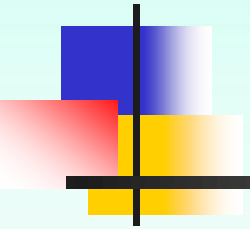
CRYPTOGRAPHY

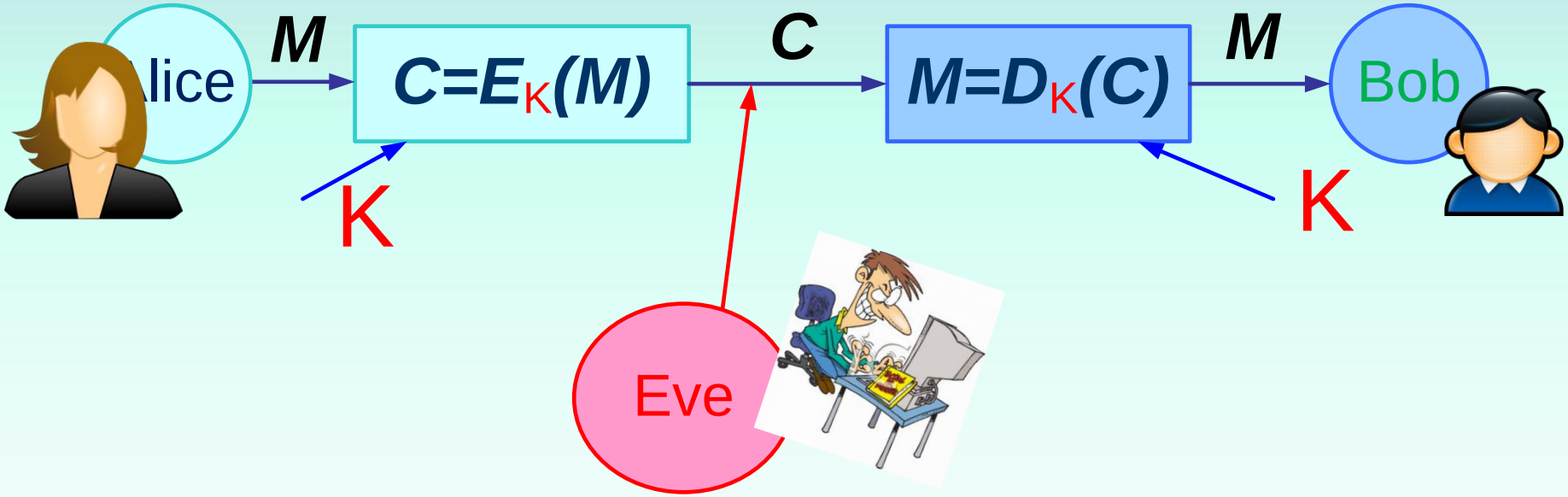


МЕТОДИ ТА ЗАСОБИ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Лек. 9 2022 КІБ-19

СТАНДАРТ DES

Data Encryption Standard



СИММЕТРИЧНЫЙ АЛГОРИТМ

→ ОДИН КЛЮЧ

как для шифрования, так и дешифрования

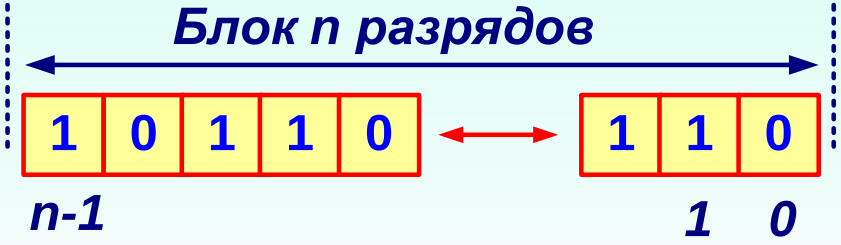
$$!!!\ D_K(*) = E_K^{-1}(*)$$

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

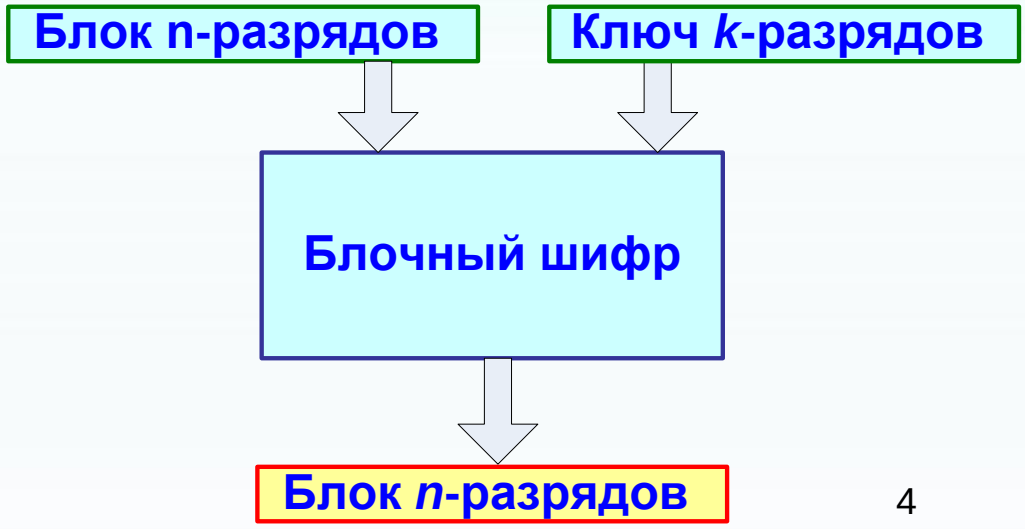
Data Encryption Standard

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

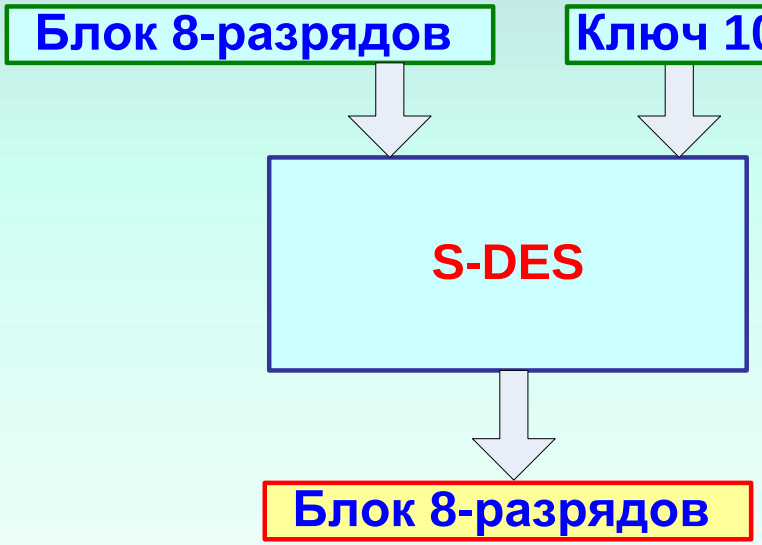
DES – блоки 64 разряда
S-DES – блоки 8 разрядов



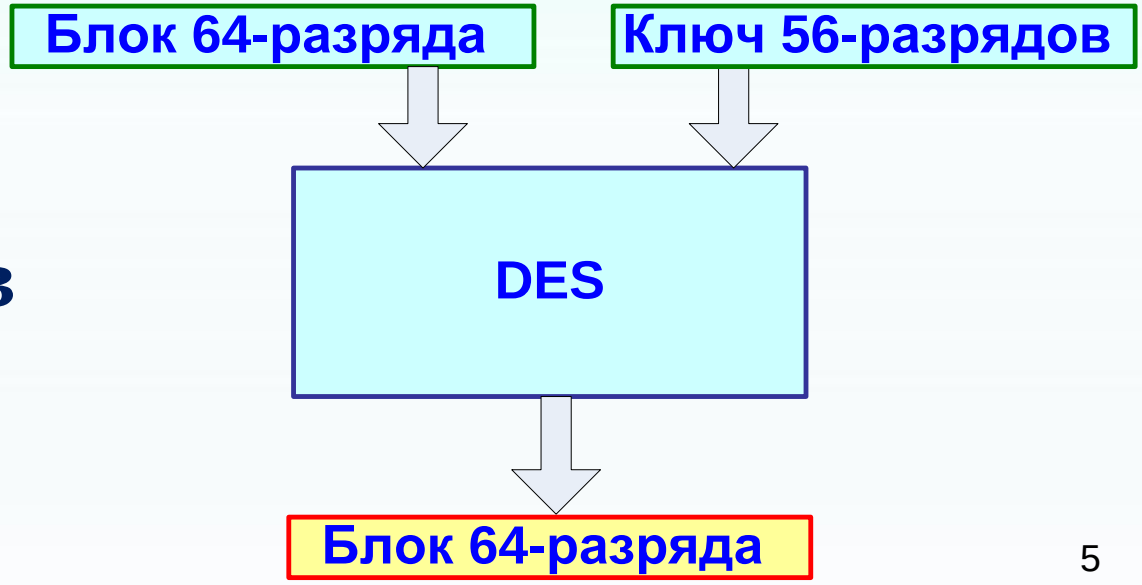
На входе:
блок *n* разрядов и ключ *k* разрядов.
На выходе:
шифрованный блок *n* разрядов.



S-DES → DES

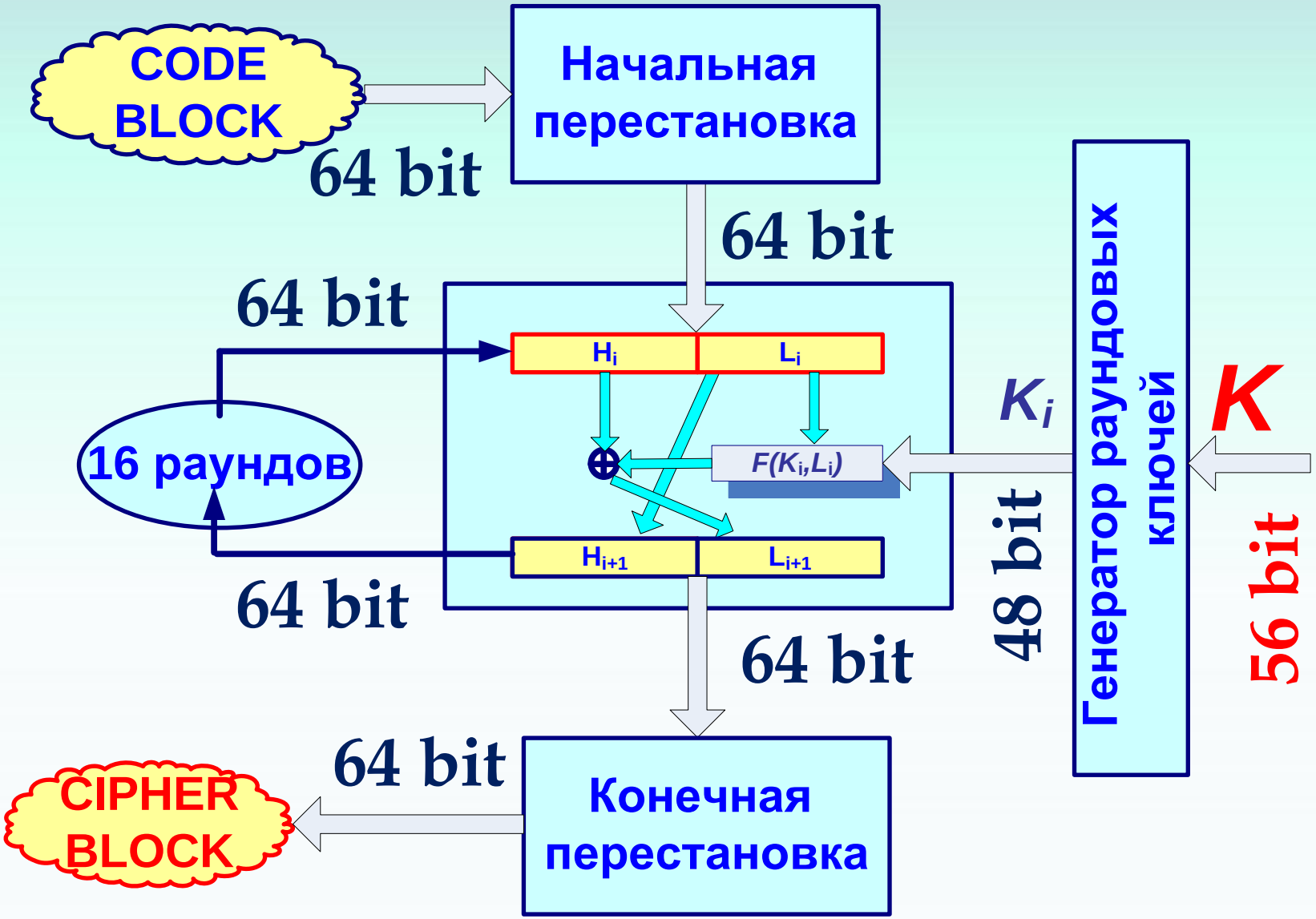


2 раунда



16 раундов

Структура DES



Элементы DES

Таблица начальной перестановки (IP)

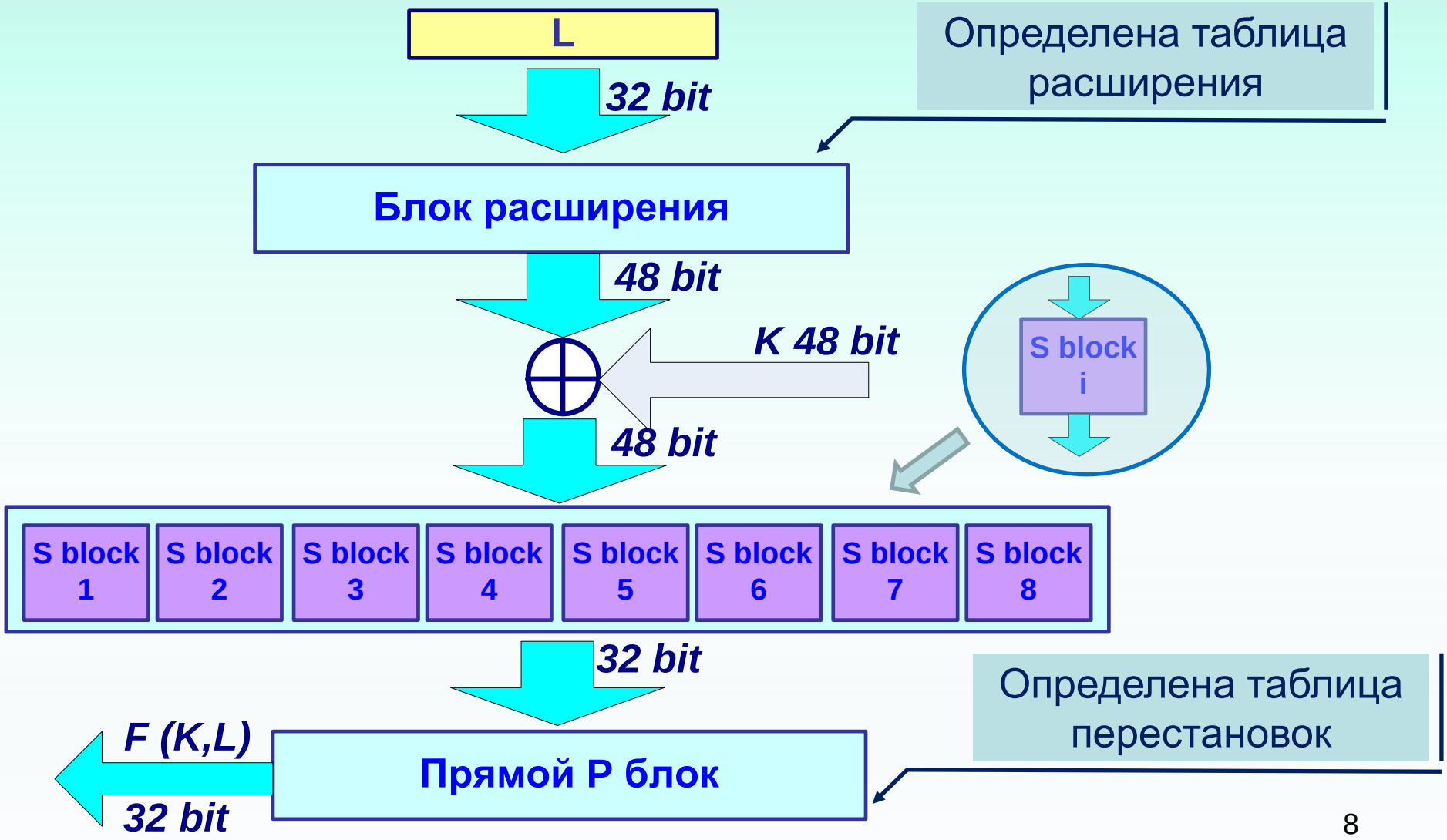
58	50	42	34	26	18	10	2	60	52	44	36	28	20	12	4
62	54	46	38	30	12	14	6	64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1	59	51	43	35	27	19	11	3
61	53	37	37	29	21	13	5	63	55	47	39	31	23	15	7

Таблица конечной перестановки (IP^{-1})

40	8	48	16	56	24	64	32	39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30	37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28	35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26	33	1	41	9	49	17	57	25

Элементы DES

Функция Фейстеля *F(K,L)*



Элементы DES

S блок

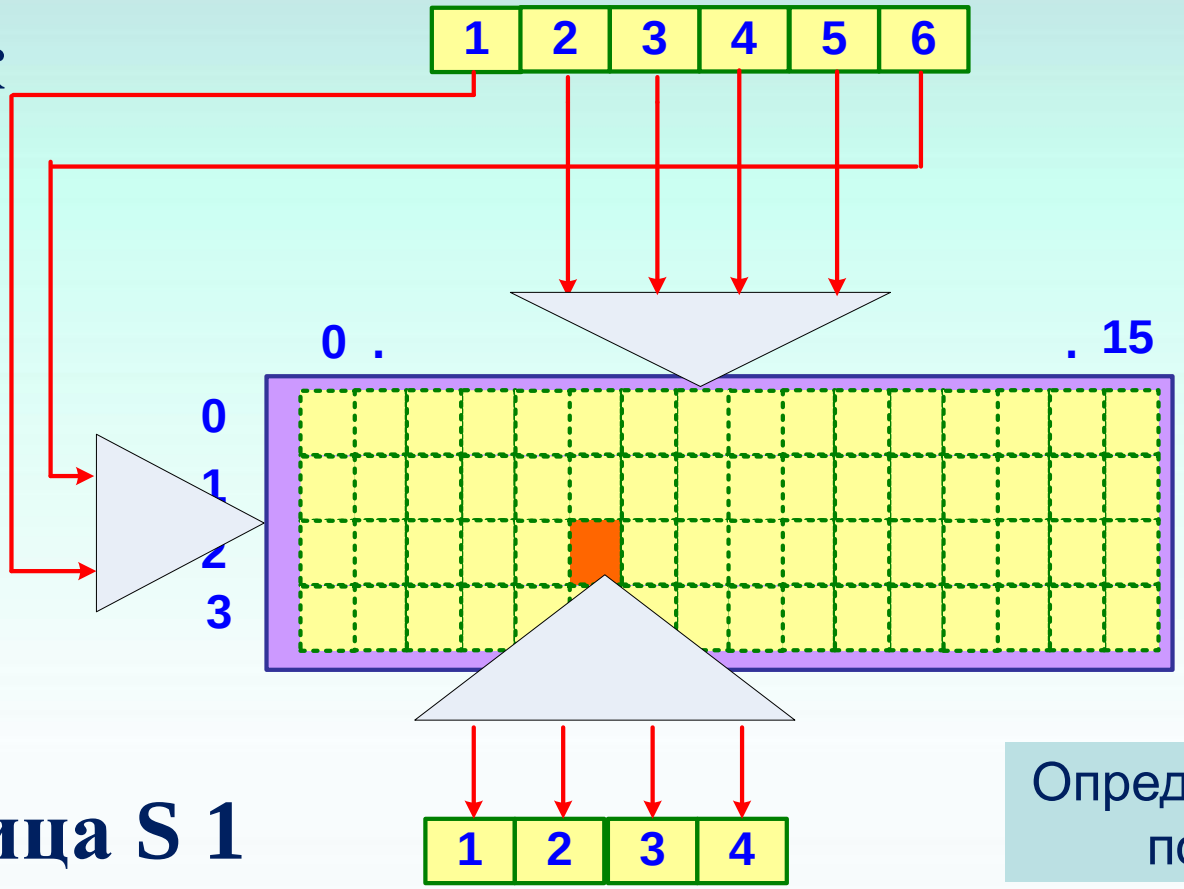


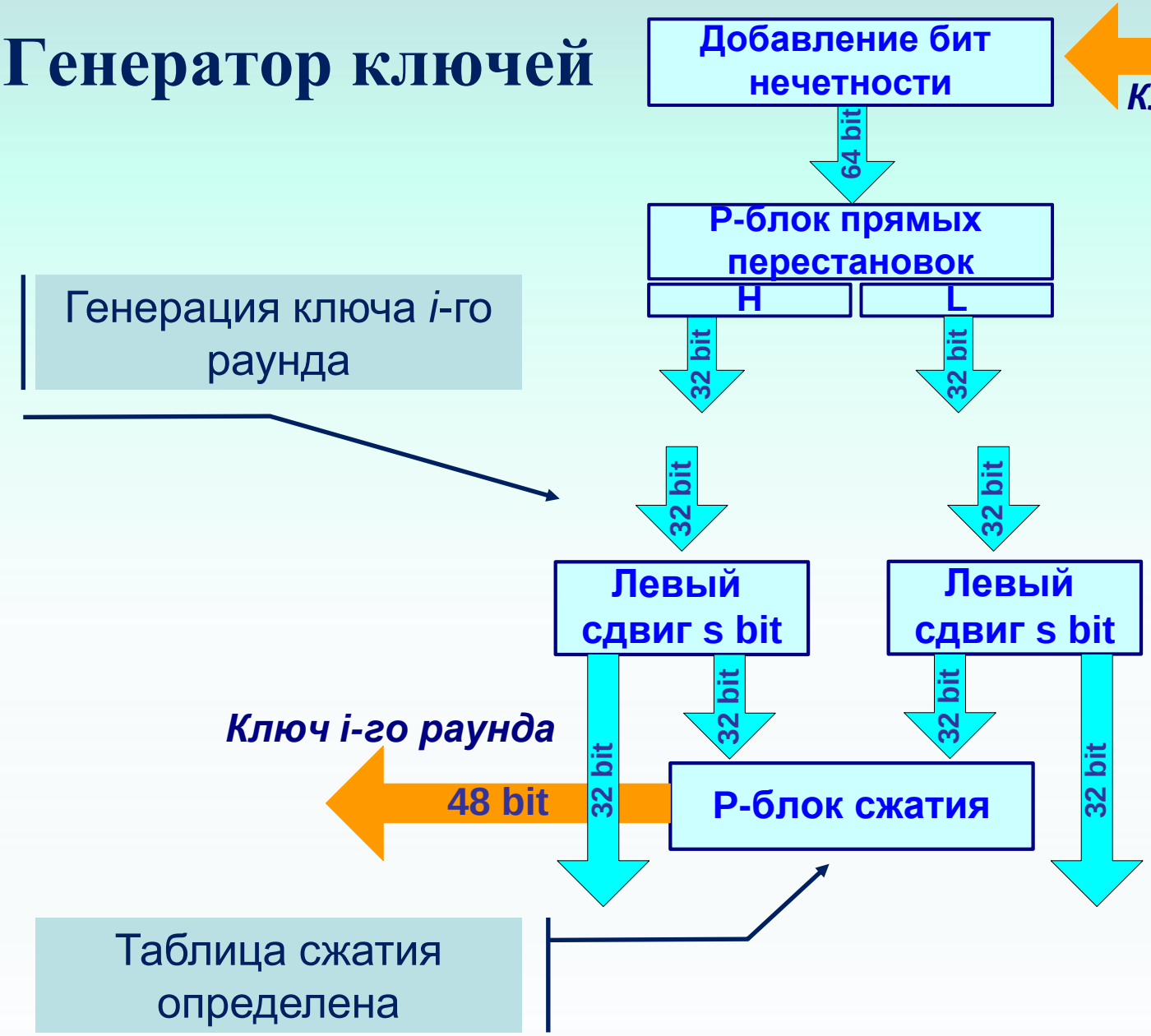
Таблица S 1

Определено 8 таблиц подстановок

14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

Элементы DES

Генератор ключей



Раунд	S
1	1
2	1
3	2
4	2
5	2
6	2
7	2
8	2
9	1
10	2
11	2
12	2
13	2
14	2
15	2
16	1

Режимы использования DES

Режим электронной кодовой книги (ECB – electronic codebook).
Стандартный режим шифрования. Текст разбивается на блоки и блоки отдельно шифруются.

Режим сцепления блоков (CBC – cipher block chaining).
Каждый очередной блок открытого текста перед шифрованием складывается по **mod2** с предыдущим блоком зашифрованного текста.

Режимы использования DES

Режим обратной связи по шифротексту (CFB – cipher feedback).
Задается начальный код синхроссылки C_0. Далее с помощью DES формируется «гамма» блоков.

$$C_i = Z_i \oplus C_i \,, \qquad \text{где} \quad Z_i = DES(C_{i-1});$$

Режим обратной связи по выходу (OFB – output feedback).
Задается начальный код синхроссылки Z_0. Далее с помощью DES формируется «гамма» блоков.

$$C_i = Z_i \oplus C_i \,, \qquad \text{где} \quad Z_i = DES(Z_{i-1});$$

В ***CFB*** *и* ***OFB*** *– DES используешься только как шифратор.*

Криптостойкость DES

Криптостойкость определяется длиной ключа.
Мощность множества ключей

$$\|K\| = 2^n$$

Здесь n - разрядность секретного ключа.
Атака грубой силы требует перебора 2^n вариантов. Для $n=56$, вариантов $= 7.2\ 10^{16}$

Оценка:

Год	Название	Флопс	Время перебора
1949	Кило	10^3	2314814 лет
1964	Мега	10^6	2380 лет
1987	Гига	10^9	2,3 года
1997	Тера	10^{12}	20 часов
2008	Пета	10^{15}	100 секунд
2021 ??	Экса	10^{18}	0,07 секунды

Криптостойкость DES

Криптостойкость определяется длиной ключа.

Мощность множества ключей

$$\|K\| = 2^n$$

Атака грубой силы:

для $n=256$, мощность $= 1.1\ 10^{77}$

Оценка:

Год	Название	Флопс	Время перебора
2008	Пета	10^{15}	$3{,}6\ 10^{54}$ лет
2021 ??	Экса	10^{18}	$3{,}6\ 10^{51}$ лет

Криптостойкость DES

Атака «линейный криптоанализ»:
Известны открытые тексты
в количестве 2^{43} → требуется 2^{43} операций .

Атака «дифференциальный криптоанализ»:
Известны открытые тексты
в количестве 2^{55} → требуется 2^{55} операций .

!!! Объем памяти для хранения открытых текстов

Криптостойкость DES

«Слабые ключи»: (4 ключа)

$$k \longrightarrow DES_k\left(DES_k(X)\right) = X$$

СЛАБЫЙ КЛЮЧ (Hex)
0101 0101 0101 0101
FEFE FEFE FEFE FEFE
1F1F 1F1F 1F1F 1F1F
E0E0 E0E0 E0E0 E0E0

«Частично слабые ключи»: (6 пар)

$$(k_1, k_2) \longrightarrow DES_{k1}\left(DES_{k2}(X)\right) = X$$

КЛЮЧ 1 (Hex)	КЛЮЧ 2 (Hex)
01FE 01FE 01FE 01FE	FE01 FE01 FE01 FE01
1FE0 1FE0 1FE0 1FE0	E0F1 E0F E0F E0F
……	……..

Шифры на основе сети Фейстеля

Название	Год	Раунд	Длина ключа	Размер блока
Lucifer	1971	16	48/64/128	48/32/128
DES	1977	16	56	64
Triple DES	1978	32/48	112/168	64
RC5	1994	1-255	0-2040 (128)	32/64/128
RC6	1998	20	128/192/256	128
KASUMI	1999	8	128	64
RTEA	2007	48/64	128/256	64

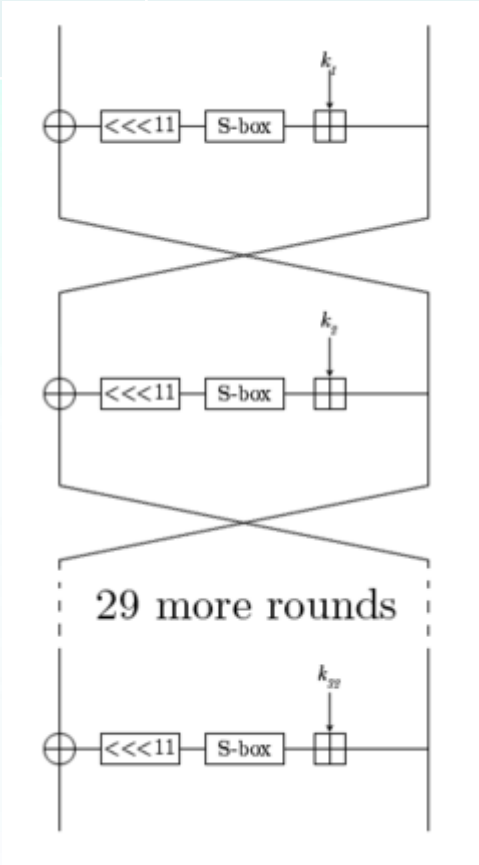
Далеко не все…

Шифры на основе сети Фейстеля

Название	Год	Раунд	Длина ключа	Размер блока
ГОСТ 28147-89	1989	4-32	256	64

Приказом Госпотребстандарта Украины №495 от 22.01.2008 г ГОСТ 28147-89 был переиздан на территории Украины и введён в действие с 1 февраля 2009 года под наименованием ДСТУ ГОСТ 28147:2009

Согласно текущим приказам, ДСТУ ГОСТ 28147:2009 будет действовать до 01.01.2022 года.
Замена – ДСТУ 7624:2014 (шифр «Калина»)



Вопросы:

- Поясните функционирование вычислителя функции Фейстеля в стандарте DES.
- Определите функцию S-блоков стандарта DES и его характеристики.
- Поясните организацию смесителя Фейстеля стандарта DES.
- Укажите режимы использования DES и их различия.
- Охарактеризуйте криптостойкость стандарта DES.

ЛИТЕРАТУРА

Block cipher cryptographic system. US patent US3798359A (1971).- *https://patents.google.com/patent/US3798359*

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 # 9