Инновационный Евразийский университет

Кафедра
«Энергетика, металлургия и информационные технологии»

СЛАЙД-ЛЕКЦИЯ

по дисциплине

«Основы информационной безопасности»

Тема: Упрощенный S-DES

Специальность: 5В070400 «Вычислительная техника и программное обеспечение»

Разработчик:
старший преподаватель, м.и. И.И. Ляшенко

План лекции:

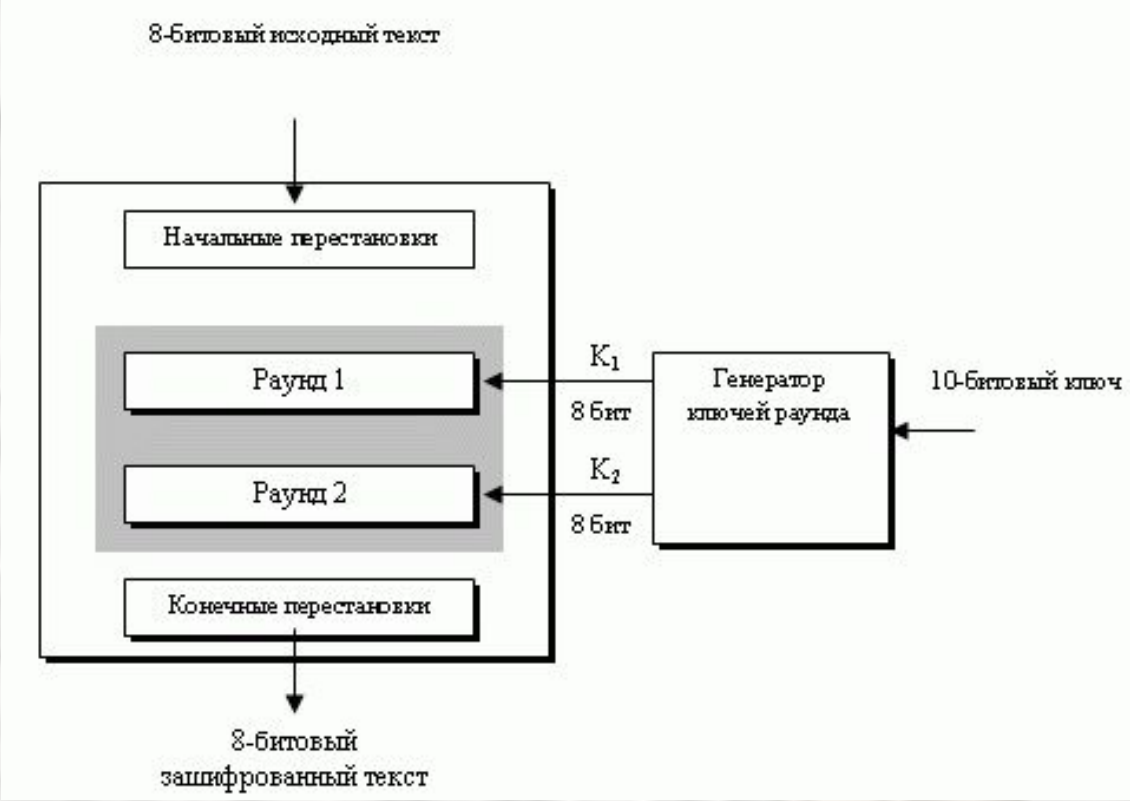
1. Алгоритм S-DES

2. Пример шифрования S-DES

1. Алгоритм S-DES

Алгоритм S-DES – это специфический вариант алгоритма DES, разработанный с учебными целями. Алгоритм шифрует данные 8-битными блоками с использованием 10-битного ключа. S-DES является как бы «уменьшенной» вариацией DES, в которой используются преобразования, аналогичные преобразованиям DES.

Как и в DES, в алгоритме S-DES выполняются начальная и финальная перестановки с аналогичным принципом действия.



Начальная и конечная перестановки:

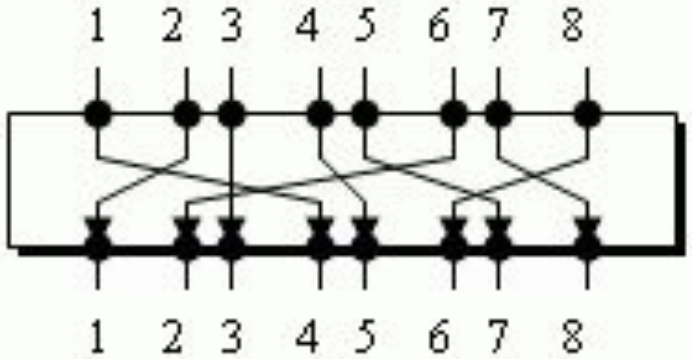


Таблица начальной перестановки

2	6	3	1	4	8	5	7

2 раунда

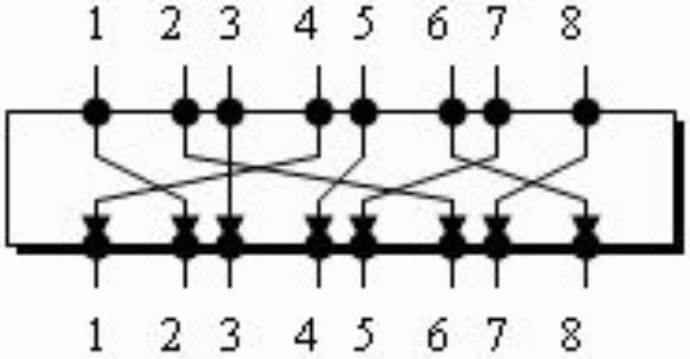
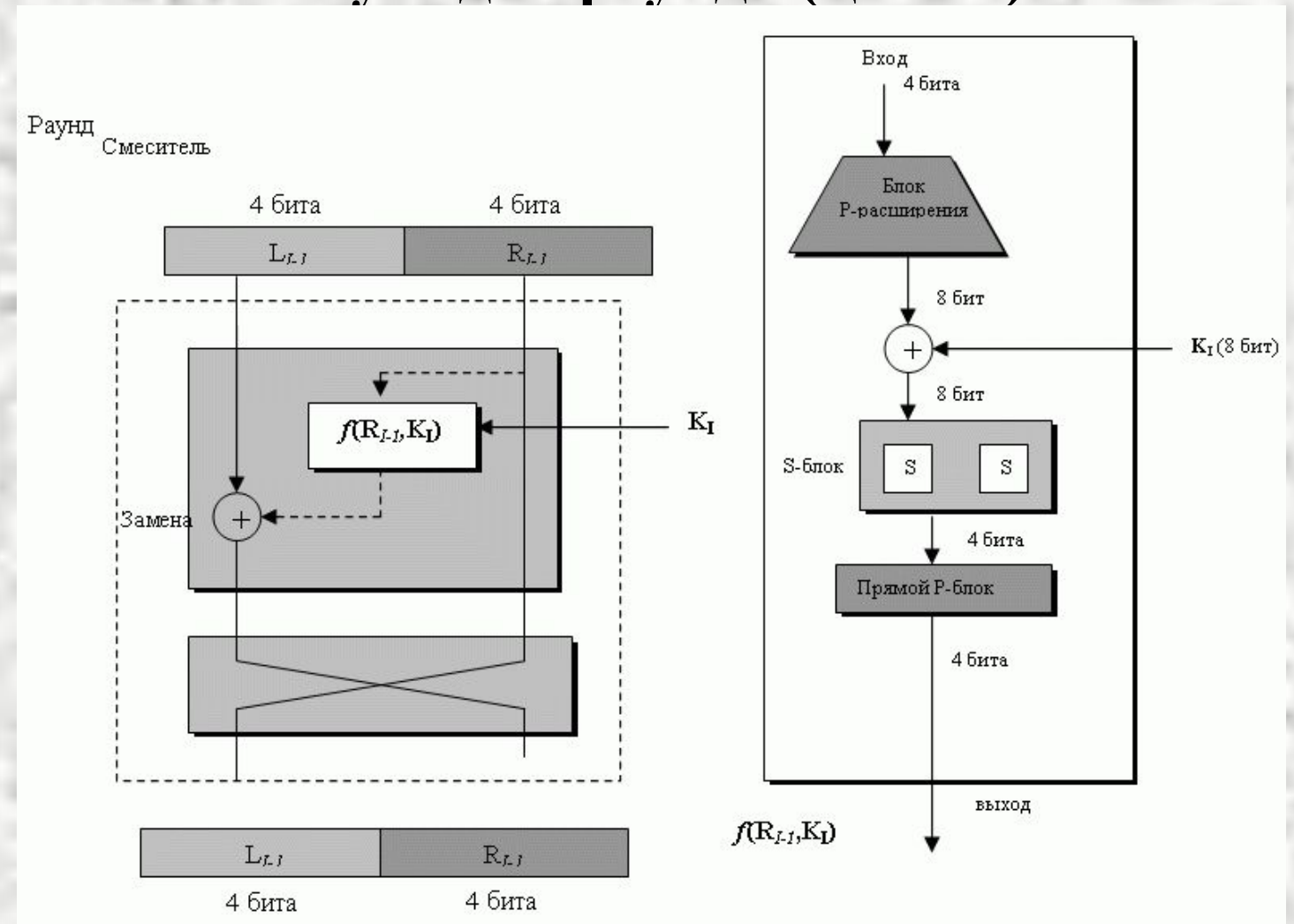


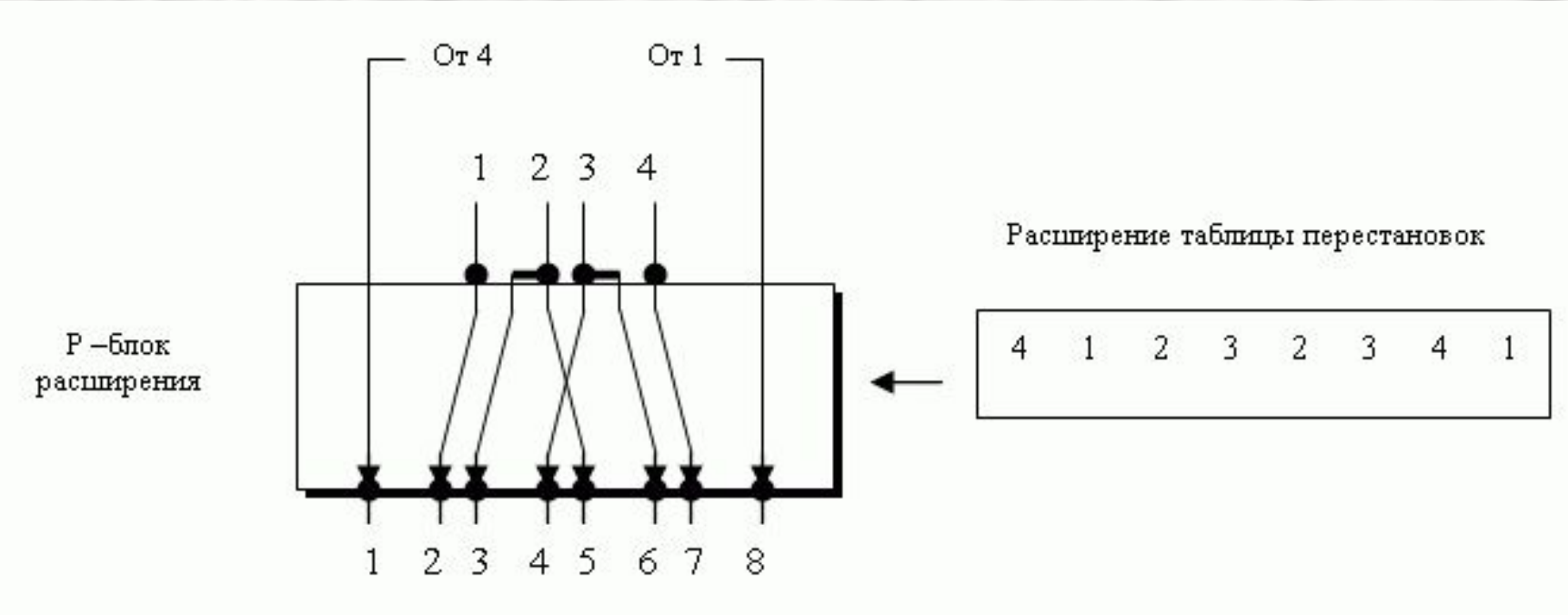
Таблица конечной перестановки

4	1	3	5	7	2	8	6

S-DES использует два раунда (цикла)



Как и в алгоритме DES, раунд начинается с выполнения расширяющей перестановки P, которая расширяет 4-битный блок с получением 8-битного результата



Затем к данным прибавляется 8-битный ключ раунда K_i (где i – номер раунда). Результат этой операции делится на два фрагмента по 4 бита, которые прогоняются через таблицы замен S_1 и S_2. Таблицы заменяют 4-битные фрагменты 2-битными, принцип их работы похож на принцип работы таблиц $S_1 \ldots S_8$ алгоритма DES:

- ✔***старший и младший биты входного значения задают номер строки таблицы;***
- ✔***остальные биты определяют номер столбца;***
- ✔***выходное 2-битное значение берется из ячейки, принадлежащей данным столбцу и строке.***

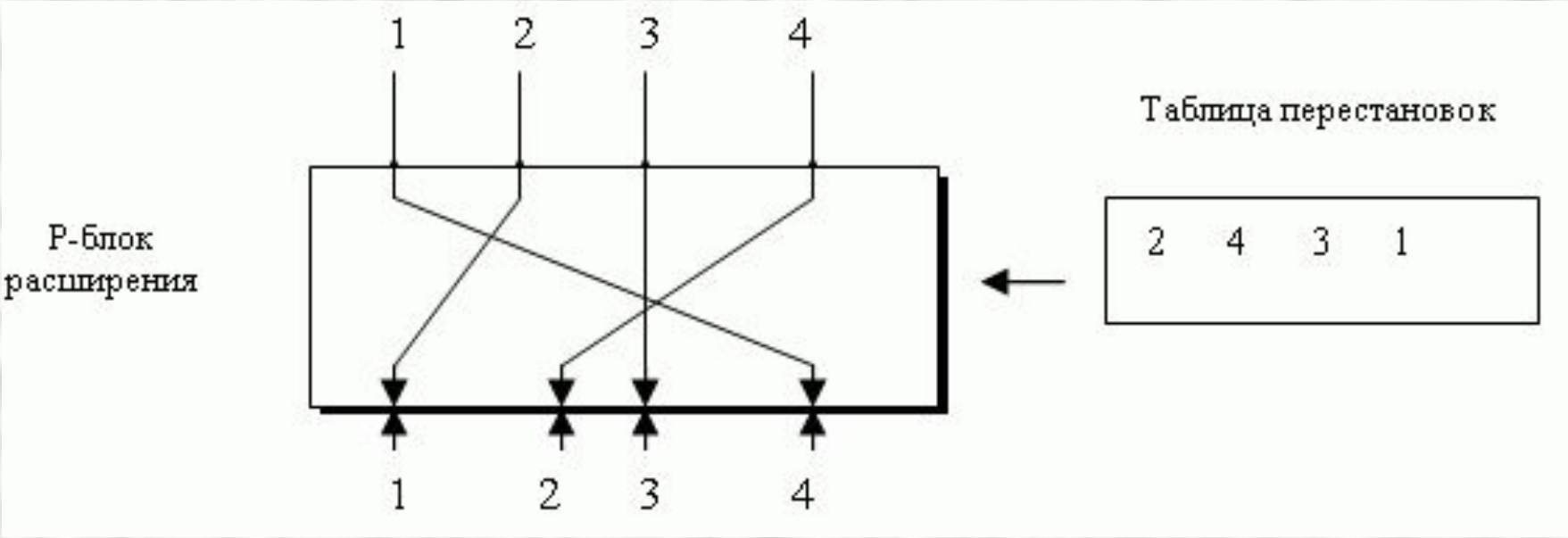
	0	1	2	3
0	1	0	3	2
1	3	2	1	0
2	0	2	1	3
3	3	1	3	2

Таблица для S -блока 1

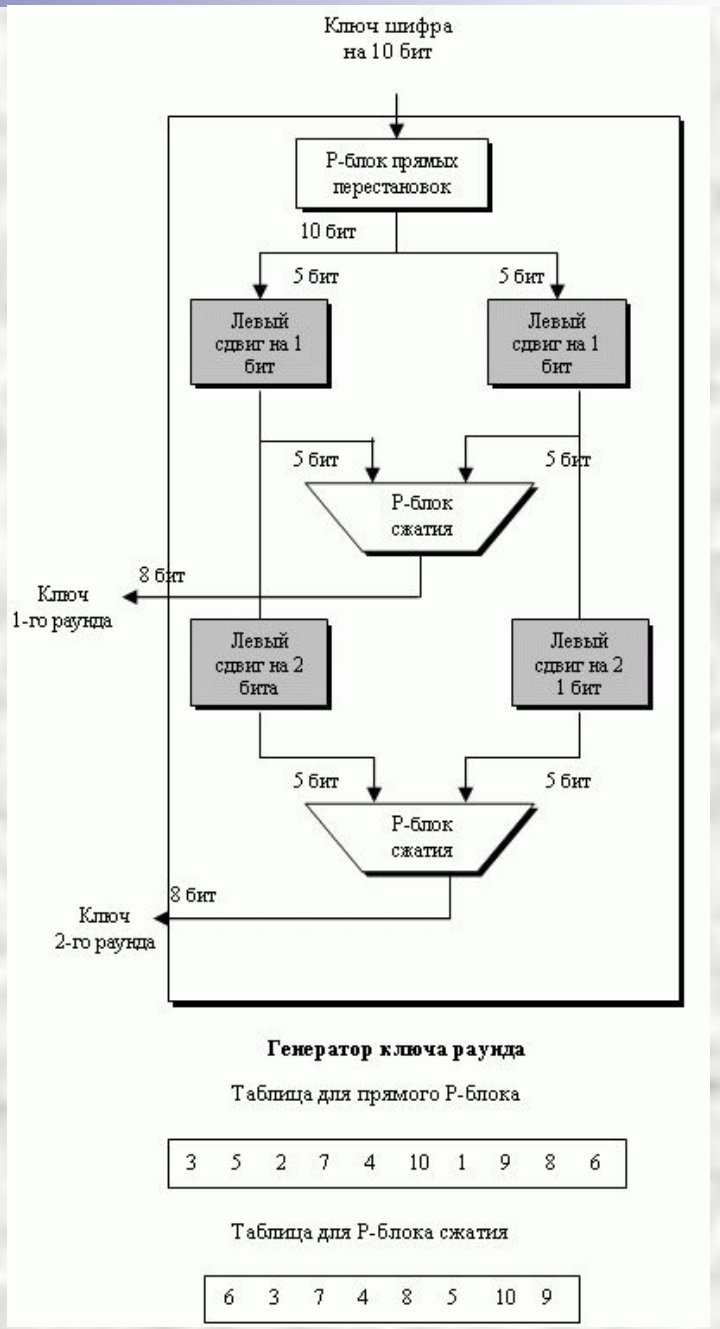
	0	1	2	3
0	0	1	2	3
1	2	0	1	3
2	3	0	1	0
3	2	1	0	3

Таблица для S -блока 2

Конечная перестановка завершает вычисление функции $f(R_{i-1},K_i)$



Процедура получения подключей алгоритма S-DES также похожа на DES с учетом уменьшенных размеров блока и ключа, а также количества раундов



Генератор ключа раунда

Таблица для прямого P-блока

3	5	2	7	4	10	1	9	8	6

Таблица для P-блока сжатия

6	3	7	4	8	5	10	9

Пример 1. ***Зашифровать текст 00001011, если ключ равен 1011100110***

Подзадача 1. Построение подключей K_1 и K_2

Шаг 1. Применить прямую перестановку P:

Перестановка P

3	5	2	7	4	10	1	9	8	6

Ключ

1	2	3	4	5	6	7	8	9	10
1	0	1	1	1	0	0	1	1	0

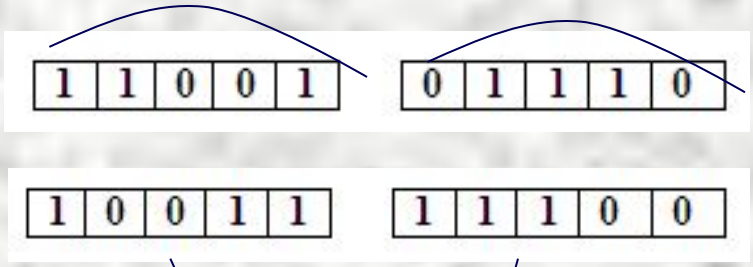
1	1	0	0	1	0	1	1	1	0

Шаг 2. Разбить ключ на два блока по 5 бит:

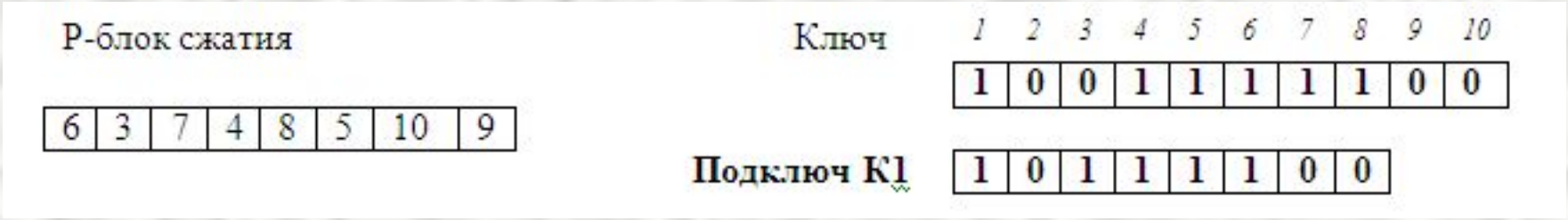
1	1	0	0	1

0	1	1	1	0

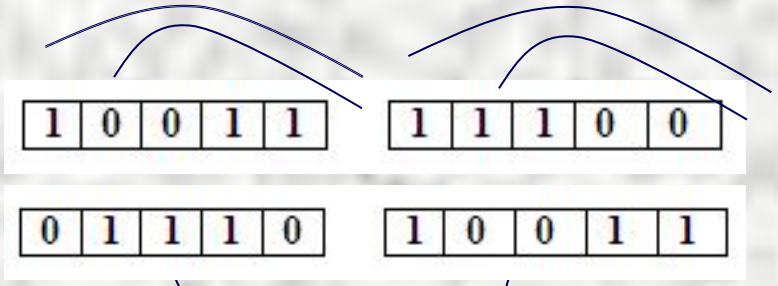
Шаг 3. Выполнить левый сдвиг на 1 бит:



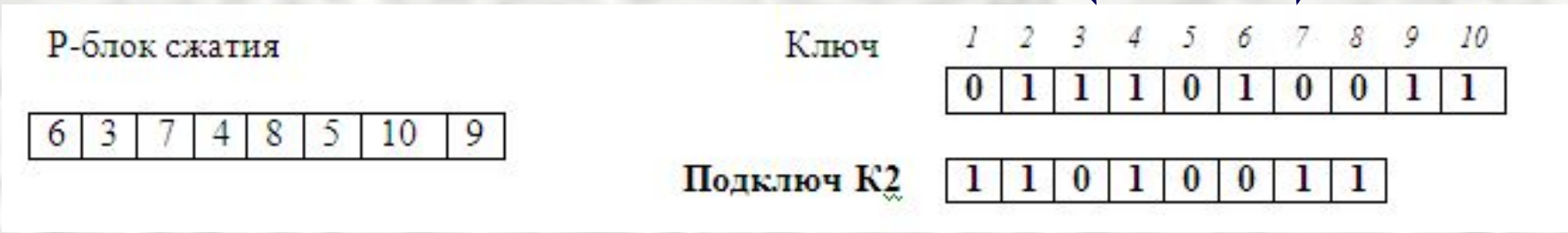
Шаг 4. Выполнить P-блок сжатия :



Шаг 5. Выполнить левый сдвиг на 2 бита (результат из шага 3):



Шаг 6. Выполнить P-блок сжатия :



Подзадача 2. Шифрование S-DES

Шаг 1. Применить начальную перестановку P к исходному тексту:

Перестановка P

2	6	3	1	4	8	5	7

Текст

1	2	3	4	5	6	7	8
0	0	0	0	1	0	1	1
0	0	0	0	0	1	1	1

Шаг 2. Разбить на два 4-битовых блока:

0	0	0	0

0	1	1	1

Раунд 1

Шаг 3. Применить к правой части из 4 бит функцию f с подключом K1, т.е. $f(R_1, K_1)$

3.1. *Применить P-блок расширения*

P-блок сжатия

4	1	2	3	2	3	4	1

R1

1	*2*	*3*	*4*
0	**1**	**1**	**1**

1	**0**	**1**	**1**	**1**	**1**	**1**	**0**

3.2 *Сложить (по модулю 2) с подключом* K_1

R_1 (*расширенный*)	**1**	**0**	**1**	**1**	**1**	**1**	**1**	**0**
K_1	**1**	**0**	**1**	**1**	**1**	**1**	**0**	**0**
	0	**0**	**0**	**0**	**0**	**0**	**1**	**0**

3.3. Применить S-преобразование к блокам по 4 бита

R_1 (*расширенный*)
K_1

1	0	1	1	1	1	1	0
1	0	1	1	1	1	0	0
0	0	0	0	0	0	1	0

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

Таблица для S -блока 1

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

Таблица для S -блока 2

0	0	0	0

$a = 0\ 0 = 0_{10}$
$b = 0\ 0 = 0_{10}$

$B'_1 = 1_{10} = 01_2$

0	0	1	0

$a = 0\ 0 = 0_{10}$
$b = 0\ 1 = 1_{10}$

$B'_2 = 1_{10} = 01_2$

3.4. Применить прямой P-блок перестановок

Перестановка P

2	4	3	1

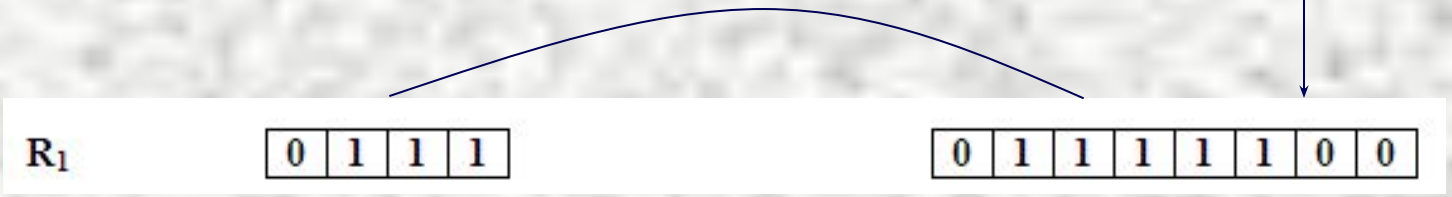
Текст

1	2	3	4
0	1	0	1
1	1	0	0

Шаг 4. Сложить результат с левым блоком (по модулю 2)

L_1 / $f(R_1,K_1)$				
	0	0	0	0
	1	1	0	0
	1	1	0	0

Шаг 5. Поменять местами левый и правый блоки



Конец раунда 1

Раунд 2

Шаг 6. Применить к правой части из 4 бит функцию f с подключом K_2, т.е. $f(R_2, K_2)$

6.1. *Применить P-блок расширения*

0	1	1	1

1	1	0	0

P-блок расширения

4	1	2	3	2	3	4	1

R_2

1	*2*	*3*	*4*
1	1	0	0

0	1	1	0	1	0	0	1

6.2 *Сложить (по модулю 2) с подключом* K_2

R_2 *(расширенный)*	0	1	1	0	1	0	0	1
K_2	1	1	0	1	0	0	1	1
	1	0	1	1	1	0	1	0

6.3. Применить S-преобразование к блокам по 4 бита

R_2 *(расширенный)*
K_2

0	1	1	0	1	0	0	1
1	1	0	1	0	0	1	1
1	0	1	1	1	0	1	0

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

Таблица для S -блока 1

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

Таблица для S -блока 2

1	0	1	1

$a = 1\ 1 = 3_{10}$
$b = 0\ 1 = 1_{10}$

$B'_1 = 1_{10} = 01_2$

1	0	1	0

$a = 1\ 0 = 2_{10}$
$b = 0\ 1 = 1_{10}$

$B'_2 = 0_{10} = 00_2$

6.4. Применить прямой P-блок перестановок

Перестановка P

2	4	3	1

Текст

1	*2*	*3*	*4*
0	1	0	0

1	0	0	0

Шаг 7. Сложить результат с левым блоком (по модулю 2)

L_2	0	1	1	1
$f(R_2,K_2)$	1	0	0	0
	1	1	1	1

Шаг 8. Совместить левый и правый блоки (*без обмена местами*)

R_2	1	1	0	0

1	1	1	1	1	1	0	0

Конец раунда 2

Шаг 9. Применить конечную перестановку P

Перестановка P

4	1	3	5	7	2	8	6

1	2	3	4	5	6	7	8
1	1	1	1	1	1	0	0
1	1	1	1	0	1	0	1

Зашифрованный текст

Список используемых источников:

1. *https://intuit.ru/studies/courses/553/409/lecture/17872?page=2*
2. **Хорев П.Б. Методы и средства защиты в компьютерных системах: Учеб. пособие для вузов. - М.: Академия, 2006. - 256 с.**
3. **Фергюсон Н., Шнайер Б. Практическая криптография/ Пер.с англ.. - М.: ИД Вильямс, 2005. - 424с.**
4. **Садердинов А.А., Трайнев В.А., Федулов А.А. Информационная безопасность предприятия: Учеб. пособие. - М.: Дашков и К, 2007. - 336 с.**

Список используемых источников:

4. **Скляров Д.В. Искусство защиты и взлома информации. - СПб.: БХВ-Петербург, 2004. - 288с.**
5. **Мао В. Современная криптография.Теория и практика/ Пер.с англ.. - М.: ИД Вильямс, 2005. - 768с.**
6. **Петренко С.А., Курбатов В.А. Политики информационной безопасности. - М.: Академия АйТи, 2006. - 400 с.**