Симметричные шифры

Типы симметричных шифров

Блочные

- Шифруется блок данных
- Типичный размер блока - 64 или 128 бит

Потоковые

- Генерируется поток псевдослучайных данных, зависящих от ключа
- Выход - поток бит (или байт), называемый *гаммой* - складывается по модулю с потоком данных

Типы симметричных шифров

Подстановки

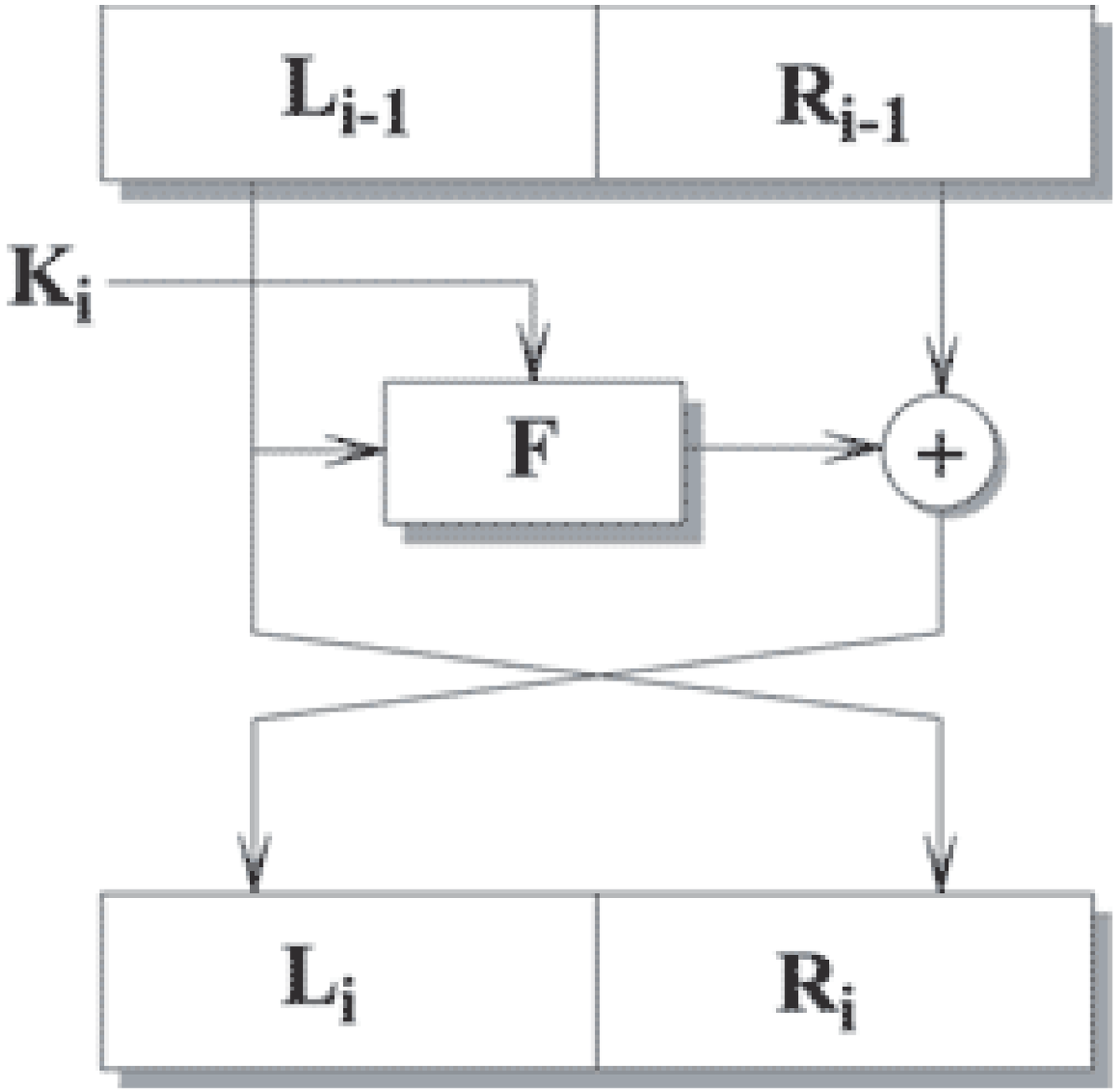
- Шифр Цезаря
- Шифр простой замены
- Шифр Виженера

Перестановки

- Простая перестановка
- Перестановка по ключу

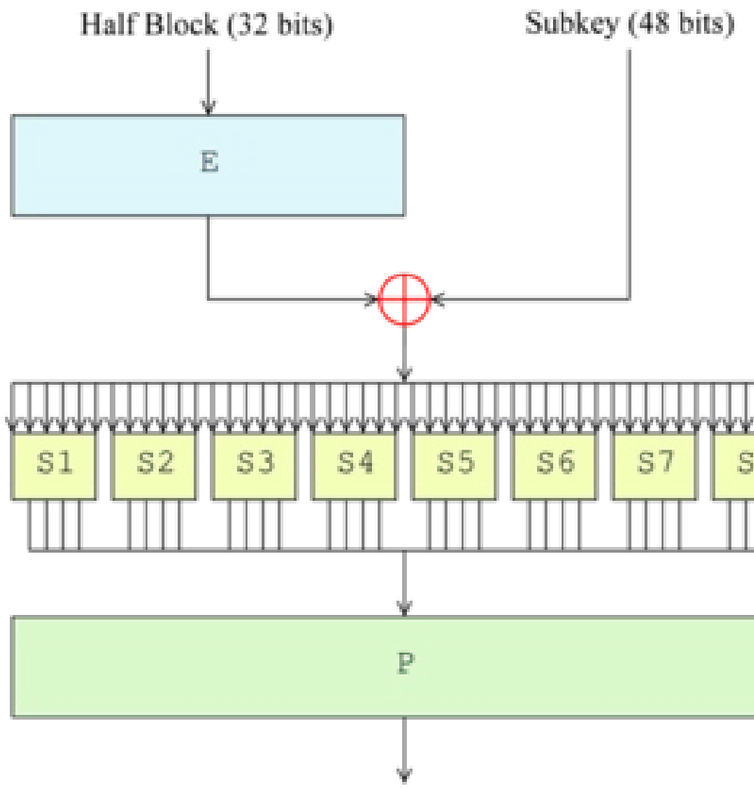
Шифр DES

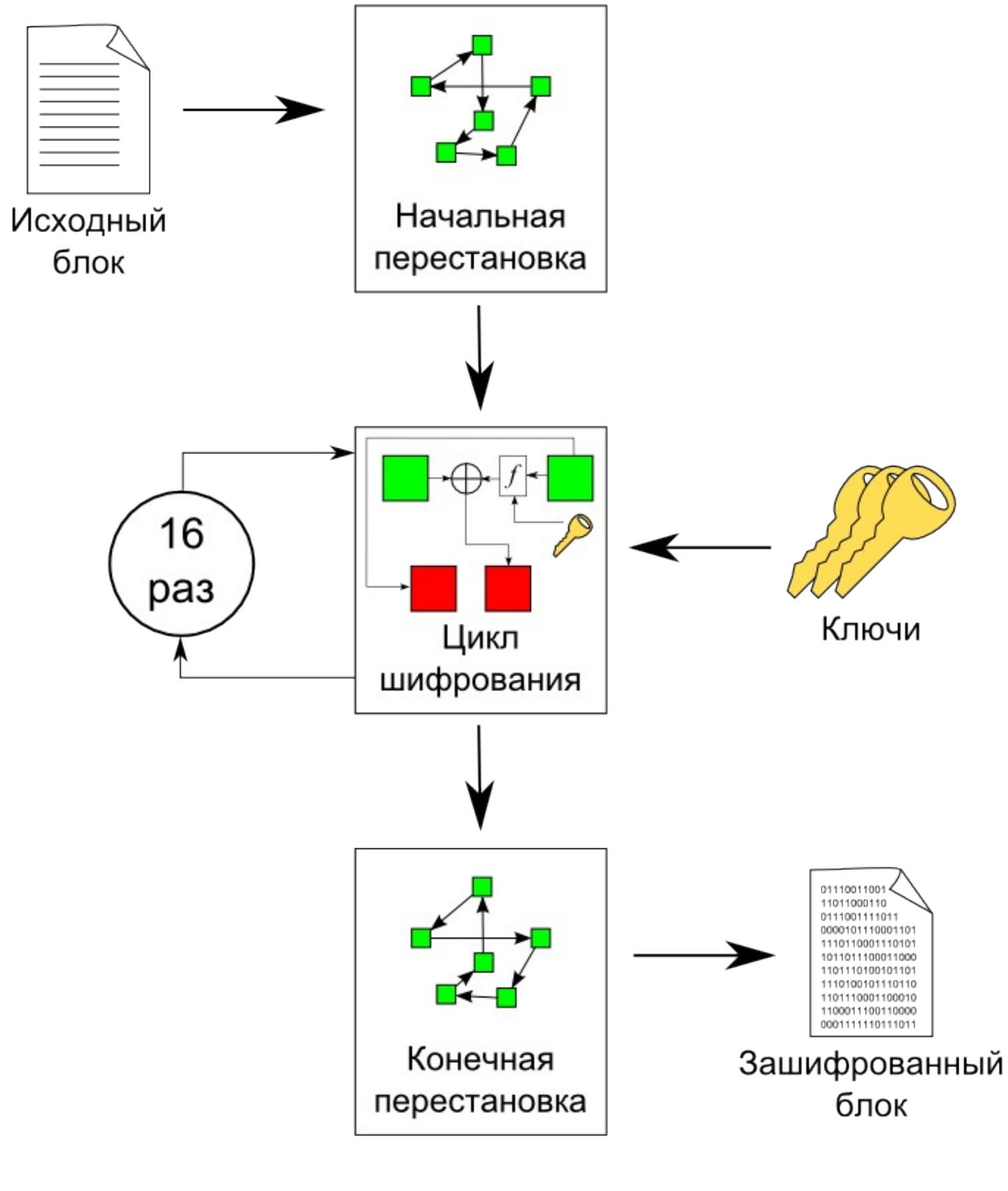
Сеть Фейстеля



DES

- Сеть Фейстеля
- Размер блока - 64 бита
- Размер ключа - 56 бит
- 16 раундов

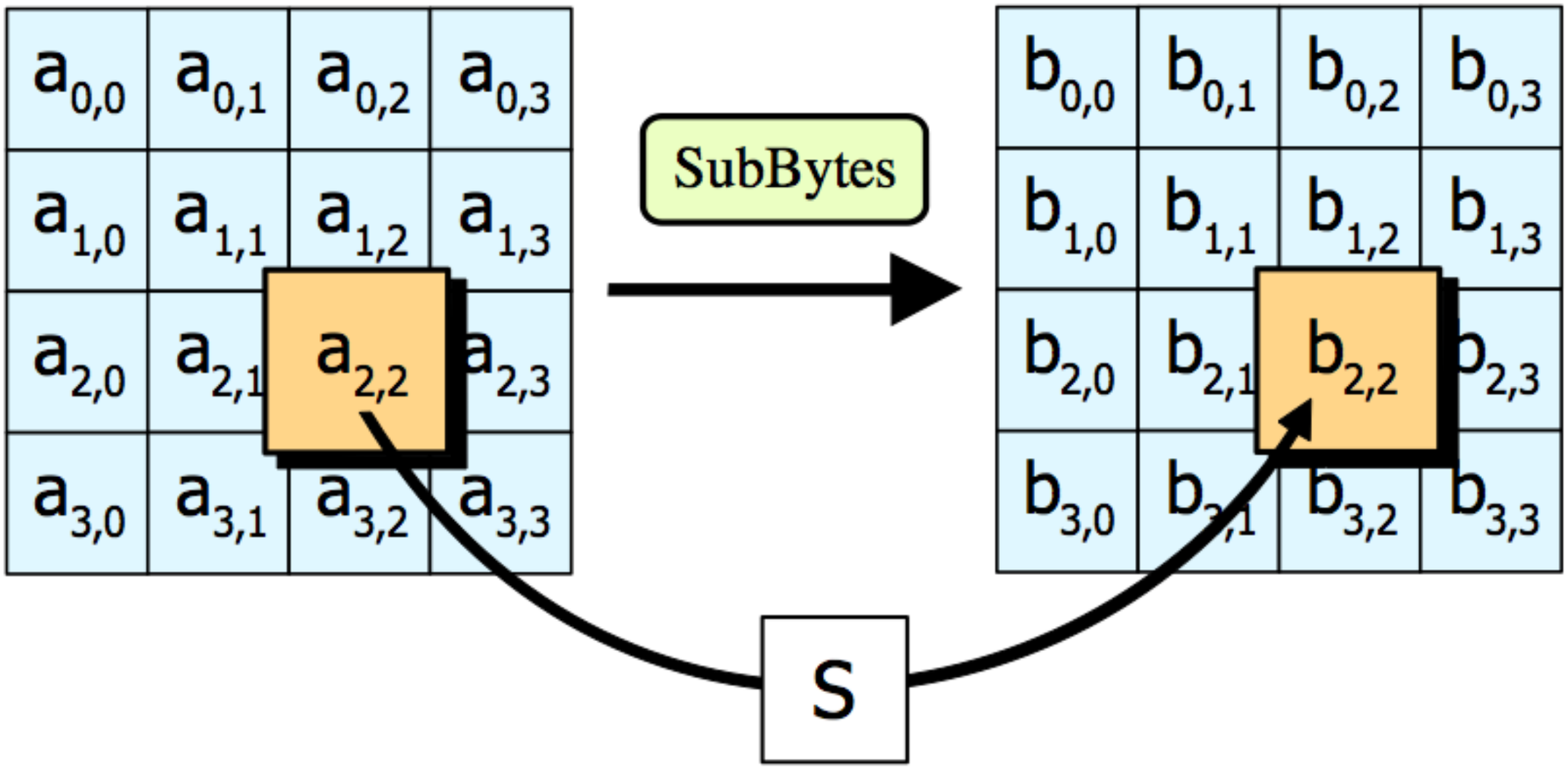



Исходный блок
Начальная перестановка
16 раз
f
Цикл шифрования
Ключи
Конечная перестановка
01110011001
11011000110
0111001111011
0000101110001101
1110110001110101
1011011100011000
1101110100101101
1110100101110110
1101110001100010
1100011100110000
0001111110111011
Зашифрованный блок

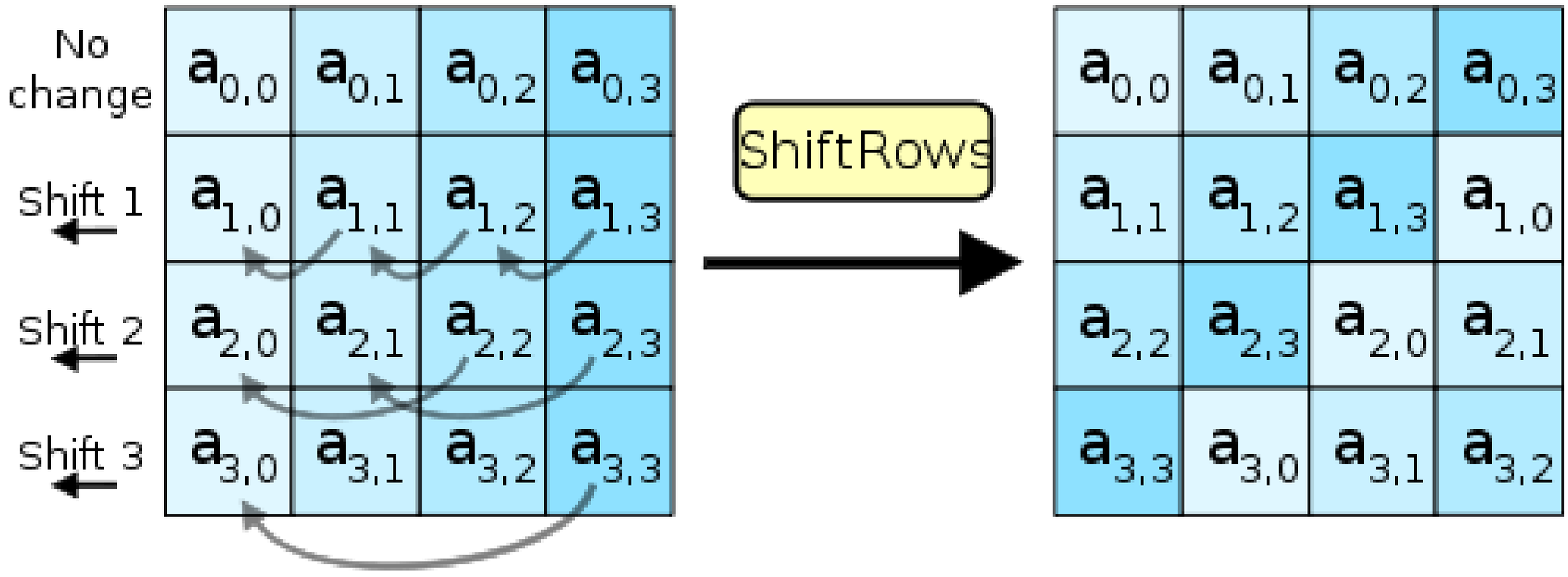
Шифр AES

1. KeyExpansion
2. Initial Round
    1. AddRoundKey
3. Rounds
    1. SubBytes
    2. ShiftRows
    3. MixColumns
    4. AddRoundKey
4. Final Round
    1. SubBytes
    2. ShiftRows
    3. AddRoundKey

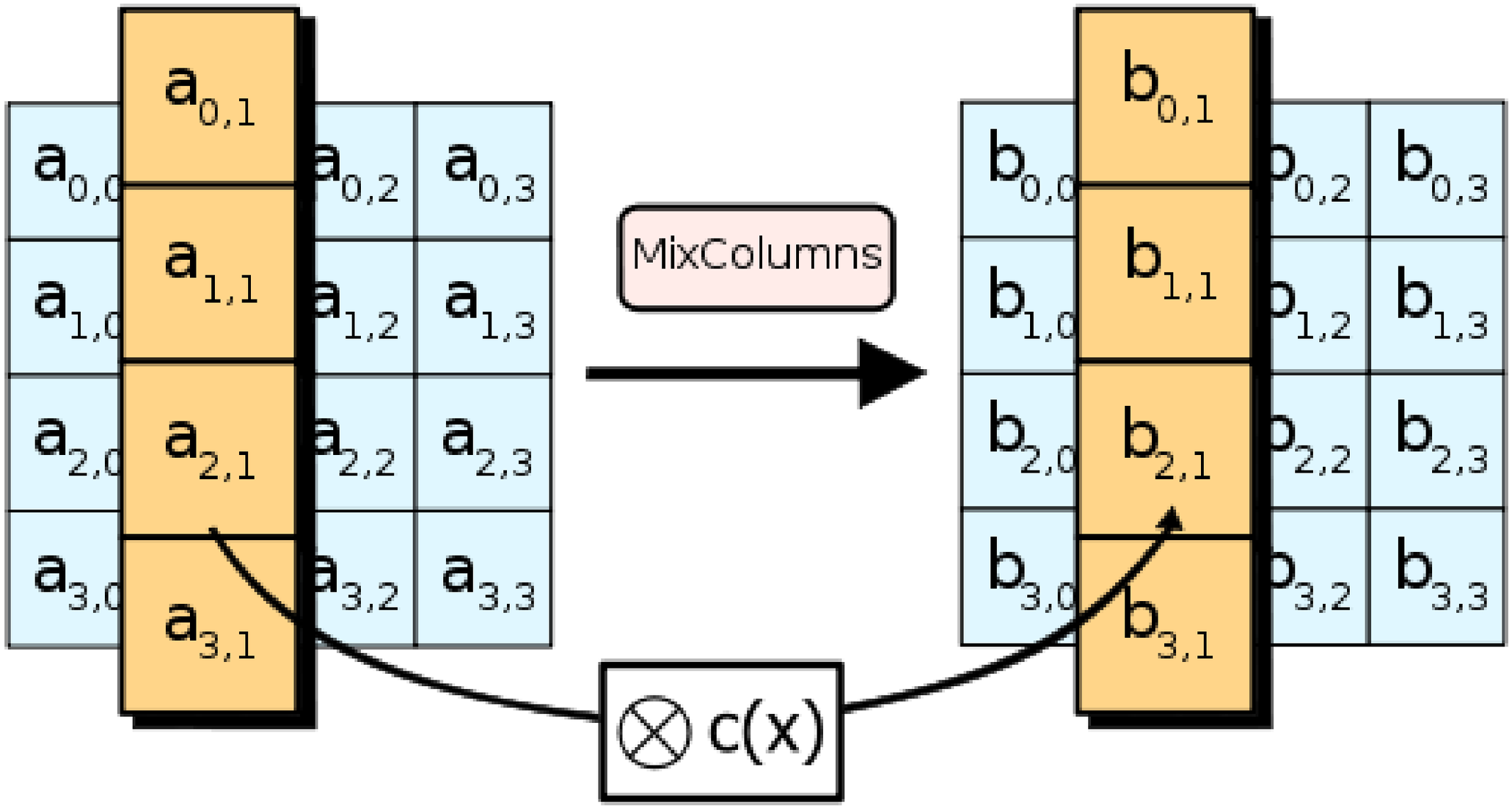
SubBytes


a0,0 a0,1 a0,2 a0,3
a1,0 a1,1 a1,2 a1,3
a2,0 a2,1 a2,2 a2,3
a3,0 a3,1 a3,2 a3,3
SubBytes
b0,0 b0,1 b0,2 b0,3
b1,0 b1,1 b1,2 b1,3
b2,0 b2,1 b2,2 b2,3
b3,0 b3,1 b3,2 b3,3
S

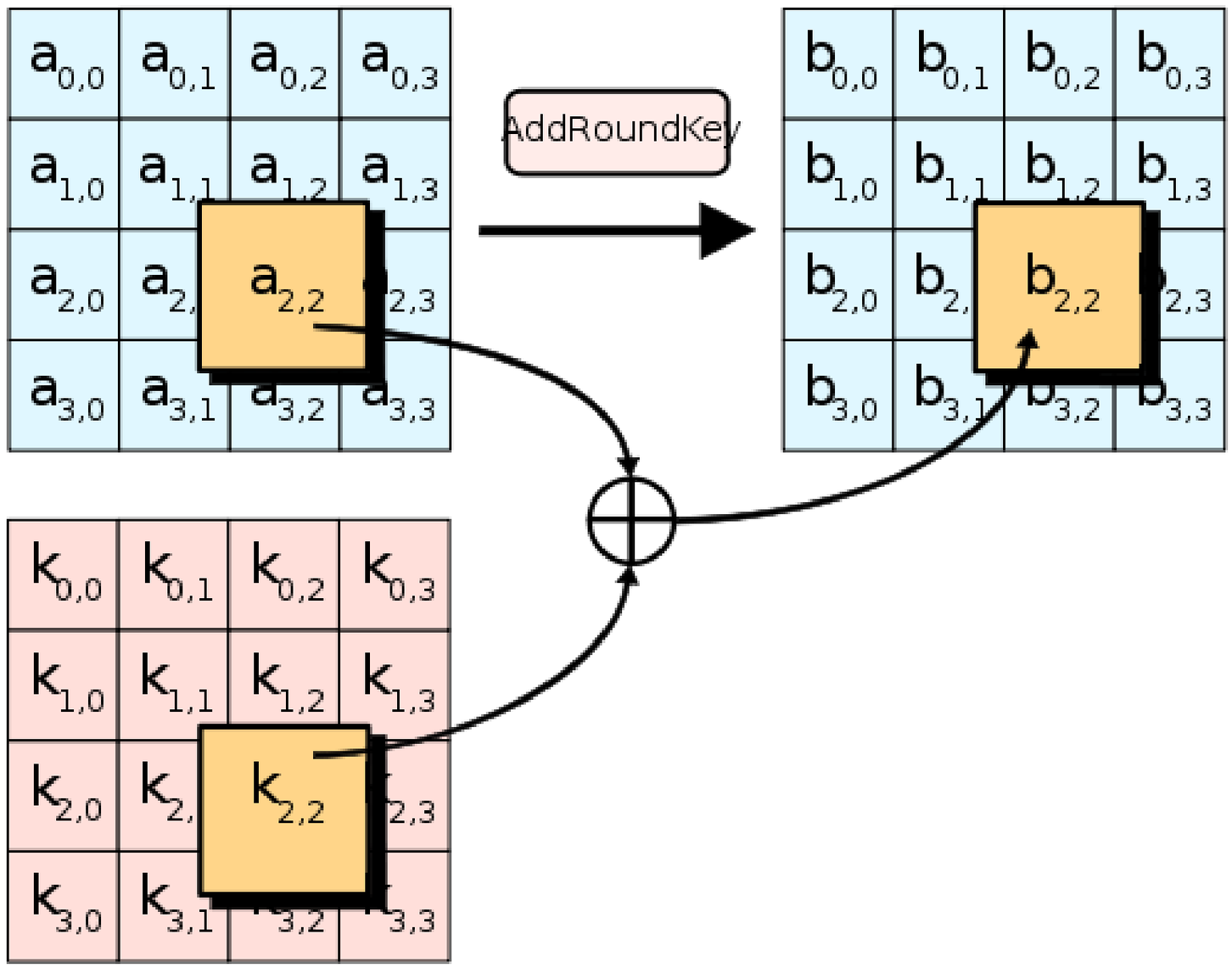
ShiftRows


No change
Shift 1
Shift 2
Shift 3
ShiftRows
$a_{0,0}$ $a_{0,1}$ $a_{0,2}$ $a_{0,3}$
$a_{1,0}$ $a_{1,1}$ $a_{1,2}$ $a_{1,3}$
$a_{2,0}$ $a_{2,1}$ $a_{2,2}$ $a_{2,3}$
$a_{3,0}$ $a_{3,1}$ $a_{3,2}$ $a_{3,3}$
$a_{0,0}$ $a_{0,1}$ $a_{0,2}$ $a_{0,3}$
$a_{1,1}$ $a_{1,2}$ $a_{1,3}$ $a_{1,0}$
$a_{2,2}$ $a_{2,3}$ $a_{2,0}$ $a_{2,1}$
$a_{3,3}$ $a_{3,0}$ $a_{3,1}$ $a_{3,2}$

MixColumns



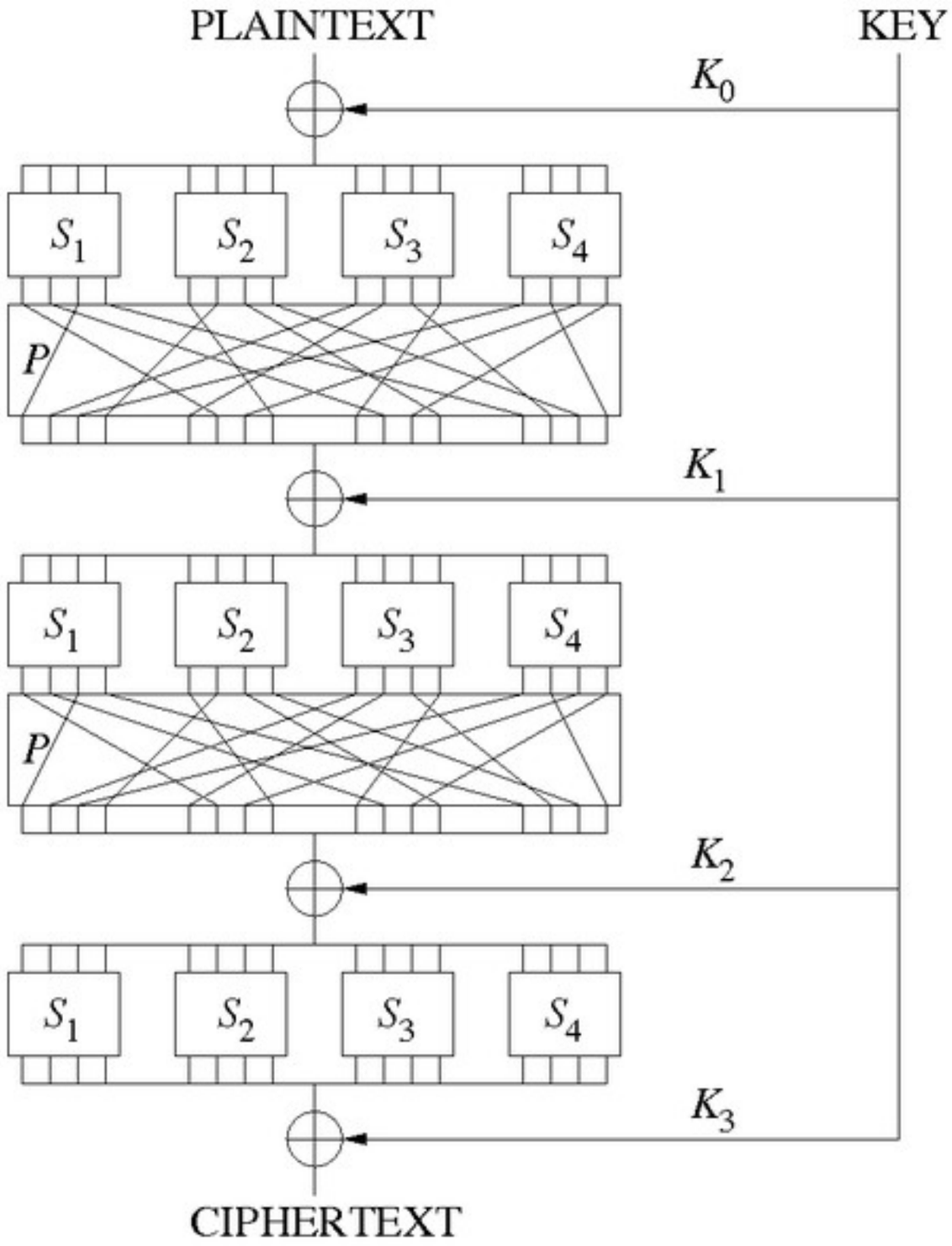
AddRound Key



AES

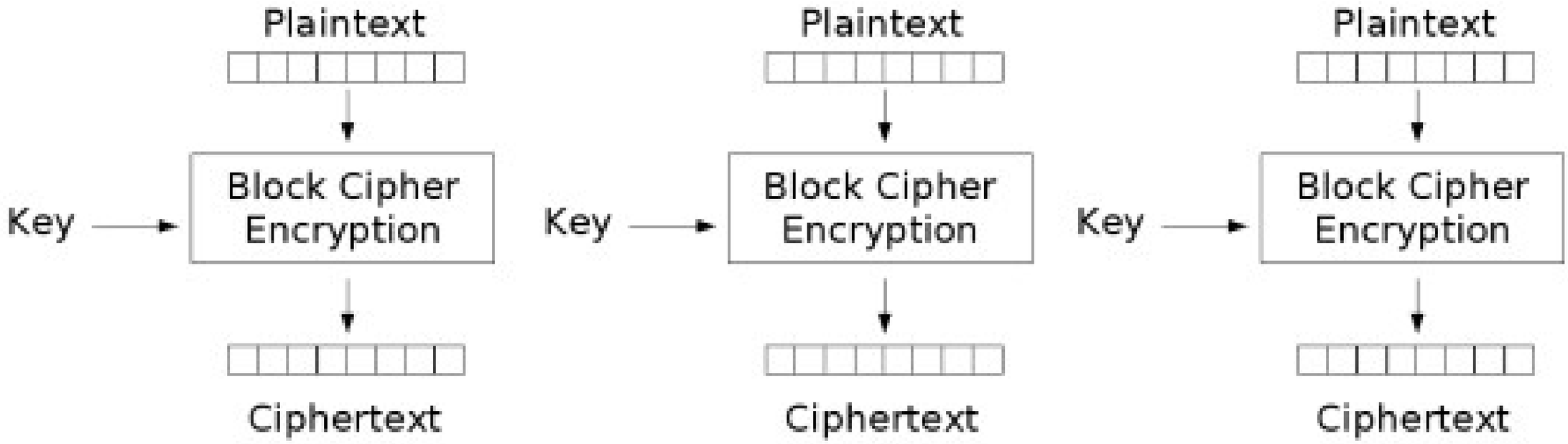
- Размер блока: 128 бит
- Размер ключа: 128, 192 или 256 бит
- Количество раундов: 10, 12 или 14

SPN


PLAINTEXT
KEY
K_0
S_1
S_2
S_3
S_4
P
K_1
S_1
S_2
S_3
S_4
P
K_2
S_1
S_2
S_3
S_4
K_3
CIPHERTEXT

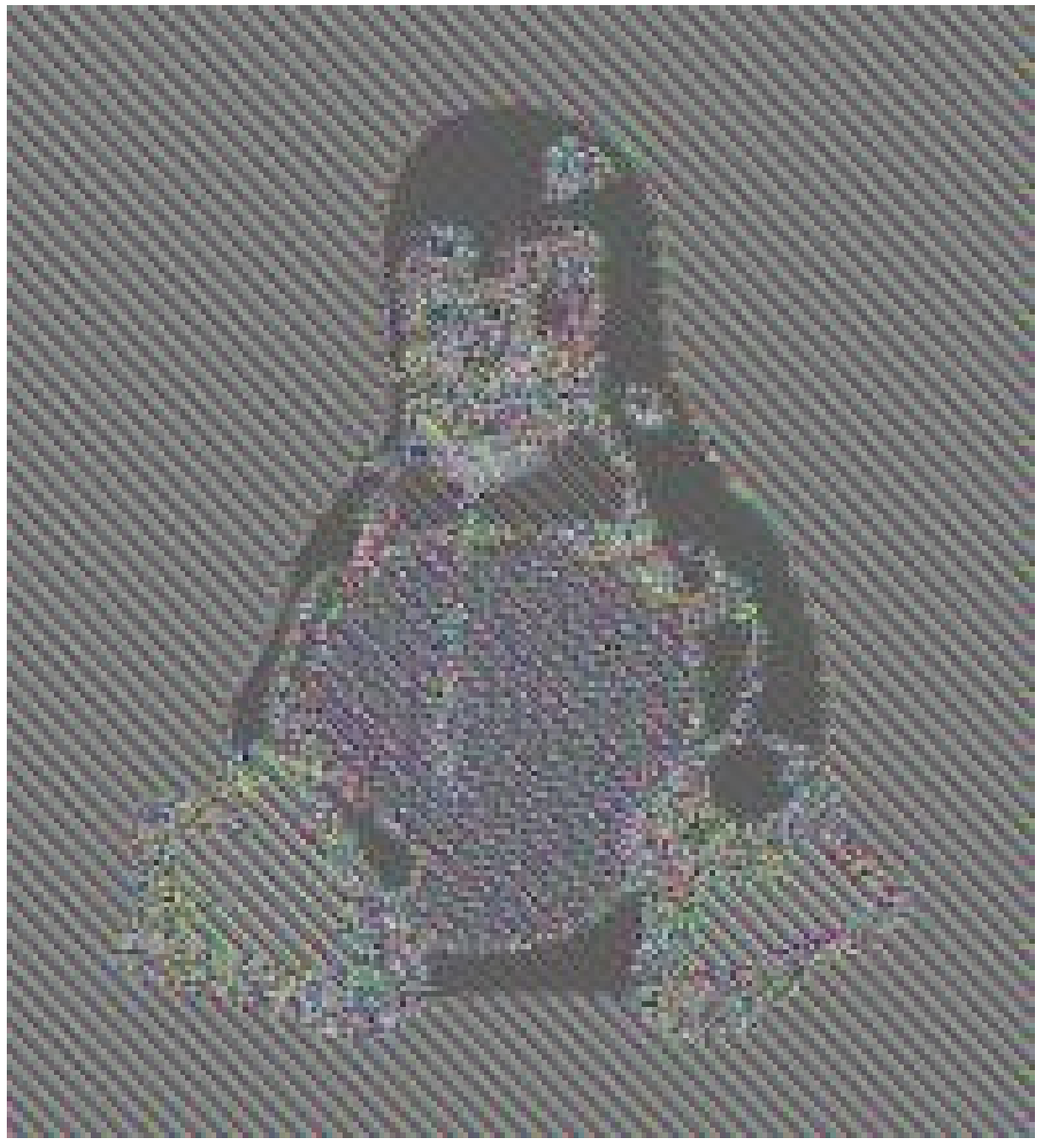
Как зашифровать несколько блоков?

ECB

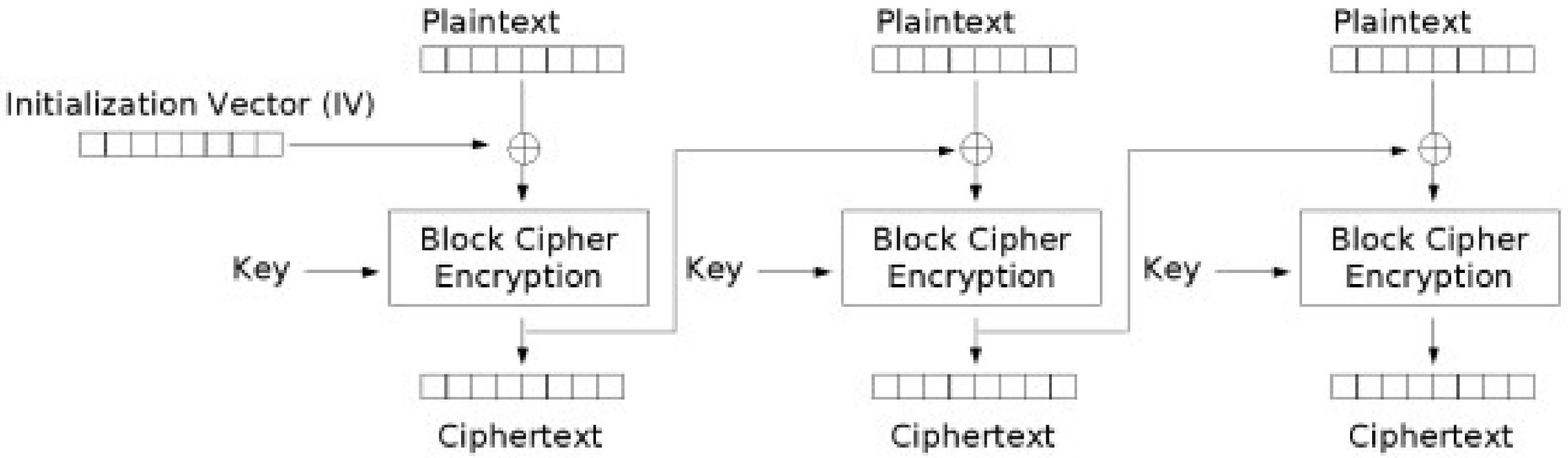


Electronic Codebook (ECB) mode encryption

ECB



CBC

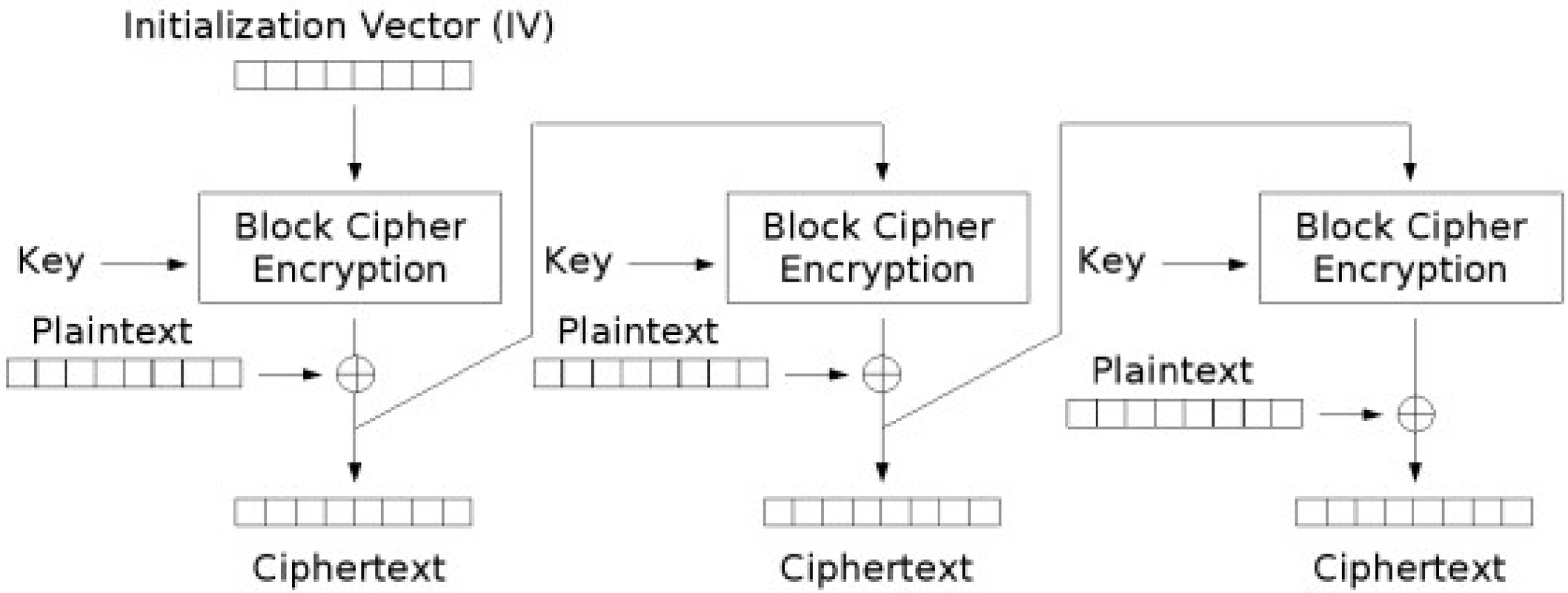


Cipher Block Chaining (CBC) mode encryption

Birthday paradox

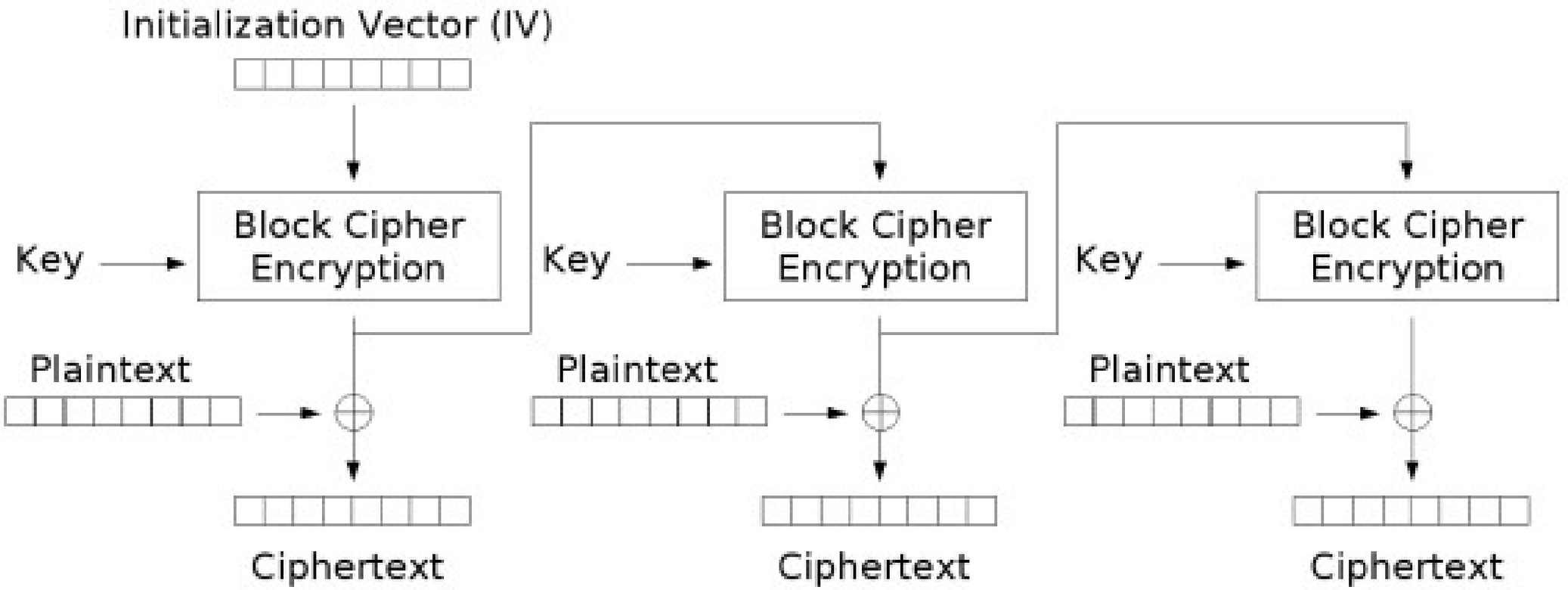
- Какова вероятность совпадения двух блоков выхода шифра?
- Как это влияет на безопасность криптосистемы?
- Сколько времени это займет на реальном трафике?

CFB



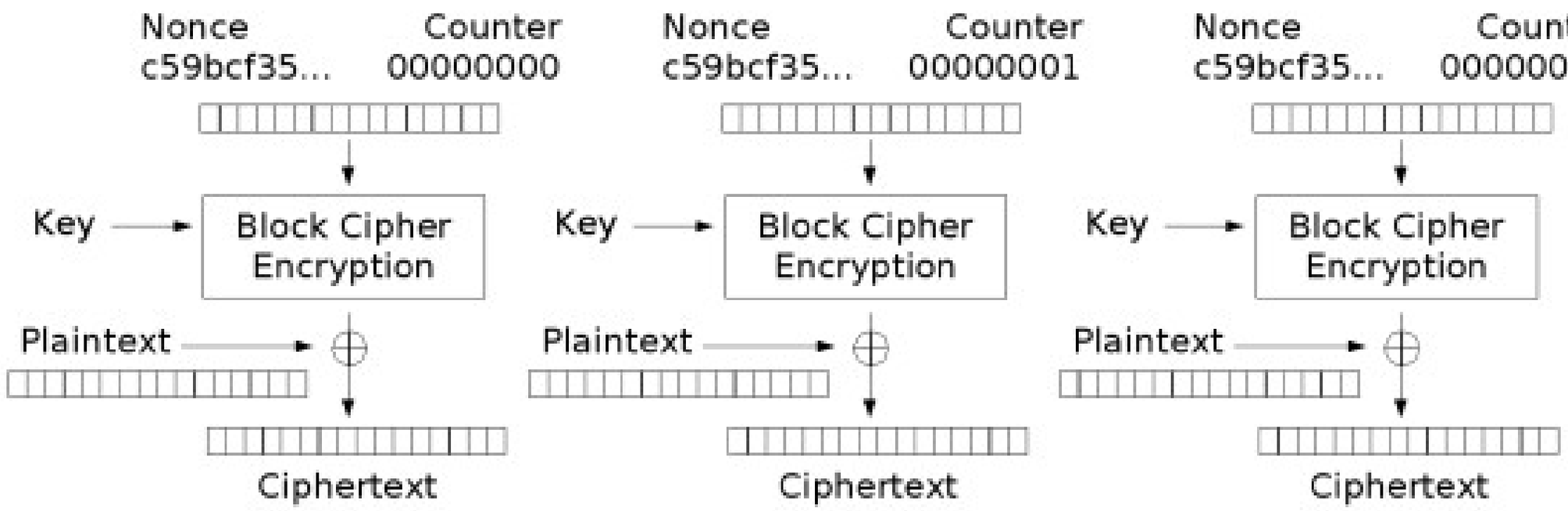
Cipher Feedback (CFB) mode encryption

OFB



Output Feedback (OFB) mode encryption

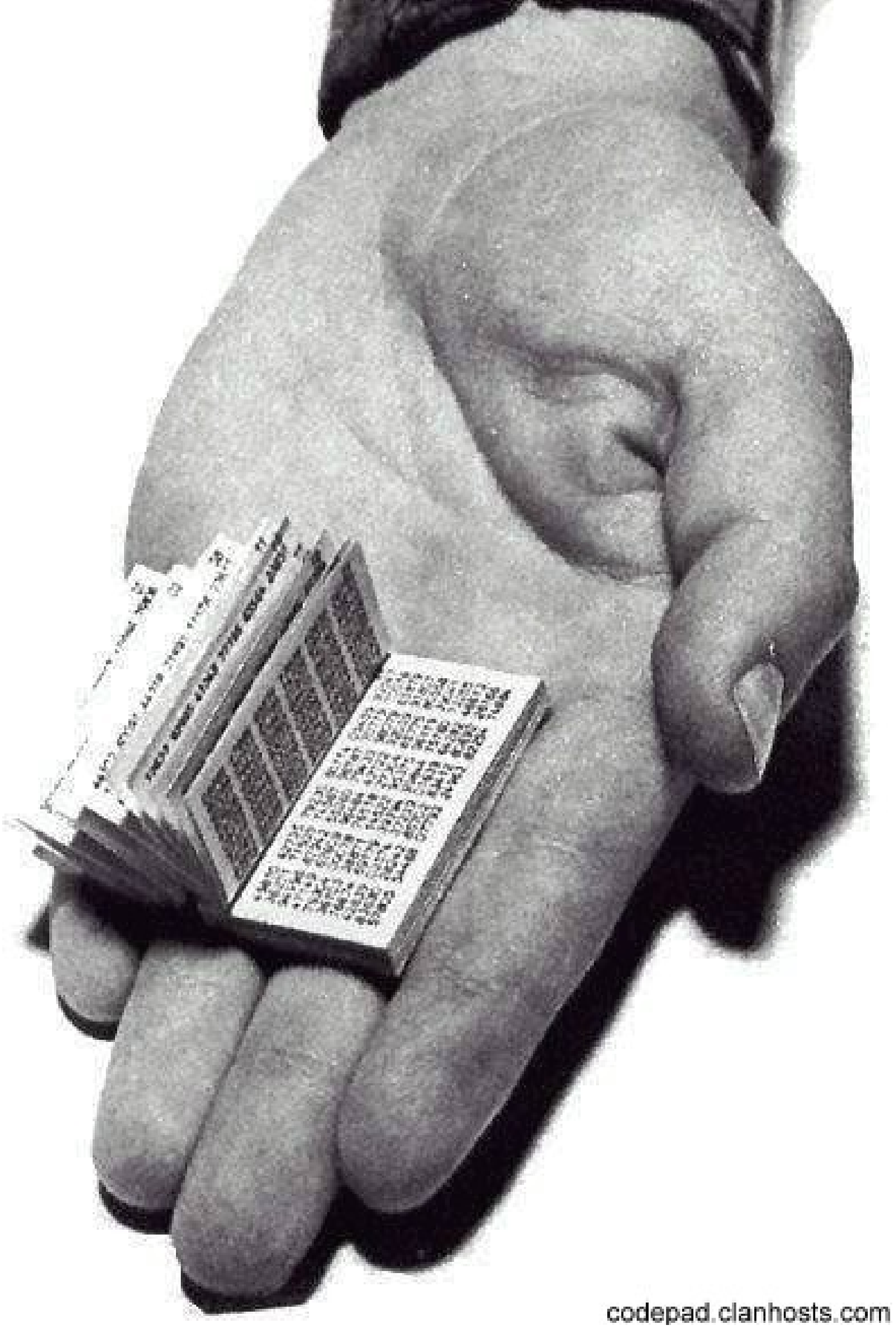
CTR



Counter (CTR) mode encryption

Поточные шифры

- Понятие *гаммы*
- Шифр Вернама



codepad.clanhosts.com