

Прикладная Криптография: Симметричные криптосистемы Блочные шифры

Макаров Артём
МИФИ 2025

Тест.

- Положить телефон экраном вниз справа от себя
- Не разговаривать с соседями
- Не пользоваться конспектами и электронными устройствами
- Написать номер (по таблице) и ФИО на листочке
- Написать краткий ответ на вопрос
- Дождаться окончания теста



Тест.

Схема ЕСВ блочного шифрования, нарисовать картинку или описать шифрование/расшифрование (формула).

Для каких сообщений ЕСВ является семантически стойким при использовании стойкого блочного шифра?

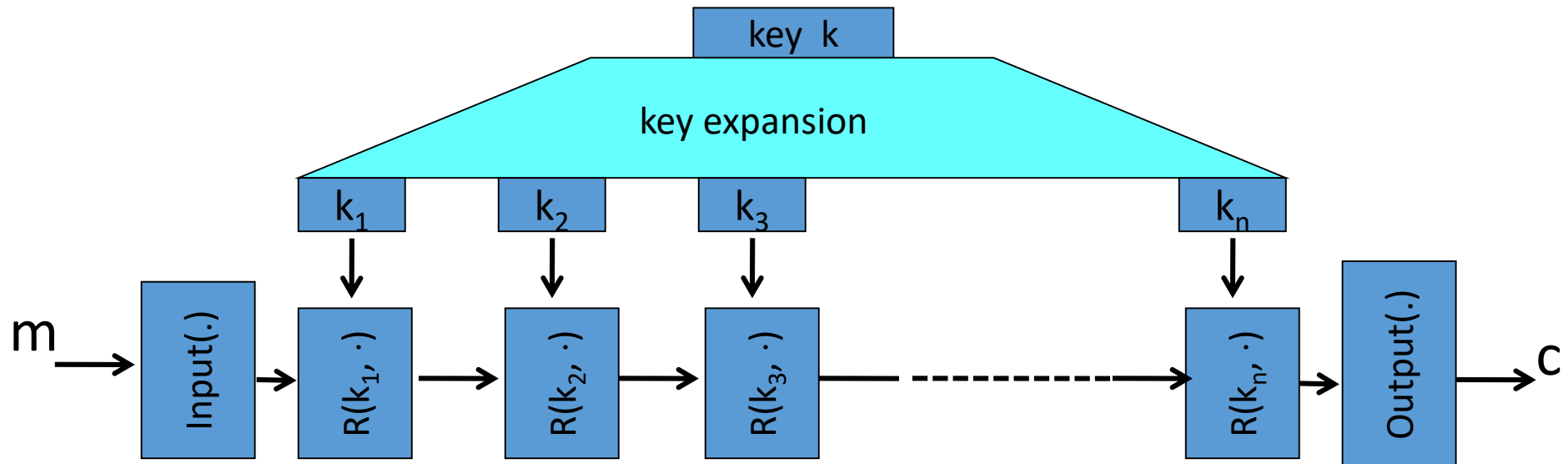
- Положить телефон экраном вниз справа от себя
- Не разговаривать с соседями
- Не пользоваться конспектами и электронными устройствами
- Написать номер (по таблице) и ФИО на листочке
- Написать краткий ответ на вопрос
- Дождаться окончания теста



TIME IS
UP

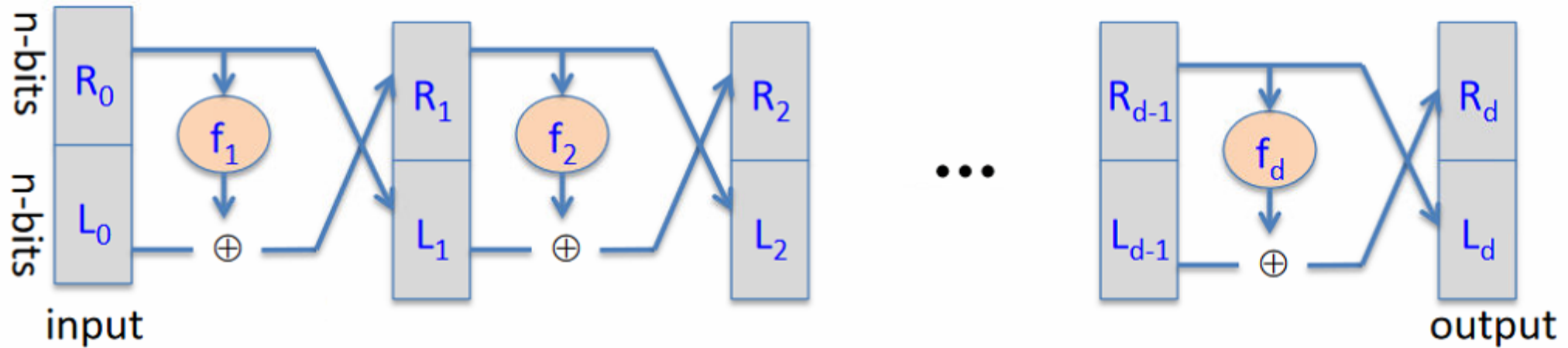
Построение блочных шифров

- Блочные шифры часто строятся с использованием итеративных (раундовых) функций и функции расширения ключей (см. прошлую лекцию)
- Сами по себе итеративные функции и функции расширения ключей могут быть не стойкими



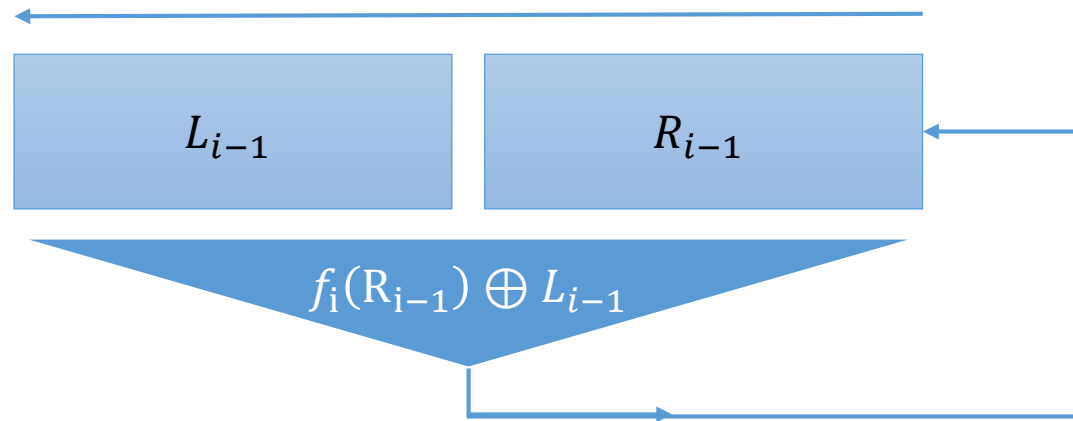
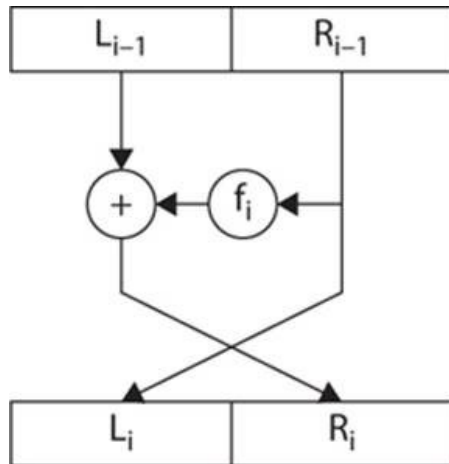
Сеть Фейстеля

- Пусть $f_1, \dots, f_d: \{0,1\}^n \rightarrow \{0,1\}^n$
- Построим функцию $F: \{0,1\}^{2n} \rightarrow \{0,1\}^{2n}$:
 - $R_i = f_i(R_{i-1}) \oplus L_{i-1}$
 - $L_i = R_{i-1}, (L_i, R_i) \in \{0,1\}^{2n}$

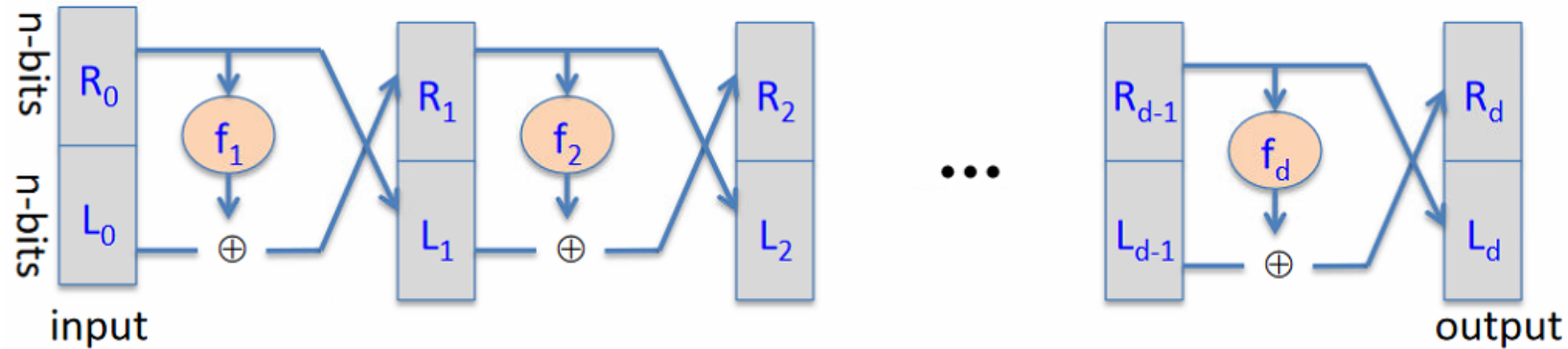


Сеть Фейстеля

- Фактически сеть Фейстеля есть линейный двухблочный регистр сдвига:

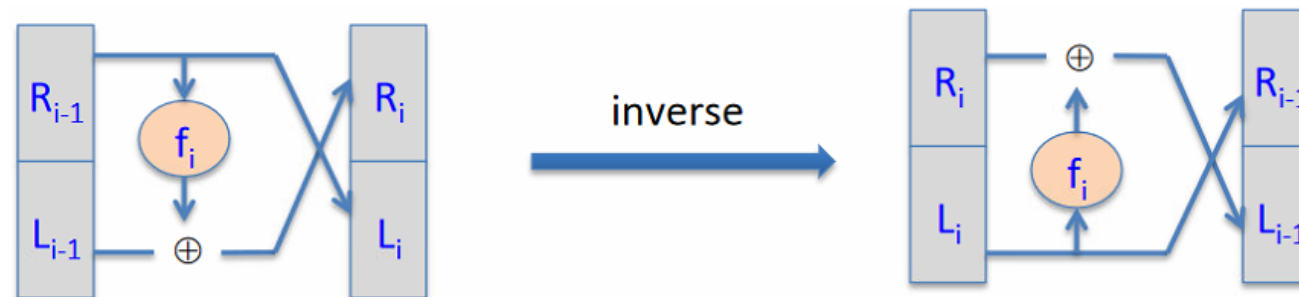


Сеть Фейстеля



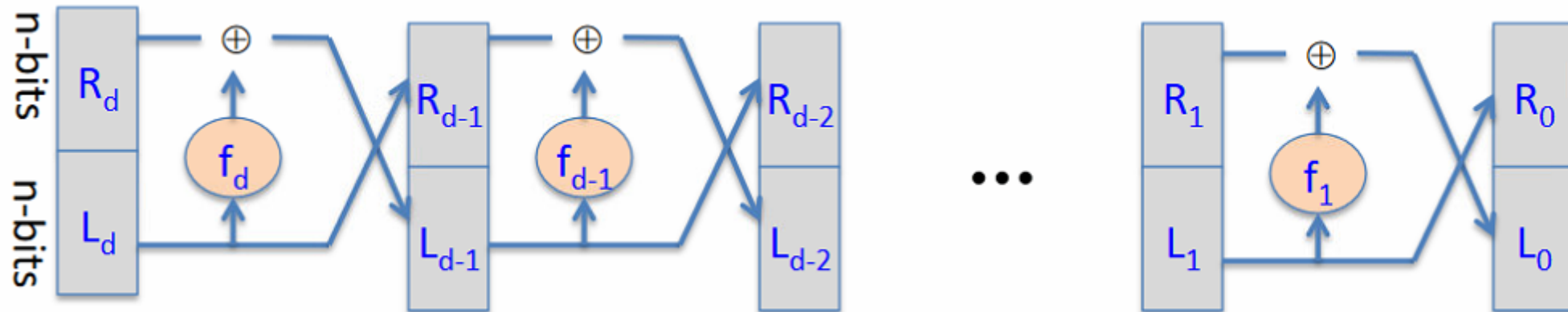
Теорема 5.1 Для любых функций $f_1, \dots, f_d: \{0,1\}^n \rightarrow \{0,1\}^n$ сеть Фейстеля обратима

$$\triangleright R_{i-1} = L_i, L_{i-1} = f_i(L_i) \oplus R_i \triangleleft$$



Сеть Фейстеля

- Обратное преобразование сети Фейстеля – сеть Фейстеля с обратным порядком следования функций f_1, \dots, f_d :



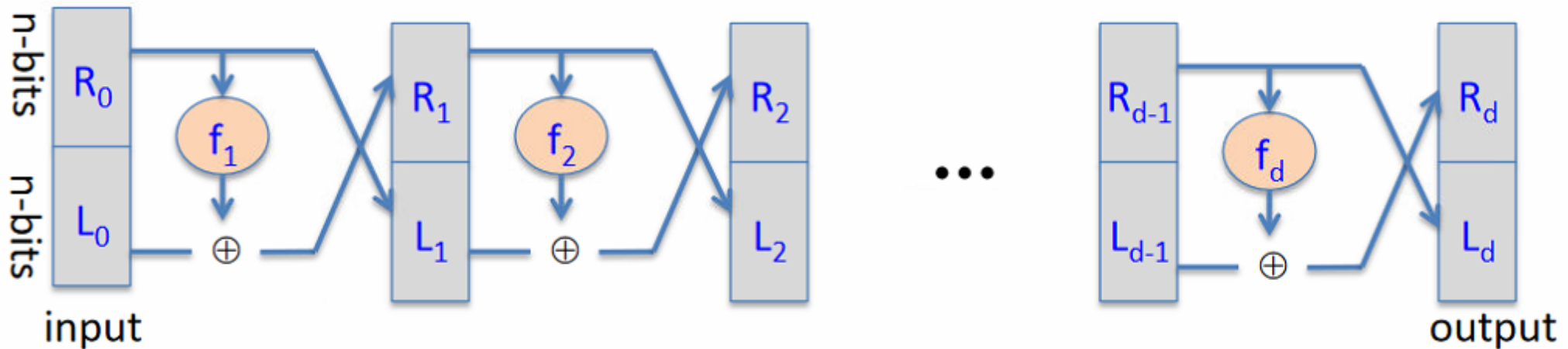
Сеть Фейстеля

Теорема 5.2. (Luby-Rackoff)

Пусть $f: \{0,1\}^n \rightarrow \{0,1\}^n$ стойкая PRF.

Тогда трехраундовая сеть Фейстеля ($d = 3$) $F = K^3 \times \{0,1\}^{2n} \rightarrow \{0,1\}^{2n}$ - стойкая PRP.

! Используются 3 независимых, случайных ключа!



DES

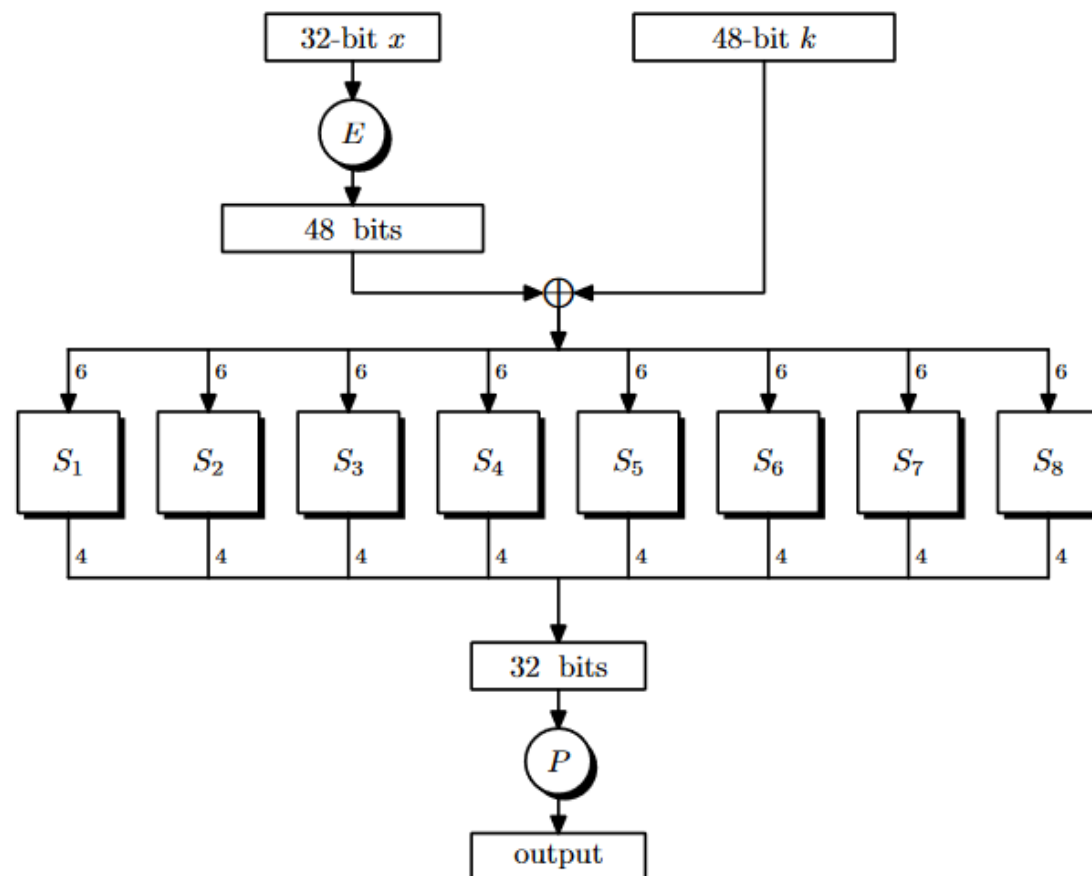
- 16 раундовая сеть Фейстеля
- Размер ключей – 56 бит
- Размер блока – 64 бита
- Производительность 80 MB/sec (OpenSSL 1.0.1e on Intel(R) Xeon(R) CPU E5-2698 v3 @ 2.30GHz (Haswell))
- Сломан. Не использовать на практике, включая вариации (например 3DES)
- Практическая атака - 2^{43} , 3DES - 2^{113} .

DES

- $f_i(x) = F(k_i, x)$, $k_i \in \{0,1\}^{48}$, $x \in \{0,1\}^{32}$ - раундовая функция в сети Фейстеля.
- $E: \{0,1\}^{32} \rightarrow \{0,1\}^{48}$ - функция расширения
- $P: \{0,1\}^{32} \rightarrow \{0,1\}^{32}$ - перемешивающая перестановка
- Функции $S_1, \dots, S_8: \{0,1\}^6 \rightarrow \{0,1\}^4$ - S боксы, фиксировано заданные таблично.

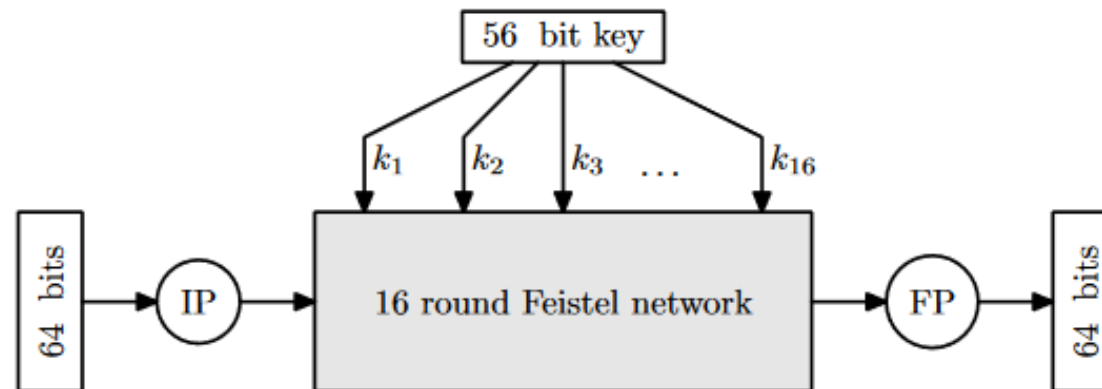
DES

- $f_i(x) = F(k_i, x)$, $k_i \in \{0,1\}^{48}$, $x \in \{0,1\}^{32}$ - раундовая функция сети Фейстеля.
- $E: \{0,1\}^{32} \rightarrow \{0,1\}^{48}$ - функция расширения блока
- $P: \{0,1\}^{32} \rightarrow \{0,1\}^{32}$ - фиксированная перестановка
- Функции $S_1, \dots, S_8: \{0,1\}^6 \rightarrow \{0,1\}^4$ - S боксы, фиксировано заданные таблично.



DES

- $G: \{0,1\}^{56} \rightarrow (\{0,1\}^{48})^{16}$ - функция расширения ключей (ключевого расписания), получает 16 раундовых (итеративных) 48 битных ключей, используя различные конкатенации подвекторов исходного ключа.
- $IP, FP: \{0,1\}^{64} \rightarrow \{0,1\}^{64}$ - входные и выходные преобразования, неизвестного назначения (возможно для замедления программной реализации, не влияют на стойкость)



ГОСТ 28147-89

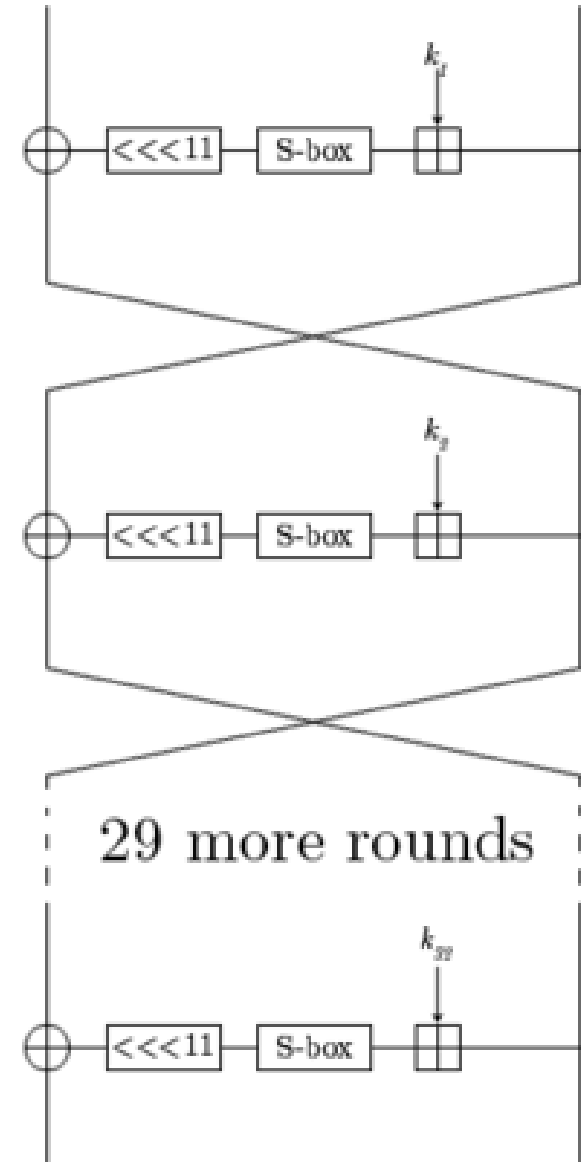
- ... он же ГОСТ Р 34.12-2015 «Магма»
- 32 раундовая сеть Фейстеля
- Размер ключа – 256 бит
- Размер блока – 64 бит
- Основной алгоритм шифрования для людей обременённых приказом ФСБ

ГОСТ 28147-89

- $f_i(x) = F(k_i, x)$, $k_i \in \{0,1\}^{32}$, $x \in \{0,1\}^{32}$ - раундовая функция в сети Фейстеля.
- Ключ складывается по модулю 2^{32}
- Функции $S_1, \dots, S_8: \{0,1\}^4 \rightarrow \{0,1\}^4$ - S боксы, фиксировано заданные таблично.
- Циклический сдвиг на 11

ГОСТ 28147-89

- $f_i(x) = F(k_i, x)$, $k_i \in \{0,1\}^{32}$, $x \in \{0,1\}^{32}$ - раундовая функция в сети Фейстеля.
- Ключ складывается по модулю 2^{32}
- Функции $S_1, \dots, S_8: \{0,1\}^4 \rightarrow \{0,1\}^4$ - S боксы, фиксировано заданные таблично.
- Циклический сдвиг на 11



ГОСТ 28147-89

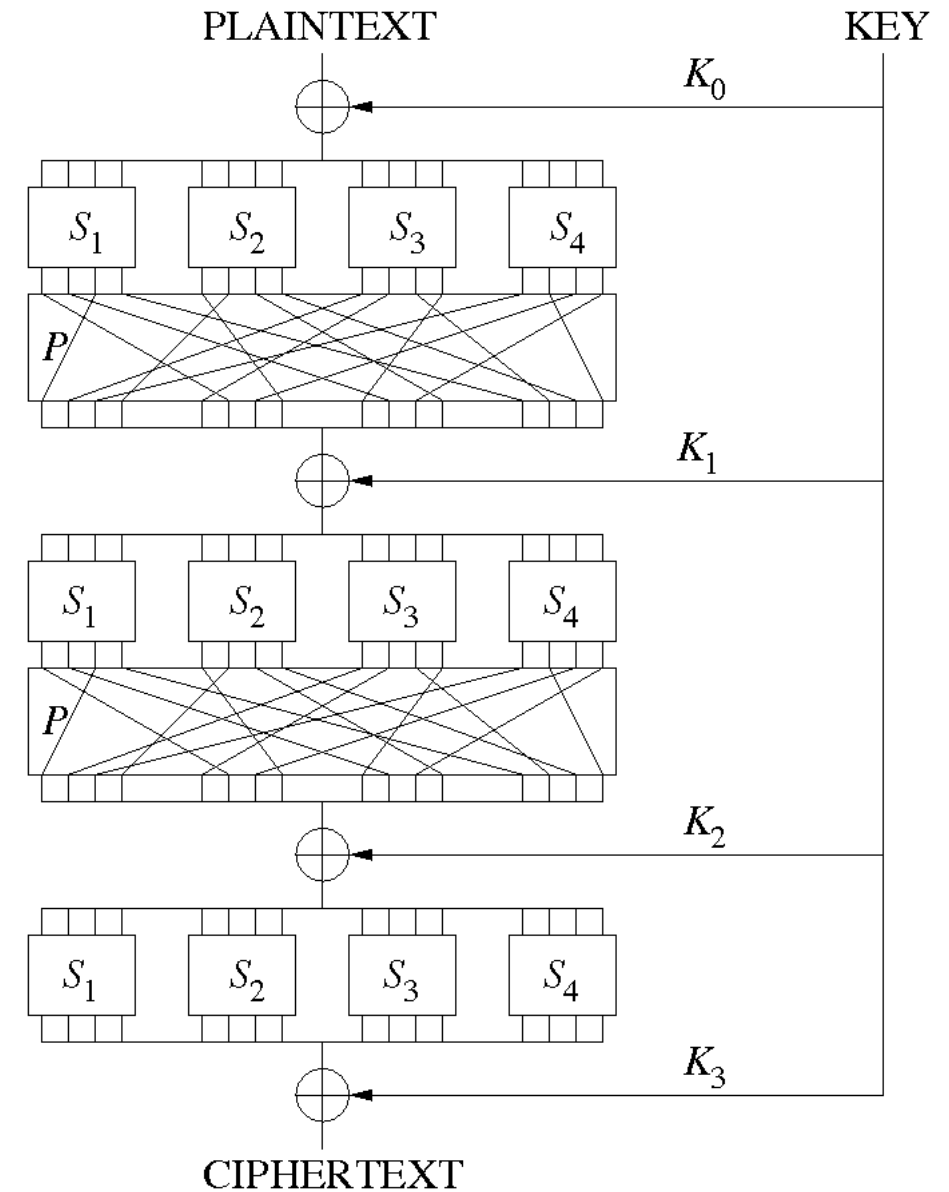
- $G: \{0,1\}^{256} \rightarrow (\{0,1\}^{32})^8$ - функция расширения ключей (ключевого расписания), получает 8 раундовых (итеративных) 32 битных ключей, путём разбиения исходного ключа на блоки.
- При шифровании ключи используются в порядке 0..7, 0..7, 0..7, 7..0

AES

- Наиболее распространённый алгоритм шифрования
- Размер ключа 128, 192, 256 бит
- Размер блока 128 бит
- Перестановочно-подстановочная сеть (Substitution – Permutation network)

SP сеть

- Предложена Фейстелем
- Основная идея – использования «двухслойной» итеративной функции.
- Слой P – перестановка блока
- Слой S – фиксированная подстановка, выполняемая поблочно с использованием фиксированных подстановок (S-Box'ов)



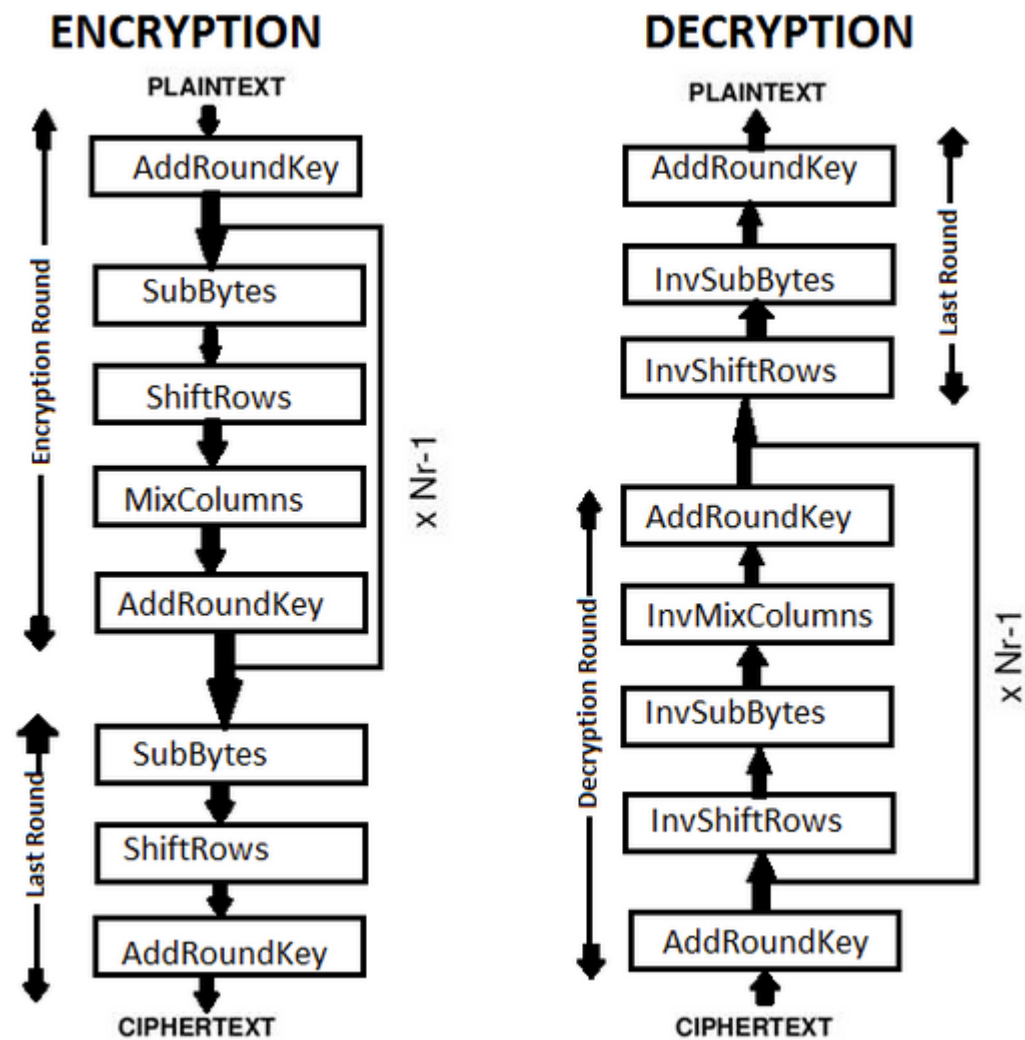
AES

- Раундовая функция – итерация SP сети
- Раундовая функция – последовательное применение 3х функций и сложение с ключом
- SubBytes: пусть $S: \{0,1\}^8 \rightarrow \{0,1\}^8$ фиксированная подстановка. Подстановка применяется для каждого из 16 подблоков входного блока.
- ShiftRows: циклический сдвиг строк 4×4 матрицы: i -я строка сдвигается на i позиций, $i = 0,1,2,3$.

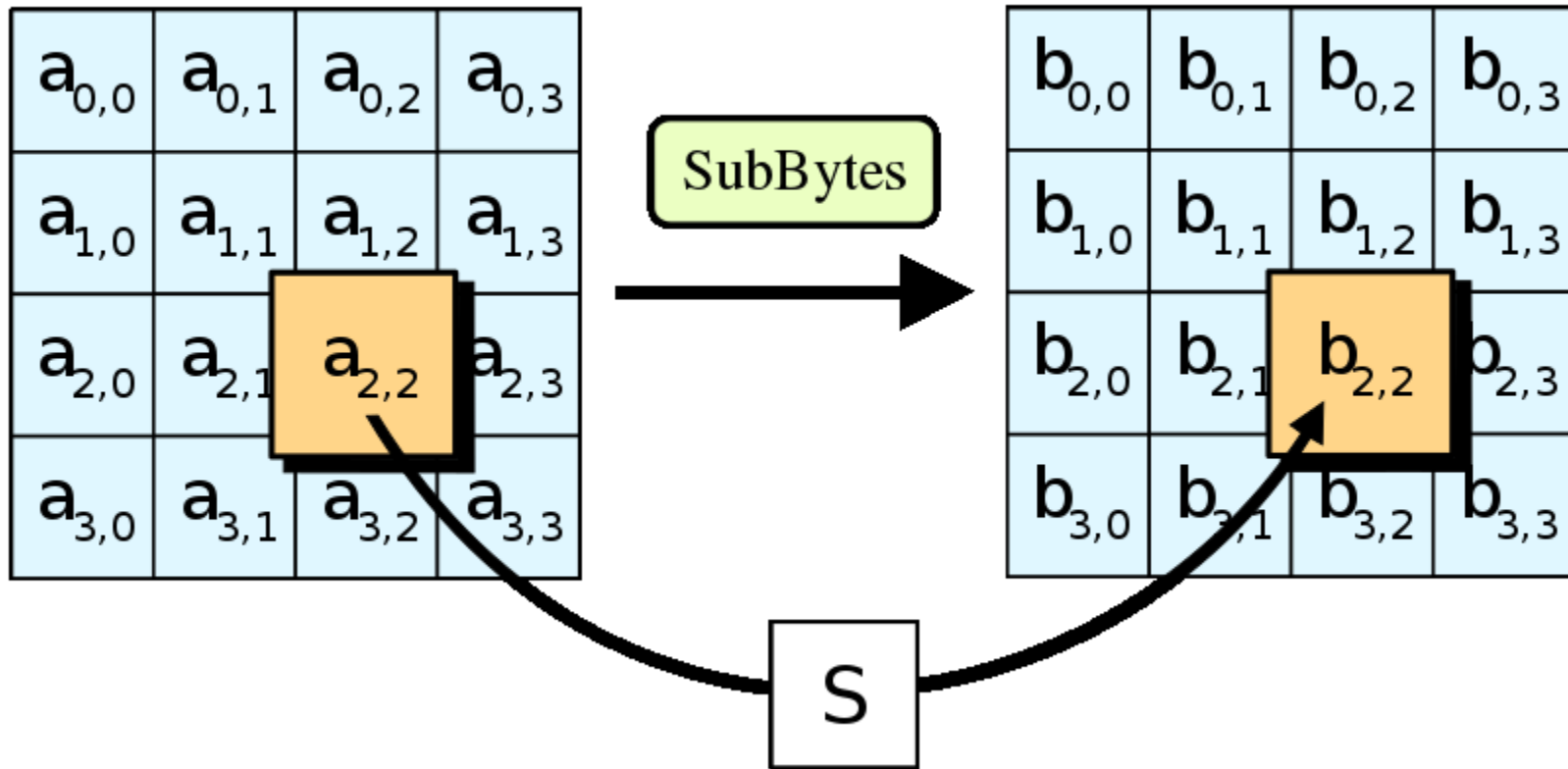
$$\begin{pmatrix} a_0 & a_1 & a_2 & a_3 \\ a_4 & a_5 & a_6 & a_7 \\ a_8 & a_9 & a_{10} & a_{11} \\ a_{12} & a_{13} & a_{14} & a_{15} \end{pmatrix} \Rightarrow \begin{pmatrix} a_0 & a_1 & a_2 & a_3 \\ a_5 & a_6 & a_7 & a_4 \\ a_{10} & a_{11} & a_8 & a_9 \\ a_{15} & a_{12} & a_{13} & a_{14} \end{pmatrix}$$

AES

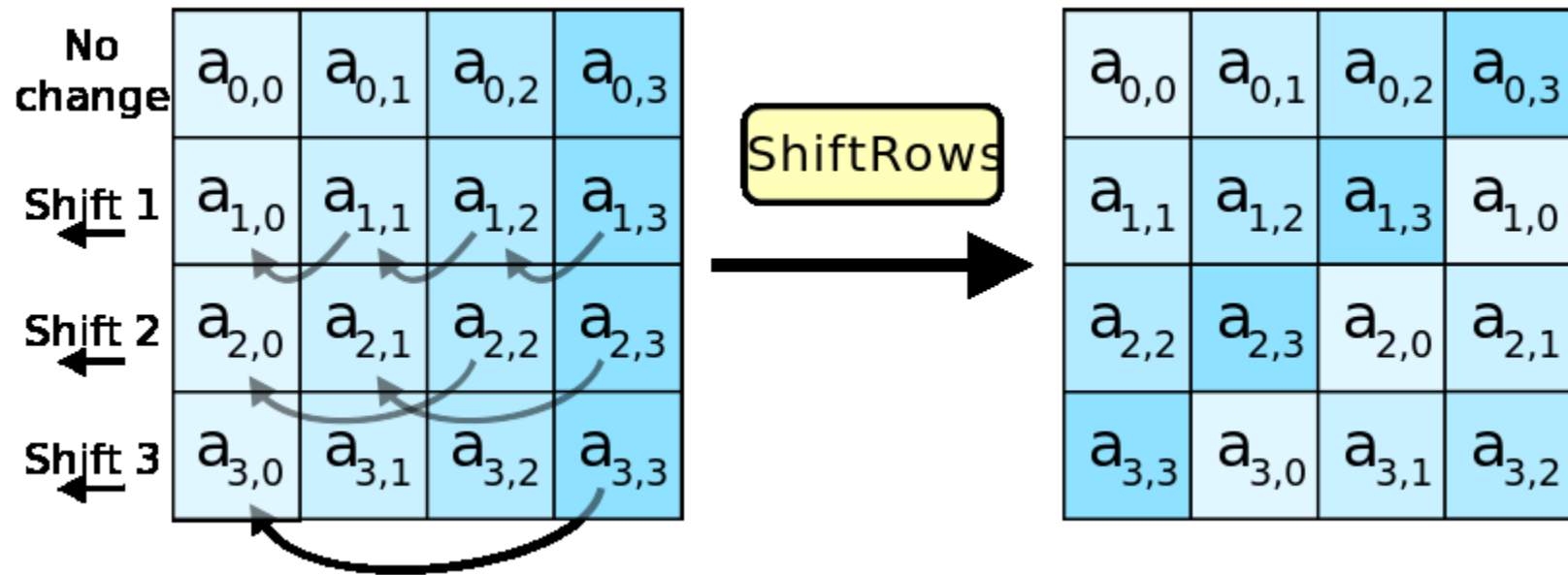
- MixColumns: умножение 4×4 матрицы на фиксированную обратимую матрицу в $GF(2^8)$.
- AddRoundKey: Сложение с ключом – побитное
- Все описанные выше преобразования – обратимы.
- В последнем раунде не выполняется MixColumns
- $G: \{0,1\}^{128} \rightarrow (\{0,1\}^{128})^{11}$



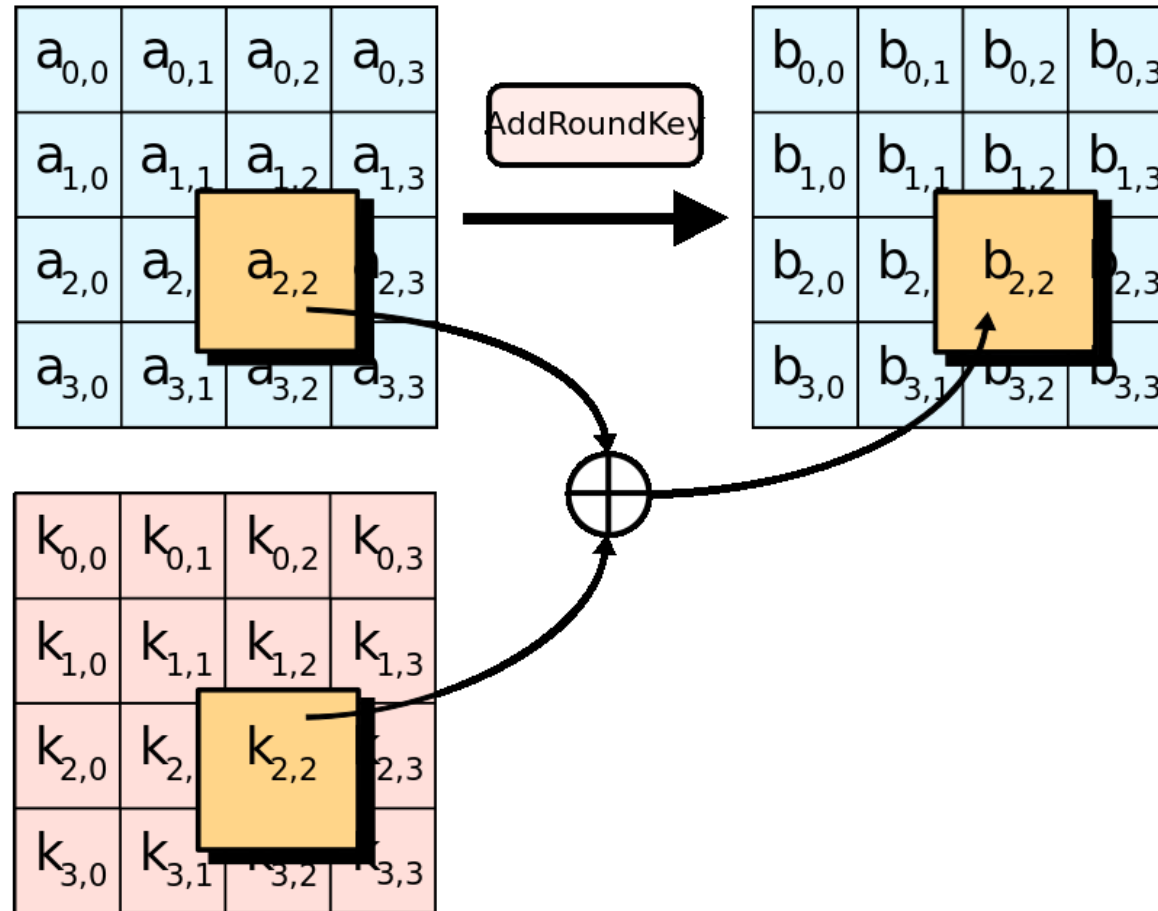
SubBytes



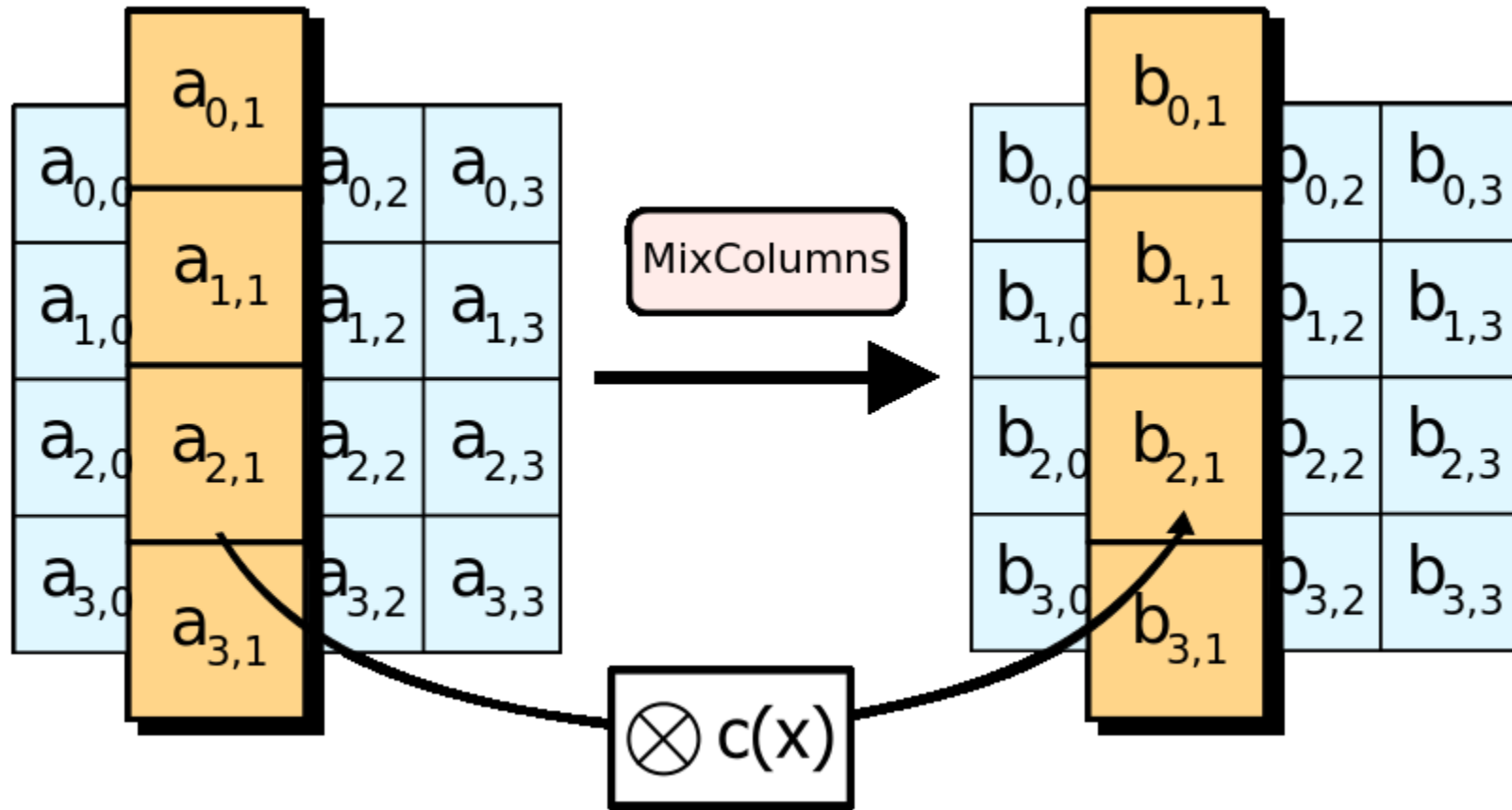
ShiftRows



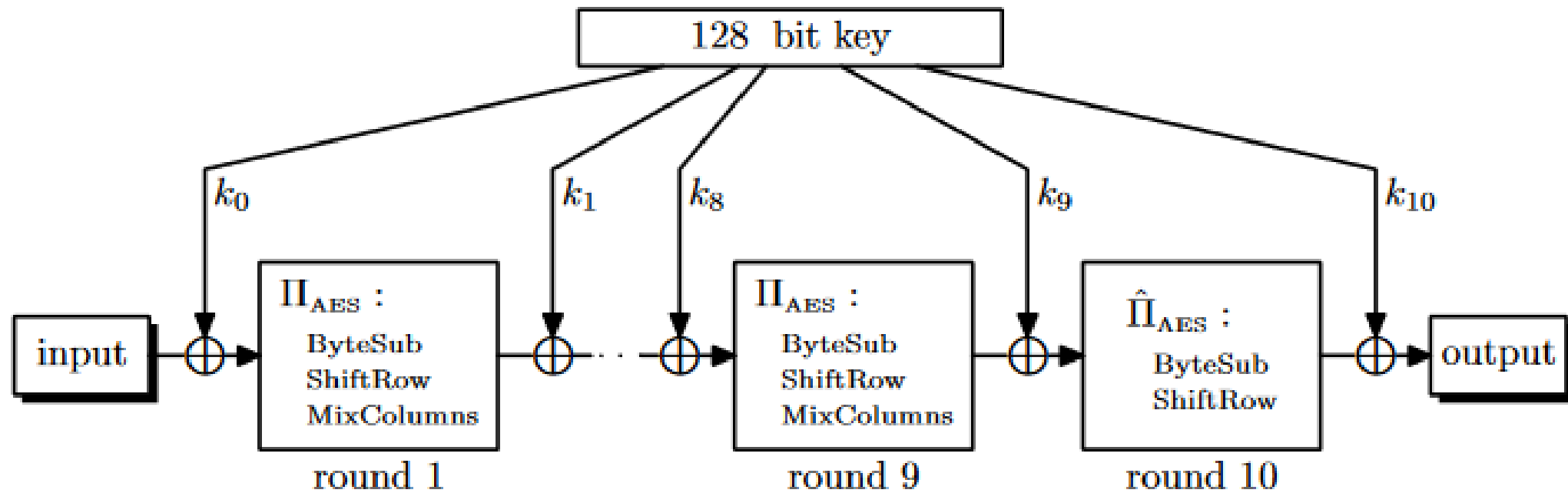
AddRoundKey



MixColumns



AES

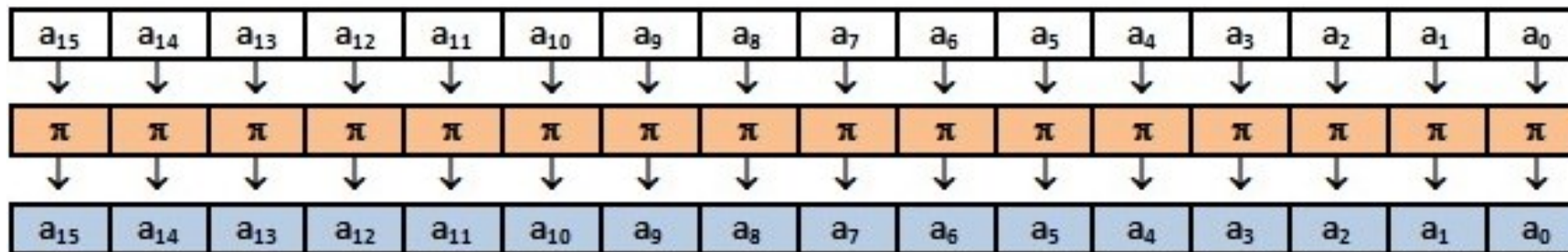


ГОСТ 34.12-2015 «Кузнечик»

- Новый алгоритм в замену 28147-89
- SP сеть (с регистром сдвига), сеть Фейстеля для генерации раундовых ключей
- Размер блока 128 бит
- Длина ключа 256 бит
- 10 раундов

ГОСТ 34.12-2015 «Кузнечик»

- Раундовая функция – итерация SP сети
- Раундовая функция – последовательное применение 2х функций и сложение с ключом (побитово)
- S: нелинейное биективное преобразование, реализуется с помощью S-box



Преобразование S

ГОСТ 34.12-2015 «Кузнечик»

- MUL: линейное преобразование, умножение в конечном поле над полиномом
- R: линейный регистр сдвига с функцией обратной связи, в виде умножения (MUL) байтов на коэффициенты (148, 32, 133, 16, 194, 192, 1, 251, 1, 192, 194, 16, 133, 32, 148, 1), и сложение по модулю 2.

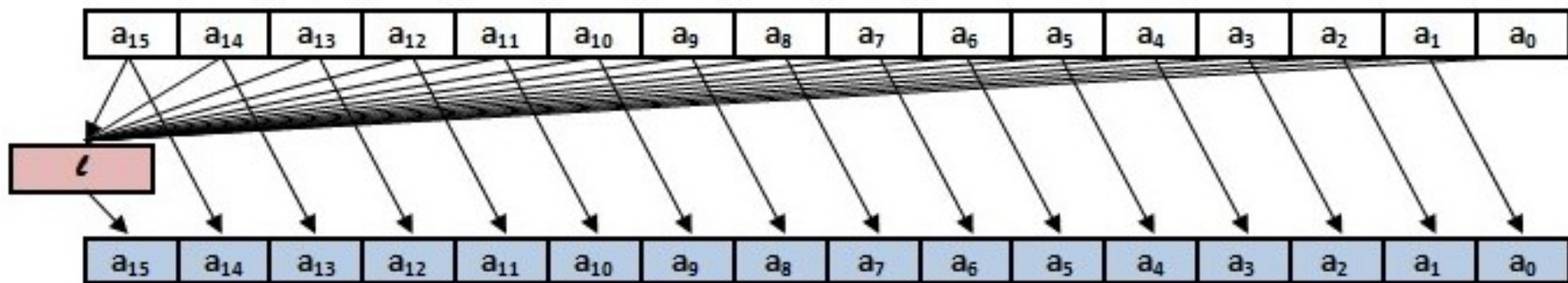
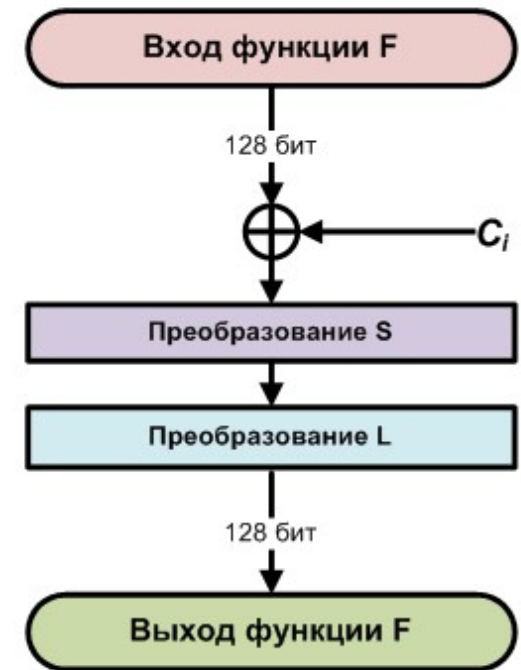
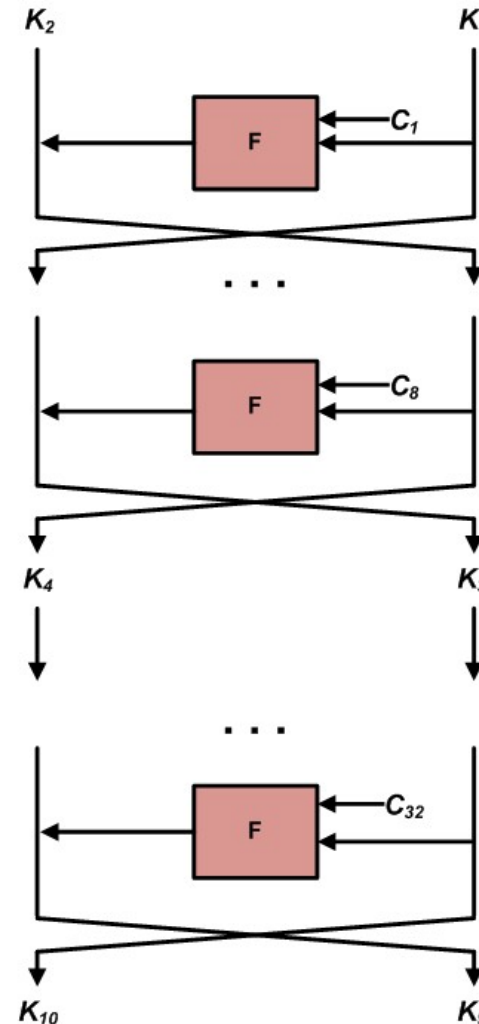


Схема преобразования R

ГОСТ 34.12-2015 «Кузнечик»

- Линейное преобразование L:
16 кратное повторение R
- Генерация раундовых ключей
 $G: \{0,1\}^{256} \rightarrow (\{0,1\}^{128})^{10}$ – сеть
Фейстеля с использованием
функции F, в виде итерации SP
сети.
- Ключ разбивается на 2 части
 K_1, K_2 , затем для получения
следующего раундового ключа
выполняется 8 итераций сети
Фейстеля, C_i – константы



ГОСТ 34.12-2015 «Кузнечик»

- Зашифрование – 10 итераций SP сети (функций S, L) и сложения с раундовым ключом.
- Расшифрование – обратный порядок ключей и преобразований.

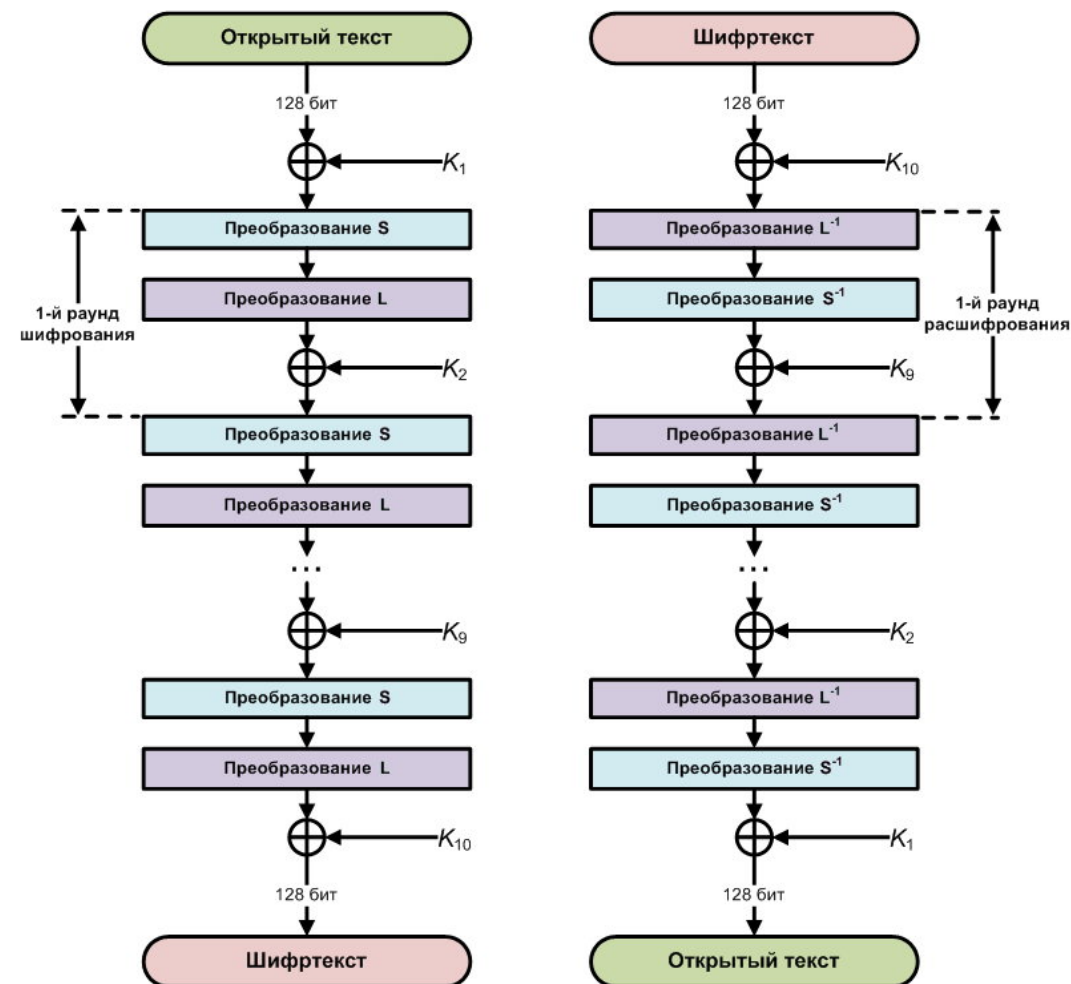
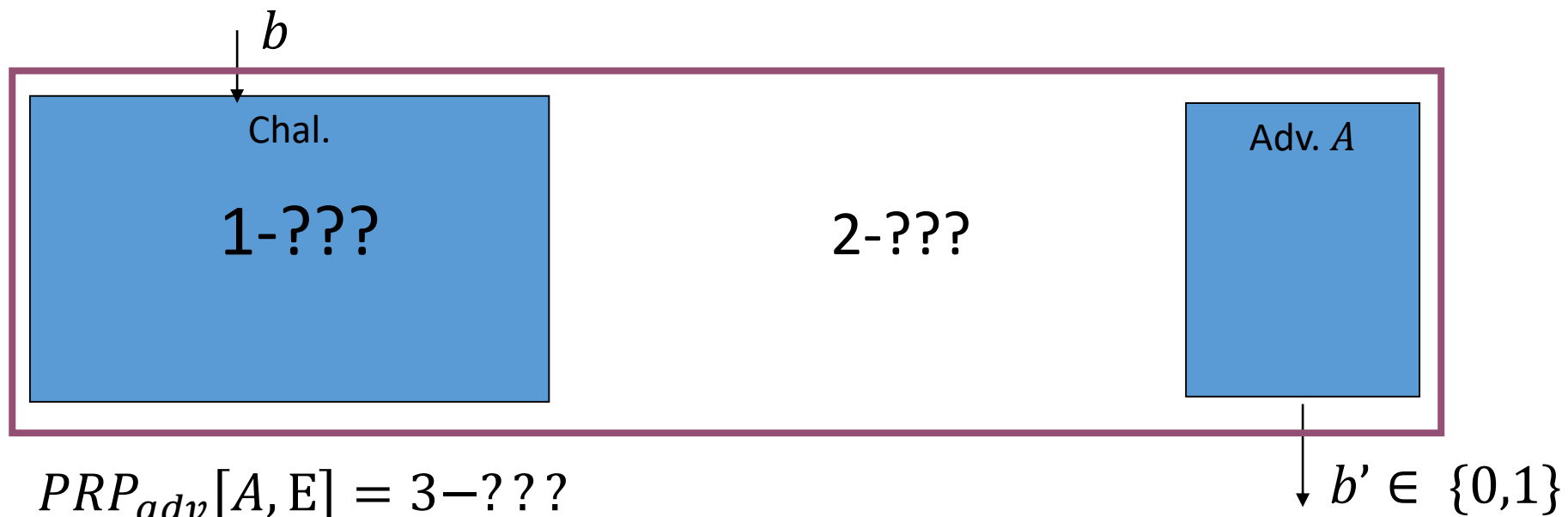


Схема работы алгоритма при зашифровании и при расшифровании

Тест.



4 - Отличия адаптивной от неадаптивной версии игры на стойкость PRP



Тест.

Схема OFB блочного шифрования,
нарисовать картинку.

- Положить телефон экраном вниз справа от себя
- Не разговаривать с соседями
- Не пользоваться конспектами и электронными устройствами
- Написать номер (по таблице) и ФИО на листочке
- Написать краткий ответ на вопрос
- Дождаться окончания теста

