**МИНОБРНАУКИ РОССИИ**

**Санкт-Петербургский государственный**

**электротехнический университет**

**«ЛЭТИ» им. В.И. Ульянова (Ленина)**

**Кафедра ИБ**

**отчет**

**по лабораторной работе №4**

**по дисциплине «Криптографические методы защиты информации»**

**Тема: Изучение шифра DES**

|  |  |  |
| --- | --- | --- |
| Студентка гр. 4383 |  | Гордеева Т.В. |
| Преподаватель |  | Племянников А.К. |

Санкт-Петербург

2017

**Цель работы:** исследовать шифры DES, 3DES, а также модификаций DESX, DESL, DESXL и получить практические навыки работы с ними, в том числе и в программном продукте 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 одного раунда 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 II инициал (всего 7 символов)

3. Выполнить вручную обратное преобразование зашифрованного сообщения

4. Убедиться в совпадении результатов

**1.2 Содержание раздела отчета**

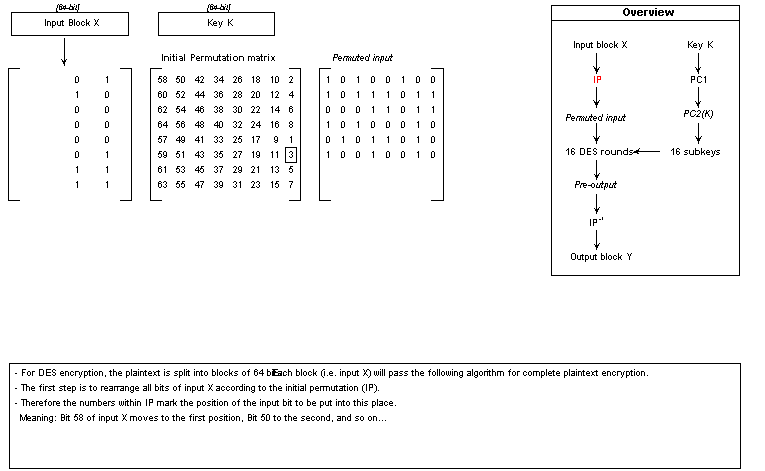
1. Формулировка задания и содержание этой части отчета.

2. Описание DES c примерами скриншотов из демоприложения.

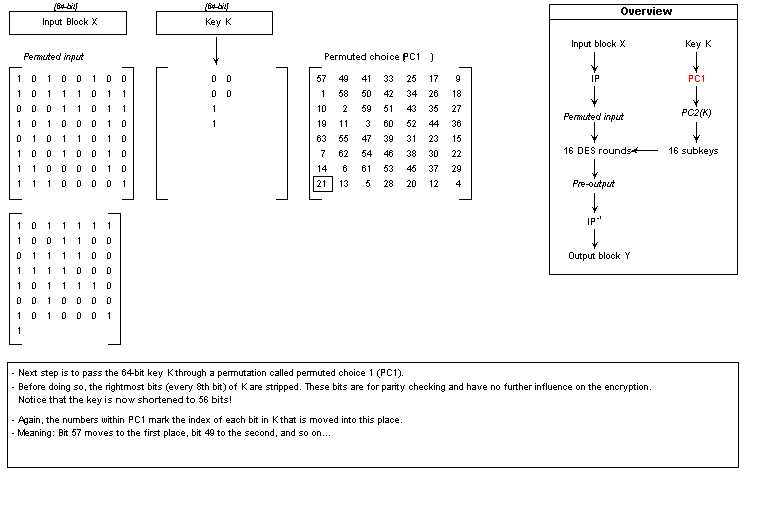
3. Ручной расчет субблоков и раундовых ключей шифра для первых двух раундов.

**1.3 Описание DES c примерами скриншотов из демоприложения**

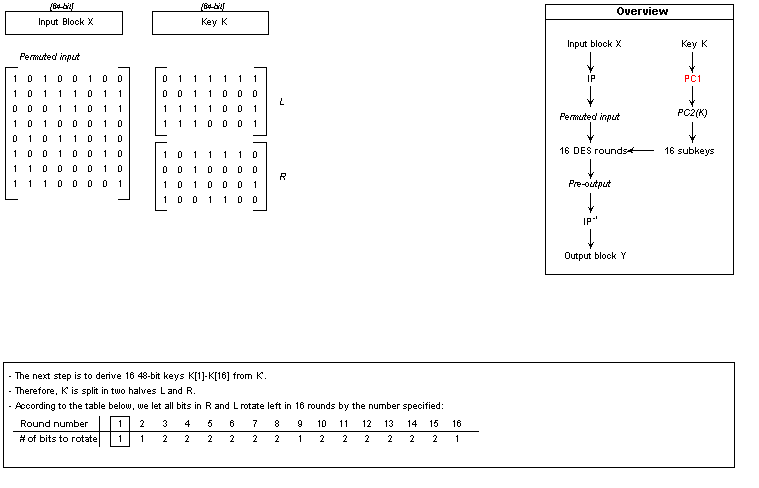
Начальная перестановка

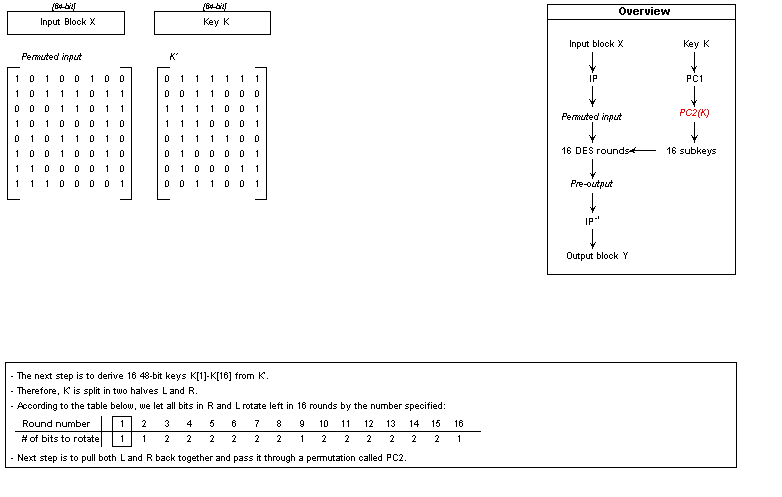


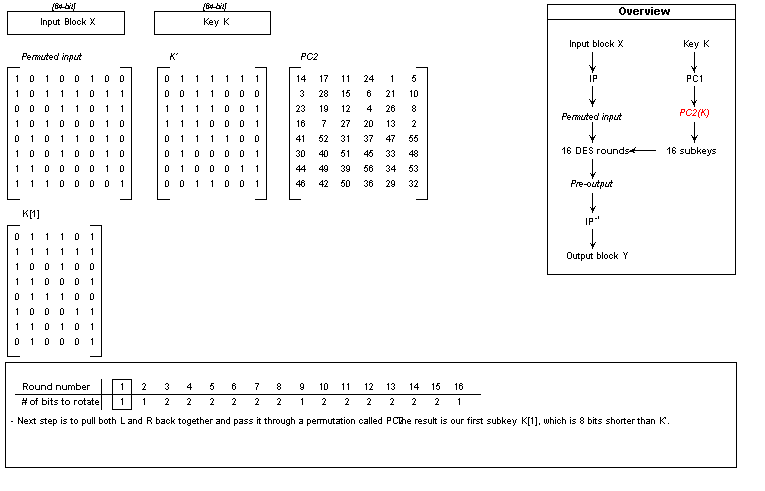
Начальная перстановка ключа



Генерация раундовых ключей

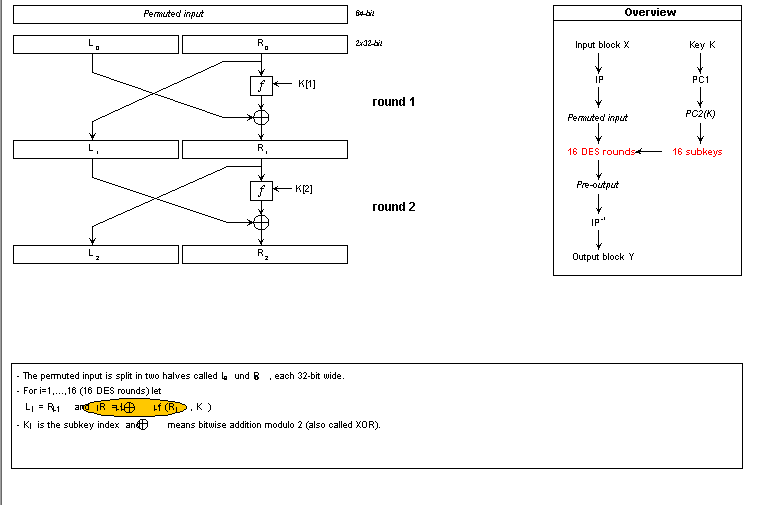


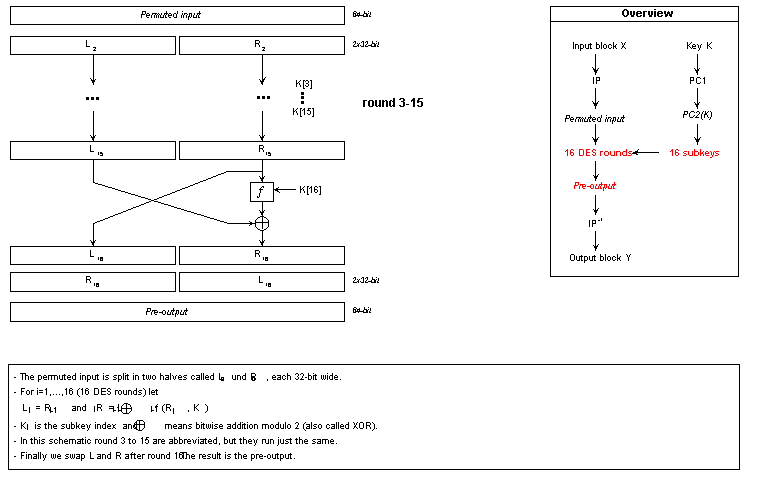


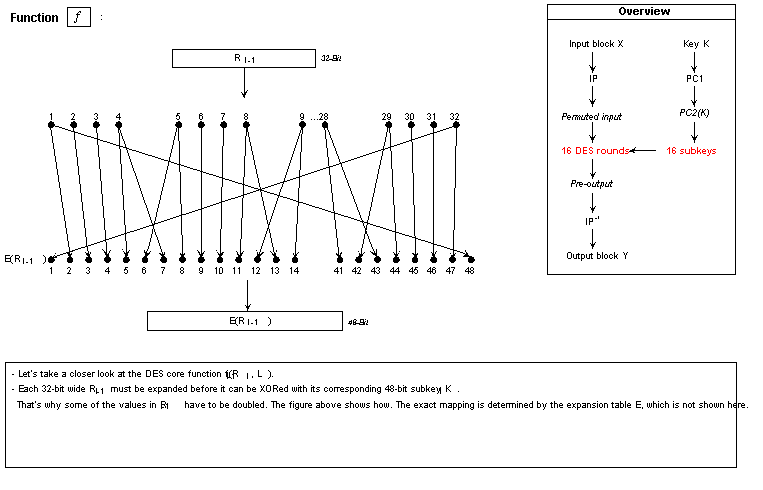




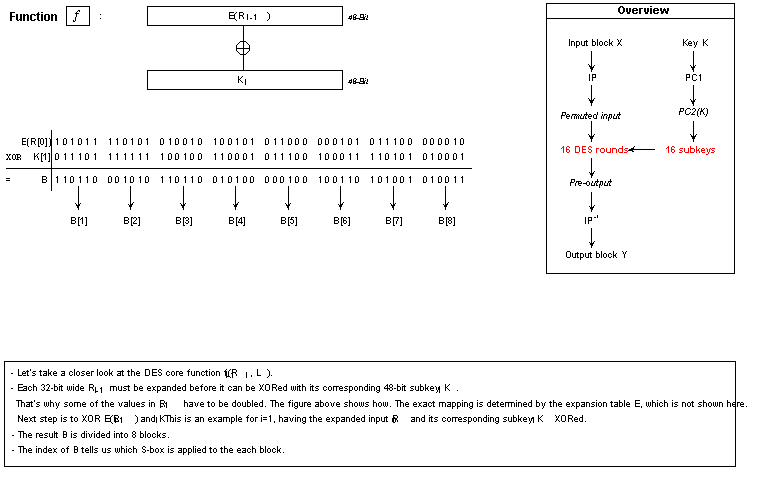
Раунды шифрования

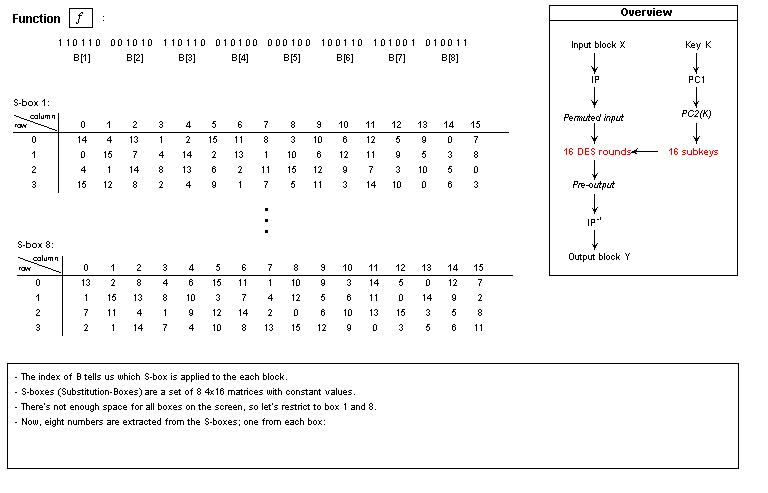
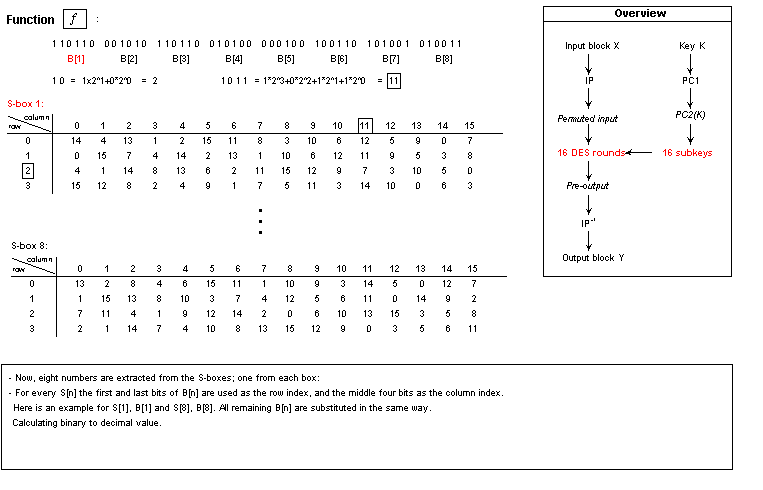
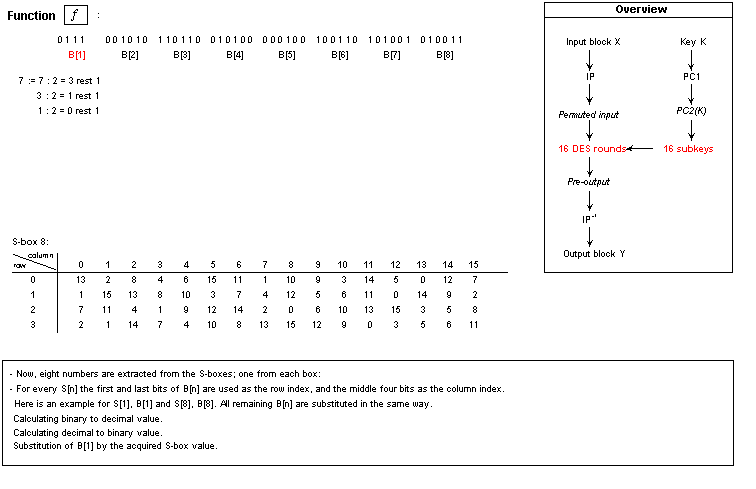




Расширяющая перестановка 

Побитовое XOR расширенного блока и раундового ключа

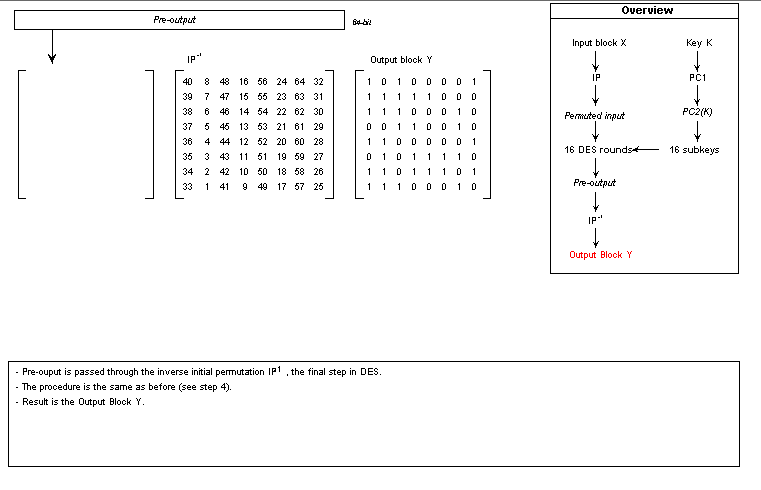


Вычисление значений с помощью S-box таблиц.   

Перестановка внутри функции f 



Конченая перестановка

****

**1.4 Ручной расчет субблоков и раундовых ключей шифра для первых двух раундов.**

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

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

Преобразуем заданный в 64-битовый блок и выполнм начальную перестановку.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| G | O | R | D | E | E | V | A |  | Матрица перестановки | | | | | | | |  | Начальная пеестановка | | | | | | | |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 58 | 50 | 42 | 34 | 26 | 18 | 10 | 2 | 1 | 1 | 1 | 1 | 0 | 0 | 1 | 0 |
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 60 | 52 | 44 | 36 | 28 | 20 | 12 | 4 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 62 | 54 | 46 | 38 | 30 | 22 | 14 | 6 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 0 |
| 0 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 64 | 56 | 48 | 40 | 32 | 24 | 16 | 8 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 0 |
| 0 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 57 | 49 | 41 | 33 | 25 | 17 | 9 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 1 | 0 |
| 1 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 59 | 51 | 43 | 35 | 27 | 19 | 11 | 3 | 0 | 1 | 0 | 0 | 1 | 0 | 1 | 0 |
| 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 61 | 53 | 45 | 37 | 29 | 21 | 13 | 5 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 0 |
| 1 | 1 | 0 | 0 | 1 | 1 | 1 | 1 | 63 | 55 | 47 | 39 | 31 | 23 | 15 | 7 | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 0 |

Разделим полученный блок по горизонтали на две части

𝐿0=

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 1 | 1 | 1 | 0 | 0 | 1 | 0 |
| 0 | 0 | 1 | 0 | 0 | 0 | 1 | 0 |
| 1 | 0 | 1 | 0 | 0 | 0 | 1 | 0 |
| 1 | 0 | 0 | 0 | 1 | 0 | 1 | 0 |
| R0= | | | | | | | |
| 1 | 1 | 1 | 0 | 0 | 0 | 1 | 0 |
| 0 | 1 | 0 | 0 | 1 | 0 | 1 | 0 |
| 1 | 0 | 1 | 0 | 0 | 0 | 1 | 0 |
| 1 | 0 | 0 | 1 | 1 | 0 | 1 | 0 |

Выполним преобразования ключа

Ключ:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 4 | 3 | 8 | 3 | 0 | 6 | G | T |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 |
| 1 | 1 | 1 | 1 | 1 | 1 | 0 | 0 |
| 1 | 1 | 1 | 1 | 1 | 1 | 0 | 1 |
| 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 0 | 0 | 0 | 1 | 1 | 1 |
| 0 | 1 | 0 | 1 | 0 | 1 | 1 | 0 |
| 0 | 1 | 0 | 1 | 0 | 0 | 1 | 0 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Ключ | | | | | | | |  | Матрица перестановки | | | | | | |  | Начальная перестановка | | | | | | |
| 0 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 57 | 49 | 41 | 33 | 25 | 17 | 9 |  | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 58 | 50 | 42 | 34 | 26 | 18 | 0 | 1 | 1 | 0 | 0 | 0 | 0 |
| 0 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 10 | 2 | 59 | 51 | 43 | 35 | 27 | 0 | 0 | 0 | 0 | 1 | 1 | 1 |
| 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 19 | 11 | 3 | 60 | 52 | 44 | 36 | 1 | 1 | 1 | 1 | 0 | 1 | 1 |
| 0 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 63 | 55 | 47 | 39 | 31 | 23 | 15 | 0 | 1 | 1 | 0 | 1 | 0 | 1 |
| 0 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 7 | 62 | 54 | 46 | 38 | 30 | 22 | 0 | 1 | 1 | 1 | 0 | 0 | 0 |
| 0 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 14 | 6 | 61 | 53 | 45 | 37 | 29 | 0 | 1 | 0 | 0 | 0 | 0 | 0 |
| 0 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 21 | 13 | 5 | 28 | 20 | 12 | 4 | 1 | 0 | 0 | 1 | 1 | 1 | 1 |

Делим ключ на 2 части:

С0=

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 1 | 1 | 0 | 0 | 0 | 0 |
| 0 | 0 | 0 | 0 | 1 | 1 | 1 |
| 1 | 1 | 1 | 1 | 0 | 1 | 1 |
| D0= | | | | | | |
| 0 | 1 | 1 | 0 | 1 | 0 | 1 |
| 0 | 1 | 1 | 1 | 0 | 0 | 0 |
| 0 | 1 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 0 | 1 | 1 | 1 | 1 |

Получаем С1 – сдвигом С0 на 1 влево.

Также 𝐷1 – сдвигом 𝐷0 – на 1 влево.

С1=

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 1 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 0 | 1 | 1 | 1 | 0 |
| 1 | 1 | 1 | 0 | 1 | 1 | 1 |
| D1= | | | | | | |
| 1 | 1 | 0 | 1 | 0 | 1 | 0 |
| 1 | 1 | 1 | 0 | 0 | 0 | 0 |
| 1 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 1 | 1 | 1 | 1 | 1 |

Получаем С2 – сдвигом С1 на 1 влево.

Также 𝐷2 – сдвигом 𝐷1 – на 1 влево.

С2=

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 0 | 0 | 0 | 0 | 1 |
| 0 | 0 | 1 | 1 | 1 | 0 | 0 |
| 1 | 1 | 0 | 1 | 1 | 1 | 1 |
| D2= | | | | | | |
| 1 | 0 | 1 | 0 | 1 | 0 | 1 |
| 1 | 1 | 0 | 0 | 0 | 0 | 1 |
| 0 | 0 | 0 | 0 | 0 | 0 | 1 |
| 0 | 1 | 1 | 1 | 1 | 1 | 0 |

Считаем 2 раундовых ключа.

Применяем перестановку PC2.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | |  | Матрица перестановки | | | | | | |  | Перестановка | | | | | |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 |  | 14 | 17 | 11 | 24 | 1 | 5 |  | | 0 | 0 | 0 | 1 | 0 | 0 |
| 1 | 1 | 0 | 0 | 0 | 0 | 0 | 3 | 28 | 15 | 6 | 21 | 10 | 0 | 1 | 0 | 0 | 0 | 0 |
| 0 | 0 | 0 | 1 | 1 | 1 | 0 | 23 | 19 | 12 | 4 | 26 | 8 | 1 | 1 | 0 | 0 | 1 | 1 |
| 1 | 1 | 1 | 0 | 1 | 1 | 1 | 16 | 7 | 27 | 20 | 13 | 2 | 0 | 0 | 1 | 1 | 0 | 0 |
| 1 | 1 | 0 | 1 | 0 | 1 | 0 | 41 | 52 | 31 | 37 | 47 | 55 | 0 | 1 | 0 | 1 | 0 | 1 |
| 1 | 1 | 1 | 0 | 0 | 0 | 0 | 30 | 40 | 51 | 45 | 33 | 48 | 1 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 0 | 0 | 0 | 0 | 0 | 44 | 49 | 39 | 56 | 34 | 53 | 0 | 0 | 0 | 1 | 1 | 1 |
| 0 | 0 | 1 | 1 | 1 | 1 | 1 | 46 | 42 | 50 | 36 | 29 | 32 | 0 | 0 | 0 | 1 | 1 | 1 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | |  | Матрица перестановки | | | | | | |  | Перестановка | | | | | |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 |  | 14 | 17 | 11 | 24 | 1 | 5 |  | | 1 | 1 | 0 | 0 | 0 | 0 |
| 1 | 0 | 0 | 0 | 0 | 0 | 1 | 3 | 28 | 15 | 6 | 21 | 10 | 0 | 1 | 0 | 0 | 0 | 0 |
| 0 | 0 | 1 | 1 | 1 | 0 | 0 | 23 | 19 | 12 | 4 | 26 | 8 | 1 | 1 | 0 | 0 | 1 | 1 |
| 1 | 1 | 0 | 1 | 1 | 1 | 1 | 16 | 7 | 27 | 20 | 13 | 2 | 0 | 0 | 1 | 0 | 0 | 0 |
| 1 | 0 | 1 | 0 | 1 | 0 | 1 | 41 | 52 | 31 | 37 | 47 | 55 | 0 | 1 | 1 | 1 | 0 | 1 |
| 1 | 1 | 0 | 0 | 0 | 0 | 1 | 30 | 40 | 51 | 45 | 33 | 48 | 0 | 0 | 1 | 0 | 1 | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 1 | 44 | 49 | 39 | 56 | 34 | 53 | 0 | 1 | 0 | 0 | 0 | 1 |
| 0 | 1 | 1 | 1 | 1 | 1 | 0 | 46 | 42 | 50 | 36 | 29 | 32 | 0 | 1 | 0 | 1 | 1 | 0 |

1-й раунд DES:

=

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 1 | 1 | 1 | 0 | 0 | 1 | 0 |
| 0 | 0 | 1 | 0 | 0 | 0 | 1 | 0 |
| 1 | 0 | 1 | 0 | 0 | 0 | 1 | 0 |
| 1 | 0 | 0 | 0 | 1 | 0 | 1 | 0 |

=

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 1 | 1 | 0 | 0 | 0 | 1 | 0 |
| 0 | 1 | 0 | 0 | 1 | 0 | 1 | 0 |
| 1 | 0 | 1 | 0 | 0 | 0 | 1 | 0 |
| 1 | 0 | 0 | 1 | 1 | 0 | 1 | 0 |

Расширяющая перестановка:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | |  | Матрица перестановки | | | | | | |  | Перестановка | | | | | |
| 1 | 1 | 1 | 0 | 0 | 0 | 1 | 0 |  | 32 | 1 | 2 | 3 | 4 | 5 |  | | 0 | 1 | 1 | 1 | 0 | 0 |
| 0 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 4 | 5 | 6 | 7 | 8 | 9 | 0 | 0 | 0 | 1 | 0 | 0 |
| 1 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 8 | 9 | 10 | 11 | 12 | 13 | 0 | 0 | 1 | 0 | 0 | 1 |
| 1 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 12 | 13 | 14 | 15 | 16 | 17 | 0 | 1 | 0 | 1 | 0 | 1 |
|  |  |  |  |  |  |  |  | 16 | 17 | 18 | 19 | 20 | 21 | 0 | 1 | 0 | 1 | 0 | 0 |
|  |  |  |  |  |  |  |  | 20 | 21 | 22 | 23 | 24 | 25 | 0 | 0 | 0 | 1 | 0 | 1 |
|  |  |  |  |  |  |  |  | 24 | 25 | 26 | 27 | 28 | 29 | 0 | 1 | 0 | 0 | 1 | 1 |
|  |  |  |  |  |  |  |  | 28 | 29 | 30 | 31 | 32 | 1 | 1 | 1 | 0 | 1 | 0 | 1 |

=

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 1 | 1 | 0 | 0 |  | 0 | 0 | 0 | 1 | 0 | 0 |  | 0 | 1 | 1 | 0 | 0 | 0 |
| 0 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 |
| 0 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 0 | 1 | 0 |
| 0 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 1 |
| 0 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 |
| 0 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 1 |
| 0 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 0 | 1 | 0 | 1 | 0 | 0 |
| 1 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 1 | 0 |

S-box 1

0 1100 0

00 = 0

1100 = 12

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

5 = 0101

S-box 2

0 1010 0

00 = 0

1010 = 10

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

2 = 0010

S-box 3

1 1101 0

10 = 2

1101 = 13

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

10 = 1010

S-box 4

0 1100 1

01 = 1

1100 = 12

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

1 = 0001

S-box 5

0 0000 1

01 = 1

0000 = 0

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

14 = 1110

S-box 6

1 0010 1

11 = 3

0010 = 2

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

2 = 0010

S-box 7

0 1010 0

00 = 0

1010 = 10

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

9 = 1001

S-box 8

1 1001 0

10 = 2

1001 = 9

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

6 = 0110

= Перестановка P =

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 0 | 1 | 0 | 0 | 1 | 0 |
| 1 | 0 | 1 | 0 | 1 | 1 | 1 | 0 |
| 1 | 1 | 1 | 0 | 0 | 0 | 1 | 0 |
| 1 | 0 | 0 | 1 | 0 | 1 | 1 | 0 |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 16 | 7 | 20 | 21 | 29 | 12 | 28 | 17 |
| 1 | 15 | 23 | 26 | 5 | 18 | 31 | 10 |
| 2 | 8 | 24 | 14 | 32 | 27 | 3 | 9 |
| 19 | 13 | 30 | 6 | 22 | 11 | 4 | 25 |

=

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 0 | 0 | 0 | 0 | 1 | 1 |
| 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 |
| 1 | 0 | 0 | 1 | 0 | 0 | 0 | 1 |
| 1 | 1 | 1 | 0 | 0 | 1 | 1 | 1 |

=

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 1 | 1 | 1 | 0 | 0 | 1 | 0 |
| 0 | 0 | 1 | 0 | 0 | 0 | 1 | 0 |
| 1 | 0 | 1 | 0 | 0 | 0 | 1 | 0 |
| 1 | 0 | 0 | 0 | 1 | 0 | 1 | 0 |

=

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 0 | 1 | 1 | 0 | 0 | 0 | 1 |
| 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 |
| 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 |
| 0 | 1 | 1 | 0 | 1 | 1 | 0 | 1 |

=

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 1 | 1 | 0 | 0 | 0 | 1 | 0 |
| 0 | 1 | 0 | 0 | 1 | 0 | 1 | 0 |
| 1 | 0 | 1 | 0 | 0 | 0 | 1 | 0 |
| 1 | 0 | 0 | 1 | 1 | 0 | 1 | 0 |

Второй раунд шифрования:

Расширяющая перестановка:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | |  | Матрица перестановки | | | | | | |  | Перестановка | | | | | |
| 1 | 0 | 1 | 1 | 0 | 0 | 0 | 1 |  | 32 | 1 | 2 | 3 | 4 | 5 |  | | 1 | 1 | 0 | 1 | 1 | 0 |
| 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 4 | 5 | 6 | 7 | 8 | 9 | 1 | 0 | 0 | 0 | 1 | 0 |
| 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 8 | 9 | 10 | 11 | 12 | 13 | 1 | 0 | 1 | 0 | 0 | 0 |
| 0 | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 12 | 13 | 14 | 15 | 16 | 17 | 0 | 0 | 1 | 0 | 0 | 0 |
|  |  |  |  |  |  |  |  | 16 | 17 | 18 | 19 | 20 | 21 | 0 | 0 | 0 | 1 | 1 | 0 |
|  |  |  |  |  |  |  |  | 20 | 21 | 22 | 23 | 24 | 25 | 1 | 0 | 0 | 1 | 1 | 0 |
|  |  |  |  |  |  |  |  | 24 | 25 | 26 | 27 | 28 | 29 | 1 | 0 | 1 | 1 | 0 | 1 |
|  |  |  |  |  |  |  |  | 28 | 29 | 30 | 31 | 32 | 1 | 0 | 1 | 1 | 0 | 1 | 1 |

=

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 1 | 0 | 1 | 1 | 0 |  | 1 | 1 | 0 | 0 | 0 | 0 |  | 0 | 0 | 0 | 1 | 1 | 0 |
| 1 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 0 |
| 1 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 1 | 1 |
| 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 1 |
| 1 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 0 |
| 1 | 0 | 1 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 0 | 0 |
| 0 | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 1 |

S-box 1 (0 0011 0) = 0001

S-box 2 (1 1001 0) = 1000

S-box 3 (0 1001 1) = 1000

S-box 4 (0 000 0) =0111

S-box 5 (0 1101 1) = 1001

S-box 6 (1 0100 0) = 0010

S-box 7 (1 1110 0) =1001

S-box 8 (0 0110 1) =0011

=

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 16 | 7 | 20 | 21 | 29 | 12 | 28 | 17 |
| 1 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 15 | 23 | 26 | 5 | 18 | 31 | 10 |
| 1 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 2 | 8 | 24 | 14 | 32 | 27 | 3 | 9 |
| 1 | 0 | 0 | 1 | 0 | 0 | 1 | 1 | 19 | 13 | 30 | 6 | 22 | 11 | 4 | 25 |

=

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 0 | 1 | 0 | 0 | 0 | 1 | 1 |
| 0 | 1 | 1 | 0 | 1 | 0 | 1 | 0 |
| 0 | 0 | 1 | 1 | 1 | 0 | 0 | 1 |
| 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 |

=

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 |
| 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 0 | 1 | 1 | 0 | 1 | 1 |
| 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 |

=

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 0 | 1 | 1 | 0 | 0 | 0 | 1 |
| 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 |
| 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 |
| 0 | 1 | 1 | 0 | 1 | 1 | 0 | 1 |

Реализация в CrypTool 1:

****

****

**2 Исследование преобразований DES**

**2.1 Задание**

1. Создать картинку со своими ФИО (формат bmp).

2. Зашифровать картинку шифром DES в режиме ECB.

3. Зашифровать картинку шифром DES в режиме CBC c тем же ключом.

4. Сохранить скриншоты картинок для отчета.

5. Сжать исходную и 2 зашифрованных картинки средствами CrypTool. Зафиксировать размеры полученных файлов в таблице.

6. Выбрать случайный текст на английском языке (не менее 1000 знаков) и зашифровать его DES в режиме ECB.

7. Для одного и того же шифротекста оцените время проведения атаки «грубой силы» в случаях, когда известно n-4, n-6, n-8,.., 2 байт секретного ключа. Зафиксировать результаты измерений в таблице.

8. Повторить подобные измерения для DES в режиме CBC.

**2.2 Содержание раздела отчета**

1. Формулировка задания и содержание этой части отчета.

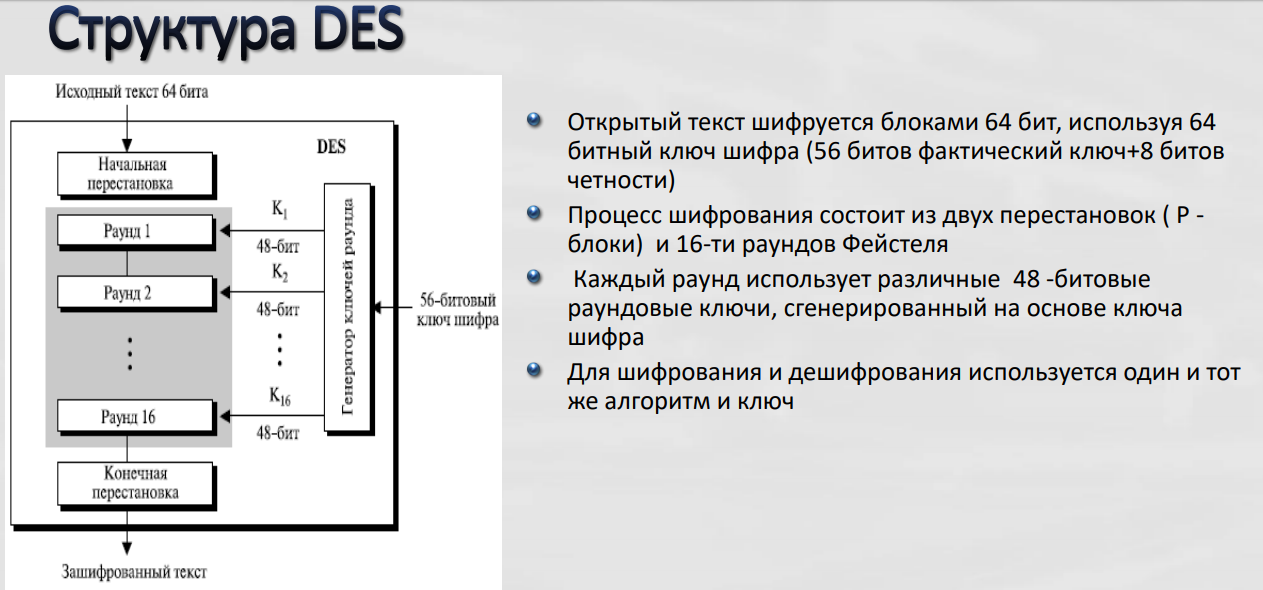
2. Основные параметры и обобщенная схема шифров (как в лекции).

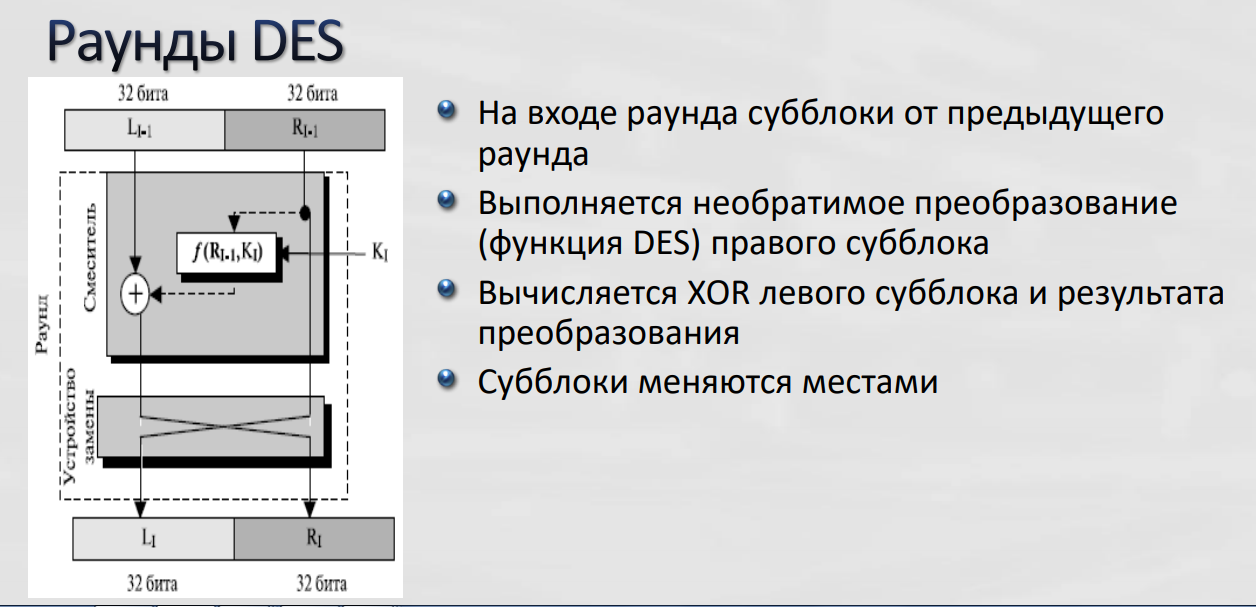
3. Скриншоты исходного и шифрованных изображений в разных режимах работы шифров.

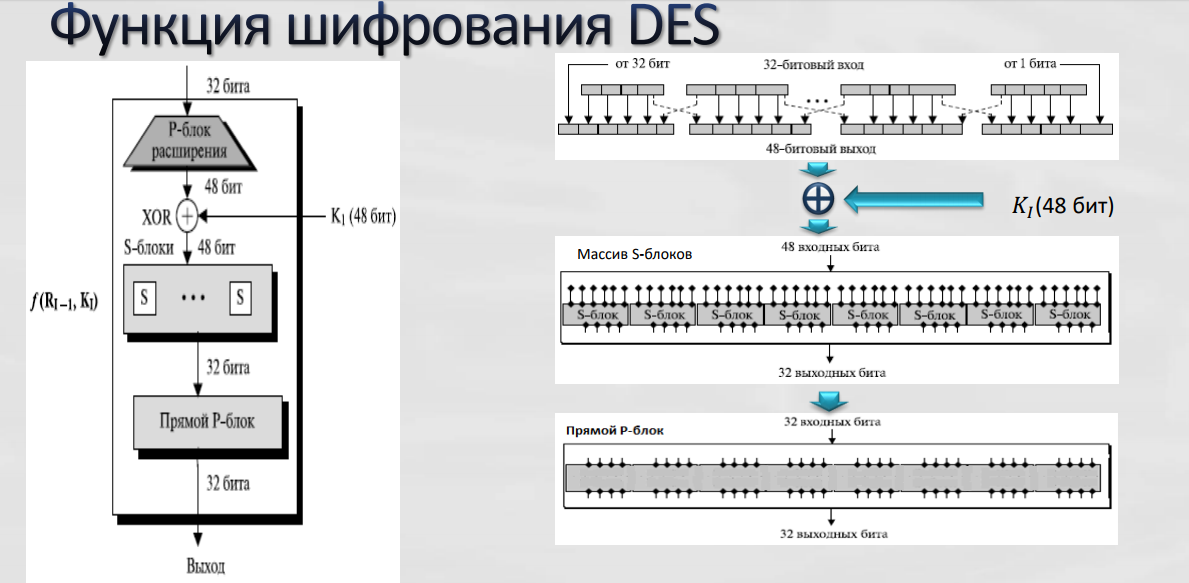
4. Таблица сравнений результатов сжатия исходного и шифрованных изображений.

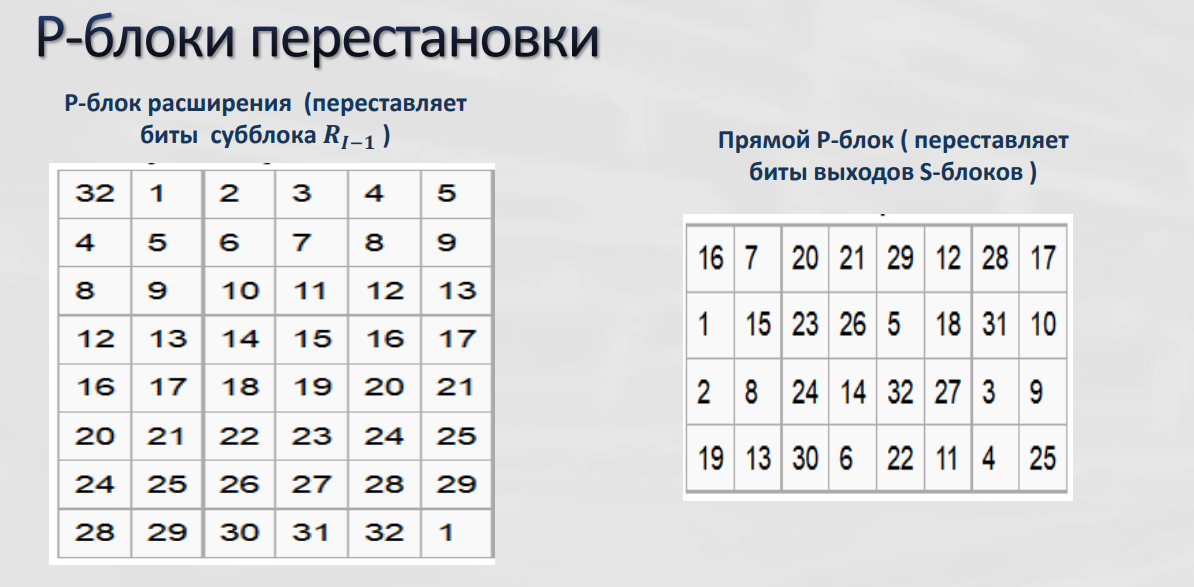
5. Таблица зависимости оценки времени атаки грубой силы от размера известной части ключа.

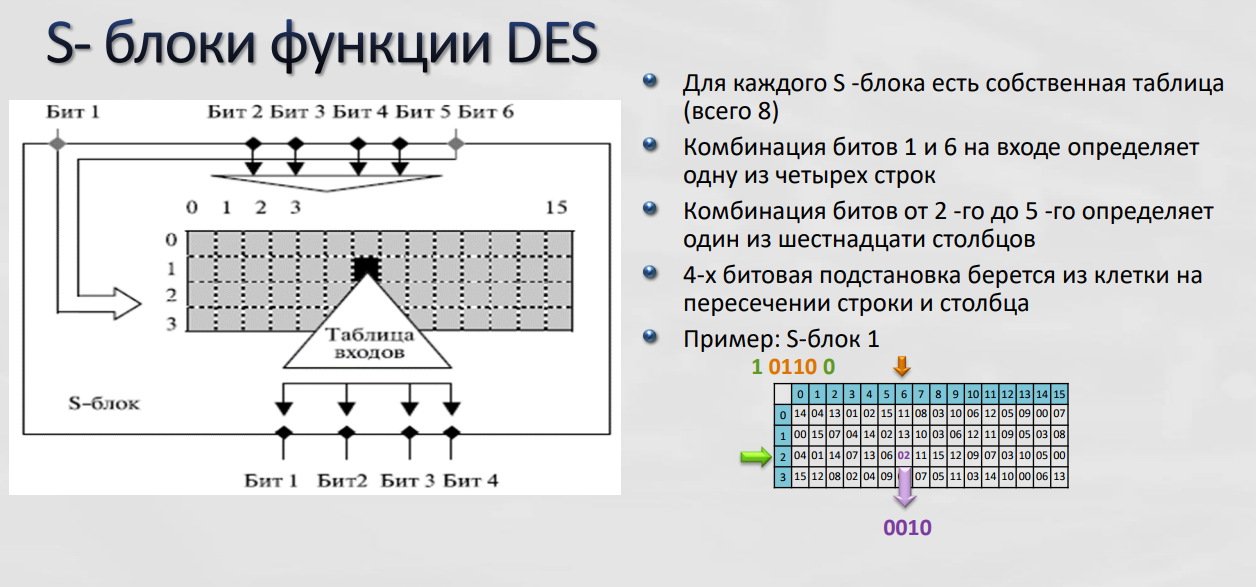
**2.3 Основные параметры и обобщенная схема шифров**

****

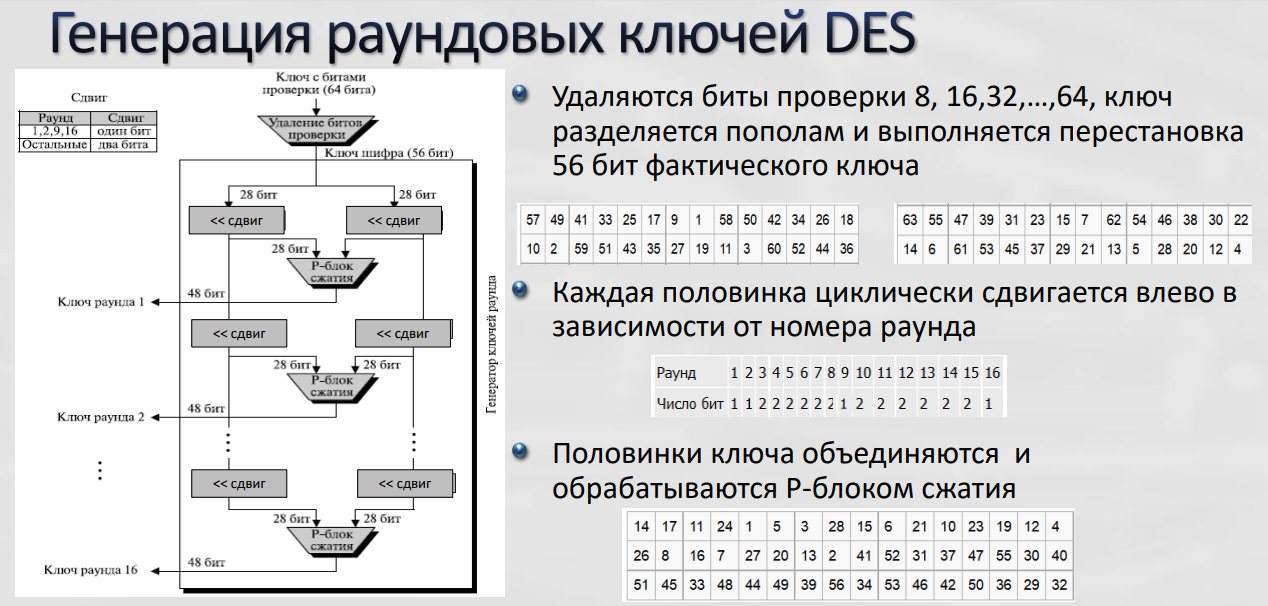
****

****

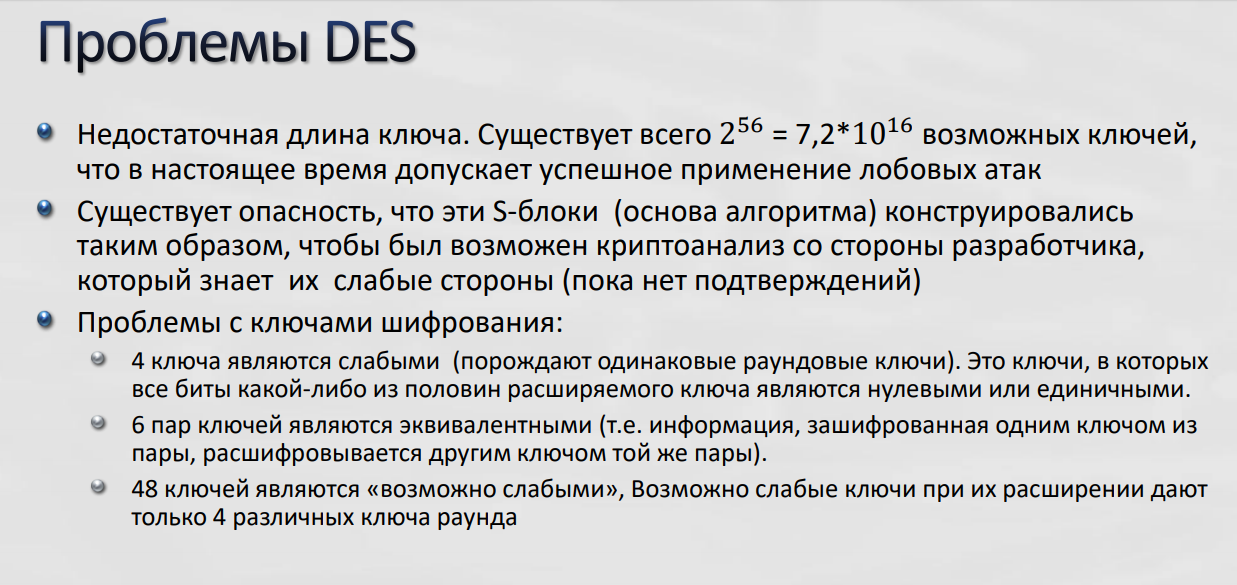
****









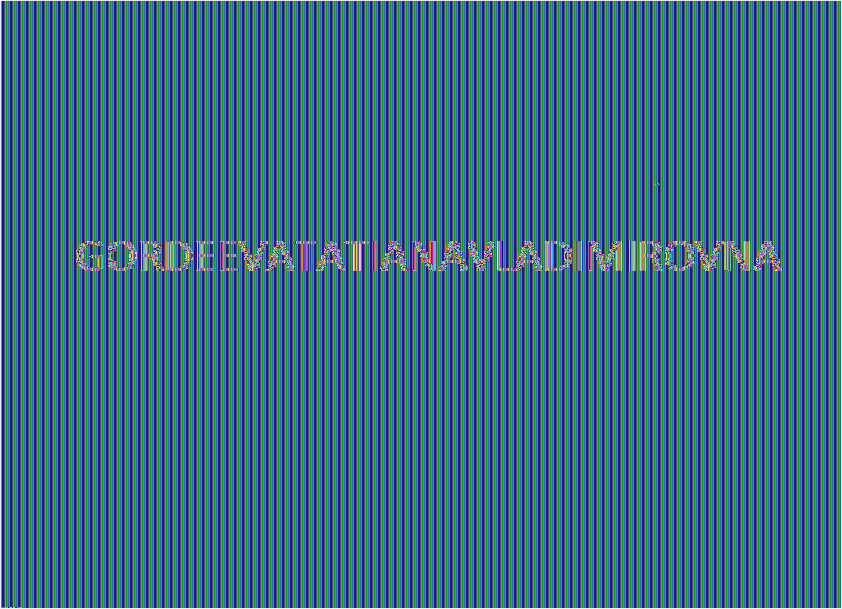


**2.3 Скриншоты исходного и шифрованных изображений в разных режимах работы шифров.**

Создадим картинку со своими ФИО (формат bmp).



Зашифруем картинку шифром DES в режиме ECB.



Зашифруем картинку шифром DES в режиме CBC c тем же ключом.



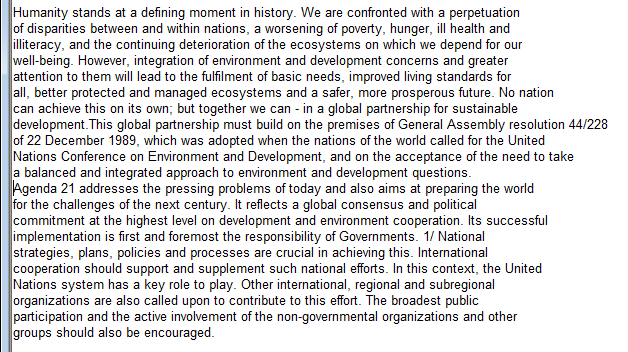
Сожмем исходную и 2 зашифрованных картинки средствами CrypTool. Зафиксируем размеры полученных файлов в таблице.

|  |  |  |
| --- | --- | --- |
|  | Начальный размер файла, Кб | Размер файла после сжатия, Кб |
| Исходная картинка | 1450 | 4.34 |
| ECB | 1450 | 11.6 |
| CBC | 1450 | 1450 |

**2.4 Таблица зависимости оценки времени атаки грубой силы от размера известной части ключа.**

Выберем случайный текст на английском языке (не менее 1000 знаков) и зашифруем его DES в режиме ECB.

Исходный текст:



Для одного и того же шифротекста оценим время проведения атаки «грубой силы» в случаях, когда известно n-4, n-6, n-8,.., 2 байт секретного ключа. Зафиксируем результаты измерений в таблице.

*Зависимость времени расшифровки при известной части ключа(ECB).*

|  |  |
| --- | --- |
| Известная часть ключа | Время расшифровки |
| 6 | около секунды |
| 5 | 28 секунд |
| 4 | 56 минут |
| 3 | 4.7 дня |
| 2 | 1.7 года |

Повторим подобные измерения для DES в режиме CBC.

*Зависимость времени расшифровки при известной части ключа(CBC).*

|  |  |
| --- | --- |
| Известная часть ключа | Время расшифровки |
| 6 | около секунды |
| 5 | 38 секунд |
| 4 | 1 час 23 минуты |
| 3 | 7.6 дня |
| 2 | 2.6 года |

**3 Исследование преобразований DES**

**3.1 Задание**

1. Выбрать случайный текст на английском языке (не менее 1000 знаков).

2. Создать бинарный файл с этим текстом, зашифровав и расшифровав его DES на 0-м ключе.

3. Снять и сохранить частотную и автокорреляционную характеристику этого файла.

4. Зашифровать бинарный файл шифром 3-DES в режиме ECB.

5. Снять и сохранить частотную и автокорреляционную характеристику файла с шифровкой.

6. Зашифровать исходный бинарный файл 3-DES в режиме CBC c тем же ключом.

7. Снять и сохранить частотную и автокорреляционную характеристику файла с шифровкой.

8. Определить экспериментальным путем по какой схеме работает реализация 3-DES в CrypTool. Сохранить подтверждающие скриншоты.

**3.2 Содержание раздела отчета**

1. Формулировка задания и содержание этой части отчета.

2. Основные параметры и обобщенная схема шифра (как в лекции).

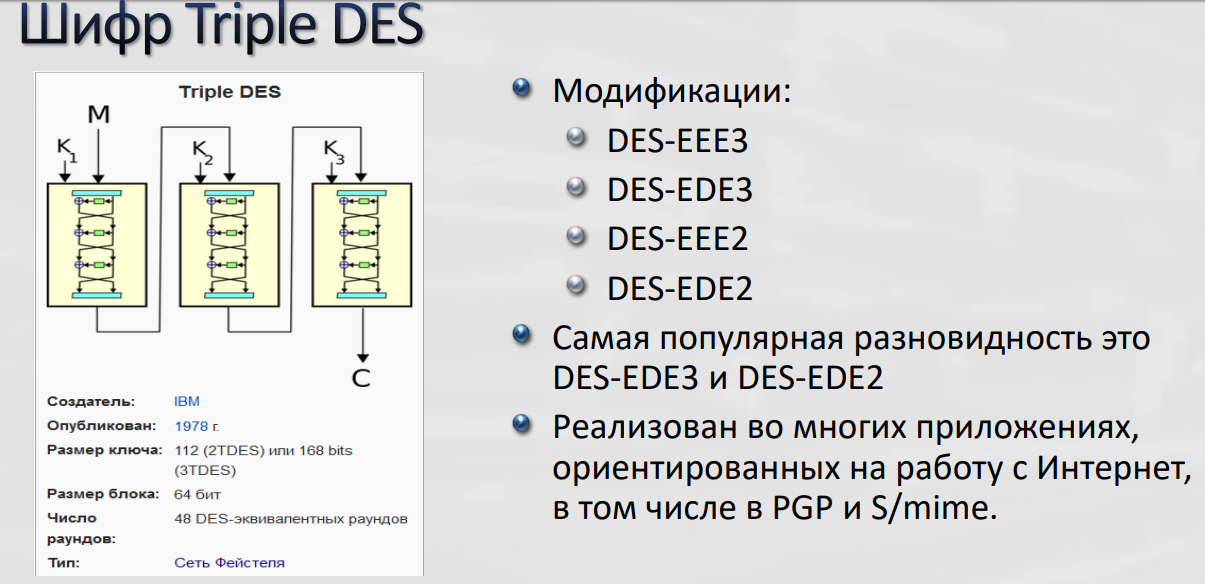
3. Скриншоты исходного и зашифрованного текста в бинарном представлении.

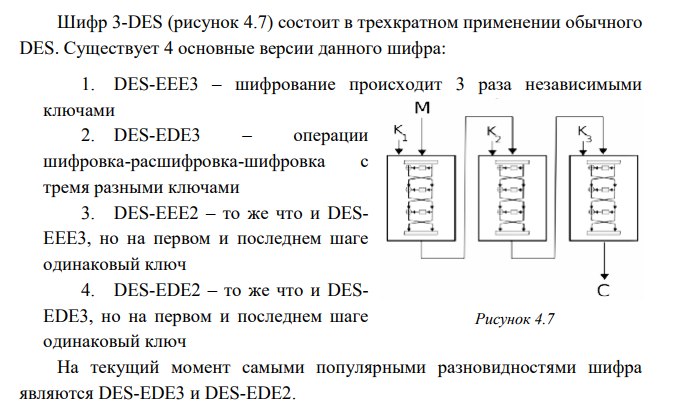
4. Скриншоты частотной и автокорреляционной характеристик исходного текста и шифровки.

5. Таблица зависимости времени атаки грубой силы от размера известной части ключа.

6. Схема реализации в CrypTool 1 и подтверждающие скриншоты.

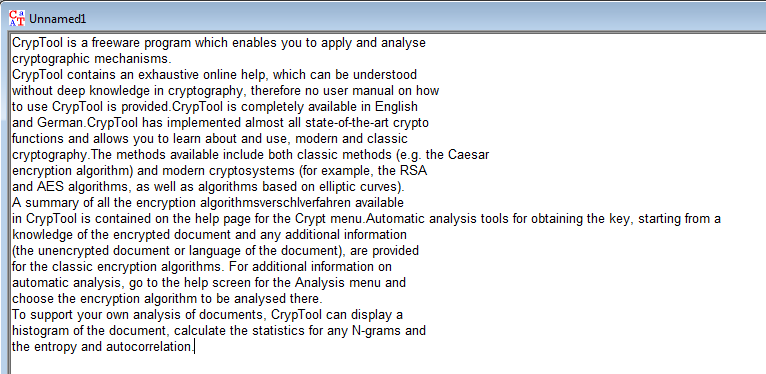
**3.3 Основные параметры и обобщенная схема шифра (как в лекции)**



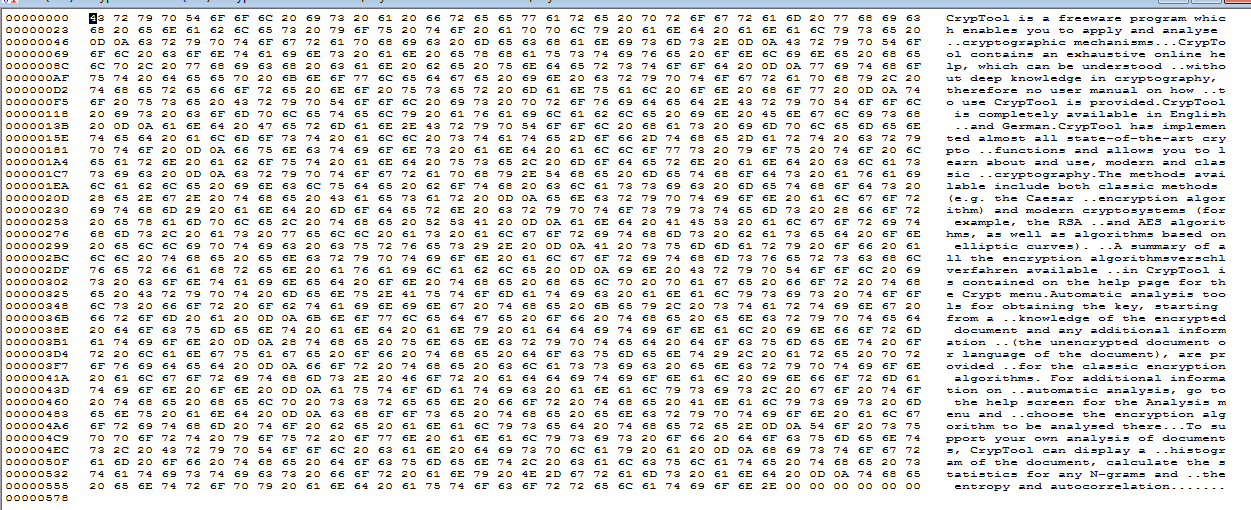


**3.4 Скриншоты исходного и зашифрованного текста в бинарном представлении. Скриншоты частотной и автокорреляционной характеристик исходного текста и шифровки.**

Выберем случайный текст на английском языке (не менее 1000 знаков).

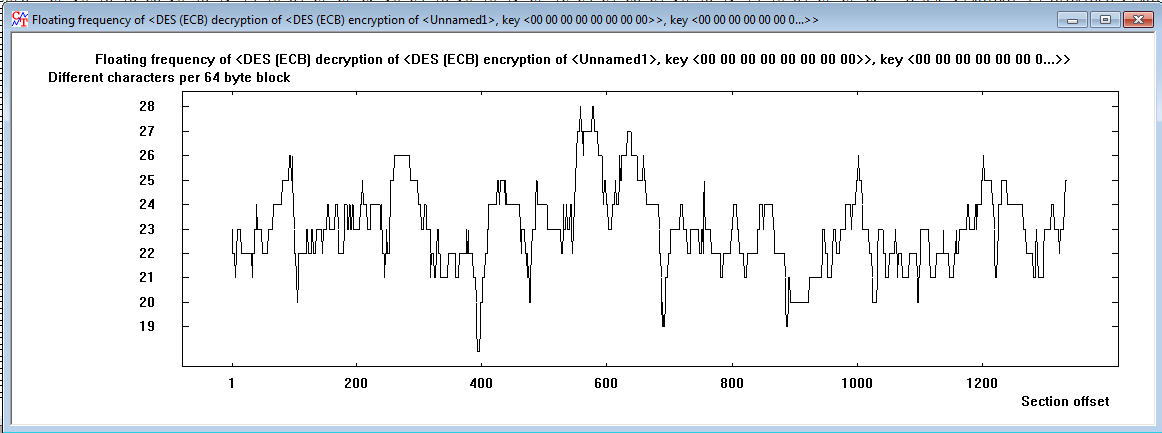


Создадим бинарный файл с этим текстом, зашифровав и расшифровав его DES на 0-м ключе.

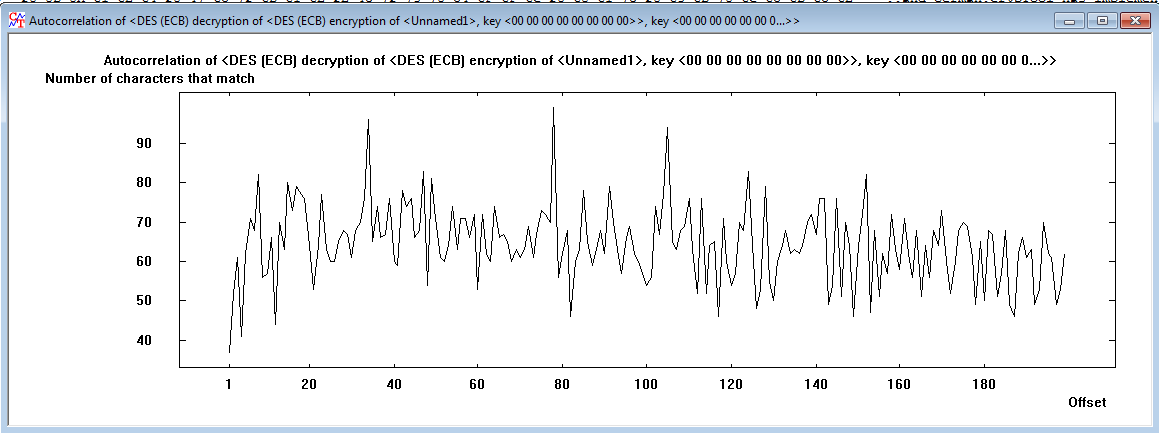


Снимем и сохраним частотную и автокорреляционную характеристику этого файла.

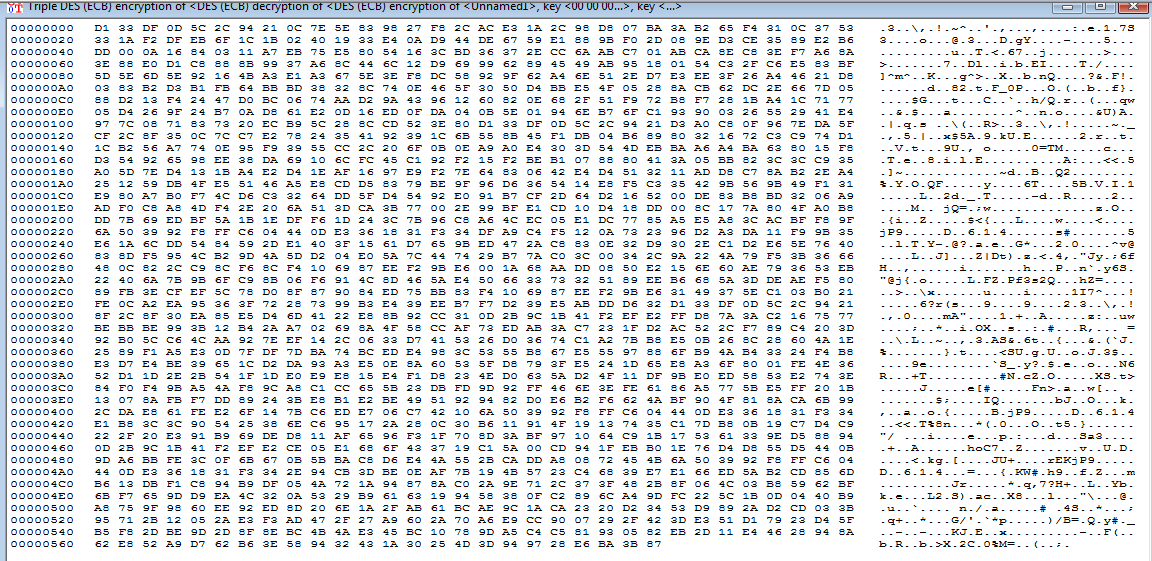
Частотная характеристика:



Автокорреляционная характеристика:

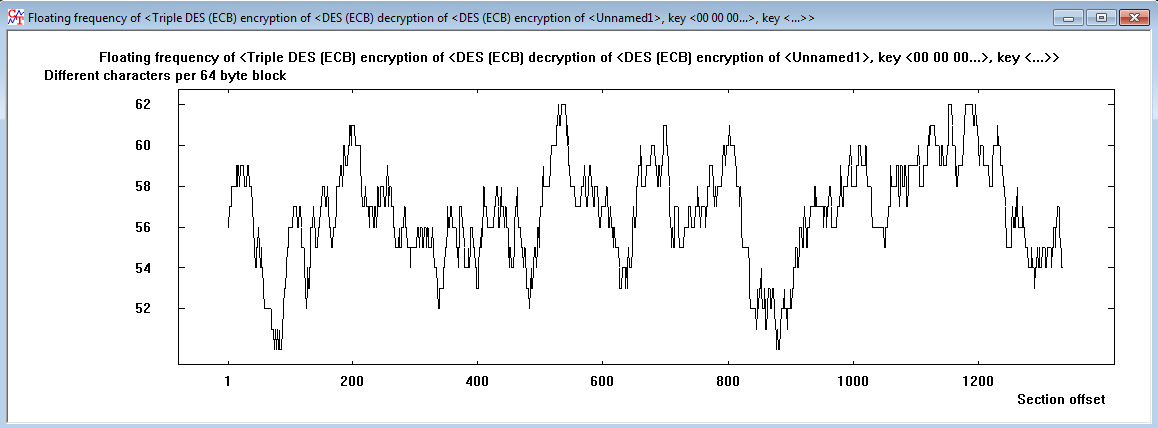


Зашифруем бинарный файл шифром 3-DES в режиме ECB.

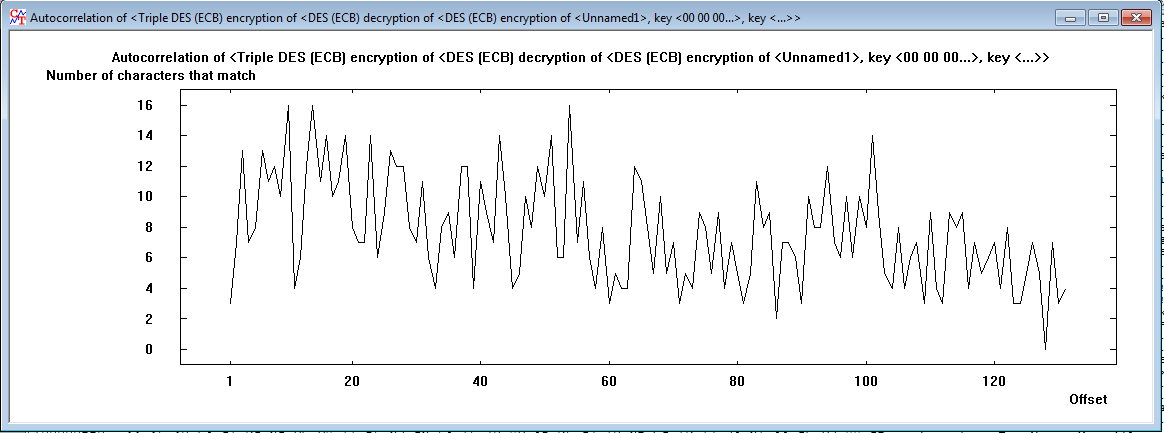


Снимем и сохраним частотную и автокорреляционную характеристику файла с шифровкой.

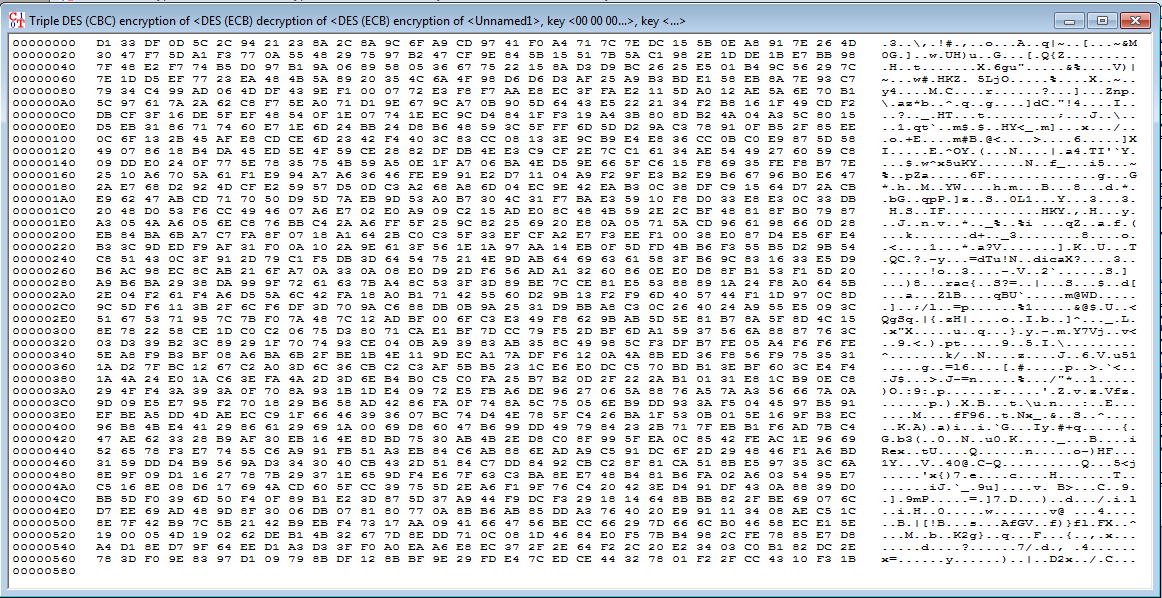
Частотная характеристика:



Автокорреляционная характеристика:

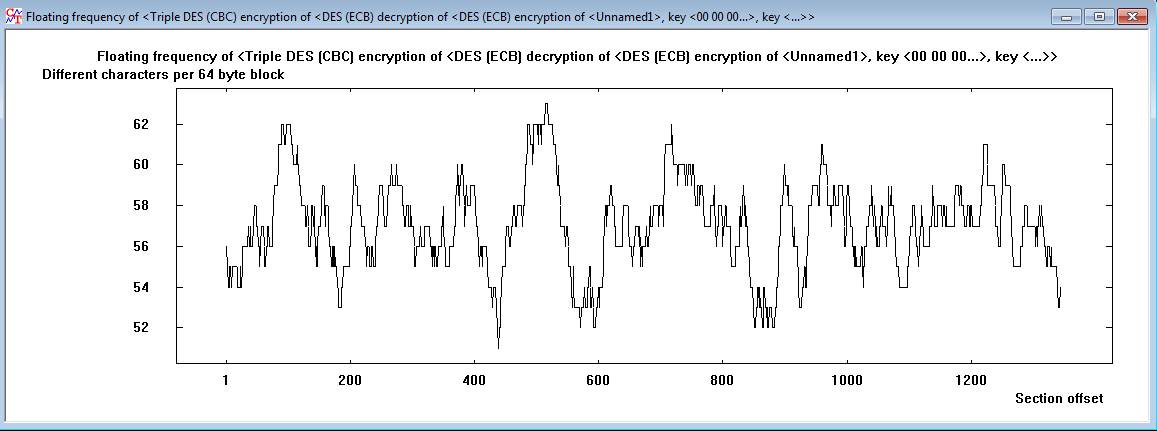


Зашифруем исходный бинарный файл 3-DES в режиме CBC c тем же ключом.

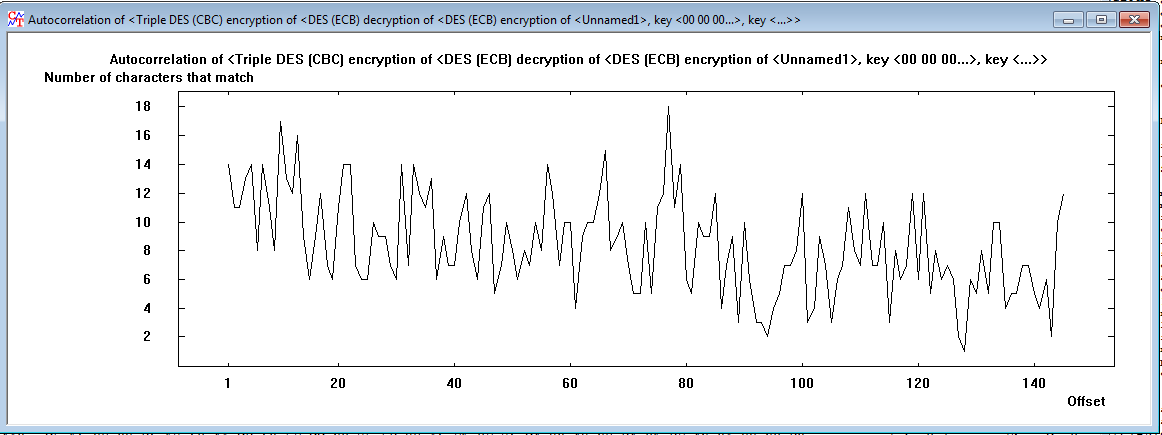


Снимем и сохраним частотную и автокорреляционную характеристику файла с шифровкой.

Частотная характеристика:



Автокорреляционная характеристика:



**3.5 Таблица зависимости времени атаки грубой силы от размера известной части ключа.**

*Зависимость времени расшифровки при известной части ключа(ECB).*

|  |  |
| --- | --- |
| Известная часть ключа | Время расшифровки |
| 14 | около секунды |
| 13 | 1 час 17 минут |
| 12 | 3 часа 15 минут |
| 11 | 18,5 дней |
| 10 | 4,5 года |
| 9 | 580 лет |

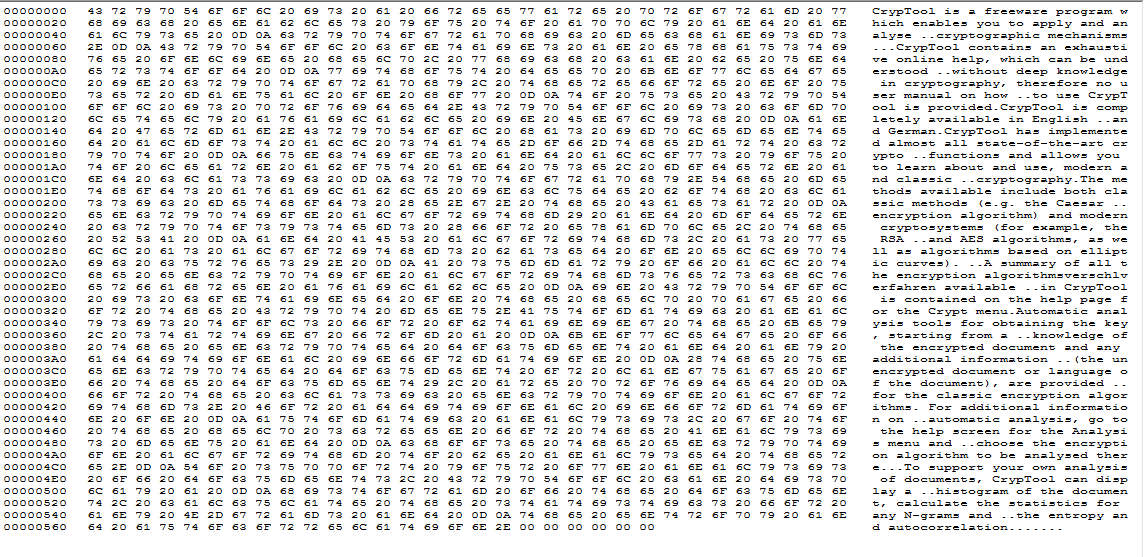
Повторим подобные измерения для 3-DES в режиме CBC.

*Зависимость времени расшифровки при известной части ключа(CBC).*

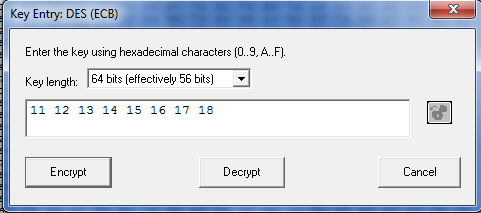
|  |  |
| --- | --- |
| Известная часть ключа | Время расшифровки |
| 14 | 1 секунда |
| 13 | 1 час 29 минут |
| 12 | 3 часа 49 минут |
| 11 | 18,1 дней |
| 10 | 6,4 года |
| 9 | 780 лет |

**3.6 Схема реализации в CrypTool 1 и подтверждающие скриншоты.**

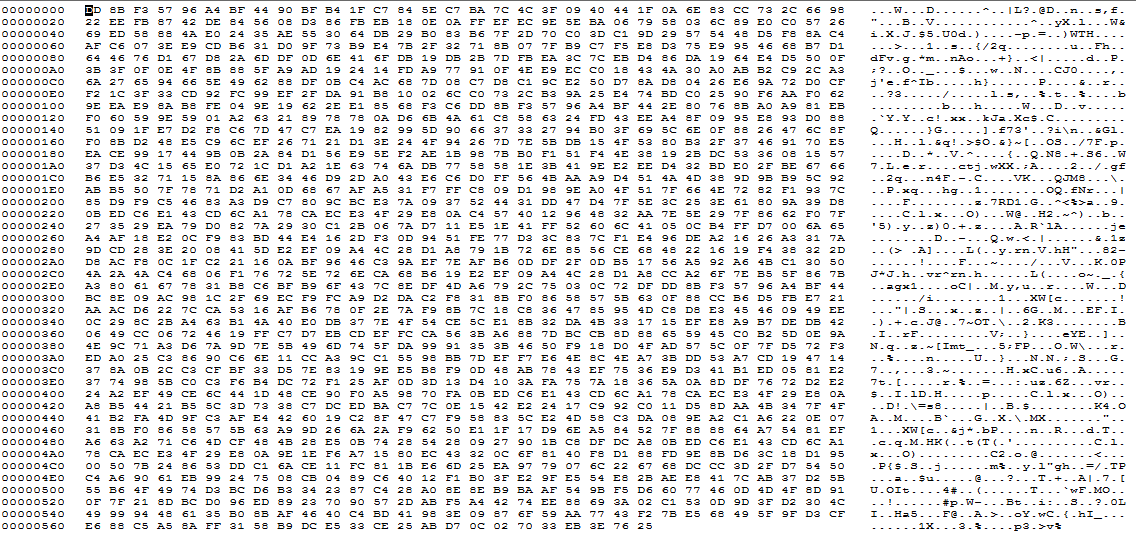
Рассмотрим следующий бинарный файл исходного текста:

****

Зашифруем его с использованием DES

****

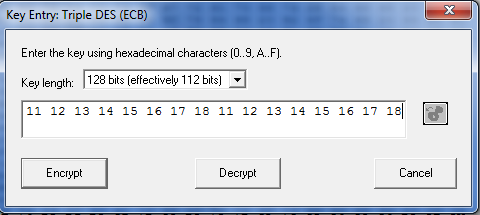
Полученный шифротекст:



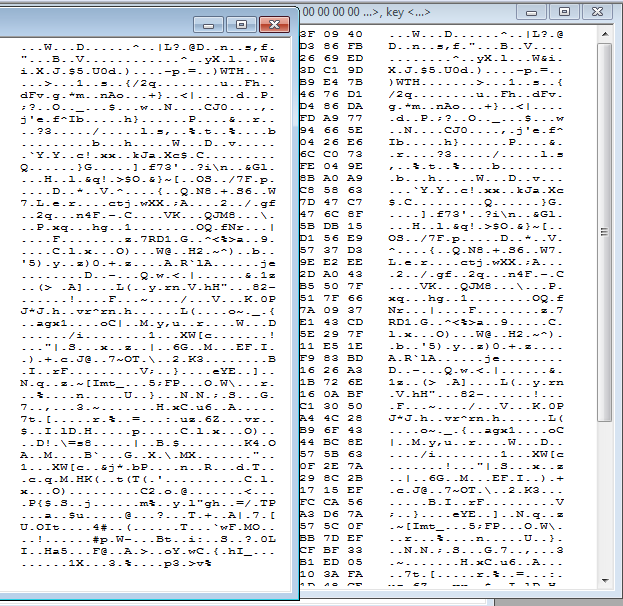
Так как длина ключа 3-DES, реализованного в Cryptool 1, состоит из 128 бит, то можно утверждать, что это не DES –EEE3, и это не DES-EDE3.

При шифровании DES-EDE2 одинаковый ключ на первом и последнем шаге. Если использовать одинаковый ключ на первом и втором этапе, то можно получить результат шифрования, аналогичный результату шифрования обычным DES.

Рассмотрим шифрование 3-DES со следующим ключом:



Полученный шифротекст:



Видно, что результат шифрования совпадает с шифрованием обычным DES. Следовательно, в CrypTool используется вариант DES-EDE2

**4 Исследование модификаций DESX, DESL, DESXL шифра DES**

**4.1 Задание**

1. Выбрать случайный текст на английском языке (не менее 1000 знаков).

2. Создать бинарный файл с этим текстом, зашифровав и расшифровав его DES на 0-м ключе.

3. С помощью CrypTool зашифровать текст с использованием шифров DESX, DESL, DESXL.

4. Средствами CrypTool вычислить энтропию исходного текста и шифротекстов, полученных в итоге. Зафиксировать результаты измерений в таблице.

5. Средствами CrypTool оцените время проведения атаки «грубой силы» при полном отсутствии информации о секретном ключе

**4.2 Содержание раздела отчета**

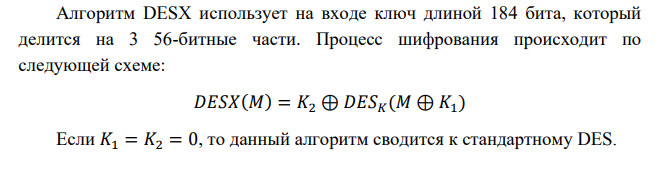
1. Формулировка задания и содержание этой части отчета.

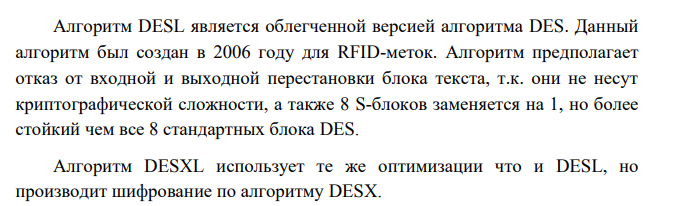
2. Основные параметры и обобщенные схемы шифров (самостоятельно).

3. Таблица зависимости энтропии шифротекста от используемого шифра.

4. Таблица зависимости времени подбора ключа от используемого шифра.

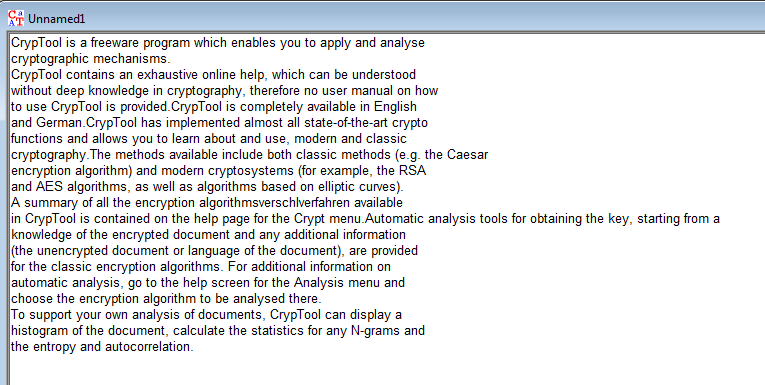
**4.3 Основные параметры и обобщенные схемы шифров (самостоятельно).**

****

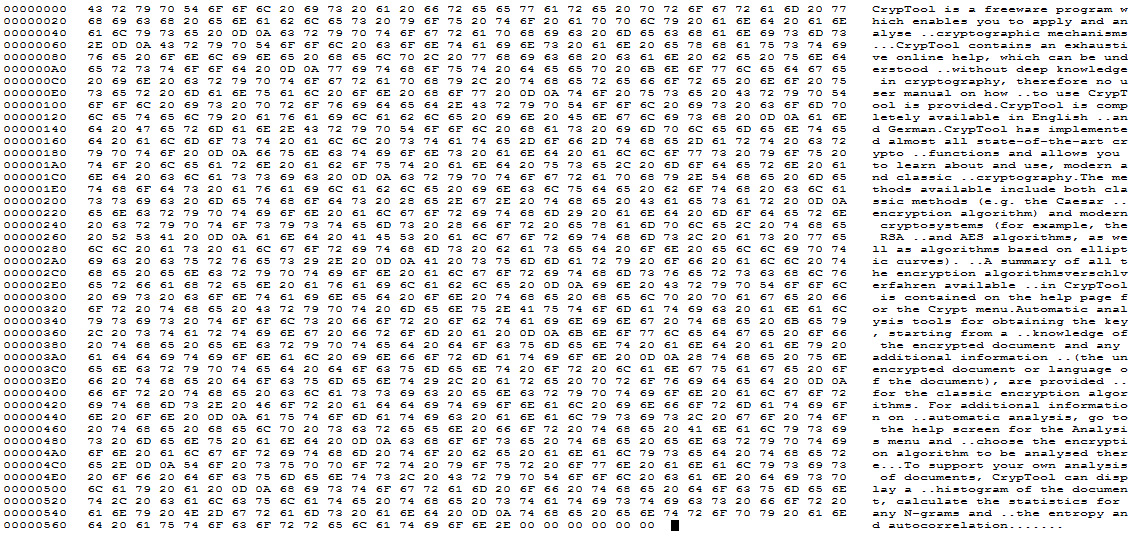
****

**4.4 Таблица зависимости энтропии шифротекста от используемого шифра.**

Выбрем случайный текст на английском языке (не менее 1000 знаков).

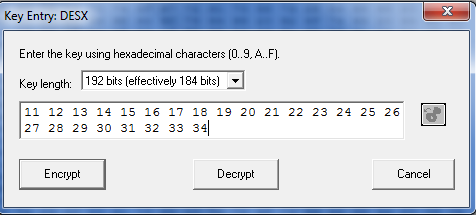


Создадим бинарный файл с этим текстом, зашифровав и расшифровав его DES на 0-м ключе.

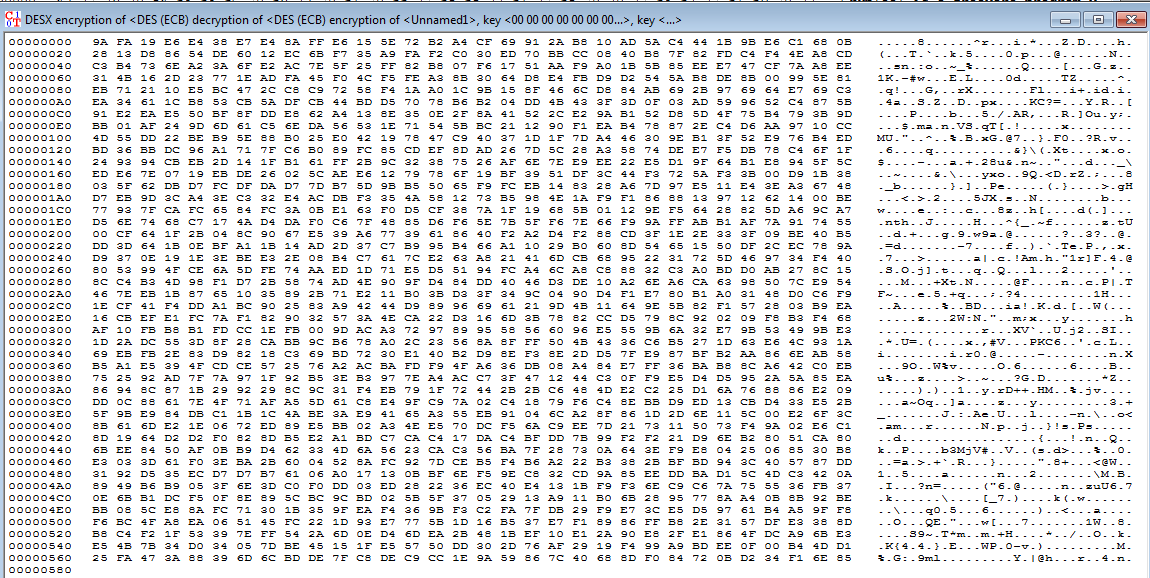


С помощью CrypTool зашифруем текст с использованием шифров DESX, DESL, DESXL.

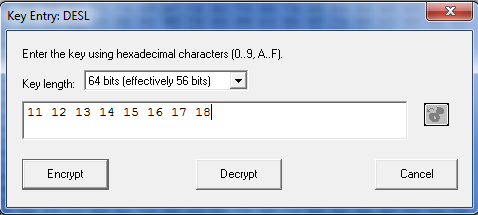
Шифрование текста с использованием шифра DESX



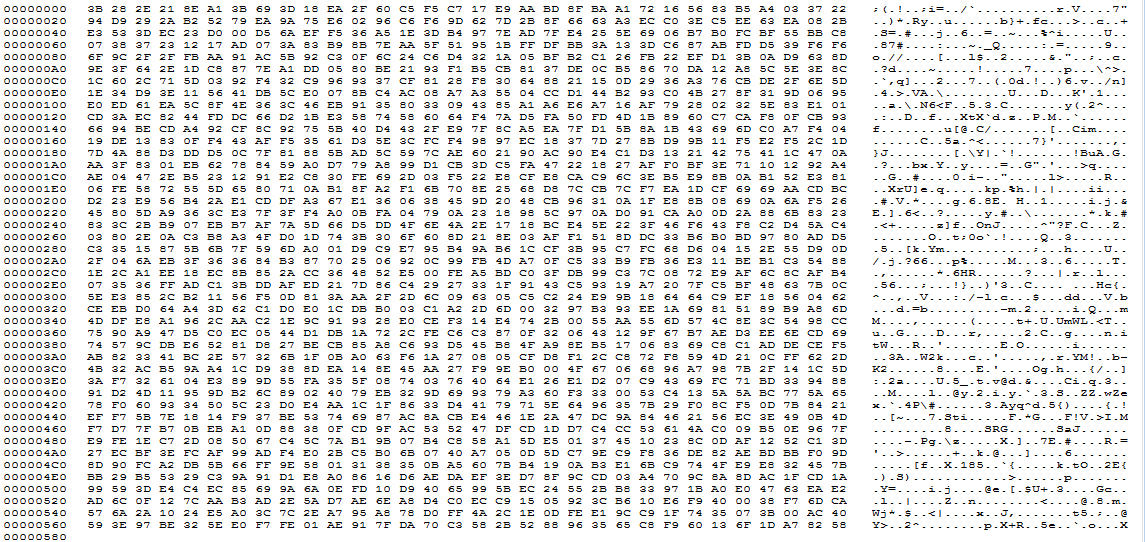
Полученный шифротекст:



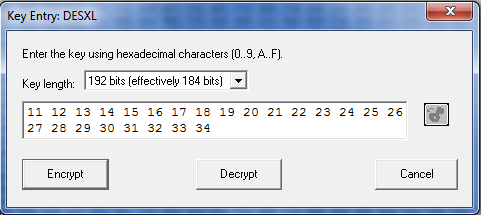
Шифрование текста с использованием шифра DESL



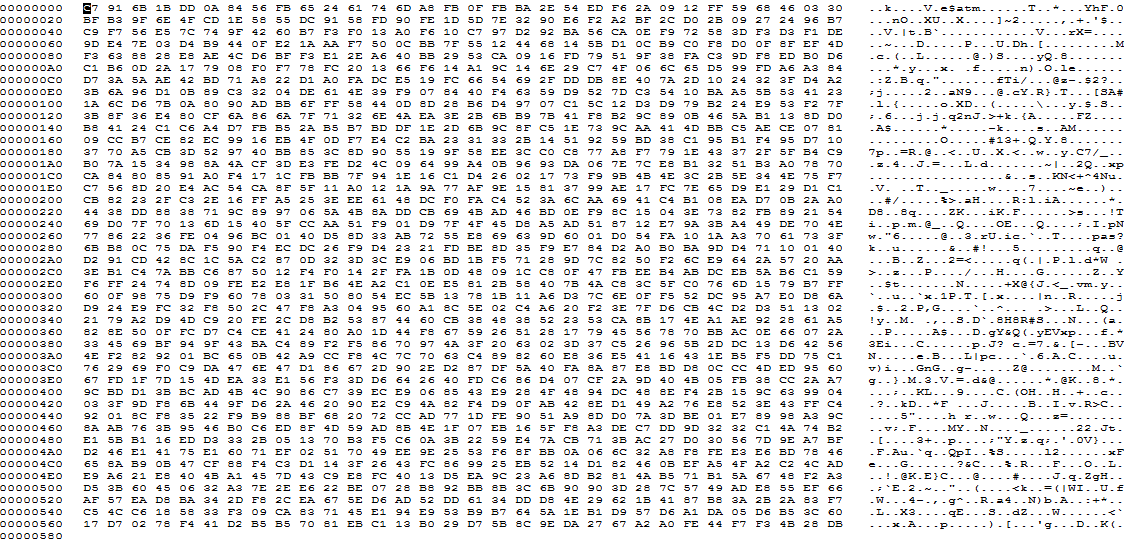
Полученный шифротекст:



Шифрование текста с использованием шифра DESLX

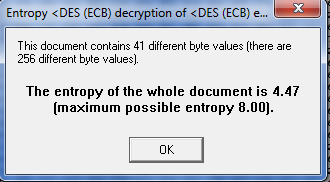


Полученный шифротекст:



Средствами CrypTool вычислим энтропию исходного текста и шифротекстов, полученных в итоге.

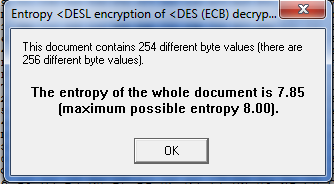
Энтропия исходного текста:



Энтропия текста, зашифрованного с использованием шифра DESX :



Энтропия текста, зашифрованного с использованием шифра DESL :



Энтропия текста, зашифрованного с использованием шифра DESLX :



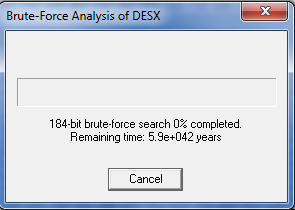
*Таблица зависимости энтропии шифротекста от используемого шифра.*

|  |  |
| --- | --- |
| Шифр | Энтропия |
| Исходный текст | 4,47 |
| DESX | 7,85 |
| DESL | 7,85 |
| DESLX | 7,85 |

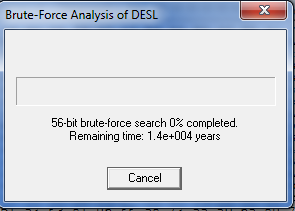
**4.5 Таблица зависимости времени подбора ключа от используемого шифра.**

Средствами CrypTool оценим время проведения атаки «грубой силы» при полном отсутствии информации о секретном ключе.

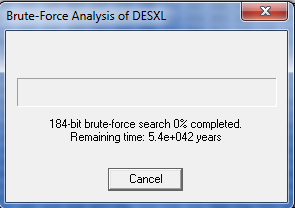
Шифр DESX :



Шифр DESL :



Шифр DESLX :



*Таблица зависимости времени подбора ключа от используемого шифра.*

|  |  |
| --- | --- |
| Шифр | Время подбора |
| DESX | 5,9\*1042 лет |
| DESL | 1,4\*104 лет |
| DESLX | 5,4\*1042 лет |

**5 Вывод** Алгоритм DES шифрует информацию блоками по 64 бита с помощью 54-битного ключа шифрования. Процесс шифрования состоит из 16 раундов операций над блоком с перестановкой и генерации 16 различных раундовых ключей. Расшифровывание данных алгоритмом DES происходит при прохождении всех шагов алгоритма в обратном порядке.

* Режим ECB

В данном режиме каждый блок шифруется отдельно. При этом можно получить различные зашифрованные блоки, которые изначально были одинаковыми.

* Режим CBC

В данном режиме каждый последующий блок использует результат шифрования предыдущего блока.

* 3-DES

Данная модификация шифра основана на трехкратном применении обычного DES с тремя или двумя независимыми ключами.

* DESX

Алгоритм DESX использует на входе ключ длиной 184 бита, который делится на 3 56-битные части. Процесс шифрования происходит по следующей схеме: 𝐷𝐸𝑆𝑋(𝑀) = 𝐾2 ⊕ 𝐷𝐸𝑆𝐾(𝑀 ⊕ 𝐾1)

* DESL

Алгоритм предполагает отказ от входной и выходной перестановки блока текста, а также 8 S-блоков заменяется на 1, но более стойкий чем все 8 стандартных блока DES.

* DESLX

Алгоритм DESXL использует те же оптимизации что и DESL, но производит шифрование по алгоритму DESX.

**Список источников**

* А. К. Племянников, Е.О. Кузнецова Криптографические методы защиты информации: лабораторный практикум. СПбГЭТУ «ЛЭТИ», 2016 55 с.