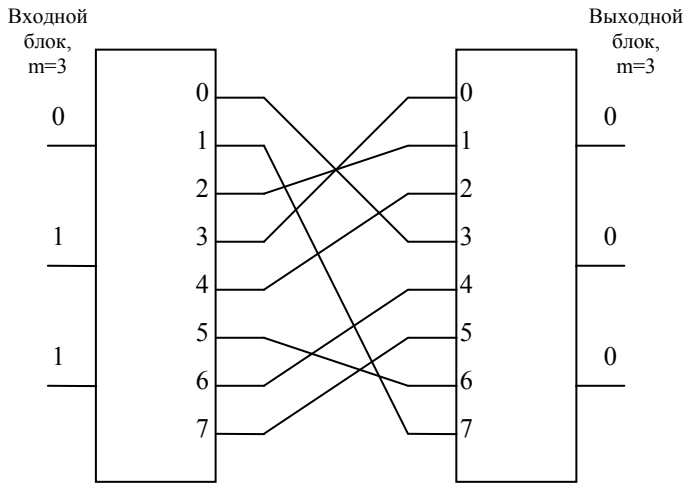
Основы блочного шифрования. S- и P-блоки, конструкция (сеть) Фейстеля.

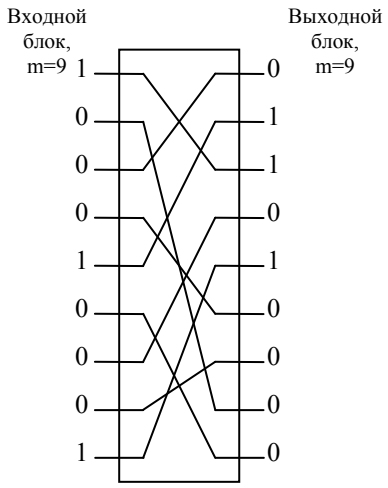
S-блок (блок подстановки)



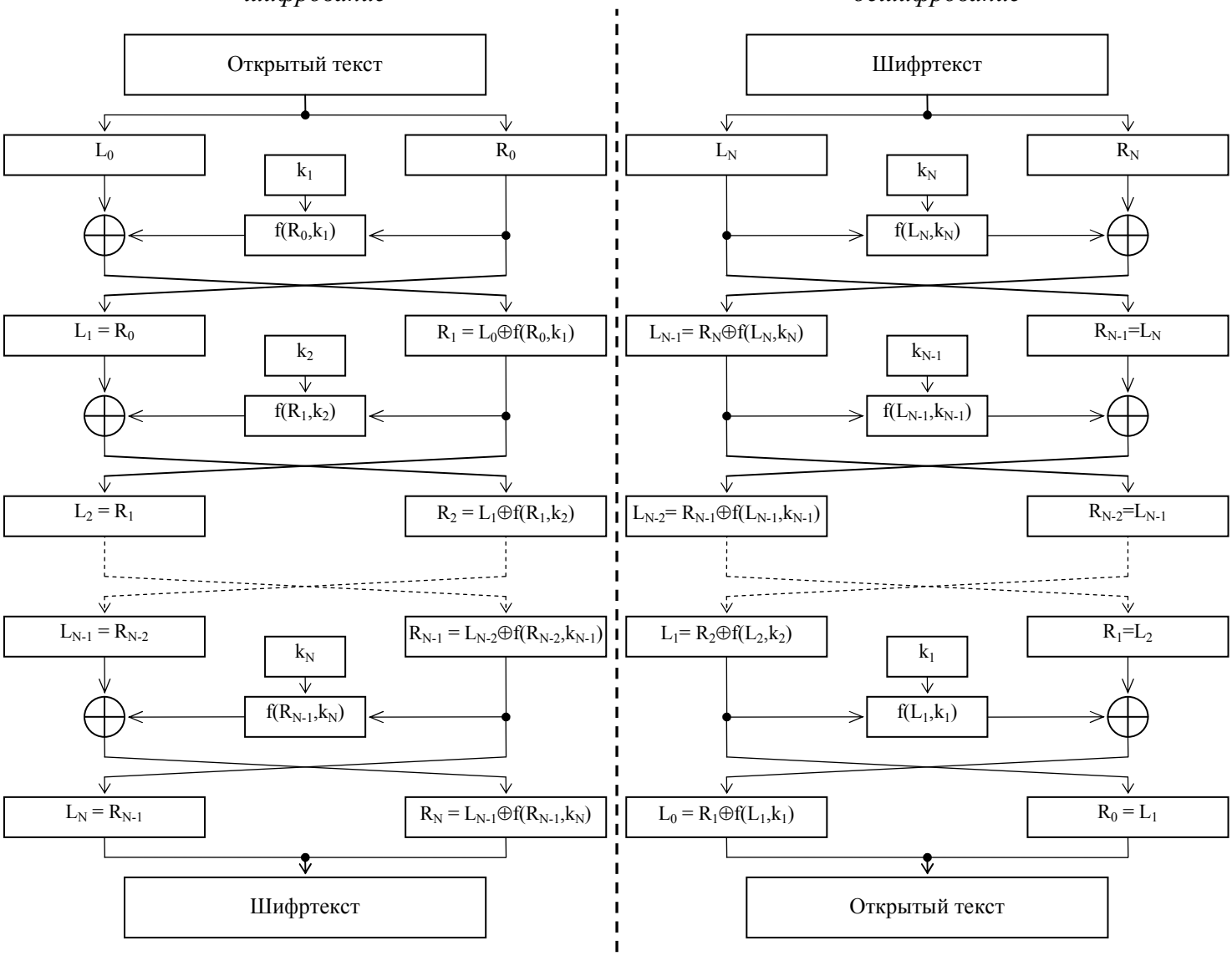
вход	000 (0)	001 (1)	010 (2)	011 (3)	100 (4)	101 (5)	110 (6)	111 (7)
выход	011 (3)	111 (7)	001 (1)	000 (0)	010 (2)	110 (6)	100 (4)	101 (5)

Таблица подстановки

P-блок (блок перестановки)



Обобщенная схема конструкции (сети) Фейстеля



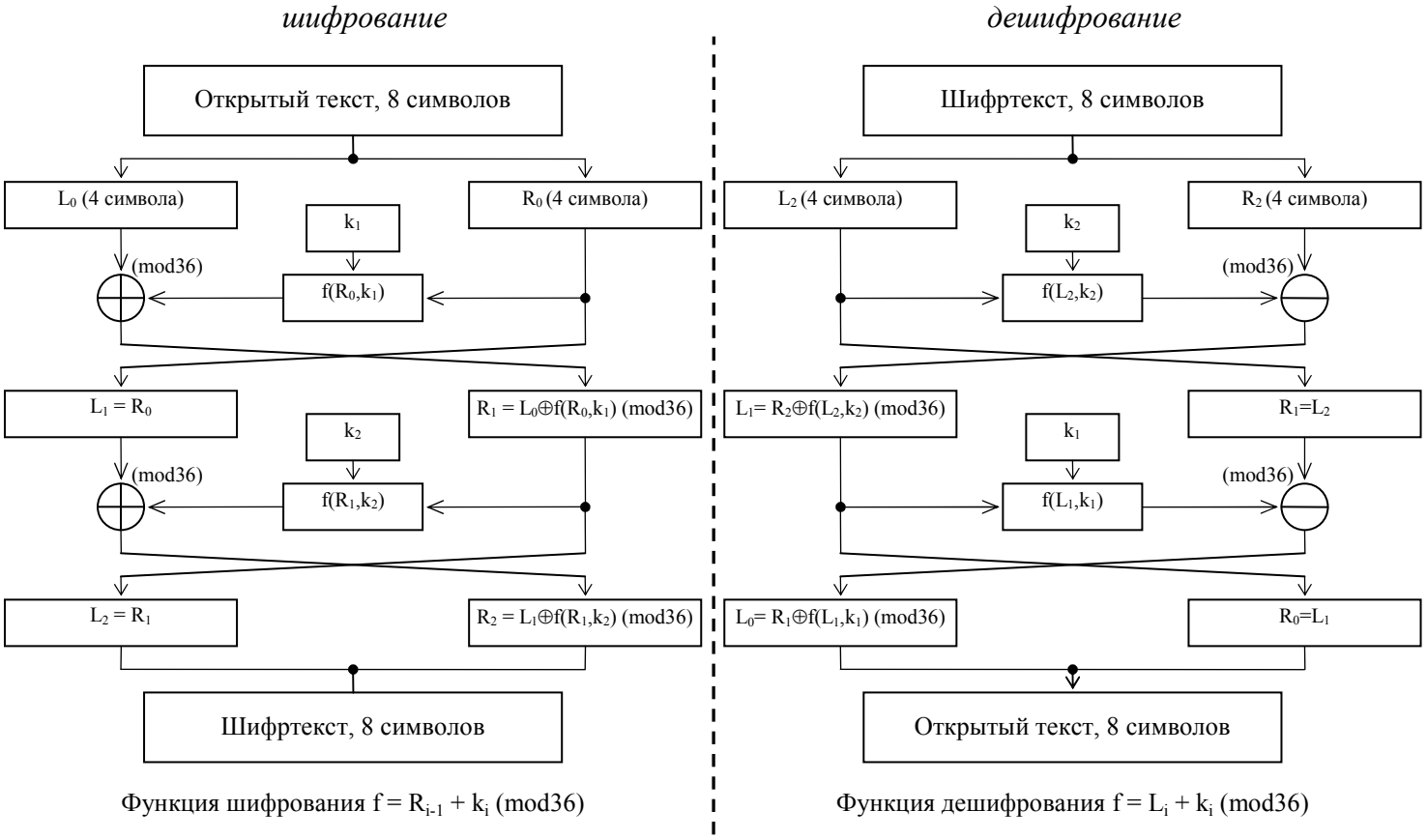
Пример блочного шифра на основе двухраундовой сети Фейстеля

Открытый текст, разбитый на блоки по 8 символов

к	о	л	о	к	о	л	_	о	к	о	л	о	_	к	о	л	о	к	о	л	ь	н	и
блок 1								блок 2								блок 3							

Начальный пользовательский ключ шифрования: КЛЮЧ

Схемы шифрования и дешифрования



Функция шифрования $f = R_{i-1} + k_i \pmod{36}$

Функция дешифрования $f = L_i + k_i \pmod{36}$

*Первый блок открытого текста: колокол_*

Шифрование

1 раунд.

L_0 = коло $\quad R_0$ = кол_

k_1 = ключ

$f(R_0,k_1) = R_0 + k_1 \pmod{36}$

R_0	к	о	л	_
k_1	к	л	ю	ч
	11	15	12	35
	11	12	31	24
	22	27	07	23
$f(R_0,k_1)$	х	ъ	ж	ц

$L_1 = R_0$ = кол_

$R_1 = L_0 + f(R_0,k_1) \pmod{36}$

L_0	к	о	л	о
$f(R_0,k_1)$	х	ъ	ж	ц
	11	15	12	15
	22	27	07	23
	33	06	19	02
R_1	.	ё	т	в

R_1 = .ётв

2 раунд.

L_1 = кол_ $\quad R_1$ = .ётв

k_2 = лючк

$f(R_1,k_2) = R_1 + k_2 \pmod{36}$

R_1	.	ё	т	в
k_2	л	ю	ч	к
	33	06	19	02
	12	31	24	11
	09	01	07	13
$f(R_1,k_2)$	и	б	ж	м

$L_2 = R_1$ = .ётв

$R_2 = L_1 + f(R_1,k_2) \pmod{36}$

L_1	к	о	л	_
$f(R_1,k_2)$	и	б	ж	м
	11	15	12	35
	09	01	07	13
	20	16	19	12
R_2	у	п	т	л

R_2 = уптл

Первый блок шифртекста: .ётвуптл

Дешифрование

1 раунд.

L_2 = .ётв R_2 = уптл

k_2 = лючк

$f(L_2,k_2) = L_2 + k_2$ (mod36) $L_1 = R_2 - f(L_2,k_2)$ (mod36)

L_2	.	ё	т	в
k_2	л	ю	ч	к
	33	06	19	02
	12	31	24	11
	09	01	07	13
$f(L_2,k_2)$	и	б	ж	м

R_2	у	п	т	л
$f(L_2,k_2)$	и	б	ж	м
	20	16	19	12
	09	01	07	13
	11	15	12	35
L_1	к	о	л	_

L_1 = кол_ $R_1 = L_2$ = .ётв

2 раунд.

L_1 = кол_ R_1 = .ётв

k_1 = ключ

$f(L_1,k_1) = L_1 + k_1$ (mod36) $L_0 = R_1 - f(L_1,k_1)$ (mod36)

L_1	к	о	л	_
k_1	к	л	ю	ч
	11	15	12	35
	11	12	31	24
	22	27	07	23
$f(L_1,k_1)$	х	ъ	ж	ц

R_1	.	ё	т	в
$f(L_1,k_1)$	х	ъ	ж	ц
	33	06	19	02
	22	27	07	23
	11	15	12	15
L_0	к	о	л	о

L_0 = коло $R_0 = L_1$ = кол_

Первый блок восстановленного открытого текста: колокол_

Второй блок открытого текста: около_ко

Шифрование

1 раунд.

L_0 = окол R_0 = о_ко

k_1 = ключ

$f(R_0,k_1) = R_0 + k_1$ (mod36) $R_1 = L_0 + f(R_0,k_1)$ (mod36)

R_0	о	_	к	о
k_1	к	л	ю	ч
	15	35	11	15
	11	12	31	24
	26	11	06	03
$f(R_0,k_1)$	щ	к	ё	г

L_0	о	к	о	л
$f(R_0,k_1)$	щ	к	ё	г
	15	11	15	12
	26	11	06	03
	05	22	21	15
R_1	е	х	ф	о

$L_1 = R_0$ = о_ко R_1 = ехфо

2 раунд.

L_1 = о_ко R_1 = ехфо

k_2 = лючк

$f(R_1,k_2) = R_1 + k_2$ (mod36) $R_2 = L_1 + f(R_1,k_2)$ (mod36)

R_1	е	х	ф	о
k_2	л	ю	ч	к
	05	22	21	15
	12	31	24	11
	17	17	09	26
$f(R_1,k_2)$	р	р	и	щ

L_1	о	_	к	о
$f(R_1,k_2)$	р	р	и	щ
	15	35	11	15
	17	17	09	26
	32	16	20	05
R_2	я	п	у	е

$L_2 = R_1$ = ехфо R_2 = япуе

Второй блок шифртекста: ехфояпуе

Дешифрование

1 раунд.

L_2 = ехфо R_2 = япуе

k_2 = лючк

$f(L_2,k_2) = L_2 + k_2$ (mod36) $L_1 = R_2 - f(L_2,k_2)$ (mod36)

L_2	е	х	ф	о
k_2	л	ю	ч	к
	05	22	21	15
	12	31	24	11
	17	17	09	26
$f(L_2,k_2)$	р	р	и	щ

R_2	я	п	у	е
$f(L_2,k_2)$	р	р	и	щ
	32	16	20	05
	17	17	09	26
	15	35	11	15
L_1	о	_	к	о

L_1 = о_ко $R_1 = L_2$ = ехфо

2 раунд.

L_1 = о_ко R_1 = ехфо

k_1 = ключ

$f(L_1,k_1) = L_1 + k_1 \pmod{36}$

L_1	о	_	к	о
k_1	к	л	ю	ч
	15	35	11	15
	11	12	31	24
	26	11	06	03
$f(L_1,k_1)$	щ	к	ё	г

$L_0 = R_1 - f(L_1,k_1) \pmod{36}$

R_1	е	х	ф	о
$f(L_1,k_1)$	щ	к	ё	г
	05	22	21	15
	26	11	06	03
	15	11	15	12
L_0	о	к	о	л

L_0 = окол $R_0 = L_1$ = о_ко

Второй блок восстановленного открытого текста: колокол_

Третий блок открытого текста: локольни

Шифрование

1 раунд.

L_0 = локо R_0 = льни

k_1 = ключ

$f(R_0,k_1) = R_0 + k_1 \pmod{36}$

R_0	л	ь	н	и
k_1	к	л	ю	ч
	12	29	14	09
	11	12	31	24
	23	05	09	33
$f(R_0,k_1)$	ц	е	и	.

$R_1 = L_0 + f(R_0,k_1) \pmod{36}$

L_0	л	о	к	о
$f(R_0,k_1)$	ц	е	и	.
	12	15	11	15
	23	05	09	33
	35	20	20	12
R_1	_	у	у	л

$L_1 = R_0$ = льни R_1 = _уул

2 раунд.

L_1 = льни R_1 = _уул

k_2 = лючк

$f(R_1,k_2) = R_1 + k_2 \pmod{36}$

R_1	_	у	у	л
k_2	л	ю	ч	к
	35	20	20	12
	12	31	24	11
	11	15	08	23
$f(R_1,k_2)$	к	о	з	ц

$R_2 = L_1 + f(R_1,k_2) \pmod{36}$

L_1	л	ь	н	и
$f(R_1,k_2)$	к	о	з	ц
	12	29	14	09
	11	15	08	23
	23	08	22	32
R_2	ц	з	х	я

$L_2 = R_1$ = _уул R_2 = цзхя

Третий блок шифртекста: _уулцзхя

Дешифрование

1 раунд.

L_2 = _уул R_2 = цзхя

k_2 = лючк

$f(L_2,k_2) = L_2 + k_2 \pmod{36}$

L_2	_	у	у	л
k_2	л	ю	ч	к
	35	20	20	12
	12	31	24	11
	11	15	08	23
$f(L_2,k_2)$	к	о	з	ц

$L_1 = R_2 - f(L_2,k_2) \pmod{36}$

R_2	ц	з	х	я
$f(L_2,k_2)$	к	о	з	ц
	23	08	22	32
	11	15	08	23
	12	29	14	09
L_1	л	ь	н	и

L_1 = льни $R_1 = L_2$ = _уул

2 раунд.

L_1 = льни R_1 = _уул

k_1 = ключ

$f(L_1,k_1) = L_1 + k_1 \pmod{36}$

L_1	л	ь	н	и
k_1	к	л	ю	ч
	12	29	14	09
	11	12	31	24
	23	05	09	33
$f(L_1,k_1)$	ц	е	и	.

$L_0 = R_1 - f(L_1,k_1) \pmod{36}$

R_1	_	у	у	л
$f(L_1,k_1)$	ц	е	и	.
	35	20	20	12
	23	05	09	33
	12	15	11	15
L_0	л	о	к	о

L_0 = локо $R_0 = L_1$ = льни

Третий блок восстановленного открытого текста: локольни