**МИНОБРНАУКИ РОССИИ**

**Санкт-Петербургский государственный**

**электротехнический университет**

**«ЛЭТИ» им. В.И. Ульянова (Ленина)**

**Кафедра МО ЭВМ**

отчет

**по лабораторной работе №2**

**“Изучение шифра DES”**

|  |  |  |
| --- | --- | --- |
| Студент гр. 8382 |  | Мирончик П.Д. |
| Преподаватель |  | Племянников А.К. |

Санкт-Петербург

2021

# Цель работы

Исследовать шифры DES, 3DES, а также другие модификации шифра DES: DESX, DESL, DESXL и получить практические навыки работы с ними, в том числе с использованием приложения Cryptool 1 и 2.

# 1. Исследование преобразований DES

## 1.1. Задание

1. Изучить преобразования шифра DES с помощью демонстрационного приложения из Cryptool 1.

a. Indiv.Procedures-> Visualization…-> DES…

2. Выполнить вручную преобразования первых двух раундов и вычисление раундовых ключей при следующих исходных данных:

a. Открытый текст (не более 64 бит) – фамилия\_имя (транслитерация латиницей)

b. Ключ (56 бит) – номер зачетной книжки и инициал отчества (всего 7 символов)

3. Выполнить вручную обратное преобразование зашифрованного сообщения

4. Убедиться в совпадении результатов

## 1.2. Описание DES

DES шифрует информацию блоками по 64 бита с помощью 64-битного ключа шифрования. Шифрование выполняется следующим образом:

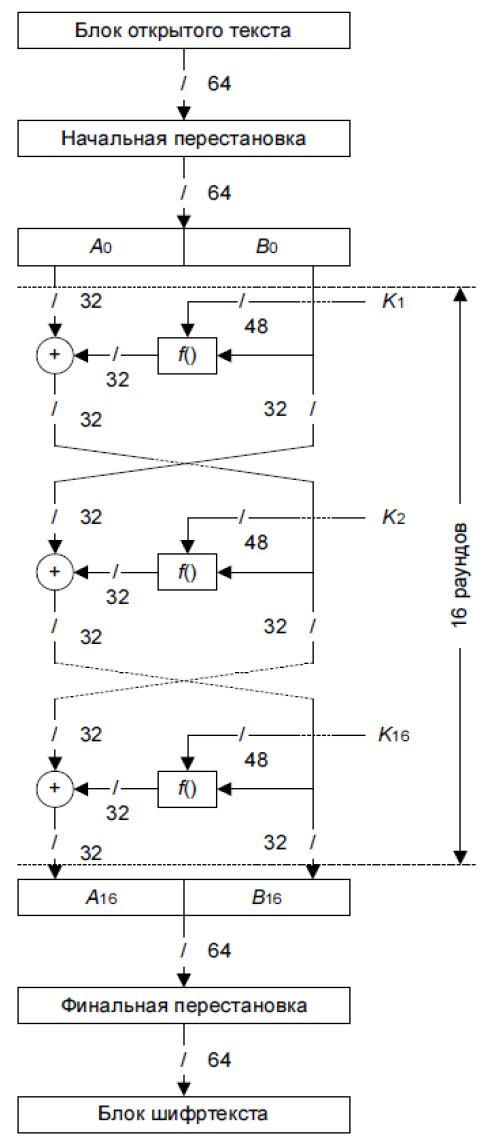


Рис.1.1 – шифр DES

1. Над 64-битными блоками производится начальная перестановка, задаваемая таблично

2. После начальной перестановки блок делится на 2 субблока по 32 бита (𝐴0 и 𝐵0), над которыми производятся 16 раундов преобразований:

Где i – номер текущего раунда, – ключ раунда, - логическая операция XOR.

Схема работы функции раунда выглядит следующим образом (Рис. 1.2):

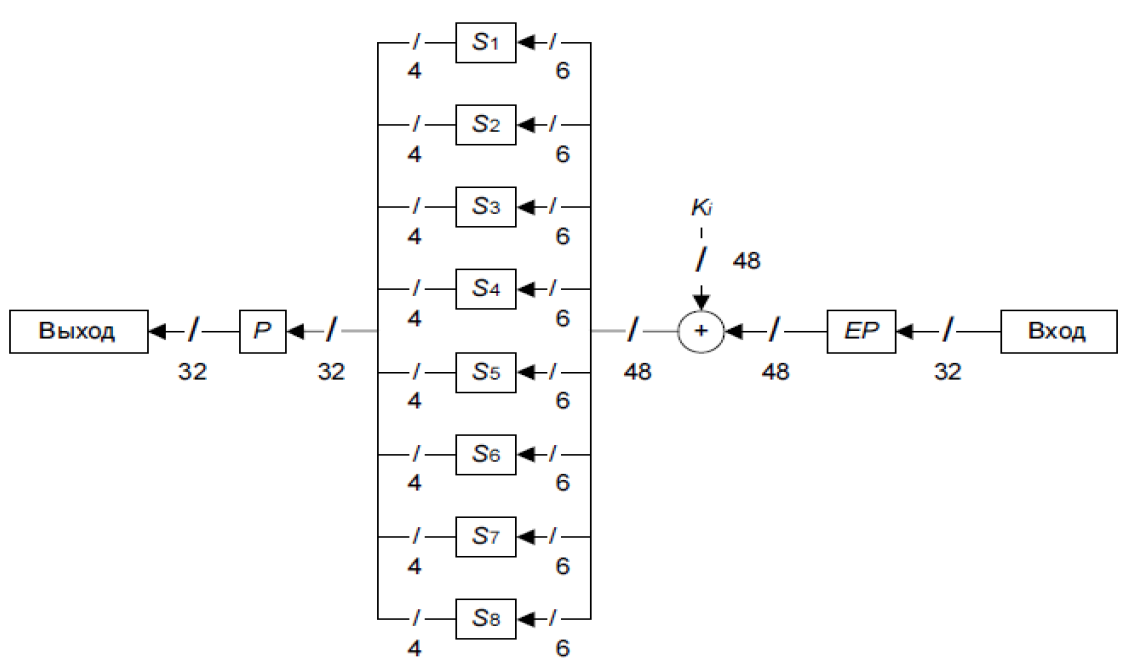


Рис.1.2 – Работа функции раунда DES

a) Выполняется расширяющая перестановка EP, преобразующая входные 32 бита в 48 бит.

b) Полученные 48 бит складываются с операцией XOR.

c) Результат сложения разбивается на 8 блоков по 6 битов. Каждый блок обрабатывается соответствующей таблицей замен:

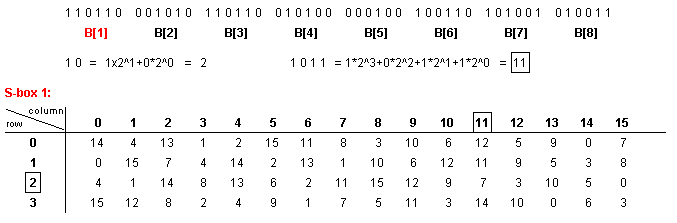


Рис.1.3 – Работа с таблицей замен в функции раунда

d) Над полученными 32 битами выполняется перестановка (обозначенная P на Рис. 1.2)

В итоге полученные субблоки и образуют 64-битный блок, над которым производится конечная перестановка и в итоге получается результирующий блок шифротекста.

Рассмотрим процедуру генерации раундовых ключей (Рис. 1.4):

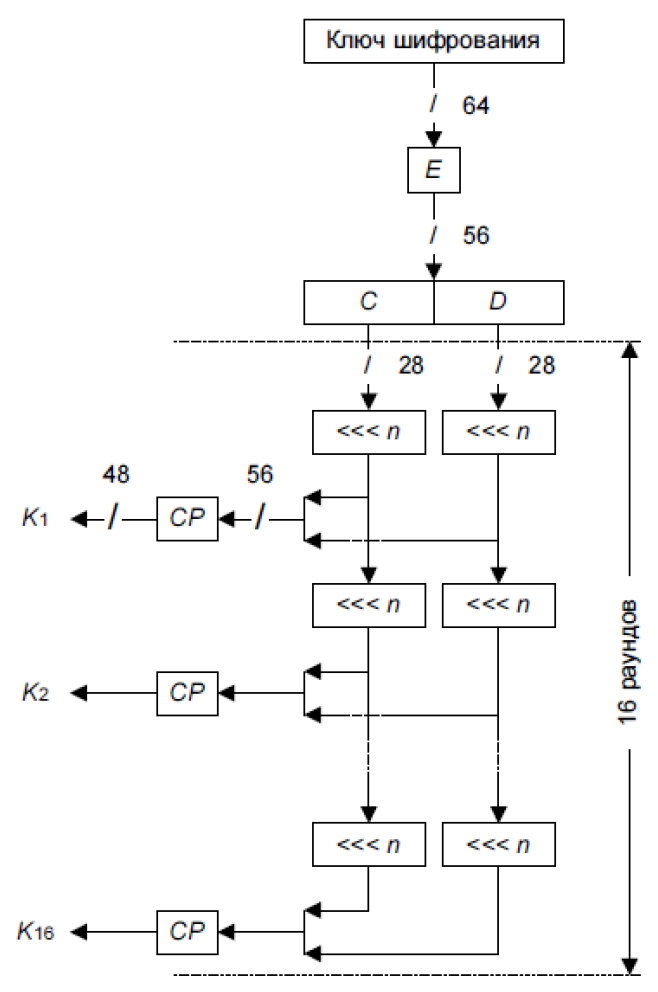


Рис. 1.4 – Генерация раундовых ключей

a) Выполняется операция E сжатия ключа и перестановка.

b) Полученные 56 бит делятся на 2 субблока C и D по 28 бит.

c) На каждом шаге C и D циклически сдвигаются на определенное количество бит, объединяются в 56-битное значение, к которому применяется сжимающая перестановка. В итоге получаются 48-битные ключи.

Расшифровывание данных алгоритмом DES происходит при прохождении всех шагов алгоритма в обратном порядке.

## 1.3. Ручной расчет субблоков и раундовых ключей шифра для первых двух раундов.