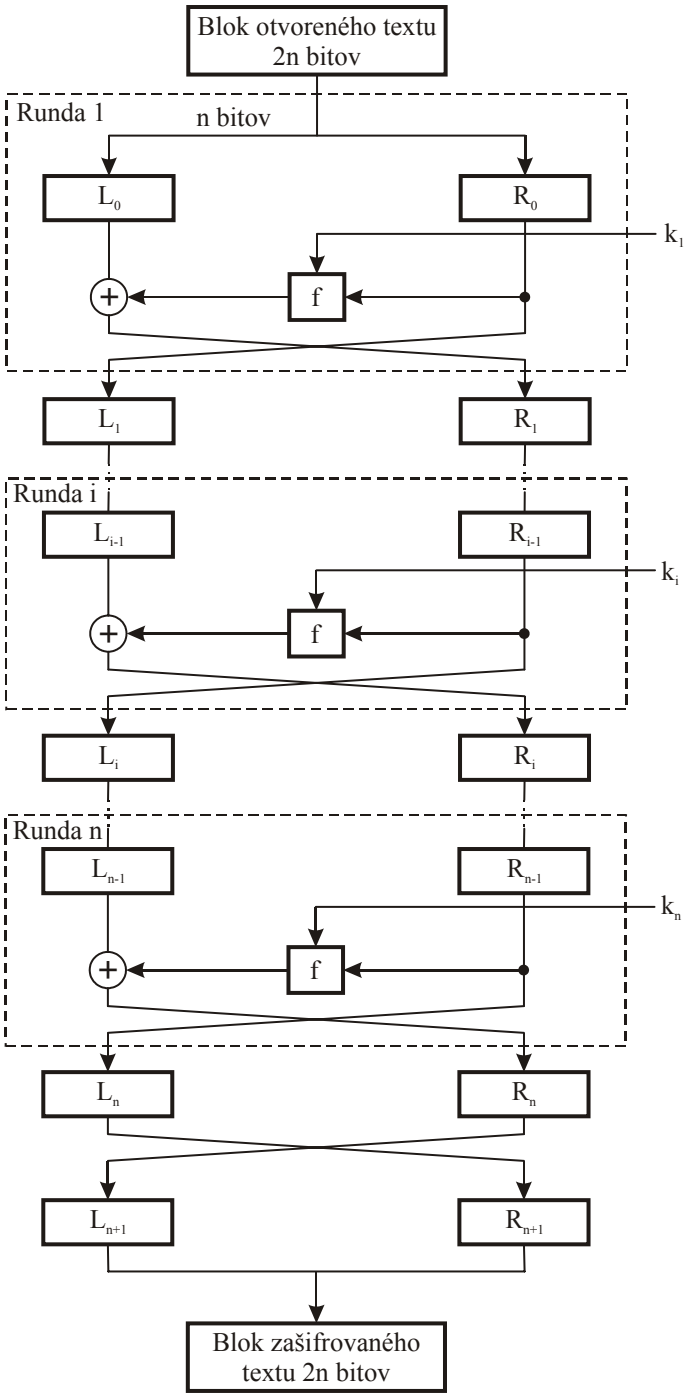
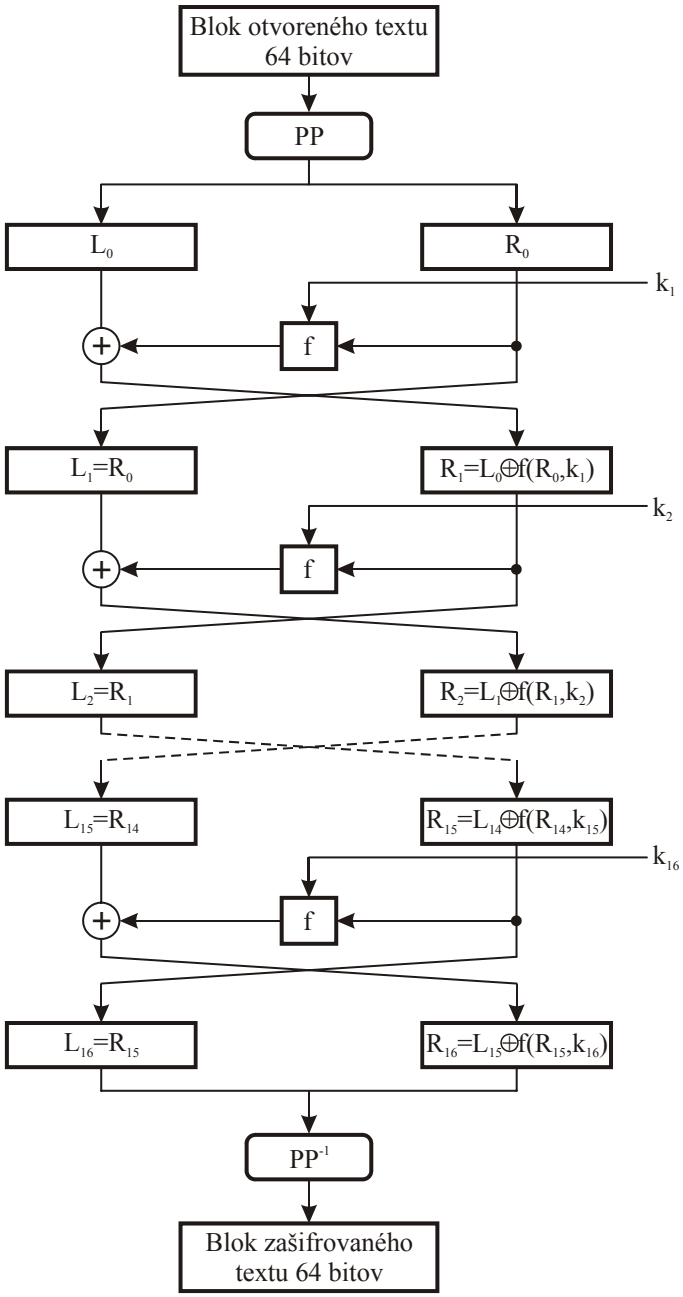
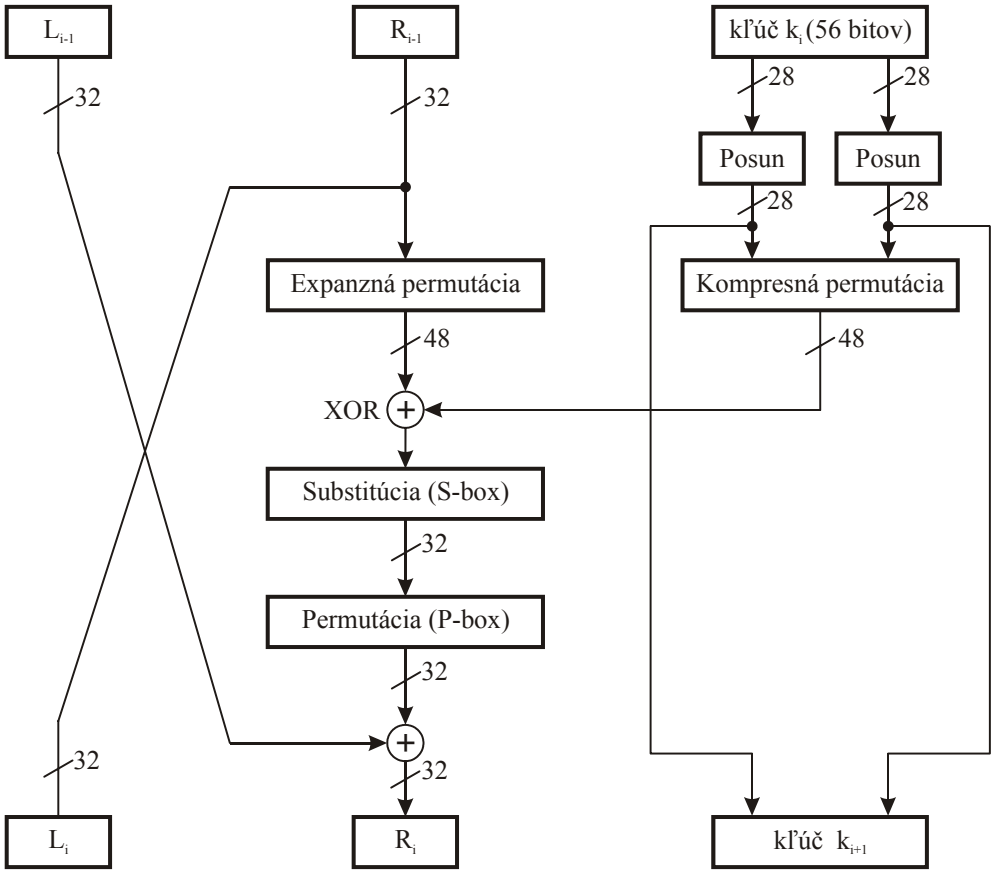


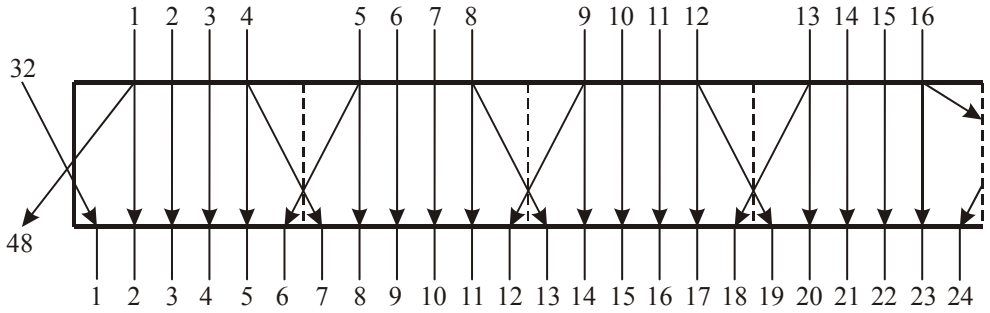
Feistelova bloková šifra



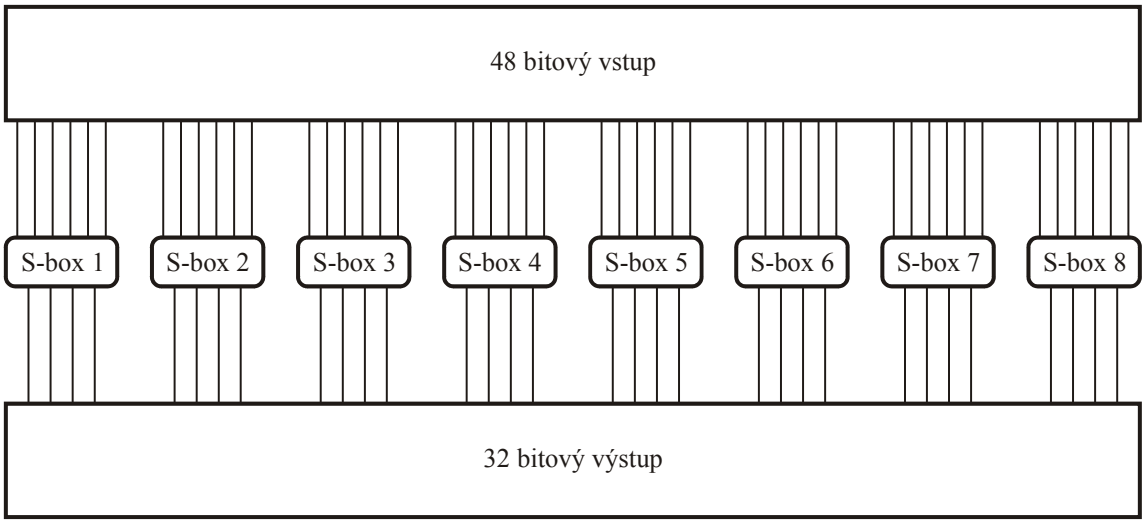
Štruktúra algoritmu DES



Štruktúra rundy DES



Realizácia expanznej permutácie



Substitúcia pomocou S-boxov

Vstupné dáta

in_0	in_4	in_8	in_{12}
in_1	in_5	in_9	in_{13}
in_2	in_6	in_{10}	in_{14}
in_3	in_7	in_{11}	in_{15}

Medzivýsledky (State array)

$s_{0,0}$	$s_{0,1}$	$s_{0,2}$	$s_{0,3}$
$s_{1,0}$	$s_{1,1}$	$s_{1,2}$	$s_{1,3}$
$s_{2,0}$	$s_{2,1}$	$s_{2,2}$	$s_{2,3}$
$s_{3,0}$	$s_{3,1}$	$s_{3,2}$	$s_{3,3}$

Výstupné dáta

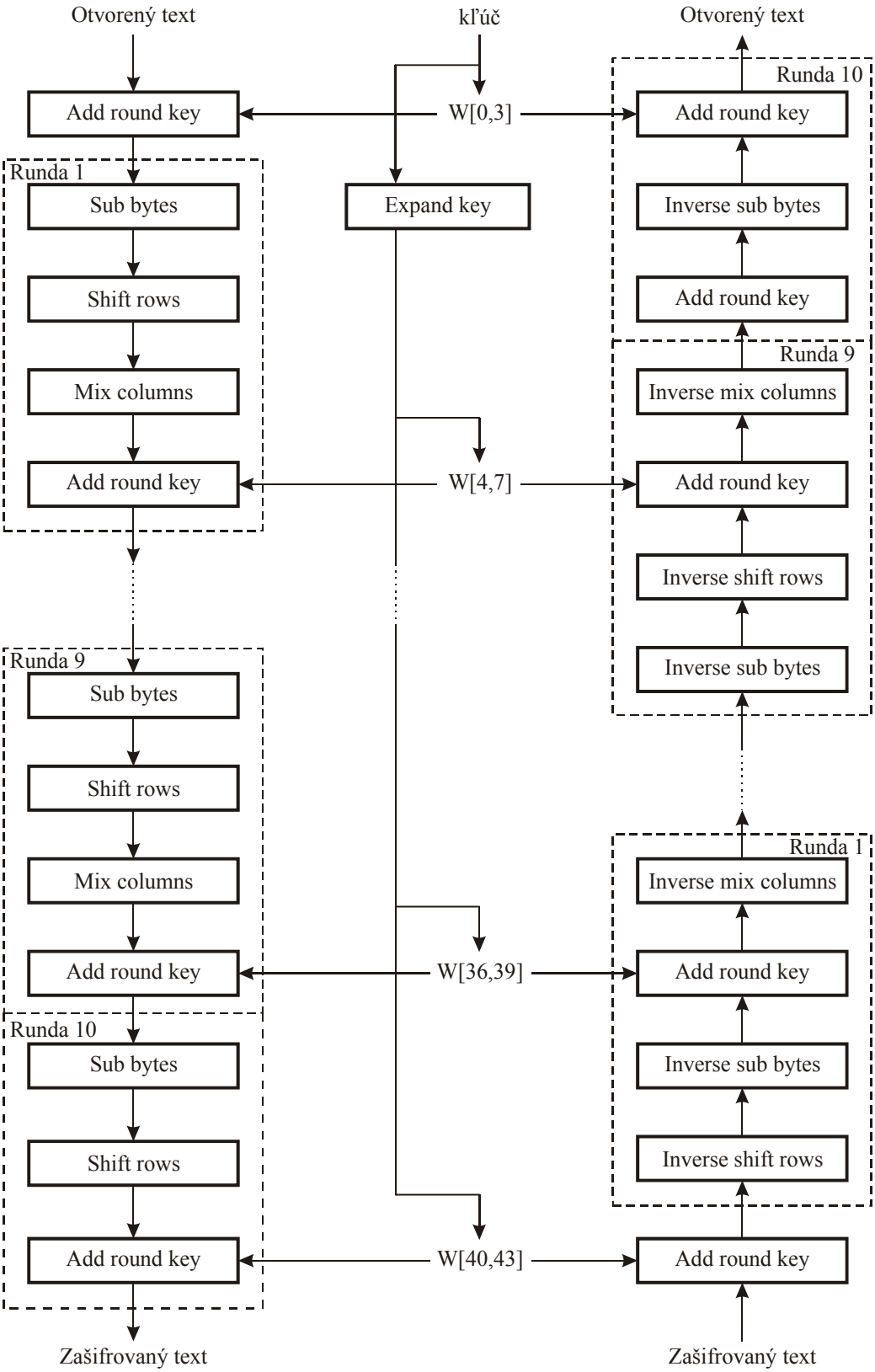
out_0	out_4	out_8	out_{12}
out_1	out_5	out_9	out_{13}
out_2	out_6	out_{10}	out_{14}
out_3	out_7	out_{11}	out_{15}

Štruktúra operácií a dát v algoritme AES

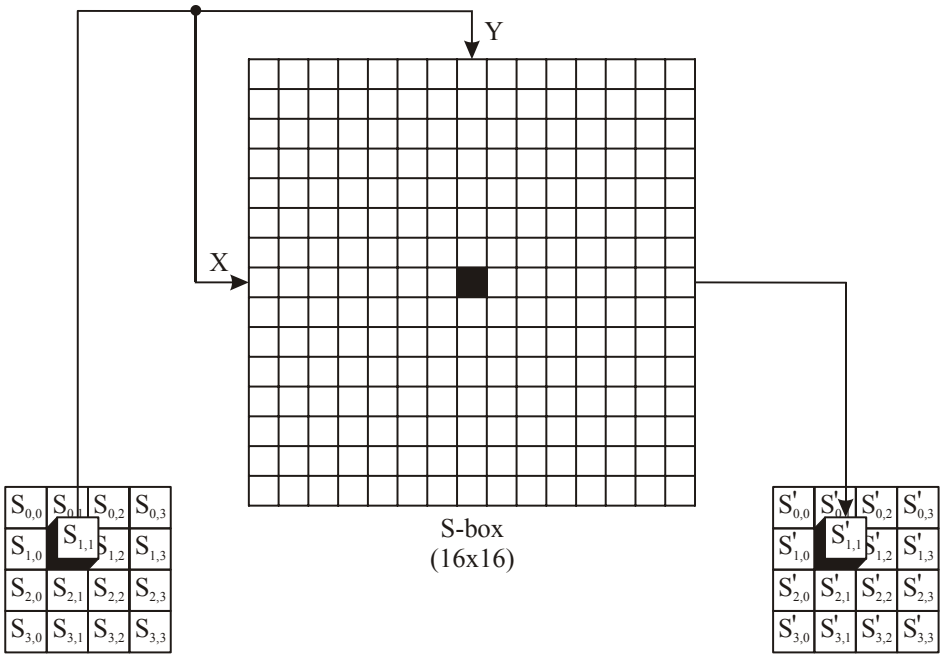
k_0	k_4	k_8	k_{12}
k_1	k_5	k_9	k_{13}
k_2	k_6	k_{10}	k_{14}
k_3	k_7	k_{11}	k_{15}

w_0	w_1	w_2	w_3

Štruktúra kľúča pre dĺžku 128 bitov



Štruktúra algoritmu šifrovania a dešifrovania v AES



Priama substitúcia bytov

$S_{i,j}$			
42	AB	48	2D
8A	7A	23	5B
56	9C	85	B1
39	CD	52	58

→

$S'_{i,j}$			
2C	62	52	D8
7E	DA	26	39
B1	DE	97	C8
12	BD	00	6A

Použitie priamej substitúcie

$S_{0,0}$	$S_{0,1}$	$S_{0,2}$	$S_{0,3}$	žiadny posun →	$S_{0,0}$	$S_{0,1}$	$S_{0,2}$	$S_{0,3}$
$S_{1,0}$	$S_{1,1}$	$S_{1,2}$	$S_{1,3}$	posun o 1 byte vľavo →	$S_{1,1}$	$S_{1,2}$	$S_{1,3}$	$S_{1,0}$
$S_{2,0}$	$S_{2,1}$	$S_{2,2}$	$S_{2,3}$	posun o 2 byty vľavo →	$S_{2,2}$	$S_{2,3}$	$S_{2,0}$	$S_{2,1}$
$S_{3,0}$	$S_{3,1}$	$S_{3,2}$	$S_{3,3}$	posun o 3 byty vľavo →	$S_{3,3}$	$S_{3,0}$	$S_{3,1}$	$S_{3,2}$

a)

48	F8	4F	95
AD	43	AE	B4
3E	AC	1A	D8
87	8D	21	FF

→

48	F8	4F	95
43	AE	B4	AD
1A	D8	3E	AC
FF	87	8D	21

b)

Shift Rows

F2	4D	97	87
4C	90	EC	6E
E7	4A	C3	46
8C	D8	95	A6

→

40	A3	4C	47
D4	70	9F	37
E4	3A	42	94
A5	A6	BC	ED

Príklad operácie Mix Columns

State

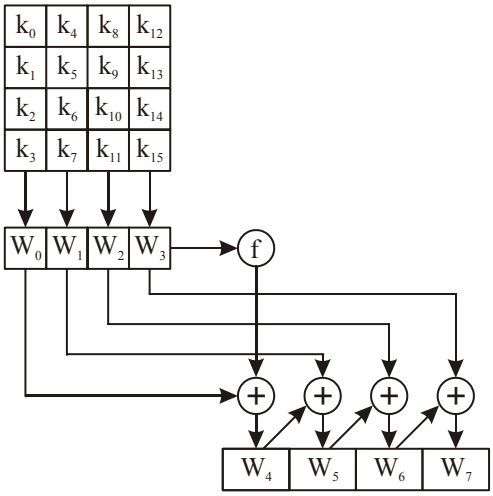
32	AB	D4	31
80	4E	B8	85
A8	5B	85	63
61	43	72	BD

⊕

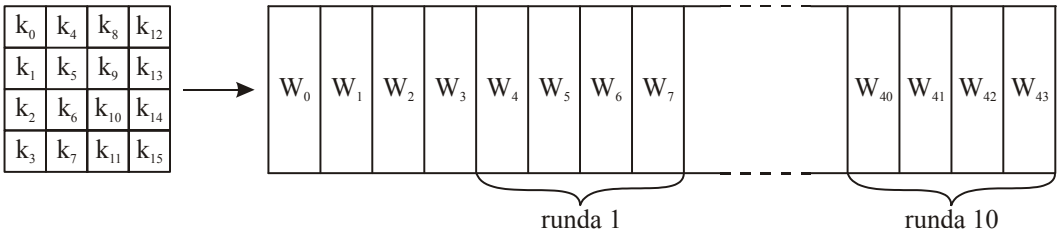
61	8B	AC	9B
6A	93	D1	5C
DC	00	3A	E4
32	32	63	BC

=

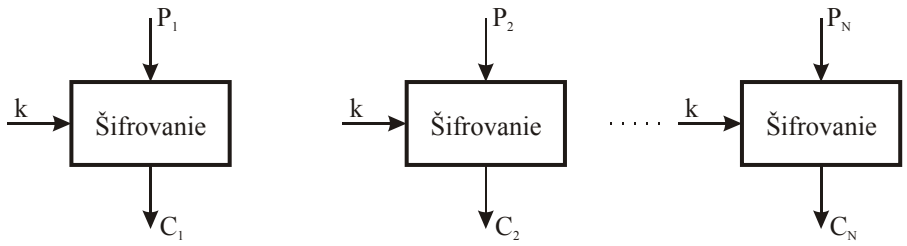
Príklad operácie Add Round Key



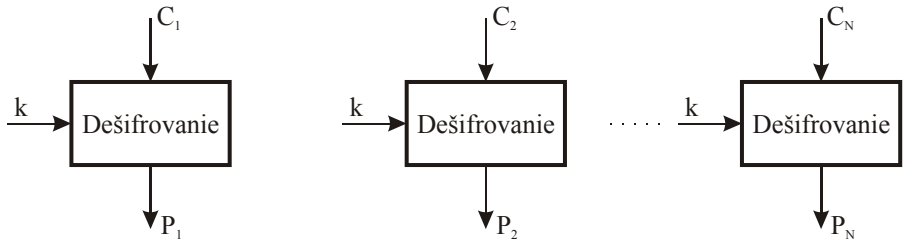
Expanzia kľúča



Expanzia kľúča pre 10 rúnd

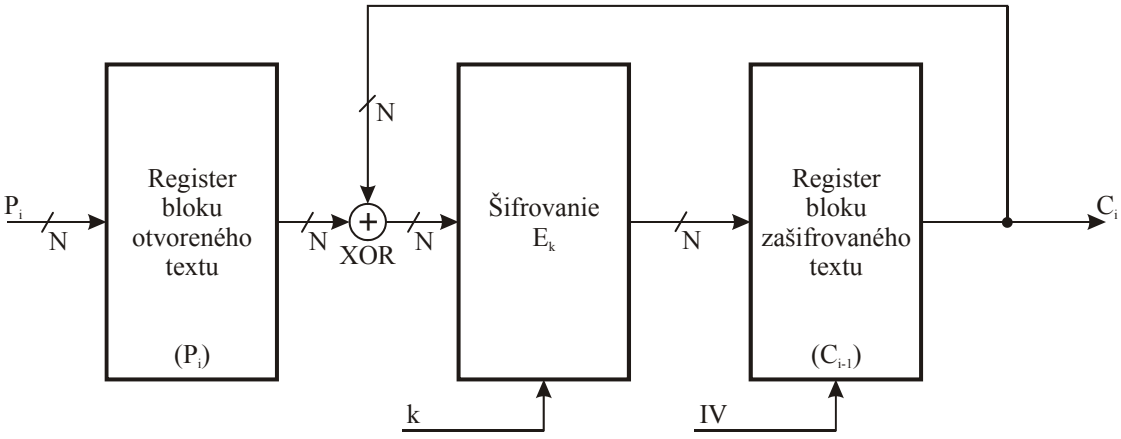


a)

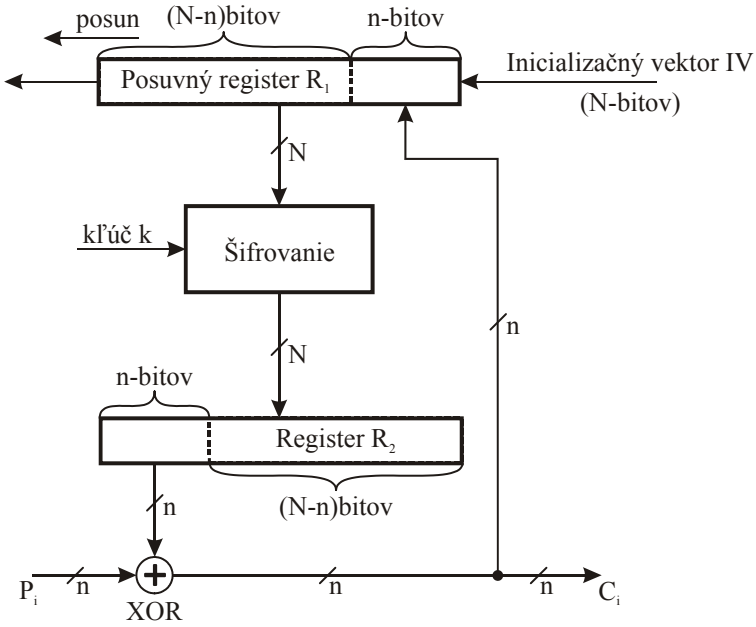


b)

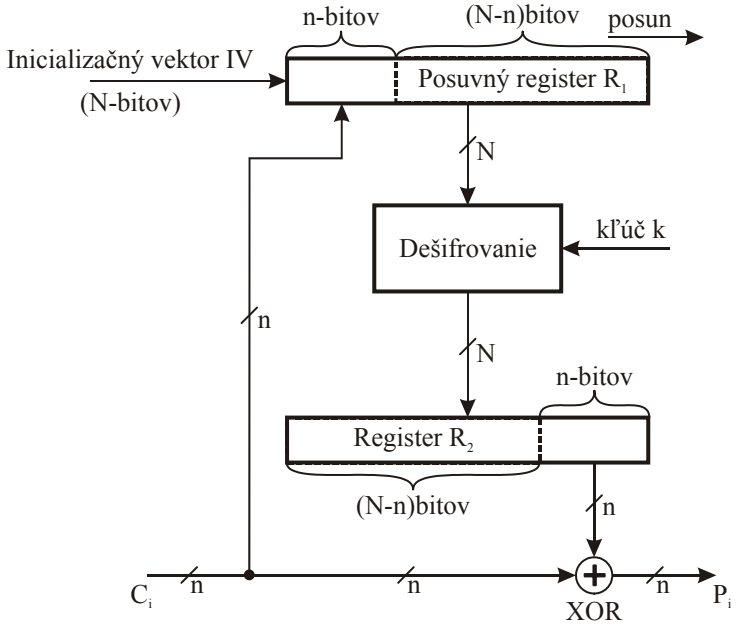
Režim ECB a – šifrovanie, b – dešifrovanie



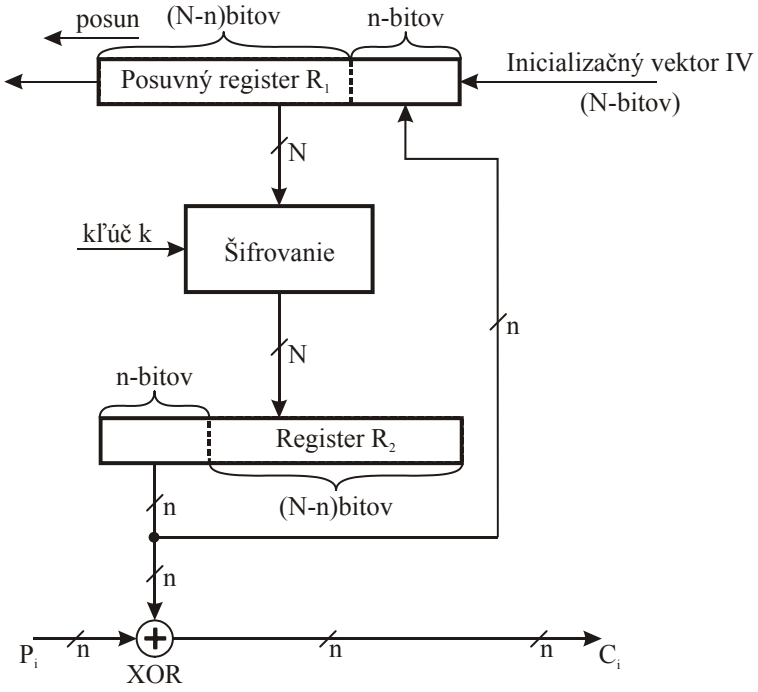
Režim CBC



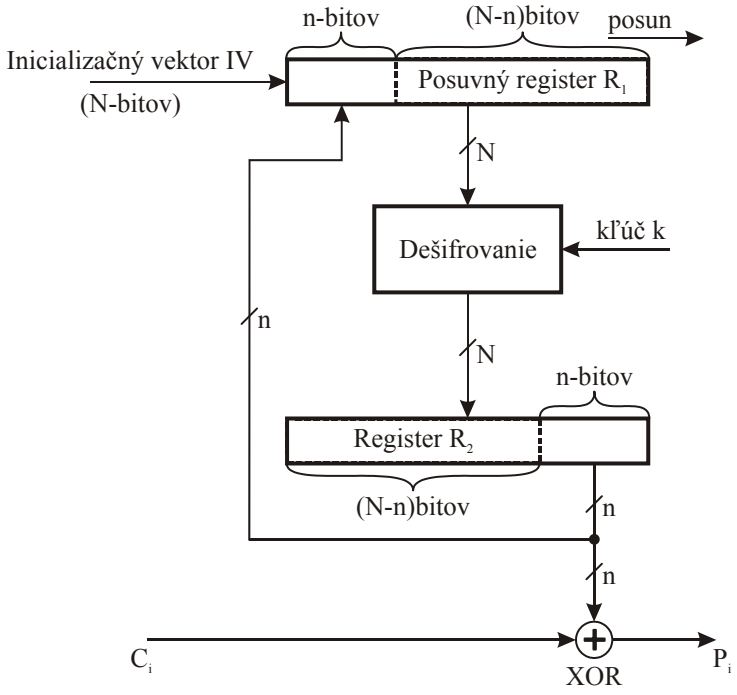
Režim CFB (šifrovanie)



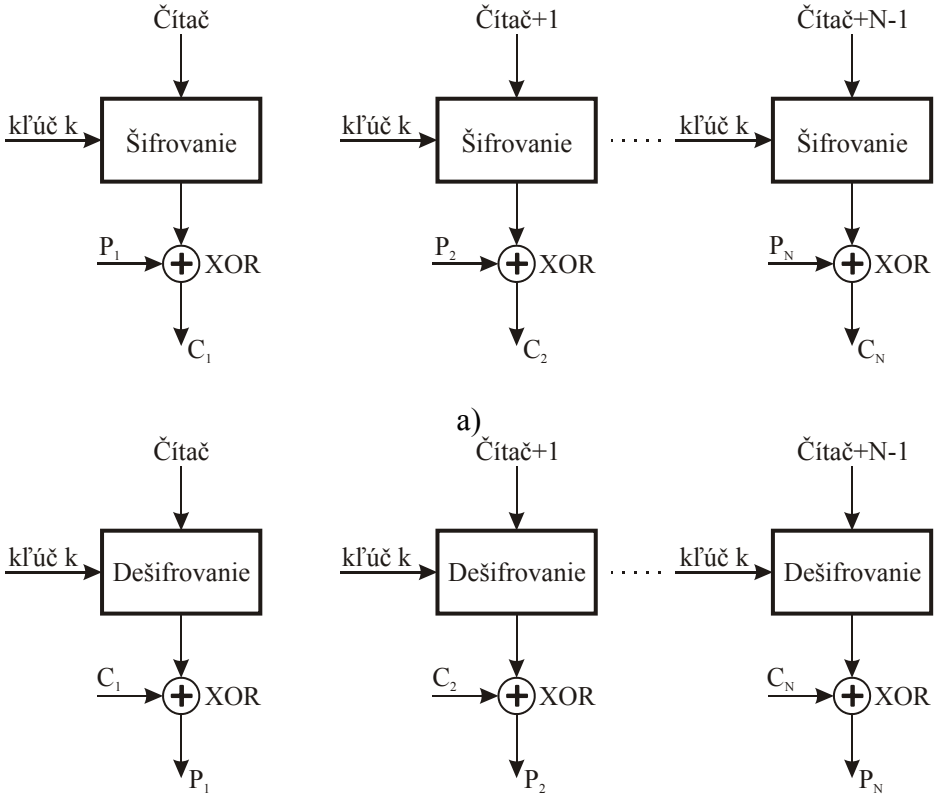
Režim CFB (dešifrovanie)



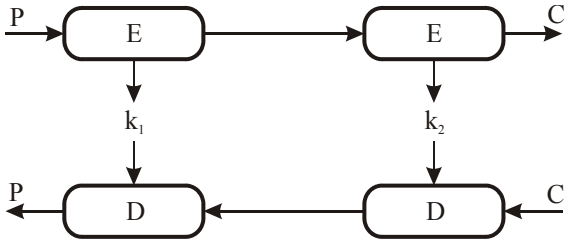
Režim OFB (šifrovanie)



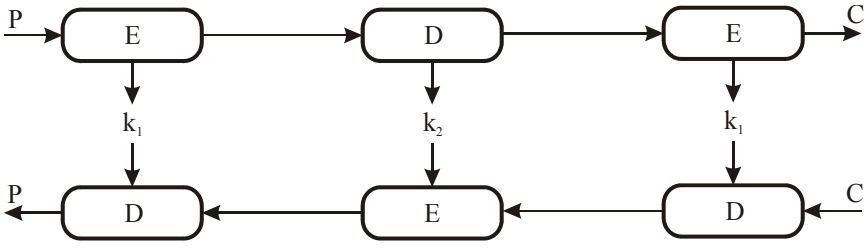
Režim OFB (dešifrovanie)



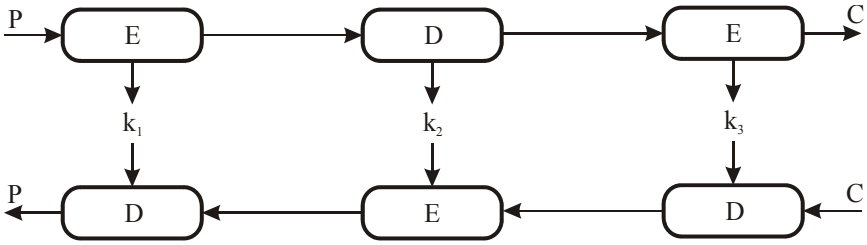
Čítačový režim a) šifrovanie, b) dešifrovanie



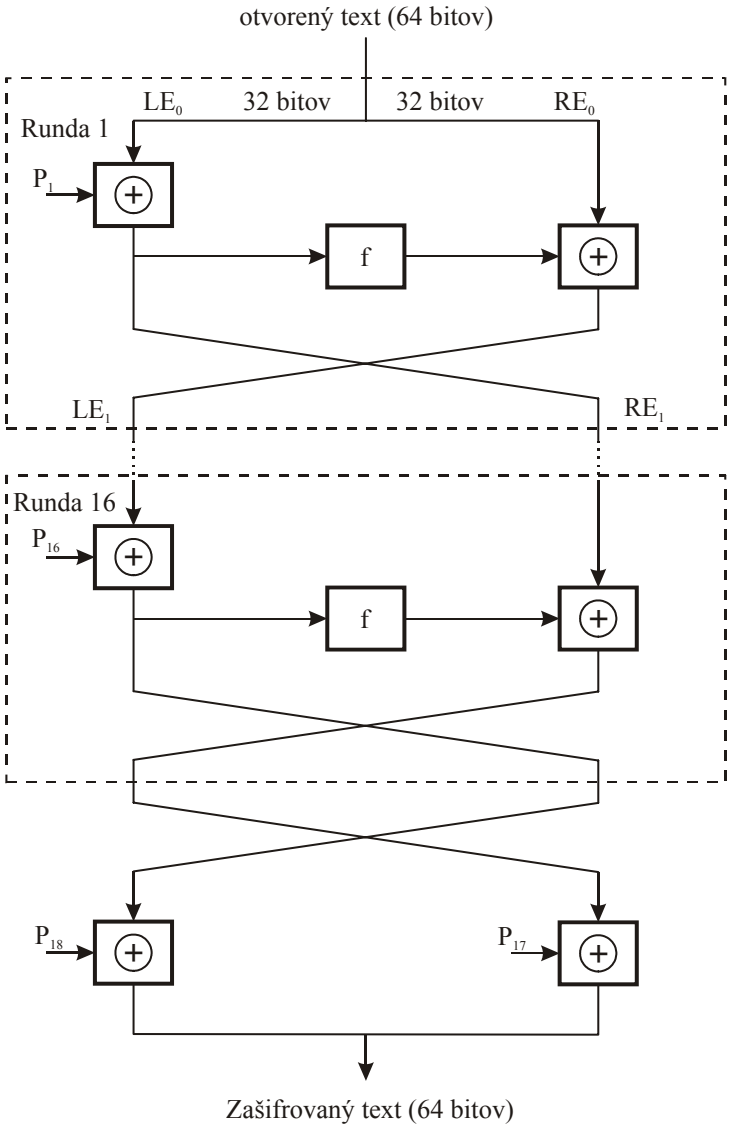
Dvojnásobný DES



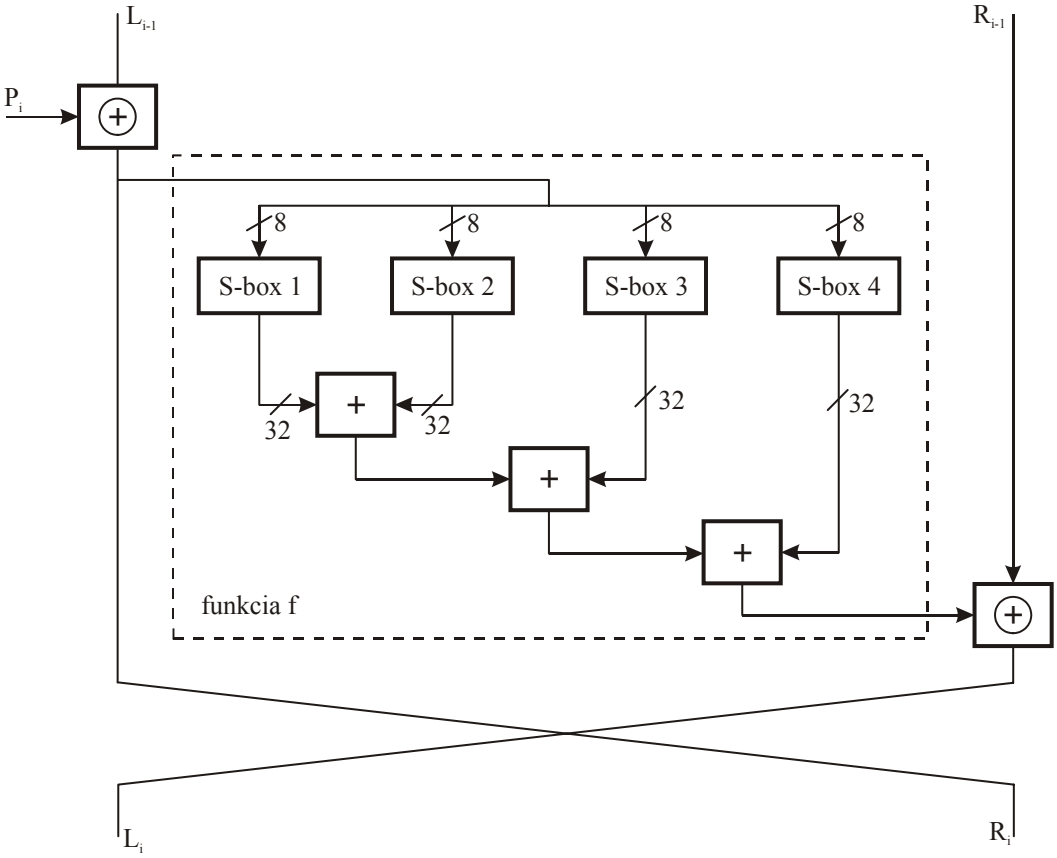
Trojnásobný DES s dvoma kľúčmi



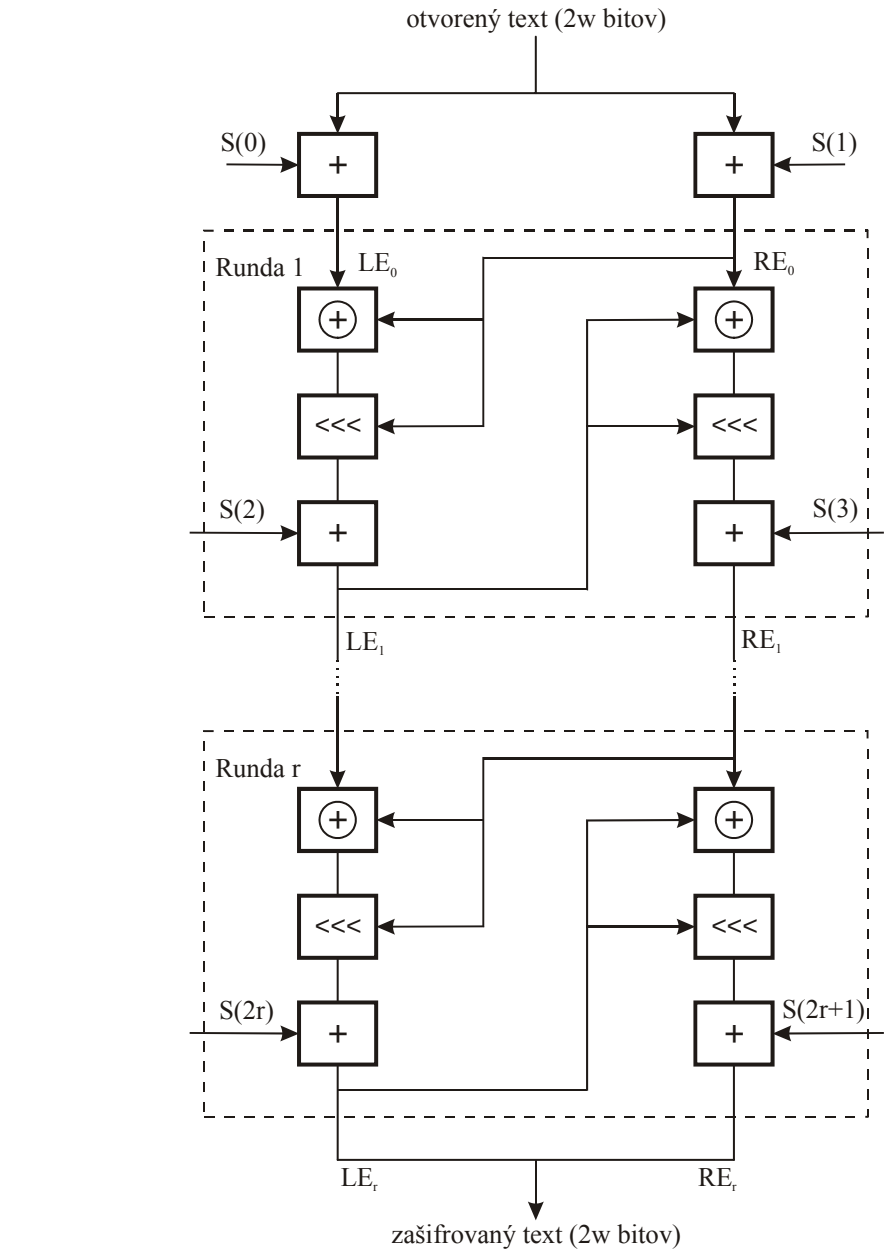
Trojnásobný DES s troma kľúčmi



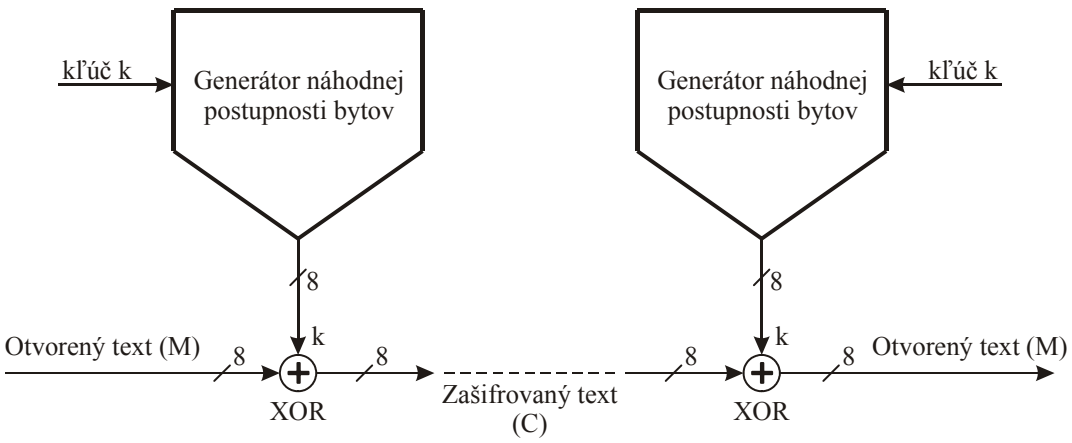
Štruktúra algoritmu Blowfish



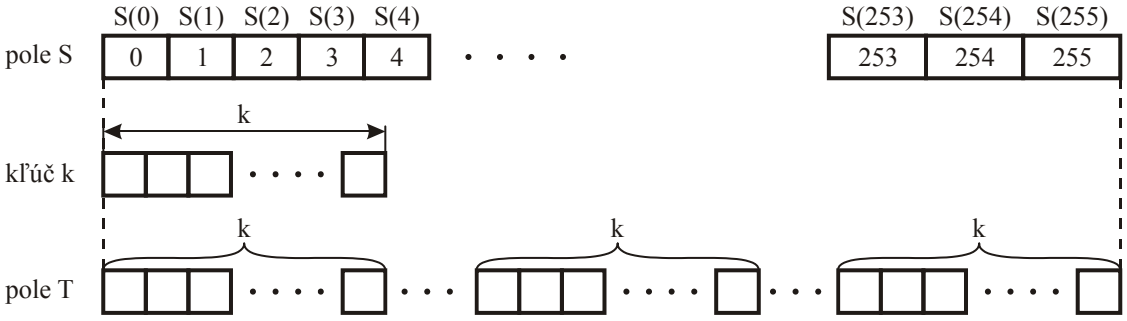
Štruktúra funkcie f



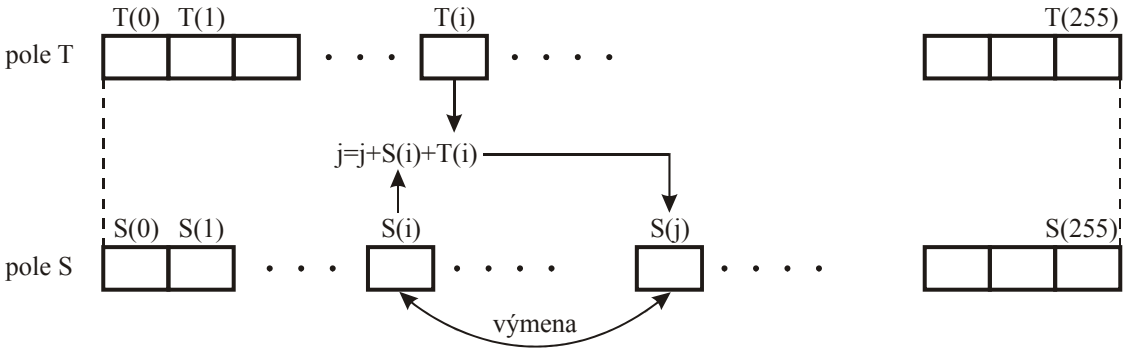
Štruktúra algoritmu šifry RC5



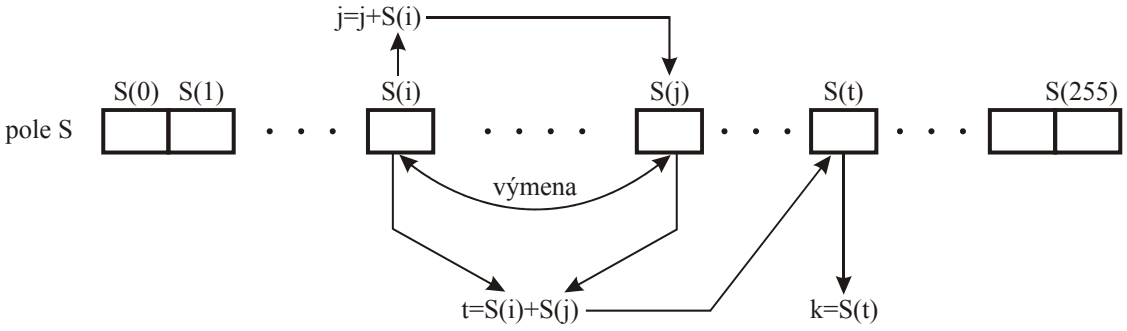
Štruktúra prúdovej šifry RC4



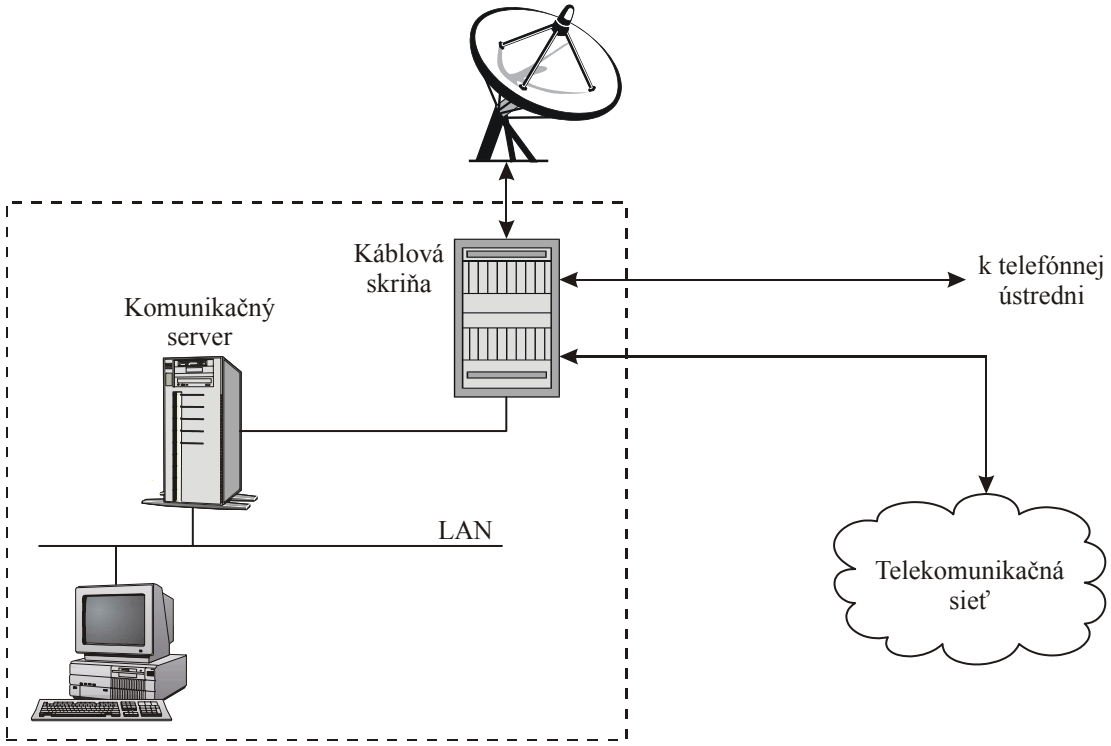
Počiatočná inicializácia



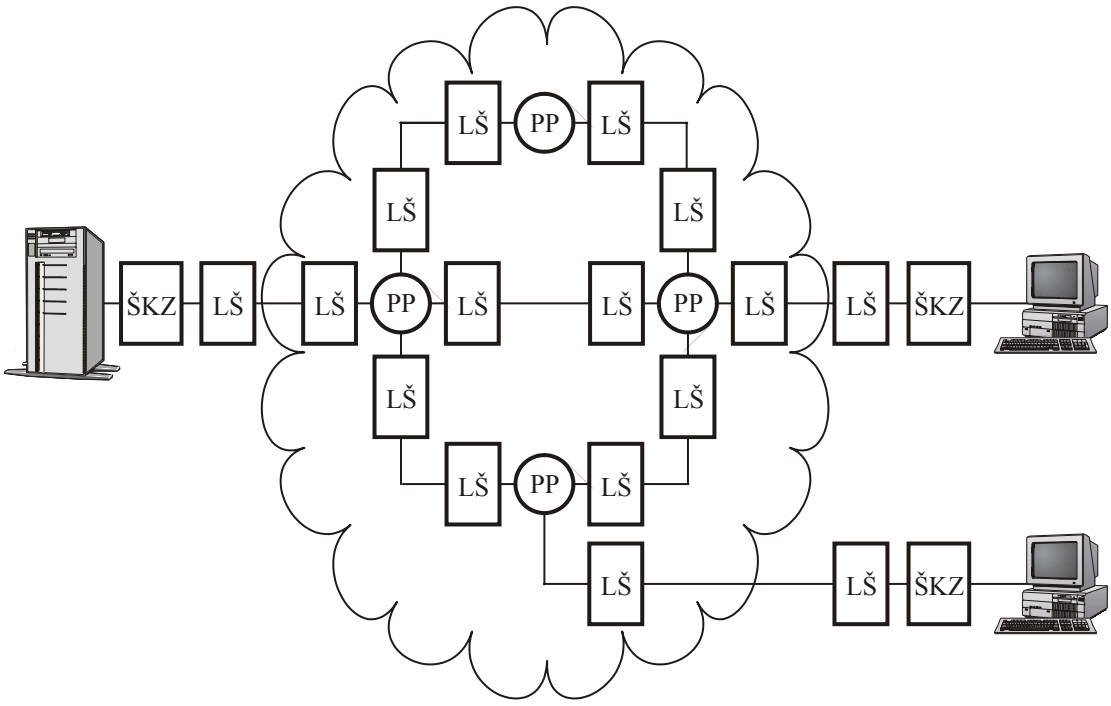
Počiatočná permutácia



Generovanie náhodnej postupnosti bytov k

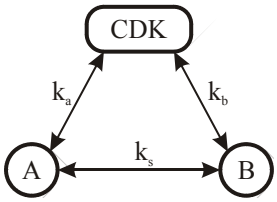


Firemný informačný systém



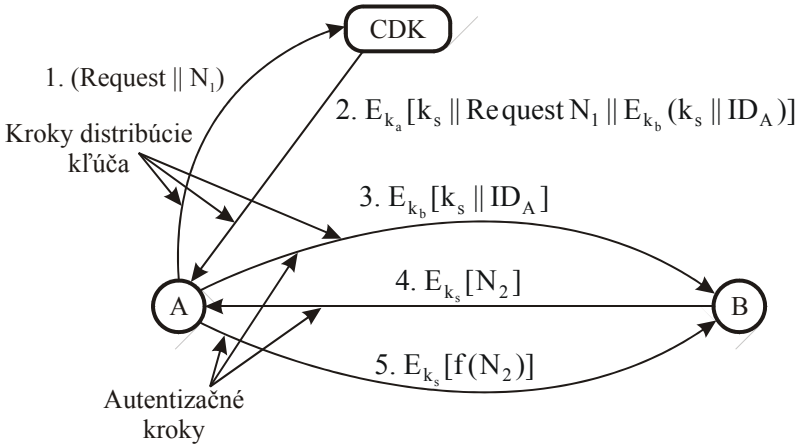
ŠKZ – šifrovanie v koncovom zariadení
LŠ – linkové šifrovanie
PP – prepínač paketov

Kombinácia linkového šifrovania a šifrovania v koncových zariadeniach v paketových sieťach



k_a – kľúč na komunikáciu A s CDK
k_b – kľúč na komunikáciu B s CDK
k_s – kľúč relácie A s B (B s A)

Hierarchia kľúčov



Distribúcia kľúčov