Комбинированные шифры

Комбинированные (композиционные) шифры

- К = (5, 436215)

1 *этап* **(***замена***):** $\overset{k1=5}{\longrightarrow}$ *СИГНАЛ* → *ЦОИТЕР*

2 *этап* **(***перестановка***):** $\overset{k2=436215}{\longrightarrow}$ *ЦОИТЕР* → *ТИРОЦЕ*

Можно записать также и так:

$\overset{K=(5,436215)}{\longrightarrow}$

СИГНАЛ → *ТИРОЦЕ*

Использование комбинированного *шифра* дважды с одним и тем же ключом:

Цикл шифрования **1**

1 *этап* (*замена*): СИГНАЛ $\xrightarrow{k1=5}$ ЦОИТЕР

2 *этап* (*перестановка*): ЦОИТЕР $\xrightarrow{k2=436215}$ ТИРОЦЕ

Цикл шифрования **2**

1 *этап* (*замена*): ТИРОЦЕ $\xrightarrow{k1=5}$ ЧОХУЫЛ

2 *этап* (*перестановка*): ЧОХУЫЛ $\xrightarrow{k2=436215}$ УХЛОЧЫ

Операция побитового сложения по модулю 2

Номер разряда:	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
Операнд 1:	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0
Операнд 2:	0	1	1	1	0	0	1	1	0	0	1	1	0	0	1	1
Сумма по мод. 2:	1	1	0	1	1	0	0	1	1	0	0	1	1	0	0	1

Операция побитового сложения по модулю 2^16 или 2^32

Номер разряда:		15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
Операнд 1:		1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0
Операнд 2:		0	1	1	1	0	0	1	1	0	0	1	1	0	0	1	1
Сумма по мод.2^{16}:	(1)	0	0	0	1	1	1	0	1	1	1	0	1	1	1	0	1

Циклический сдвиг

Циклический сдвиг

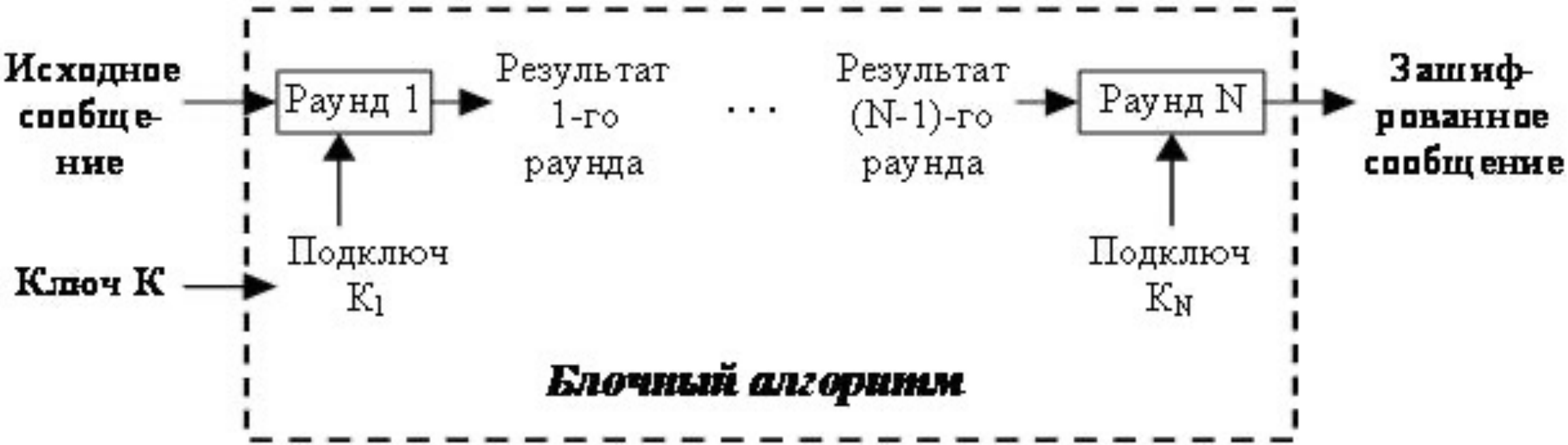
Табличная подстановка

Вход	Выход
000	011
001	101
010	000
011	111
100	010
101	110
110	001
111	100

0->3, 1->5, 2->0, 3->7, 4->2, 5->6, 6->1, 7->4

3, 5, 0, 7, 2, 6, 1, 4.

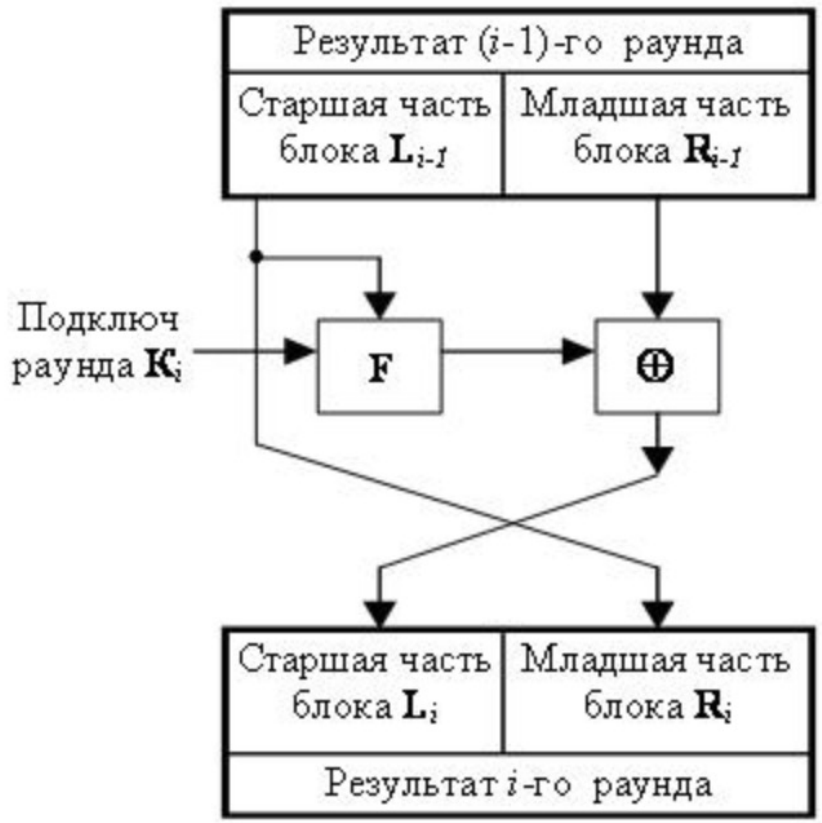
Структура блочного алгоритма симметричного шифрования



Блочные алгоритмы шифрования

- Блочные *алгоритмы шифрования* применяются к двоичным данным. В общем случае процедура *блочного шифрования* преобразовывает n-битный блок открытого текста в k-битный блок зашифрованного текста. Число блоков длины n равно 2^n. Для того чтобы преобразование было обратимым, каждый из таких блоков должен преобразовываться в свой уникальный блок зашифрованного текста. *Длина* блока всегда выбирается равной степени двойки, например, 64, 128, 256 *бит*.

Сеть Фейштеля



Ключевые термины

- **Комбинированный (композиционный) шифр** – криптографическое *преобразование данных*, получаемое в результате комбинации нескольких подряд примененных простых шифров.
- **Ключ** – *информация*, необходимая для шифрования и расшифрования сообщений.
- **Шифр** – совокупность заранее оговоренных способов преобразования исходного секретного сообщения с целью его защиты.
- **Шифрование с закрытым ключом (симметричное шифрование)** – методы обратимого преобразования данных, в которых используется один и тот же *ключ*, который обе стороны информационного обмена должны хранить в секрете от противника. Все известные из истории шифры, например, *шифр* Цезаря – это шифры с закрытым ключом.