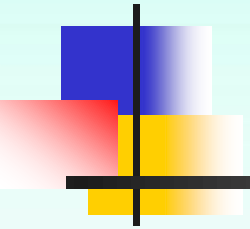
CRYPTOGRAPHY

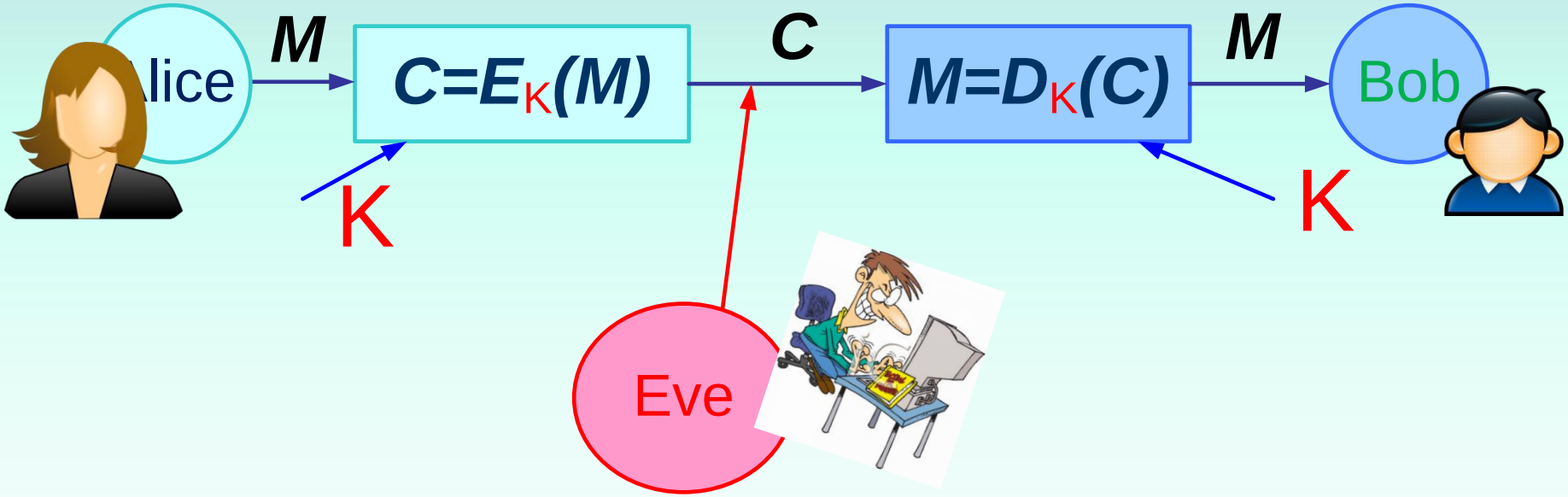


МЕТОДИ ТА ЗАСОБИ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Лек. 8 2022 КІБ-19

СТАНДАРТ DES

Data Encryption Standard



СИММЕТРИЧНЫЙ АЛГОРИТМ

→ ОДИН КЛЮЧ

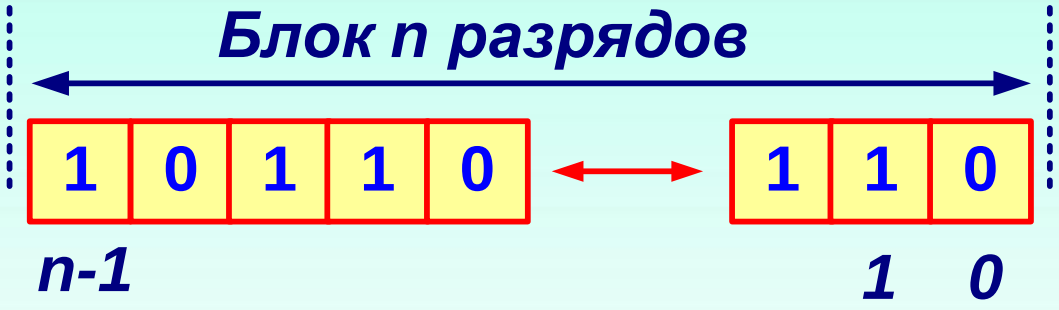
как для шифрования, так и дешифрования

$$!!!\ D_K(*) = E_K^{-1}(*)$$

$$M = D_K(E_K(M))$$

Двоичные коды и операции над ними

Двоичный блок



Представление:

- Набор (последовательность) нулей и единиц, например, *0110101010* , *n* = 10
- Полином $0*2^9 + 1*2^8 + 1*2^7 + 0*2^6 + 1*2^5 + 0*2^4 + 1*2^3 + 0*2^2 + 1*2^1 + 0*2^0$
- Целое без знака 426

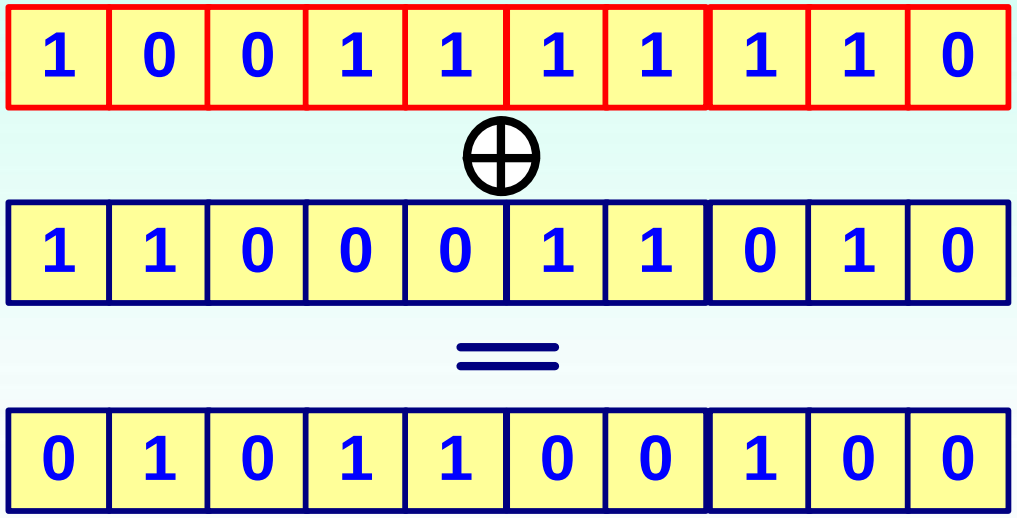
- $1*2^1 + 0*2^0 = 2$
- $1*2^2 + 1*2^1 + 0*2^0$

$MAX = 2^n - 1$

Двоичные коды и операции над ними

Операция:
Исключающее ИЛИ , Сумма по модулю 2, ⊕

	0	1
0	0	1
1	1	0



0 + 0 = 0 mod 2 = 0
1 + 0 = 1 mod 2 = 1
0 + 1 = 1 mod 2 = 1
1 + 1 = 2 mod 2 = 0

Двоичные коды и операции над ними

Свойства операции «Исключающее ИЛИ»

Замкнутость: два *n*-бит операнда дают *n*-бит результат.

Коммутативность:

$$x \oplus y = y \oplus x$$

Ассоциативность:

$$x \oplus (y \oplus z) = (x \oplus y) \oplus z$$

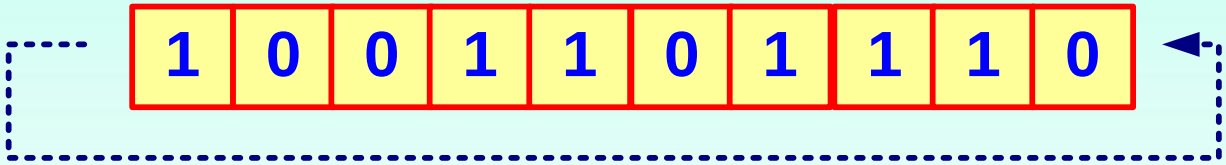
Существует нулевой (нейтральный) элемент:
0 = 000000 … . 0. $x \oplus 0 = x$

Существует аддитивная инверсия – само слово $x \oplus x = 0$**.**

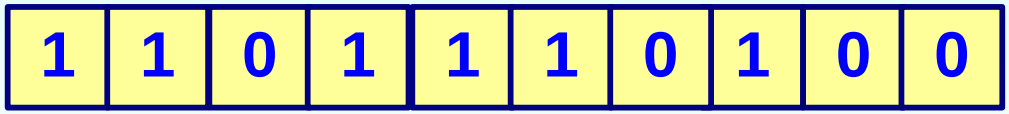
Двоичные коды и операции над ними

Операция циклического сдвига

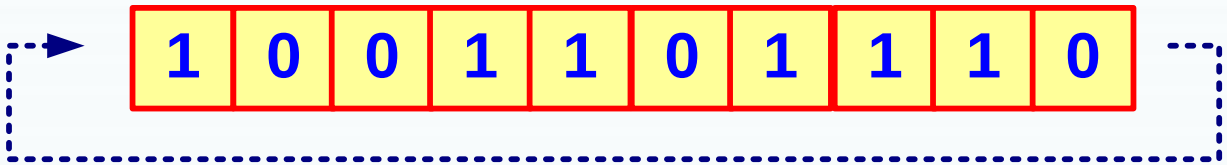
Циклический сдвиг влево на k-разрядов



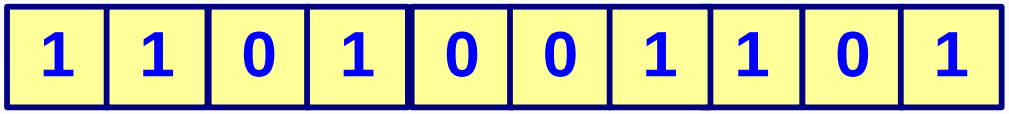
k = 3



Циклический сдвиг вправо на k-разрядов

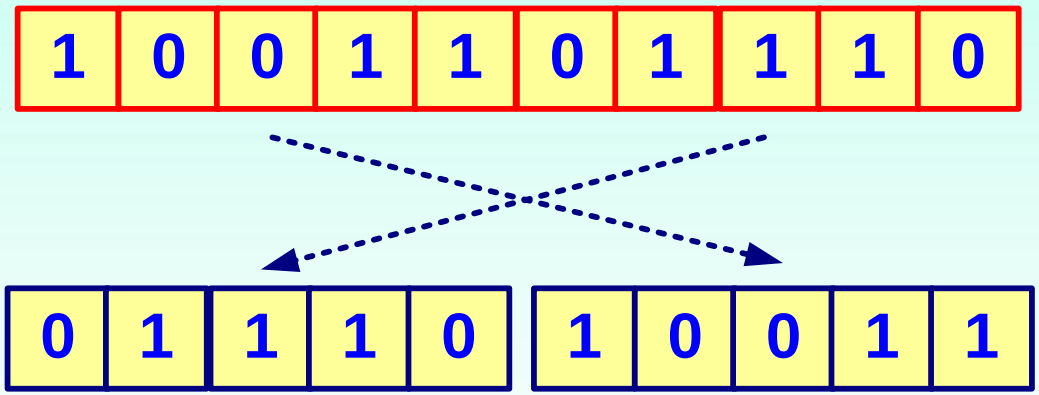


k = 3



Двоичные коды и операции над ними

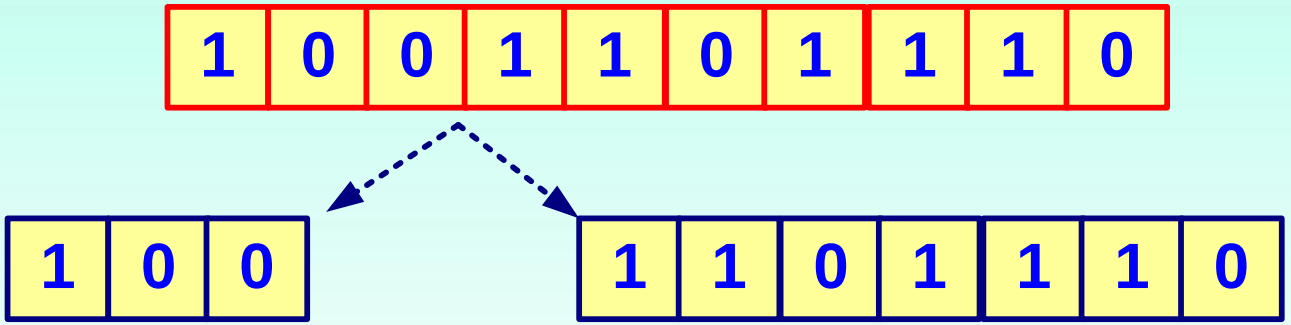
Операция замены = циклический сдвиг на k = *n*/2 разрядов. *n* – четное.



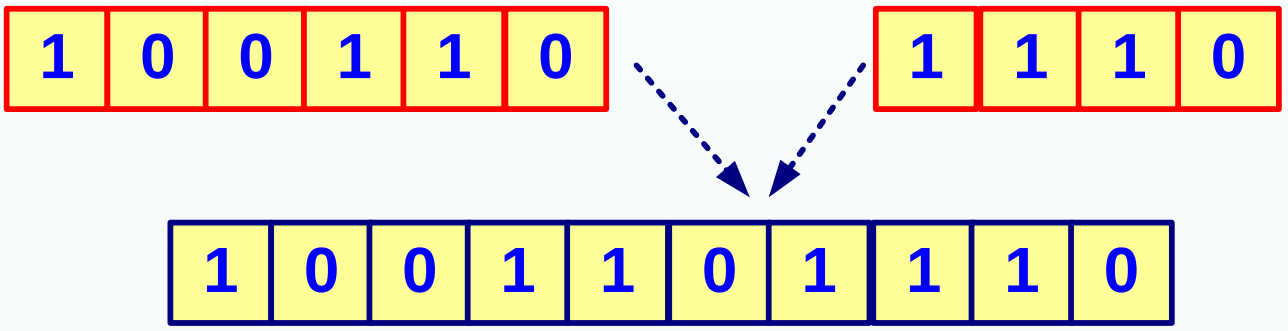
$n = 10$
$k = 5$

Двоичные коды и операции над ними

Операция разбиения

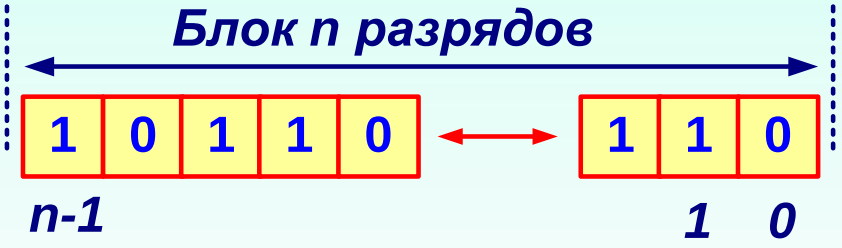


Операция объединения

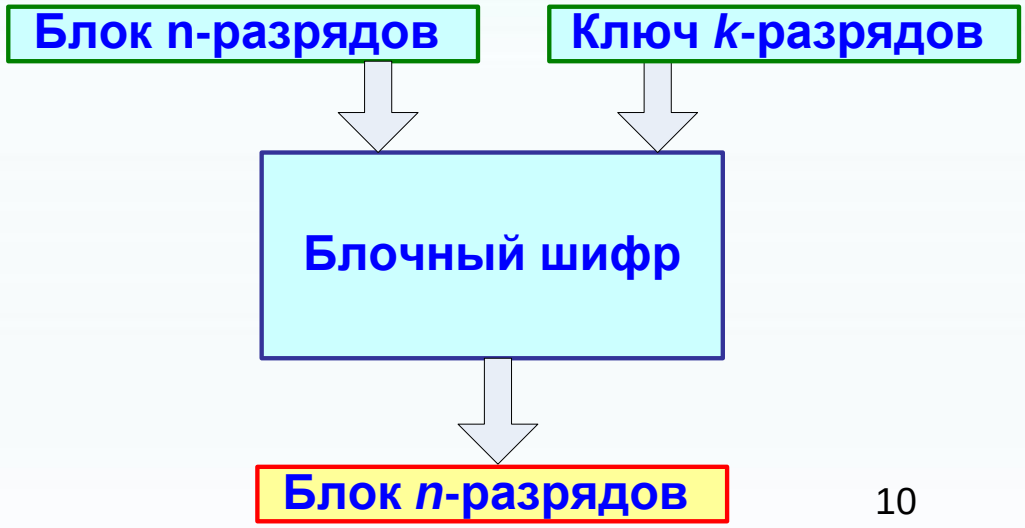


Блочные шифры

Блочный шифр → оперирует группами бит фиксированной длины — блоками, характерный размер которых меняется в пределах 64–256 бит.



На входе:
блок *n* разрядов и ключ *k* разрядов.
На выходе:
шифрованный блок *n* разрядов.



Data Encryption Standard

Алгоритм симметричного блочного шифрования.
Разработан фирмой IBM
Стандарт США, 1977 год (FIPS 46-3)

DES – блоки 64 разряда
S-DES – блоки 8 разрядов !!! студенческий

FIPS: Federal Information Processing Standards – открытые стандарты правительства США.
Для использования всеми гражданскими правительственными учреждениями США.

Базовые модули DES

1. **Модуль перестановки (транспозиции) - P-блок.**
2. **Модуль подстановки - S-блок.**
3. **Сеть (функция, смеситель) Фейстеля.**
4. **Генератор ключей**

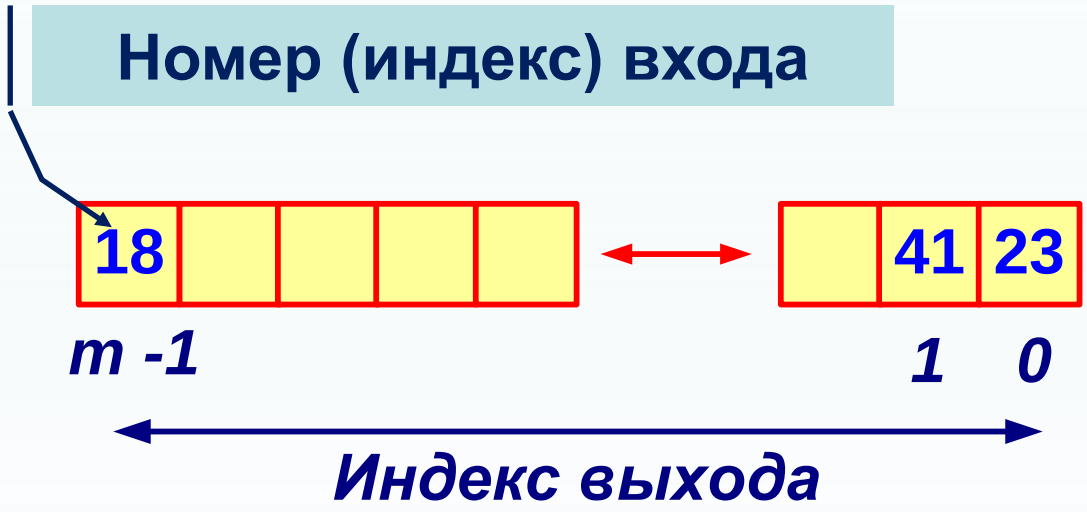
Базовые преобразования DES

P-блок: перемещает биты.

Прямой P-блок: *n* входов → *n* выходов. Задается таблицей *n X n*

P-блок расширения: *n* входов → *m* выходов, *m* > *n*. Задается таблицей *m X n*

P-блок сжатия: *n* входов → *m* выходов, *m* < *n*. Задается таблицей *n X m*.



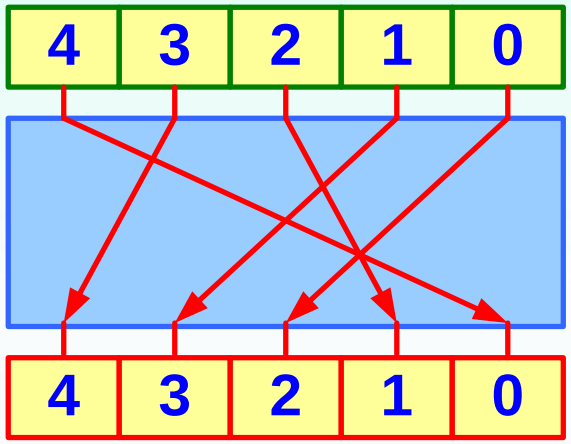
Прямой P-блок обратим, блоки сжатия и расширения - необратимы

Базовые преобразования DES

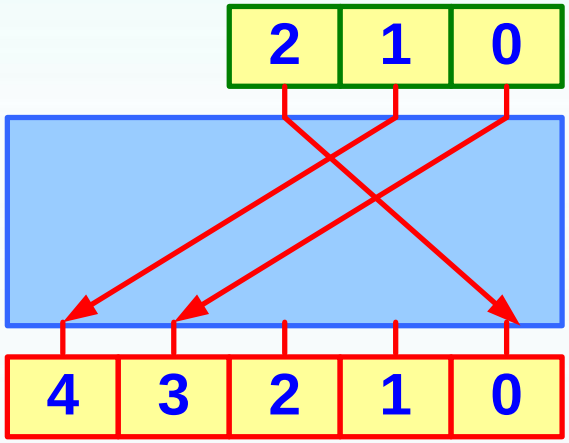
1. **Модуль перестановки (транспозиции) - P-блок.**

P-блок: перемещает биты.

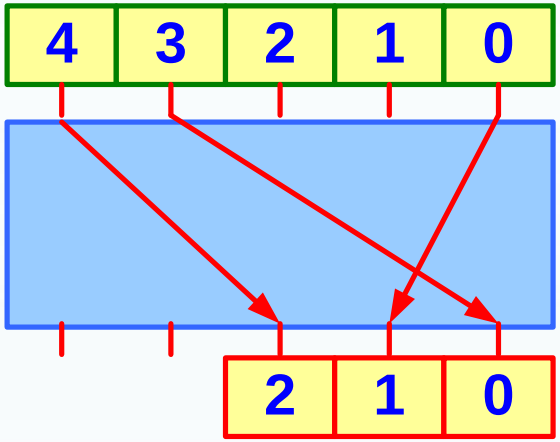
Прямой P-блок



P-блок расширения



P-блок сжатия



Базовые модули DES / S-DES

P-блоки S-DES

Блок начальной перестановки

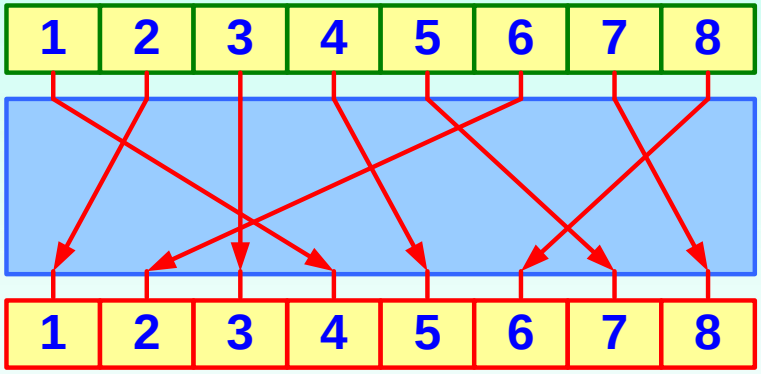


Таблица перестановок							
2	6	3	1	4	8	5	7

Блок конечной перестановки

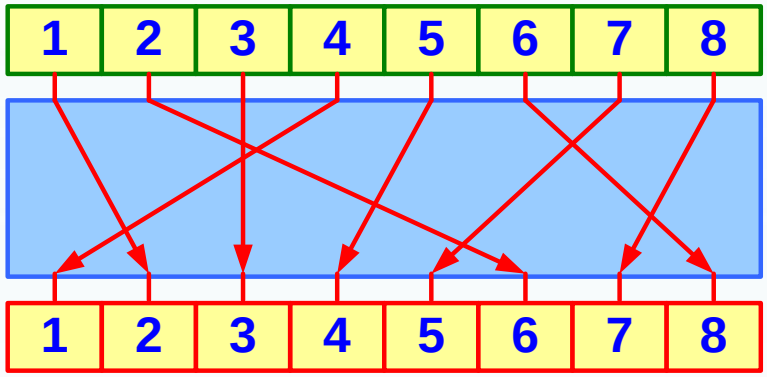


Таблица перестановок							
4	1	3	5	7	2	8	6

Базовые модули DES / S-DES

P-блоки S-DES

Блок прямой перестановки

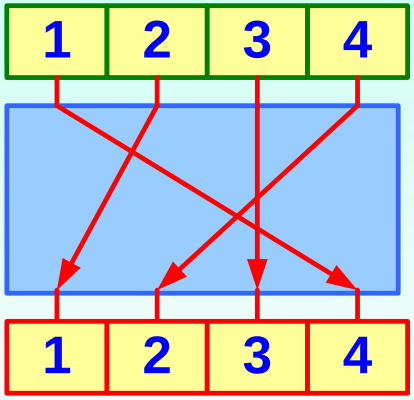


Таблица перестановок
2 4 3 1

Блок расширения

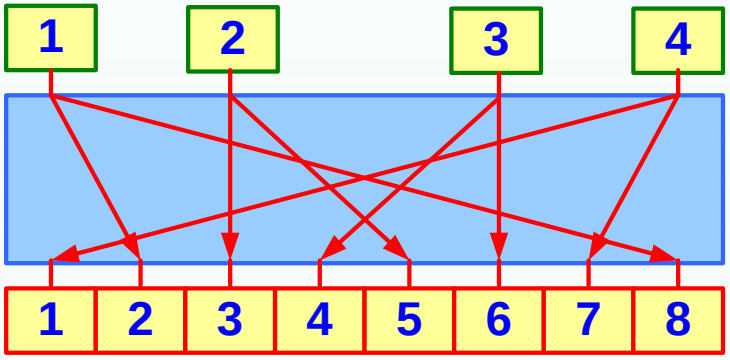
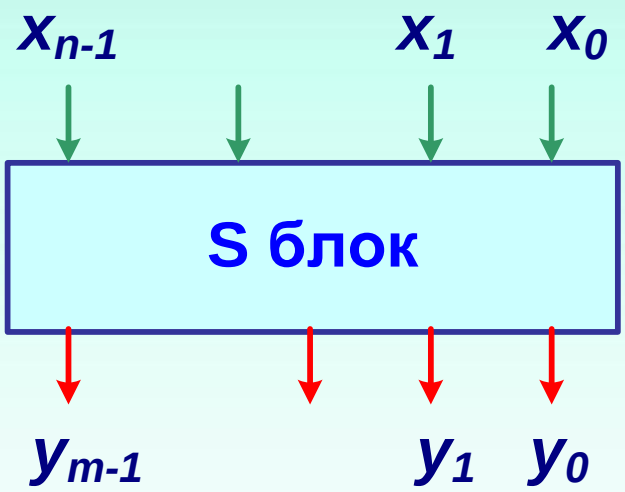


Таблица перестановок
4 1 2 3 2 3 4 1

Базовые преобразования DES

2. S-блок: шифр подстановки.



Нелинейный S-блок в общем виде:

$$y_0 = f_0(x_0, x_1, \dots, x_{n-1})$$
$$y_1 = f_1(x_0, x_1, \dots, x_{n-1})$$
$$y_{m-1} = f_{m-1}(x_0, x_1, \dots, x_{n-1})$$

Линейный S-блок: в общем виде:

$$y_0 = a_{0,0}x_0 \oplus a_{0,1}x_1 \oplus \dots \oplus a_{0,n-1}x_{n-1}$$
$$y_1 = a_{1,0}x_0 \oplus a_{1,1}x_1 \oplus \dots \oplus a_{1,n-1}x_{n-1}$$

$$y_{m-1} = a_{m-1,0}x_0 \oplus a_{m-1,1}x_1 \oplus \dots \oplus a_{m-1,n-1}x_{n-1}$$

Базовые преобразования DES

Линейный S-блок

$$\boldsymbol{X} = \boldsymbol{A} \oplus \boldsymbol{X}$$

$$\boldsymbol{A} = \begin{bmatrix} a_{0,0} & a_{0,1} & a_{0,m-1} \\ a_{1,0} & a_{1,1} & a_{1,m-1} \\ a_{n-1,0} & a_{n-1,1} & a_{n-1,m-1} \end{bmatrix}$$

$$a_{i,j} = \{0,1\}$$

Базовые преобразования DES

Линейный S-блок (пример)

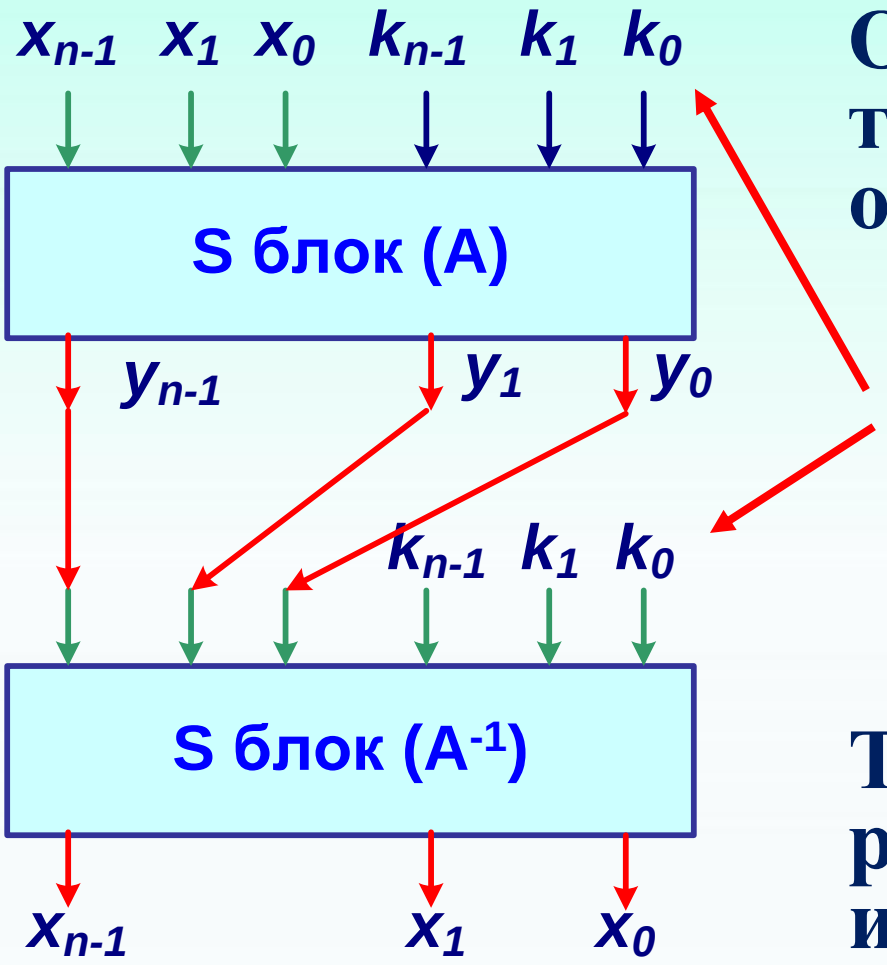
$$A = \begin{matrix} \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{1} \\ \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} \\ \mathbf{0} & \mathbf{1} & \mathbf{1} & \mathbf{0} \\ \mathbf{1} & \mathbf{0} & \mathbf{1} & \mathbf{1} \end{matrix}$$

$$y_0 = x_0 \oplus x_3$$
$$y_1 = x_0 \oplus x_1 \oplus x_2 \oplus x_3$$
$$y_2 = x_1 \oplus x_2$$
$$y_3 = x_0 \oplus x_2 \oplus x_3$$

Линейный S-блок может быть обратимым (n=m) и необратимым. Существует A^{-1} .

Базовые преобразования DES

+ **Свойства операции исключающее ИЛИ**



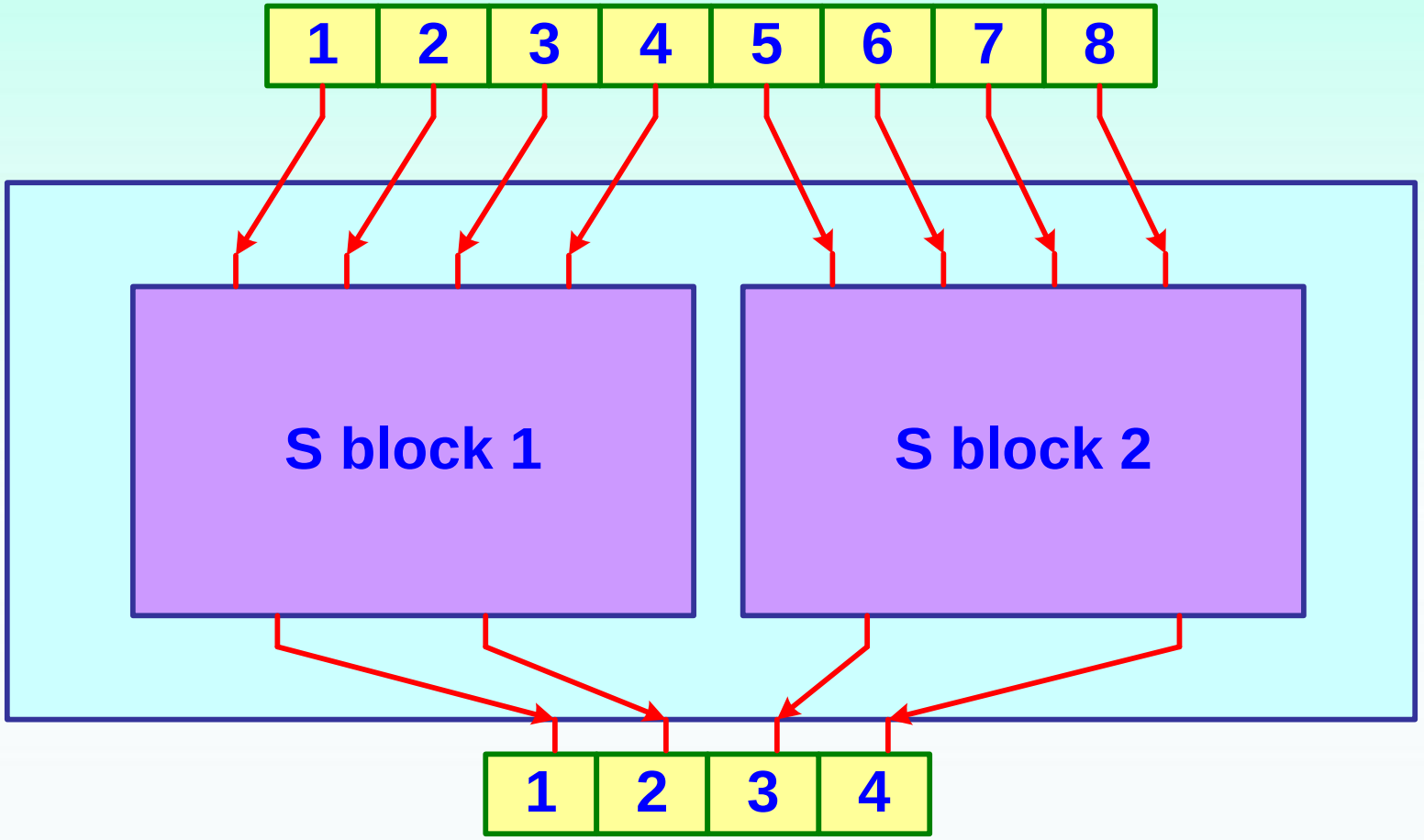
Операция обратима, только если один из операндов известен.

КЛЮЧ

То есть, если известен результат $z = x \oplus k$ и известен y , то $x = z \oplus k$.

Базовые модули DES / S-DES

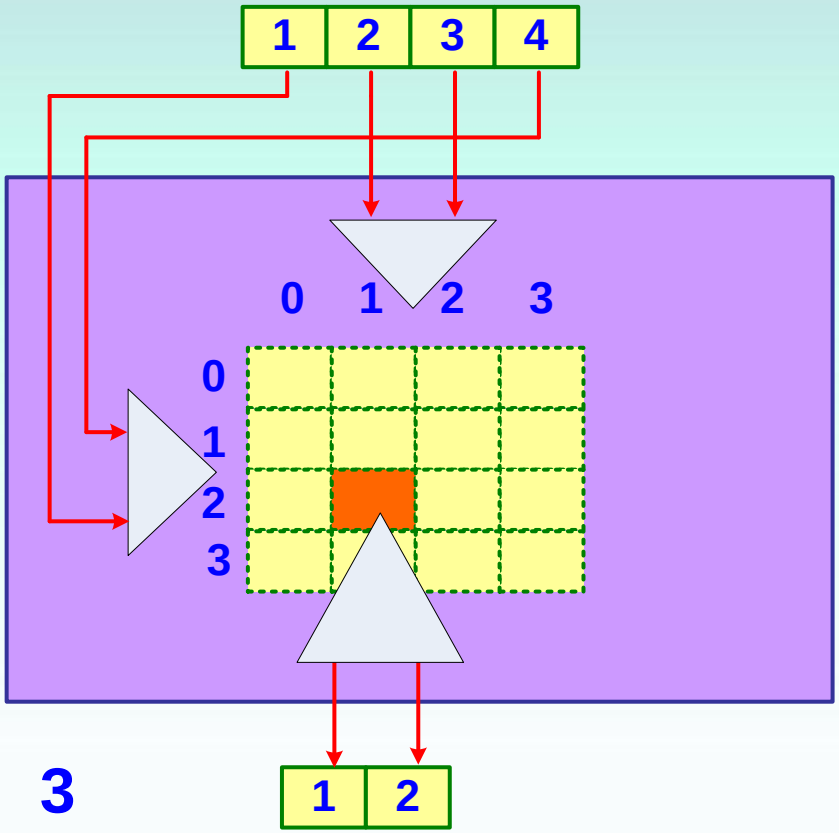
S блок = S блок 1 || S блок 2



Базовые модули DES / S-DES

S блок 1

S блок 2



Матрица S блока 1

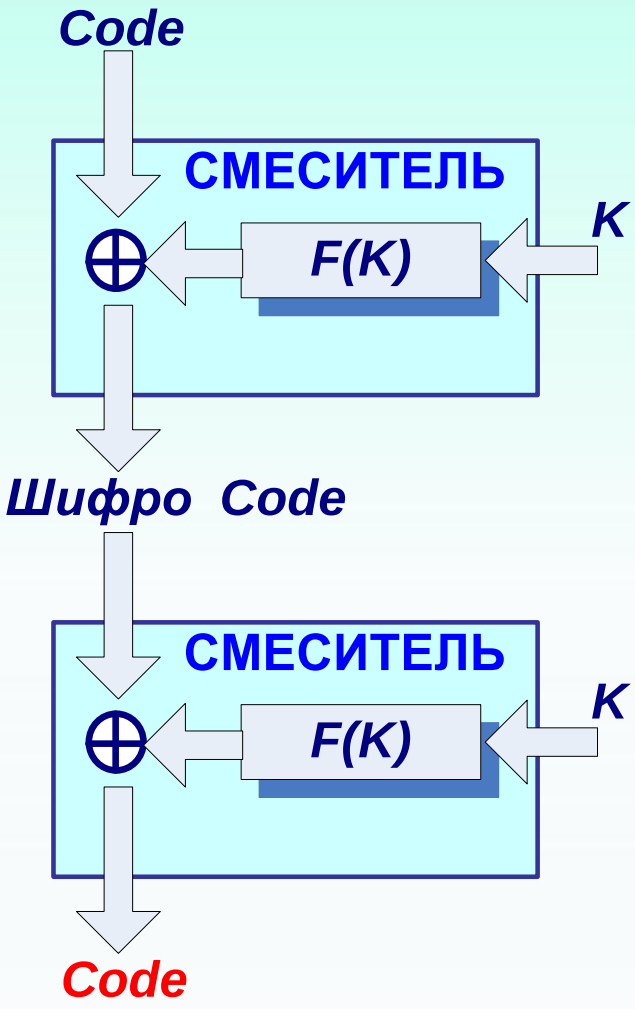
	0	1	2	3
0	1	0	3	2
1	3	2	1	0
2	0	2	1	3
3	3	1	3	2

Матрица S блока 2

	0	1	2	3
0	0	1	2	3
1	2	0	1	3
2	3	0	1	0
3	2	1	0	3

Базовые преобразования DES

Простой смеситель (сеть функция) Фейстеля.



Шифрование: ключ поступает на вход необратимой функции *F(K)*. Далее ⊕ с входным кодом.

F(K) – необратимо.

Дешифрование: повторение операций. На вход – шифрокод. На выходе – исходный код

Базовые преобразования DES

Шифрование.

$$CipherCode = CODE \oplus F(K)$$

Дешифрование.

$$CODEout = CipherCode \oplus F(K)$$
$$CODEout = CODE \oplus F(K) \oplus F(K)$$
$$CODEout = CODE \oplus [F(K) \oplus F(K)]$$

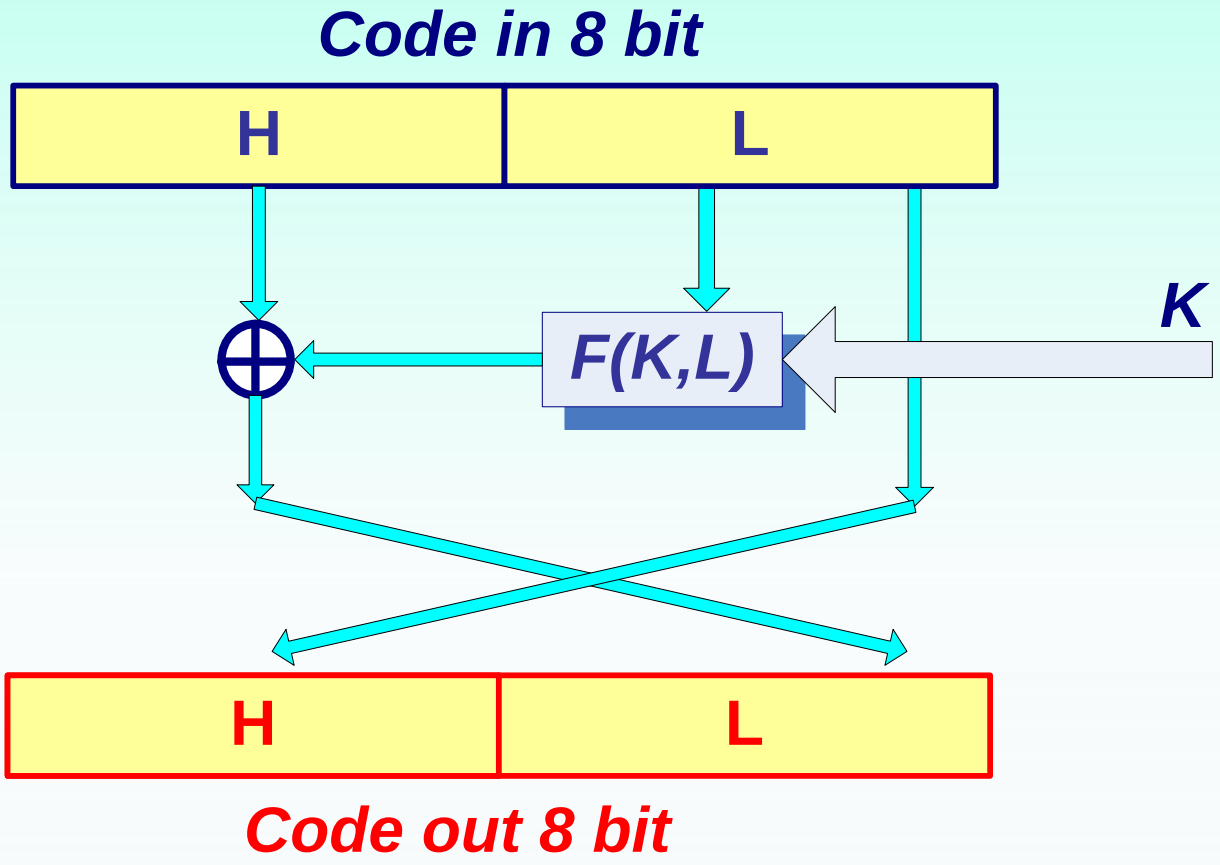
$$[F(K) \oplus F(K)] = 0$$

$$CODEout = CODE \oplus 0 = CODE$$

Смеситель Фейстеля имеет необратимый элемент, но сам является обратимым.

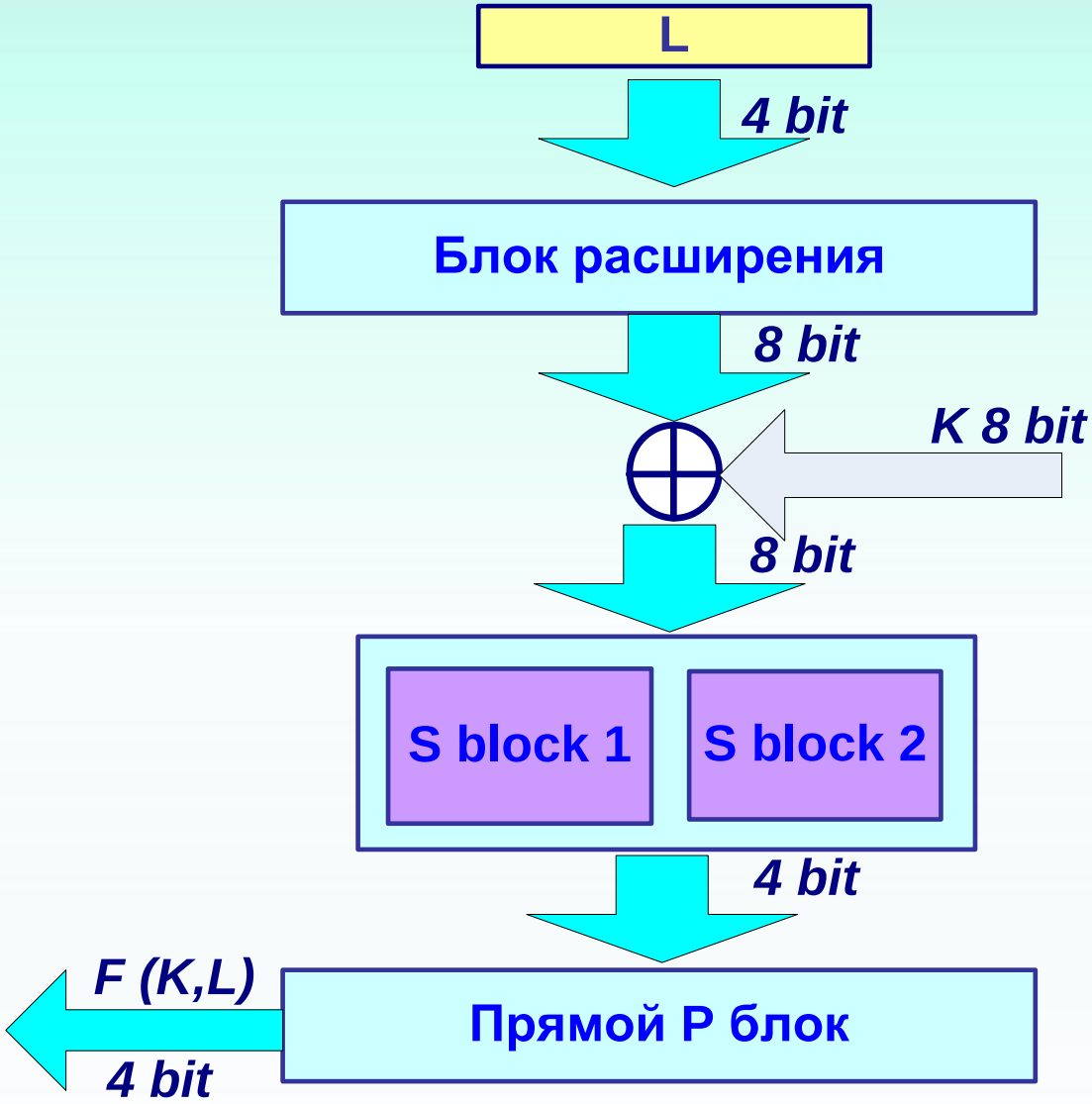
Базовые модули DES / S-DES

Смеситель Фейстеля.

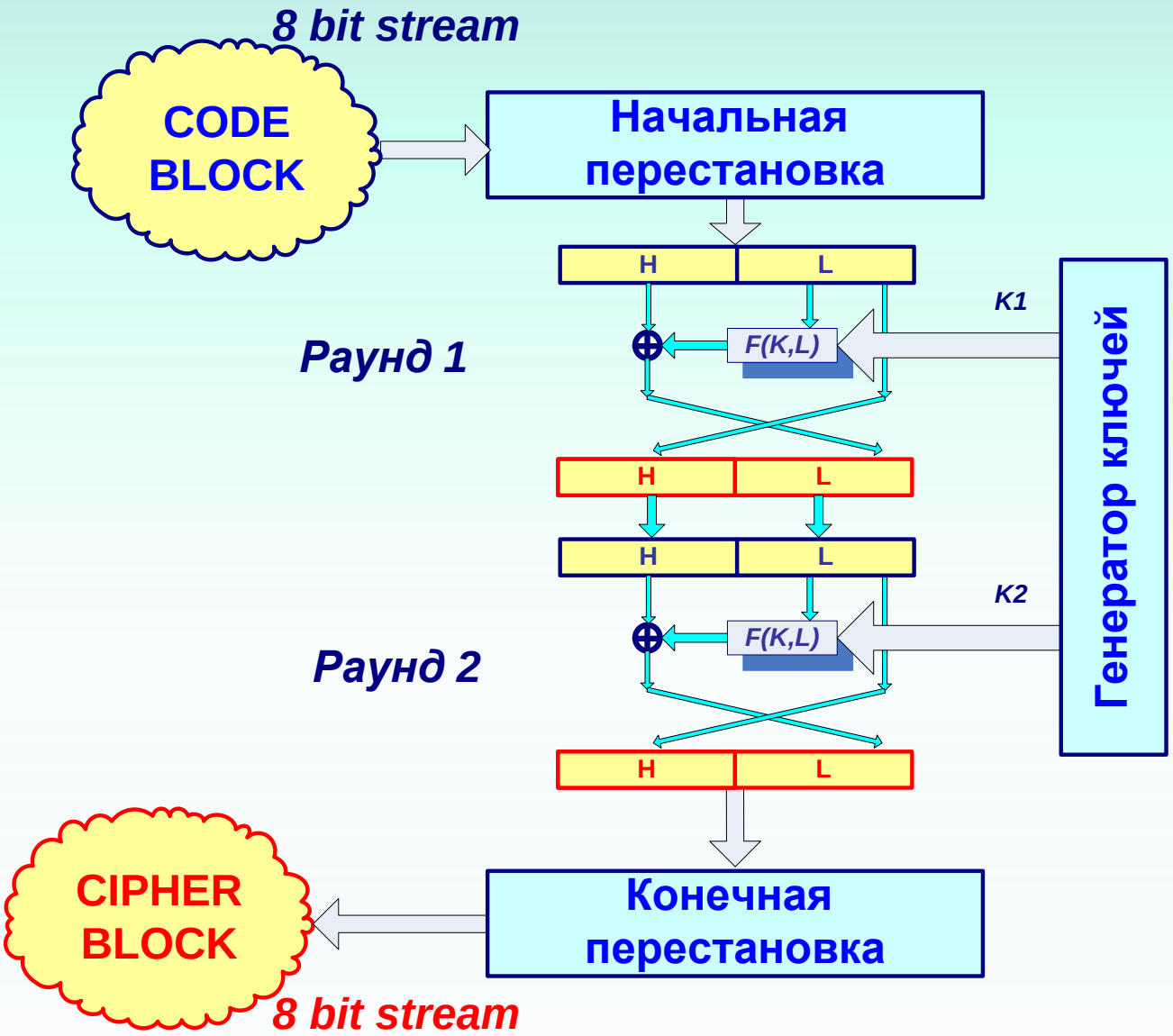


Базовые модули DES / S-DES

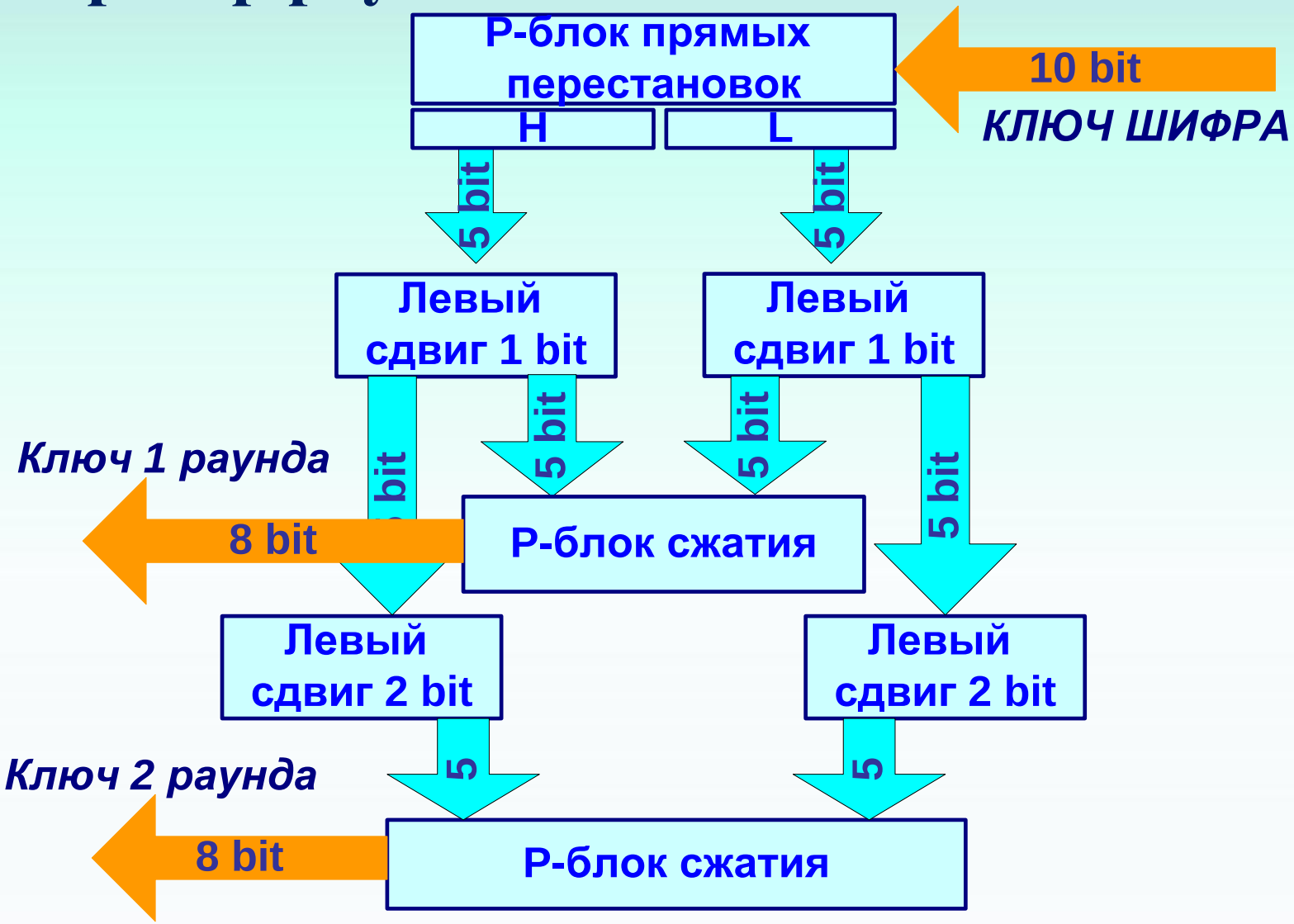
Смеситель Фейстеля. Функция F



Структура S-DES



Структура S-DES
Генератор раундовых ключей



Структура S-DES

Генератор раундовых ключей

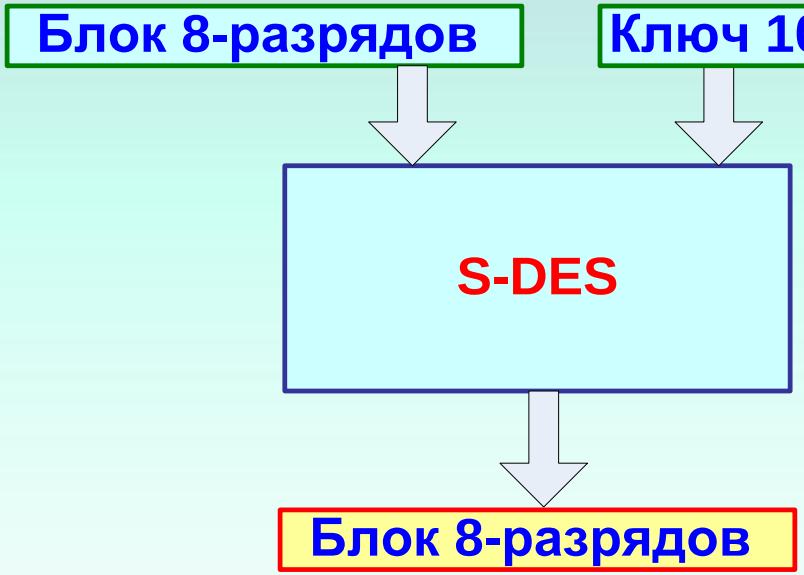
Таблица прямого P-блока

3	5	2	7	4	10	1	9	8	6

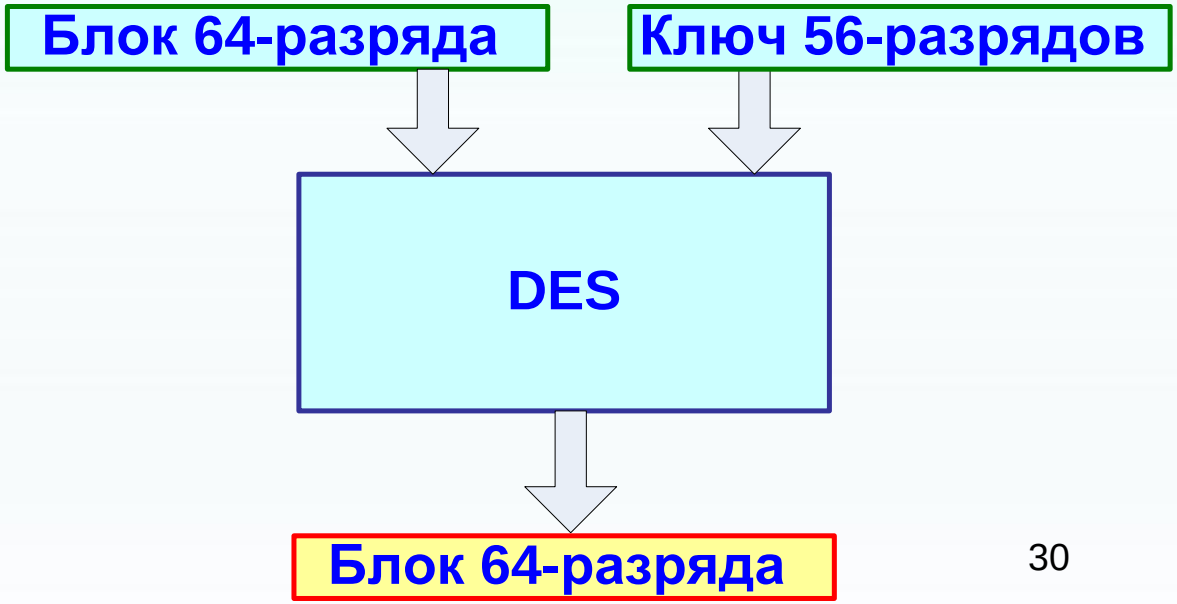
Таблица P-блока сжатия

6	3	7	4	8	5	10	9

S-DES → DES

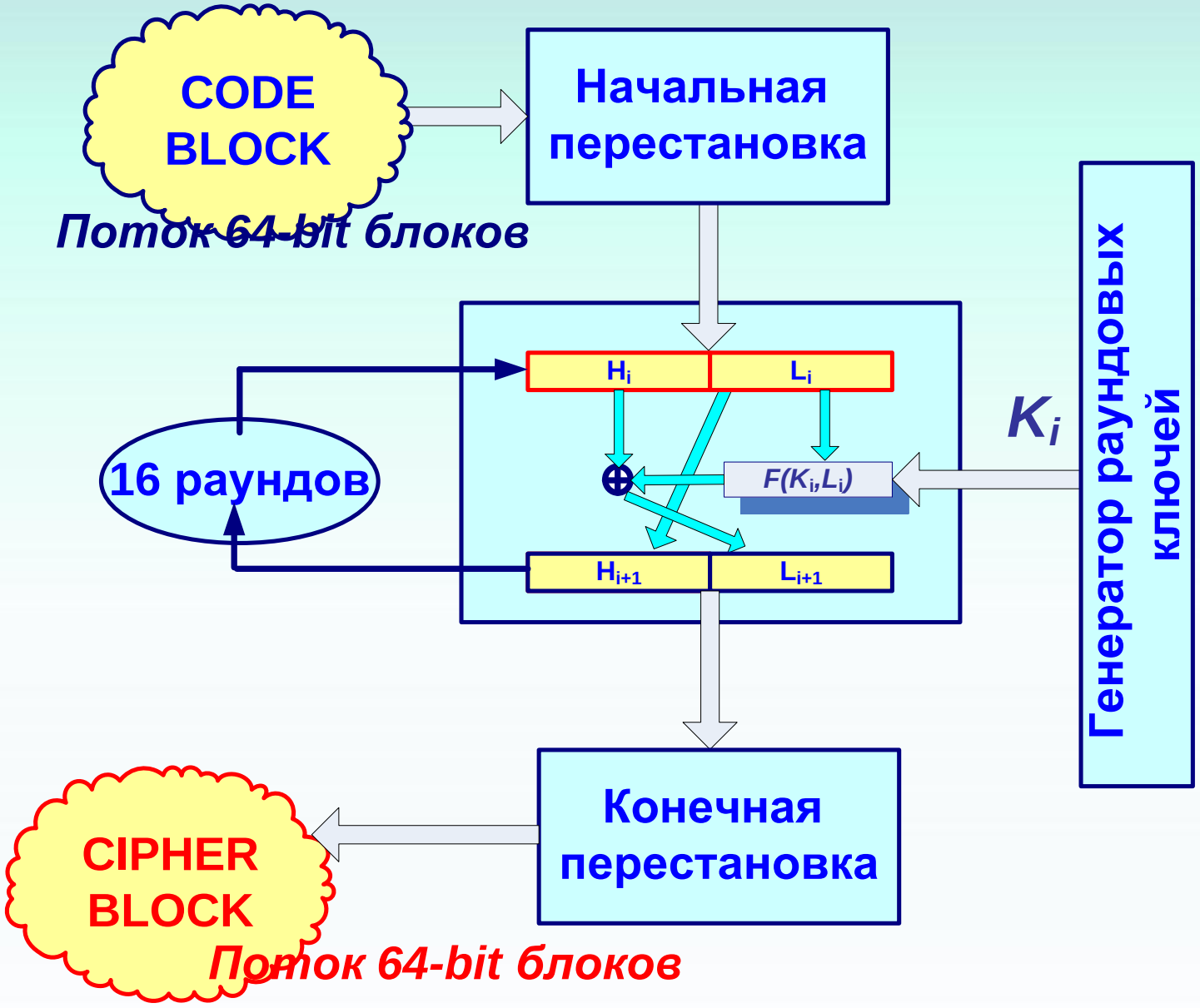


2 раунда



16 раундов

Структура DES



Вопросы:

- Поясните общность представления информации в виде множества двоичных кодов. Определите двоичный код и его численное представление.
- Укажите определение и свойства операции XOR над двоичными кодами.
- Определите функцию P-блока, его разновидности и свойства.
- Определите функцию S-блока, его свойства.
- Поясните организацию смесителя Фейстеля.
- Поясните функционирование вычислителя функции Фейстеля.

Вопросы:

- Поясните организацию и функционирование генератора раундовых ключей.
- Определите различие между стандартами DES и S-DES.
- Укажите основные характеристики стандарта DES.

ЛИТЕРАТУРА

Нечаев В.И. Элементы криптографии (Основы теории защиты информации).- Учеб. пособие. – М.:, ВШ., 1999.- 109 с.

Введение в криптографию. **Под общ. ред. В.В.Ященко.** – 4-е изд., доп. М.: МЦНМО, 2012 – 348 с. ISBN 978-5-4439-0026-1

ЛИТЕРАТУРА

Венбо Мао. Современная криптография: теория и практика.—М.: Издательский дом «Вильямс», 2005.—768 с.: ил. ISSN 5-8459-0847-7 (рус.)

Шнайер Б. Прикладная криптография. Протоколы, алгоритмы и исходный код на Си. – Москва: Вильямс, 2016. 1024 с.

ЛИТЕРАТУРА

Francisco Rodriguez-Henriquez, N.A. Saqib, A. Diaz-Perez, Cetin Kaya Koc.

Cryptographic Algorithms on Reconfigurable Hardware. - Springer, 2006.

A. Menezes, P. van Oorschot, S. Vanstone.

Handbook of Applied Cryptography.- CRC Press, 1996.

END # 8