МИНОБРНАУКИ РОССИИ
САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ
ЭЛЕКТРОТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
«ЛЭТИ» ИМ. В.И.УЛЬЯНОВА (ЛЕНИНА)
Кафедра ИБ

ЛАБОРАТОРНАЯ РАБОТА №4

по дисциплине «Криптография и защита информации»

Тема: Изучение шифра DES

Студент гр. 6304 _____ Корытов П.В.
Преподаватель _____ Племянников А.К.

Санкт-Петербург
2019

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. Описание

DES (англ. Data Encryption Standart) — стандарт шифрования данных — блочный шифр с симетричными ключами. Разработан NIST (National Institute of Standarts and Technology).

1.1.1. Сеть Фейстеля

Шифр DES основан на сети Фейстеля (см. рисунок 1). Принцип работы сети следующий:

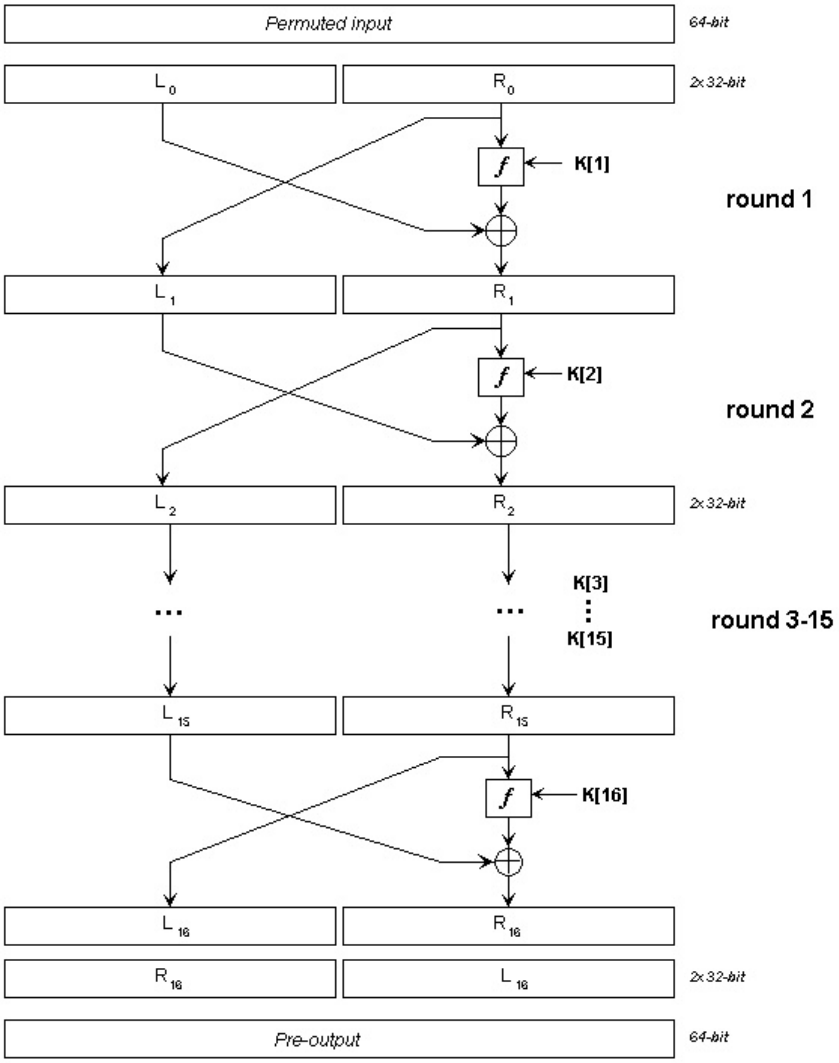


Рисунок 1. Сеть Фейстеля

1. Выбранный блок делится на два равных субблока L_0 и R_0
2. R_0 преобразуется функцией шифра $f(R_0, K_0)$, после чего складывается по модулю 2 с L_0
3. Результат сложения становится R_1, а R_0 становится L_1 для следующего раунда
4. Операция повторяется $N-1$ раз. При переходе между раундами меняются раундовые ключи $K_0, K_1, \ldots$.

Т.е.:

$$L_i = R_{i-1};$$

$$R_i = L_{i-1} \oplus f(R_{i-1}),$$

где i — номер текущего рауда, K_i — ключ раунда.

В шифре DES размер блока — 64 бита, число раундов — 16. Перед входом в сеть производится начальная перестановка.

1.1.2. Структура раудовой функции

Структура функции представлена на рисунке 2.

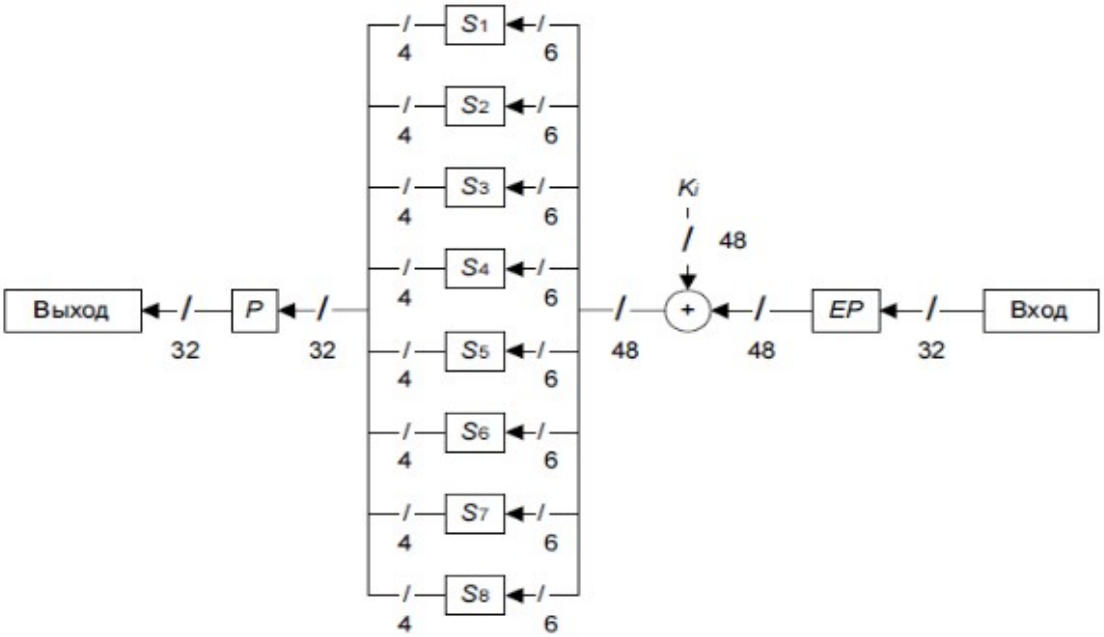


Рисунок 2. Структура f

Этапы функции:

1. Расширяющая перестановка, преобразует 32 бита в 48 бит (рисунок 3)
2. Полученные 48 бит складываются с K_i операцией xor (рисунок 4)

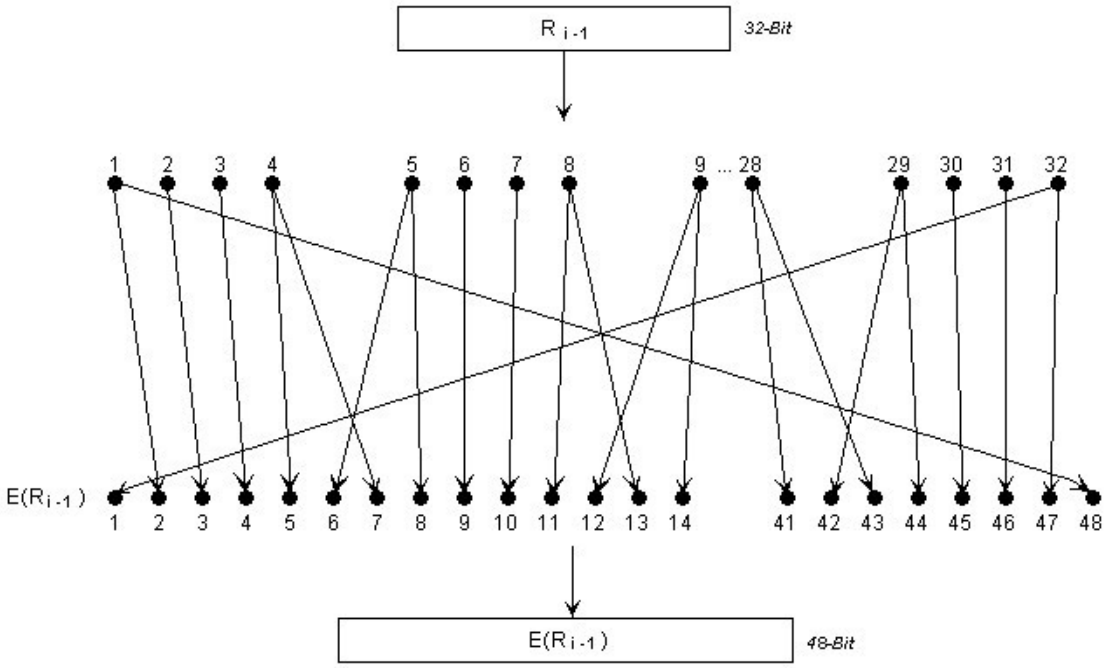


Рисунок 3. Расширящая перестановка

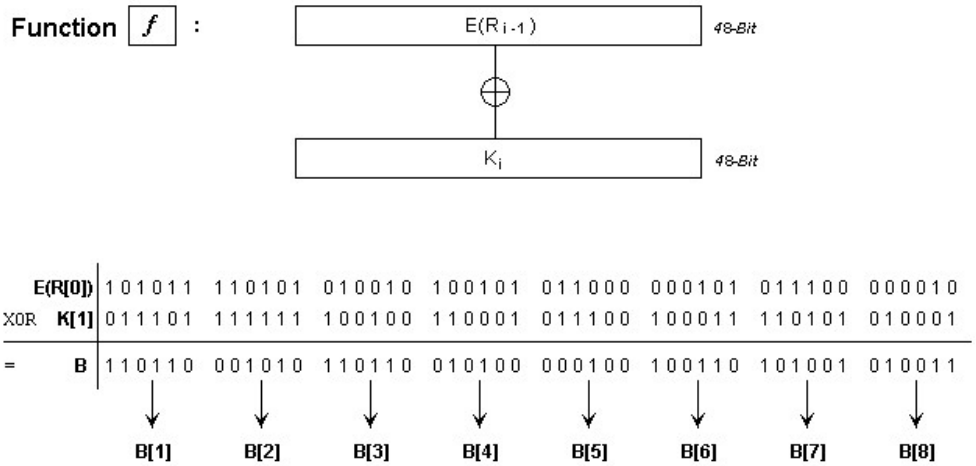


Рисунок 4. Побитовое сложение

3. Результат сложения разбивается на 8 блоков по 6 битов. Каждый блок обрабатывается соответствующей таблицей замен (рис. 5).
   - Первый и последний биты составляют стороку
   - Средние 4 бита — номер столбца

   Таблицы замен для каждого блока свои.
4. Над полученными 32 битами, после выполнения замен, выполняется перестановка (P)

1.1.3. Генерация раундовых ключей

Генерация раундовых ключей представлена на рисунке 6. Из 64-битного

110110	001010	110110	010100	000100	100110	101001	010011
B[1]	B[2]	B[3]	B[4]	B[5]	B[6]	B[7]	B[8]

10 = 1x2^1+0*2^0 = 2 1011 = 1*2^3+0*2^2+1*2^1+1*2^0 = 11

S-box 1:

row \ column	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	3

Рисунок 5. Таблица замен

ключа используется только 56 бит — каждый 8-й бит исключается. После выполняется перестановка (E).

После перестановки блок в 56 бит делится на два 28-битных блока (C, D). Затем выполняются 16 раудов преобразований:

1. Текущие C, D циклически сдвигаются влева на определенное количество бит
2. C, D объединяются в 56-битное значение, к которому применяется сжимающая перестановка CP. Получается 48-битный ключ.

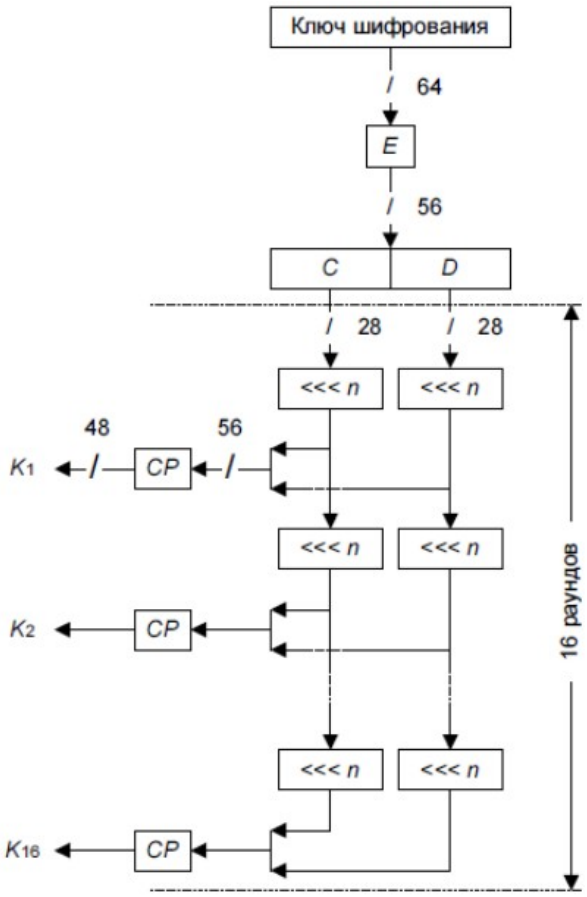


Рисунок 6. Генерация раундовых ключей

1.2. Формулировка задания

1. Изучить преобразования шифра DES с помощью демонстрационного приложения из Cryptool 1.
   - Indiv.Procedures-> Visualization…-> DES…
2. Выполнить вручную преобразования одного раунда и вычисление раундовых ключей при следующих исходных данных:
   - Открытый текст (не более 64 бит) – фамилия_имя (транслитерация латиницей)
   - Ключ (56 бит) – номер зачетной книжки II инициал (всего 7 символов)
3. Выполнить вручную обратное преобразование зашифрованного сообщения

1.3. Ход работы

1. С помощью демонстрационного приложения изучена работа шифра. В 1.1 вставлены скриншоты.
2. Проведено ручное преобразование одного раунда.

Открытый текст — `KORYTOVP`, ключ — `0630417`. Перестановки выбраны отсутствующие.

3. Произведено преобразование в бинарный формат:
   - `KORYTOVP` — `01001011 01001111 01010010 01011001 01010100 01001111 01010110 01010000`
   - `0630417` — `00110000 00110110 00110011 00110000 00110100 00110001 00110111`

   В матричном виде:

$$I = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \end{bmatrix}; K = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \end{bmatrix} \tag{1.1}$$

4. Сначала нужно вычислить раундовый ключ. Из таблиц DES взята перестановка PC1:

$$PC1 = \begin{bmatrix} 57 & 49 & 41 & 33 & 25 & 17 & 9 \\ 1 & 58 & 50 & 42 & 34 & 26 & 18 \\ 10 & 2 & 59 & 51 & 43 & 35 & 27 \\ 19 & 11 & 3 & 60 & 52 & 44 & 36 \\ 63 & 55 & 47 & 39 & 31 & 23 & 15 \\ 7 & 62 & 54 & 46 & 38 & 30 & 22 \\ 14 & 6 & 61 & 53 & 45 & 37 & 29 \\ 21 & 13 & 5 & 28 & 20 & 12 & 4 \end{bmatrix} \tag{1.2}$$

   К ключу добавлен ещё один пустой столбец, произведена перестановка:

$$K_{perm} = PC1(K) = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \end{bmatrix} \tag{1.3}$$

5. Ключ разделен на две части, произведен циклический сдвиг:

$$K_L = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

$$K_R = \begin{bmatrix} 0 & 1 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \end{bmatrix}$$

$$\Rightarrow K_{roll1} = \begin{bmatrix} >> K_L \\ >> K_R \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \end{bmatrix} \tag{1.4}$$

6. К сдвинутому ключу применена перестановка PC2. Получен первый раундовый ключ

$$PC2 = \begin{bmatrix} 14 & 17 & 11 & 24 & 1 & 5 \\ 3 & 28 & 15 & 6 & 21 & 10 \\ 23 & 19 & 12 & 4 & 26 & 8 \\ 16 & 7 & 27 & 20 & 13 & 2 \\ 41 & 52 & 31 & 37 & 47 & 55 \\ 30 & 40 & 51 & 45 & 33 & 48 \\ 44 & 49 & 39 & 56 & 34 & 53 \\ 46 & 42 & 50 & 36 & 29 & 32 \end{bmatrix}; K_1 = PC2(K_{roll1}) = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix} \tag{1.5}$$

7. Ко входному тексту (1.1) применена перестановка IP:

$$\begin{bmatrix} 58 & 50 & 42 & 34 & 26 & 18 & 10 & 2 \\ 60 & 52 & 44 & 36 & 28 & 20 & 12 & 4 \\ 62 & 54 & 46 & 38 & 30 & 22 & 14 & 6 \\ 64 & 56 & 48 & 40 & 32 & 24 & 16 & 8 \\ 57 & 49 & 41 & 33 & 25 & 17 & 9 & 1 \\ 59 & 51 & 43 & 35 & 27 & 19 & 11 & 3 \\ 61 & 53 & 45 & 37 & 29 & 21 & 13 & 5 \\ 63 & 55 & 47 & 39 & 31 & 23 & 15 & 7 \end{bmatrix} \tag{1.6}$$

$$I_{perm} = IP(I) = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 \end{bmatrix} \tag{1.7}$$

8. Текст разделен на два блока:

$$\begin{aligned} L_0 &= \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \end{bmatrix} \\ R_0 &= \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 \end{bmatrix} \end{aligned} \tag{1.8}$$

9. К R_0 применена функция f. Сначала применена расширяющая переста-

новка:

$$EP = \begin{bmatrix} 32 & 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 6 & 7 & 8 & 9 \\ 8 & 9 & 10 & 11 & 12 & 13 \\ 12 & 13 & 14 & 15 & 16 & 17 \\ 16 & 17 & 18 & 19 & 20 & 21 \\ 20 & 21 & 22 & 23 & 24 & 25 \\ 24 & 25 & 26 & 27 & 28 & 29 \\ 28 & 29 & 30 & 31 & 32 & 1 \end{bmatrix}; R_{0E} = EP(R_0) = \begin{bmatrix} 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix} \tag{1.9}$$

Затем — сложение по модулю с раундовым ключом K_1 (1.5):

$$R_{0X} = R_{0E} \oplus K_1 = \begin{bmatrix} 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \tag{1.10}$$

После применены таблицы подстановки:

$$S_0 = \begin{bmatrix} 14 & 4 & 13 & 1 & 2 & 15 & 11 & 8 & 3 & 10 & 6 & 12 & 5 & 9 & 0 & 7 \\ 0 & 15 & 7 & 4 & 14 & 2 & 13 & 1 & 10 & 6 & 12 & 11 & 9 & 5 & 3 & 8 \\ 4 & 1 & 14 & 8 & 13 & 6 & 2 & 11 & 15 & 12 & 9 & 7 & 3 & 10 & 5 & 0 \\ 15 & 12 & 8 & 2 & 4 & 9 & 1 & 7 & 5 & 11 & 3 & 14 & 10 & 0 & 6 & 13 \end{bmatrix}$$

$$S_1 = \begin{bmatrix} 15 & 1 & 8 & 14 & 6 & 11 & 3 & 4 & 9 & 7 & 2 & 13 & 12 & 0 & 5 & 10 \\ 3 & 13 & 4 & 7 & 15 & 2 & 8 & 14 & 12 & 0 & 1 & 10 & 6 & 9 & 11 & 5 \\ 0 & 14 & 7 & 11 & 10 & 4 & 13 & 1 & 5 & 8 & 12 & 6 & 9 & 3 & 2 & 15 \\ 13 & 8 & 10 & 1 & 3 & 15 & 4 & 2 & 11 & 6 & 7 & 12 & 0 & 5 & 14 & 9 \end{bmatrix} \tag{1.11}$$

$$S_2 = \begin{bmatrix} 10 & 0 & 9 & 14 & 6 & 3 & 15 & 5 & 1 & 13 & 12 & 7 & 11 & 4 & 2 & 8 \\ 13 & 7 & 0 & 9 & 3 & 4 & 6 & 10 & 2 & 8 & 5 & 14 & 12 & 11 & 15 & 1 \\ 13 & 6 & 4 & 9 & 8 & 15 & 3 & 0 & 11 & 1 & 2 & 12 & 5 & 10 & 14 & 7 \\ 1 & 10 & 13 & 0 & 6 & 9 & 8 & 7 & 4 & 15 & 14 & 3 & 11 & 5 & 2 & 12 \end{bmatrix}$$

$$S_3 = \begin{bmatrix} 7 & 13 & 14 & 3 & 0 & 6 & 9 & 10 & 1 & 2 & 8 & 5 & 11 & 12 & 4 & 15 \\ 13 & 8 & 11 & 5 & 6 & 15 & 0 & 3 & 4 & 7 & 2 & 12 & 1 & 10 & 14 & 9 \\ 10 & 6 & 9 & 0 & 12 & 11 & 7 & 13 & 15 & 1 & 3 & 14 & 5 & 2 & 8 & 4 \\ 3 & 15 & 0 & 6 & 10 & 1 & 13 & 8 & 9 & 4 & 5 & 11 & 12 & 7 & 2 & 14 \end{bmatrix}$$

$$S_4 = \begin{bmatrix} 2 & 12 & 4 & 1 & 7 & 10 & 11 & 6 & 8 & 5 & 3 & 15 & 13 & 0 & 14 & 9 \\ 14 & 11 & 2 & 12 & 4 & 7 & 13 & 1 & 5 & 0 & 15 & 10 & 3 & 9 & 8 & 6 \\ 4 & 2 & 1 & 11 & 10 & 13 & 7 & 8 & 15 & 9 & 12 & 5 & 6 & 3 & 0 & 14 \\ 11 & 8 & 12 & 7 & 1 & 14 & 2 & 13 & 6 & 15 & 0 & 9 & 10 & 4 & 5 & 3 \end{bmatrix}$$

$$S_5 = \begin{bmatrix} 12 & 1 & 10 & 15 & 9 & 2 & 6 & 8 & 0 & 13 & 3 & 4 & 14 & 7 & 5 & 11 \\ 10 & 15 & 4 & 2 & 7 & 12 & 9 & 5 & 6 & 1 & 13 & 14 & 0 & 11 & 3 & 8 \\ 9 & 14 & 15 & 5 & 2 & 8 & 12 & 3 & 7 & 0 & 4 & 10 & 1 & 13 & 11 & 6 \\ 4 & 3 & 2 & 12 & 9 & 5 & 15 & 10 & 11 & 14 & 1 & 7 & 6 & 0 & 8 & 13 \end{bmatrix}$$

$$S_6 = \begin{bmatrix} 4 & 11 & 2 & 14 & 15 & 0 & 8 & 13 & 3 & 12 & 9 & 7 & 5 & 10 & 6 & 1 \\ 13 & 0 & 11 & 7 & 4 & 9 & 1 & 10 & 14 & 3 & 5 & 12 & 2 & 15 & 8 & 6 \\ 1 & 4 & 11 & 13 & 12 & 3 & 7 & 14 & 10 & 15 & 6 & 8 & 0 & 5 & 9 & 2 \\ 6 & 11 & 13 & 8 & 1 & 4 & 10 & 7 & 9 & 5 & 0 & 15 & 14 & 2 & 3 & 12 \end{bmatrix}$$

$$S_7 = \begin{bmatrix} 13 & 2 & 8 & 4 & 6 & 15 & 11 & 1 & 10 & 9 & 3 & 14 & 5 & 0 & 12 & 7 \\ 1 & 15 & 13 & 8 & 10 & 3 & 7 & 4 & 12 & 5 & 6 & 11 & 0 & 14 & 9 & 2 \\ 7 & 11 & 4 & 1 & 9 & 12 & 14 & 2 & 0 & 6 & 10 & 13 & 15 & 3 & 5 & 8 \\ 2 & 1 & 14 & 7 & 4 & 10 & 8 & 13 & 15 & 12 & 9 & 0 & 3 & 5 & 6 & 11 \end{bmatrix} \tag{1.12}$$

$$S = \langle S_0, S_1, S_2, S_3, S_4, S_5, S_6, S_7 \rangle \tag{1.13}$$

$$R_{0S} = S(R_{0X}) = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{bmatrix} \tag{1.14}$$

После чего применена перестановка P:

$$P = \begin{bmatrix} 16 & 7 & 20 & 21 \\ 29 & 12 & 28 & 17 \\ 1 & 15 & 23 & 26 \\ 5 & 18 & 31 & 10 \\ 2 & 8 & 24 & 14 \\ 32 & 27 & 3 & 9 \\ 19 & 13 & 30 & 6 \\ 22 & 11 & 4 & 25 \end{bmatrix}; R_1 = P(R_{0X}) = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix} \tag{1.15}$$

10. $L_1 = R_0$. Для IP (1.6) вычислена обратная перестановка IP^{-1}:

$$IP^{-1} = \begin{bmatrix} 40 & 8 & 48 & 16 & 56 & 24 & 64 & 32 \\ 39 & 7 & 47 & 15 & 55 & 23 & 63 & 31 \\ 38 & 6 & 46 & 14 & 54 & 22 & 62 & 30 \\ 37 & 5 & 45 & 13 & 53 & 21 & 61 & 29 \\ 36 & 4 & 44 & 12 & 52 & 20 & 60 & 28 \\ 35 & 3 & 43 & 11 & 51 & 19 & 59 & 27 \\ 34 & 2 & 42 & 10 & 50 & 18 & 58 & 26 \\ 33 & 1 & 41 & 9 & 49 & 17 & 57 & 25 \end{bmatrix} \tag{1.16}$$

11. Получен шифротекст.

$$T = IP^{-1}\left(\begin{bmatrix} L_1 \\ R_1 \end{bmatrix}\right) = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} \tag{1.17}$$

12. Проведена расшифровка. Для этого сначала проведена перестановка IP (1.6):

$$T_{IP} = IP(T) = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} \tag{1.18}$$

13. Текст разделен на две части. $R_0 = L_1$ — известна. К $R0$ применена функция f, результаты применения совпадают с описанными в уравнениях 1.9–1.15

$$f(R_0, K_1) = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix} \tag{1.19}$$

Теперь по R_1 и $f(R_0)$ вычислен L_0:

$$L_0 = R_1 \oplus f(R_0) = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \end{bmatrix} \tag{1.20}$$

14. К получившемуся тексту применена IP^{-1}:

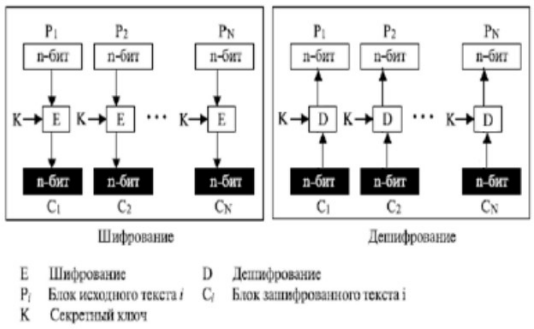
$$I_d = IP^{-1}\left(\begin{bmatrix} L_0 \\ R_0 \end{bmatrix}\right) = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \end{bmatrix} \tag{1.21}$$

Результаты совпадают.

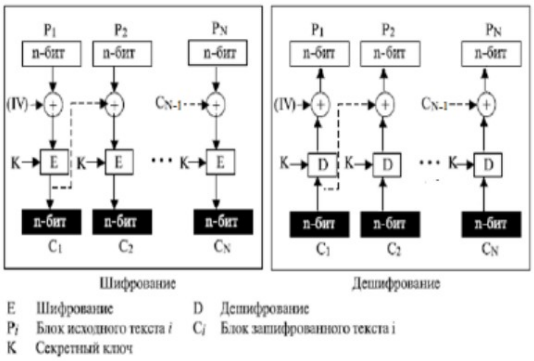
2. Исследование DES в режимах ECB и CBC

2.1. Описание

Режим ECB (рис. 7a) шифра DES работает независимо с каждым 64-битным блоком шифруемых данных. Режим CBC (рис. 7b) перед запуском шифрования каждого очередного блока складывает его с предыдущим операцией xor



(a) Режим ECB



(b) Режим CBC

Рисунок 7. Режимы DES

2.2. Формулировка задания

- Создать картинку со своими ФИО (формат bmp).
- Зашифровать картинку шифром DES в режиме ECB.
- Зашифровать картинку шифром DES в режиме CBC с тем же ключом.
- Сохранить скриншоты картинок для отчета.
- Сжать исходную и 2 зашифрованных картинки средствами CrypTool. Зафиксировать размеры полученных файлов в таблице.
- Выбрать случайный текст на английском языке (не менее 1000 знаков) и зашифровать его DES в режиме ECB.
- 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.

2.3. Ход работы

- Создана картинка с ФИО автора в формате .bmp

Рисунок 8. ФИО автора

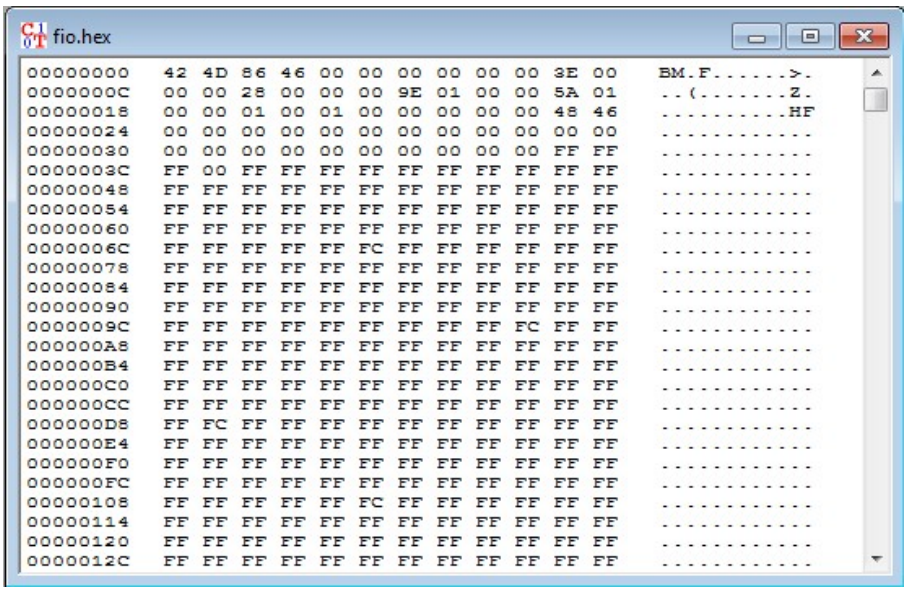


Рисунок 9. fio.hex

- В формате BMP первые 54 бита являются заголовком; их нужно убрать, чтобы потом можно было открыть расшифрованную картинку.

  Картинка зашифрована в режиме ECB ключом `88 00 55 53 53 50 63 04`. 54 бита из заголовка восстановлены. Результаты на рис. 10. Как можно

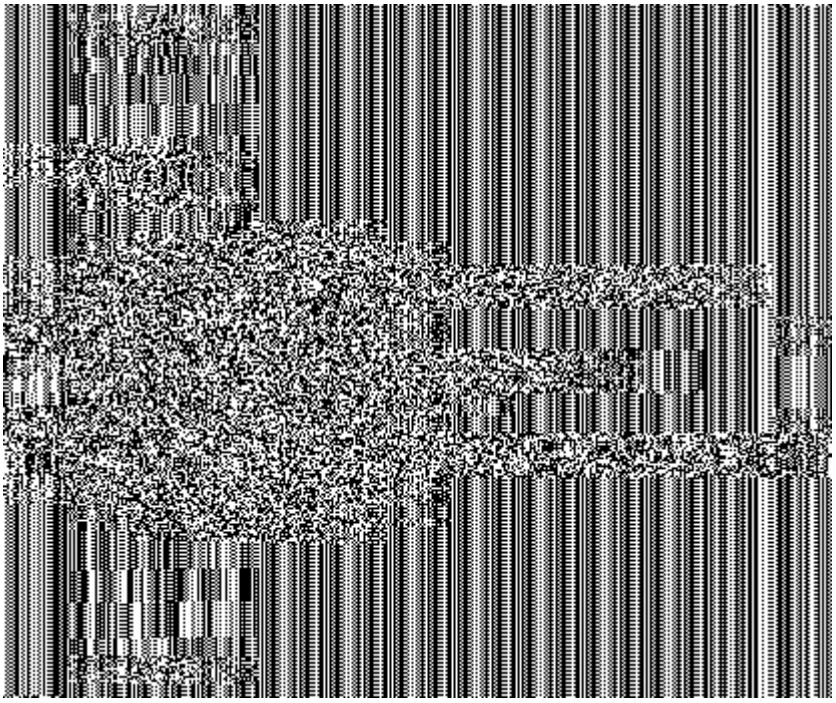


Рисунок 10. Шифрование DES (ECB)

видеть, из-за того, что блоки независимы, однаковые блоки шифруются одинаково. Контуры фигуры всё ещё видно.

Если сделать изображение 16-битное, то становится видно ещё лучше (рис. 11)

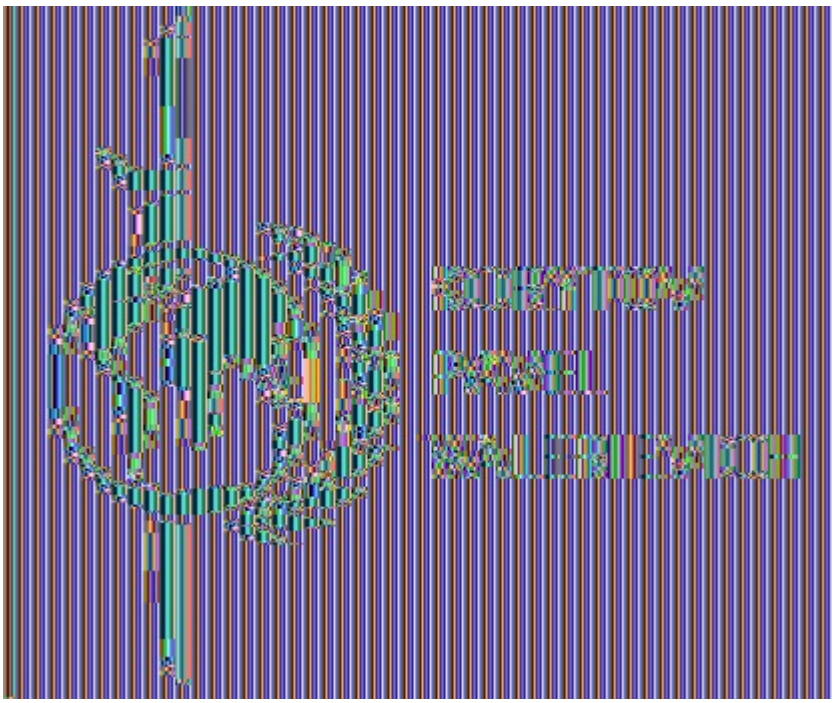


Рисунок 11. Шифрование DES (ECB) для 16-битного изображения

- Проведено шифрование в режиме CBC. Изображение более неразличимо (рис. 12)
- Произведено сжатие (Indiv. Procedures > Tools > Compression > Zip) получившихся файлов.

Файл	**Процент сжатия**
Исходный	87%
DES (ECB)	66%
DES (CBC)	0%

Как можно заметить, файл, сжатый DES в режиме CBC, не сжался вовсе

- Для шифрования взят абзац из книги Ричарда Докинза “Delusion God”. Произведено зашифрование DES (ECB).
- Исследовано время атак грубой силой на шифр, если известно некоторое количество байт ключа:

Известно байт	6	5	4	3	2
Время дешифровки	0 с	21 с	43 мин	3.8 дней	1.8 лет

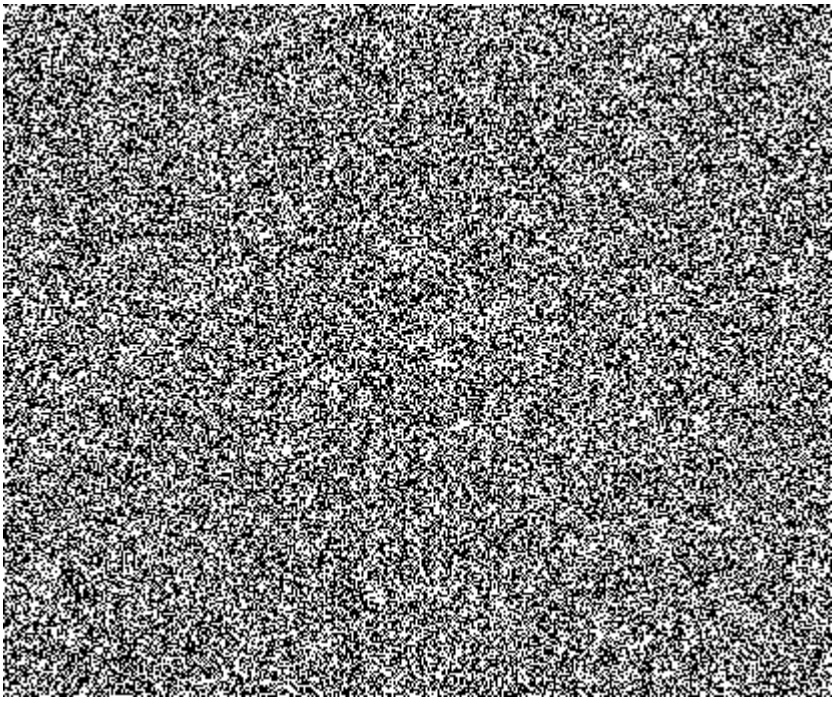


Рисунок 12. Шифрование DES (CBC)

Unnamed3

Here's another weird example of the privileging of religion. On 21 February 2006 the United States Supreme Court ruled that a church in New Mexico should be exempt from the law, which everybody else has to obey, against the taking of hallucinogenic drugs. 8 Faithful members of the Centro Espirita Beneficiente Uniao do Vegetal believe that they can understand God only by drinking hoasca tea, which contains the illegal hallucinogenic drug dimethyl-tryptamine. Note that it is sufficient that they believe that the drug enhances their understanding. They do not have to produce evidence. Conversely, there is plenty of evidence that cannabis eases the nausea and discomfort of cancer sufferers undergoing chemotherapy. Yet the Supreme Court ruled, in 2005, that all patients who use cannabis for medicinal purposes are vulnerable to federal prosecution (even in the minority of states where such specialist use is legalized). Religion, as ever, is the trump card. Imagine members of an art appreciation society pleading in court that they 'believe' they need a hallucinogenic drug in order to enhance their understanding of Impressionist or Surrealist paintings. Yet, when a church claims an equivalent need, it is backed by the highest court in the land. Such is the power of religion as a talisman.

DES (ECB) encryption of <Unnamed3>, key <12 34 56 78 9A BC DE F0>

```
00000000   BF 2F B9 90 4D CC FF 92 D0 AF E9 9D EA 5F 76 D6 87 A3   ./..M........_v...
00000012   D6 40 D0 3A C7 68 C2 4A 01 F2 B2 A8 6D 66 64 85 2A 6C   .@.:.h.J....mfd.*l
00000024   10 F5 1C E7 19 16 2F 7C 40 58 55 B7 47 FC 17 D0 96 65   ....../|@XU.G....e
00000036   91 1F 3B AC B6 38 D0 96 93 80 E5 8E 14 D0 B2 84 BA 77   ..;..8...........w
00000048   F9 7B 1E DB 71 2C A8 DF 31 87 61 65 AE 6C 8D 87 7D 41   .{..q,..1.ae.l..}A
0000005A   4D 7D F5 15 6F 1C EB 03 4F 84 31 2A C8 F3 D3 84 EA 04   M}..o...O.1*......
0000006C   44 A9 4D 76 78 0D F3 DD 7B 1E 23 32 97 85 99 87 19 9F   D.Mvx...{.#2......
0000007E   B3 CD CD 94 0D A0 66 EB 33 C2 77 C9 2E 03 9A 42 EB 6E   ......f.3.w....B.n
00000090   AF E2 FE CF 30 4D 61 99 F3 A8 23 B1 50 D3 98 FD A5 A3   ....0Ma...#.P.....
000000A2   B6 5B 46 12 55 1D BA 1E 0A 64 92 31 81 2B FF B3 A2 68   .[F.U....d.1.+...h
000000B4   A4 79 F2 FF 5C BA 11 56 51 F4 7E C3 2B 7D EB A1 D8 EC   .y..\..VQ.~.+}....
000000C6   5C 1D 38 F6 B8 6E E5 59 AE 56 B0 AB ED 93 FD CD FD 9C   \.8..n.Y.V........
000000D8   85 28 D6 ED D9 40 21 75 59 28 B7 E5 F3 C2 99 3C E7 E0   .(...@!uY(.....<..
000000EA   D0 14 E1 22 88 C7 11 19 AB 7C 26 79 F6 A1 49 09 84 E1   ...".....|&y..I...
000000FC   FB 16 55 D3 B6 E6 AB B7 14 13 78 96 8A 01 73 BF 59 2C   ..U.......x...s.Y,
```

Рисунок 13. Шифрование

3. Исследование 3-DES

3.1. Описание

Шифр 3-DES состоит в трехкратном применении обычного шифра DES. Существуют 4 основные версии этого шифра:

1. `DES-EEE3` — шифрование происходит 3 раза независимыми ключасми
2. `DES-EDE3` — операция шифровка-расшифровка-шифровка с тремя разными ключами
3. `DES-EEE2` — то же, что и `DES-EE3`, но на первом и последнем шаге одинаковый ключ
4. `DES-EDE2` — то же, что и `DES-EDE2`, но на первом и последнем шаге одинаковый ключ

На текущий момент самыми популярными разновидностями шифра являются `DES-EDE3` и `DES-EDE2`.

3.2. Формулировка задания

- Выбрать случайный текст на английском языке (не менее 1000 знаков).
- Создать бинарный файл с этим текстом, зашифровав и расшифровав его DES на 0-м ключе.
- Снять и сохранить частотную и автокорреляционную характеристику этого файла.
- Зашифровать бинарный файл шифром 3-DES в режиме ECB.
- Снять и сохранить частотную и автокорреляционную характеристику файла с шифровкой.
- Зашифровать исходный бинарный файл 3-DES в режиме CBC с тем же ключом.
- Снять и сохранить частотную и автокорреляционнуюх арактеристику файла с шифровкой.
- Определить экспериментальным путем по какой схеме работает реализация 3-DES в CrypTool. Сохранить подтверждающие скриншоты.

3.3. Ход работы

1. Выбран тот же текст, что и в предыдущем пункте
2. Создан бинарный файл с текстом
3. Снята частотная (рис. 15) характеристика и автокорелляционная (рис. 16) характеристика.

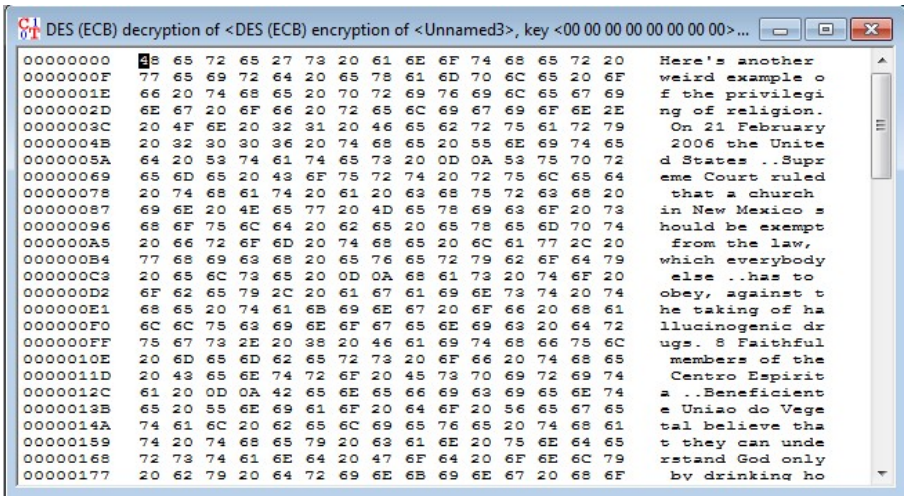


Рисунок 14. Текст в бинарном виде

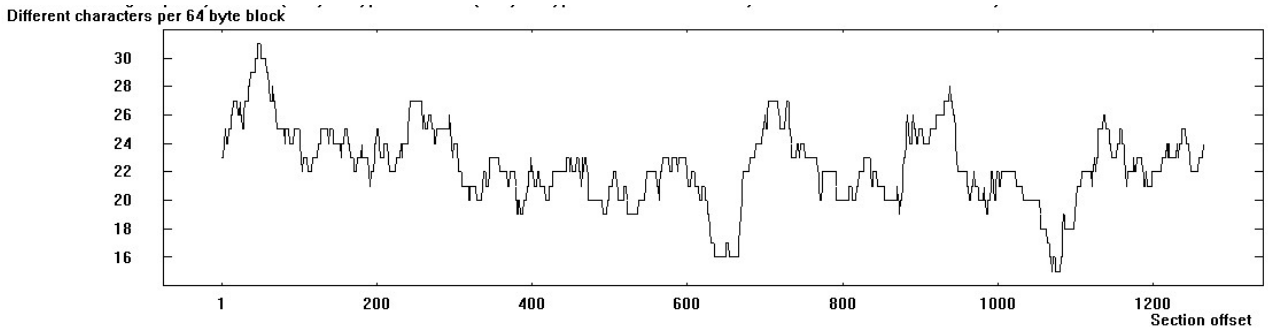


Рисунок 15. Частотная характеристика исходного текста

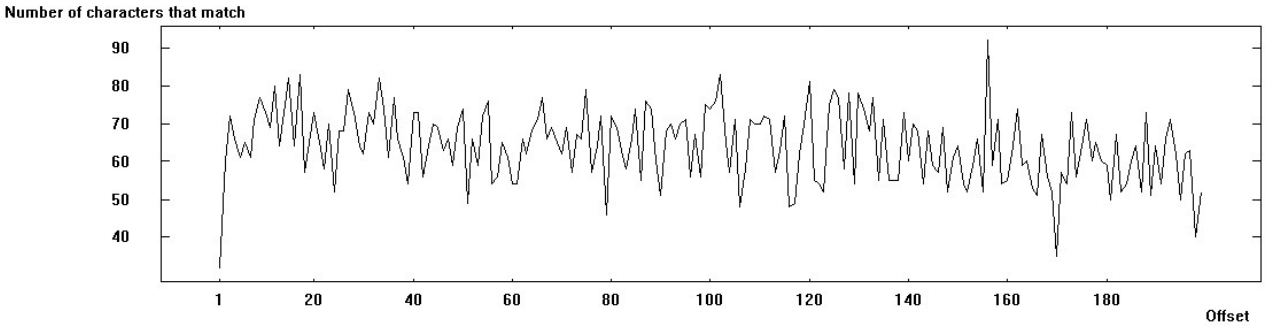


Рисунок 16. Автокорелляционная характеристика исходного текста

4. Произведено зашифрование 3-DES (ECB)
5. Сняты те же характеристики для шифротекста (рис. 17, 18)

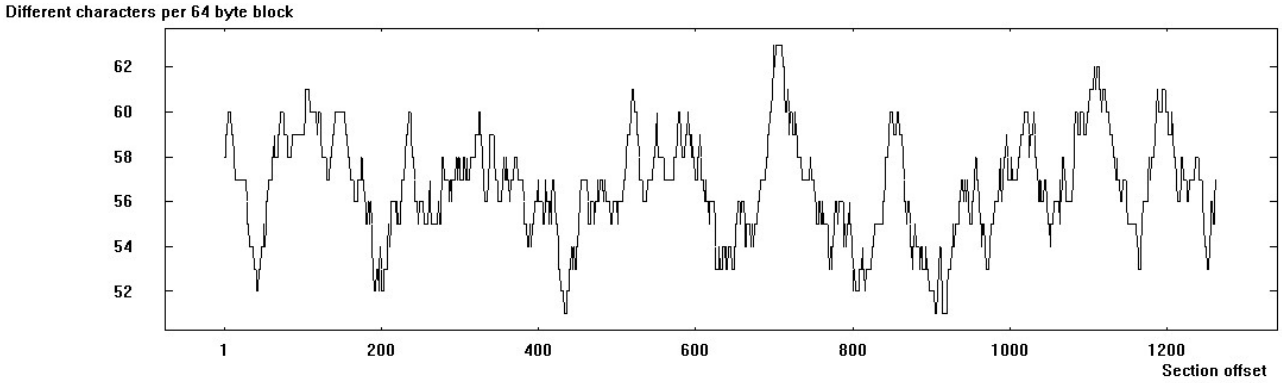


Рисунок 17. Частотная характеристика шифротекста 3-DES (ECB)

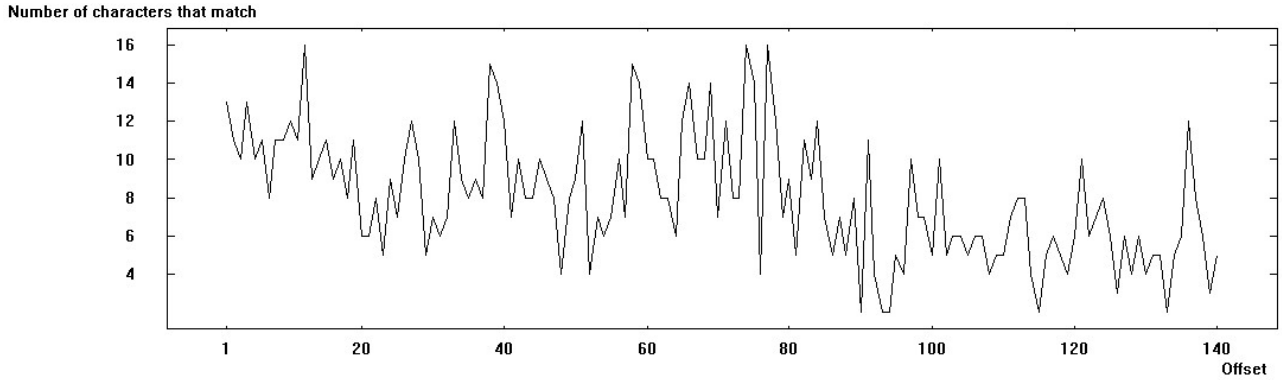


Рисунок 18. Автокорелляционная характеристика шифротекста 3-DES (ECB)

6. Произведено зашифрование 3-DES (CBC)
7. Снова сняты частотная и автокорелляционная характеристики (рис. 19, 20)

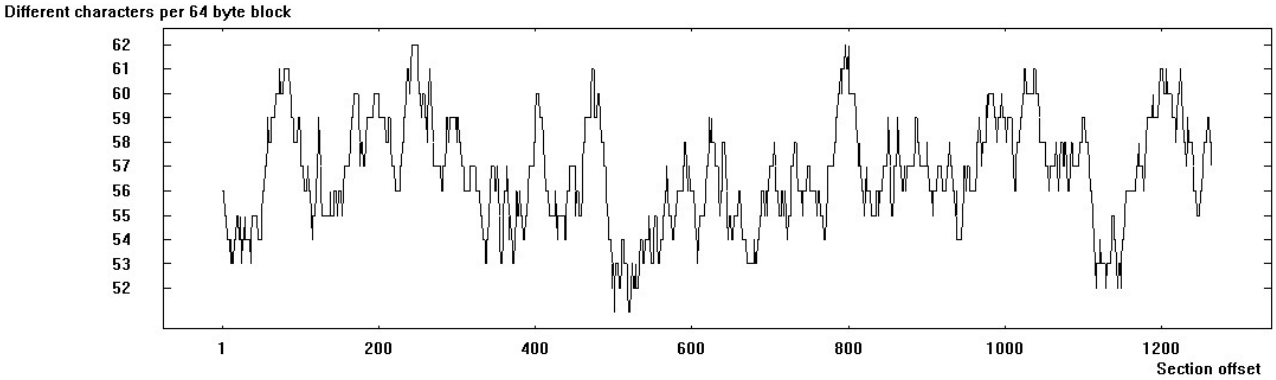


Рисунок 19. Частотная характеристика шифротекста 3-DES (CBC)

8. Используемая длина ключа — 112 бит (рис. 21), значит исключаются варианты DES-EEE3 и DES-EDE3. Чтобы выбрать между DES-EEE2 и DES-

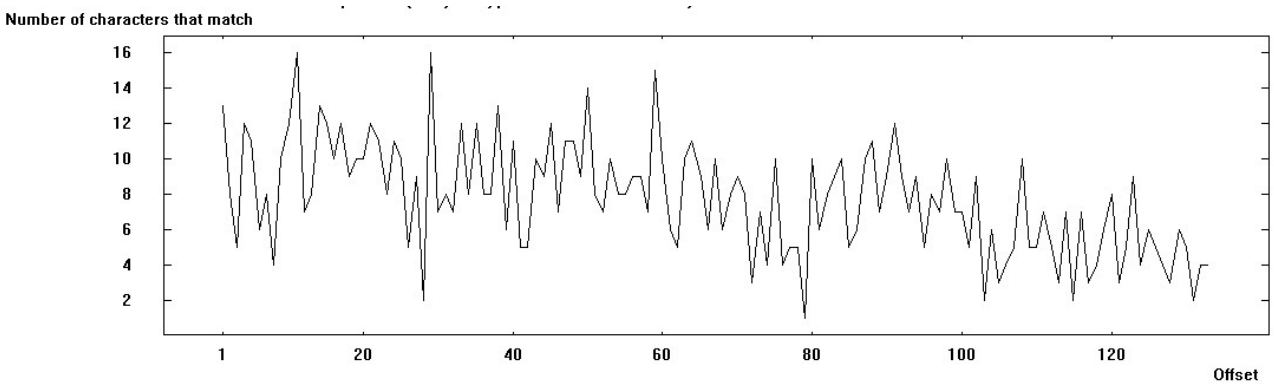


Рисунок 20. Автокорелляционная характеристика шифротекста 3-DES (CBC)

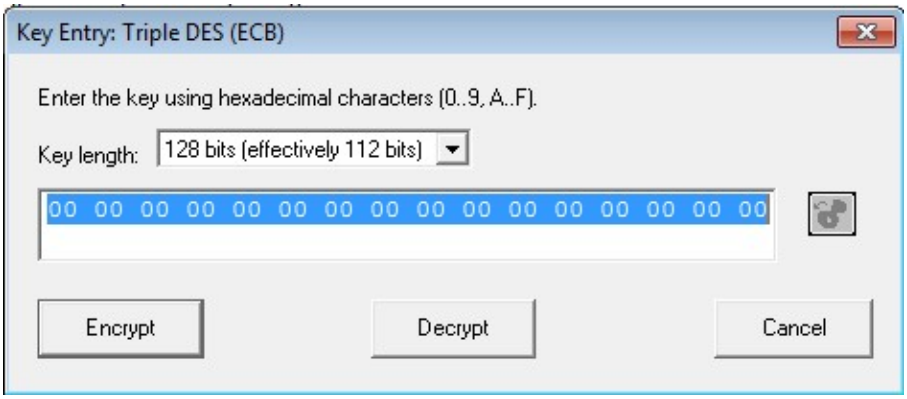


Рисунок 21. Параметры шифра 3-DES

EDE2, произведено зашифрование текста нулевым ключом обычным DES и исследуемым 3-DES. Результаты совпали (рис. 22).

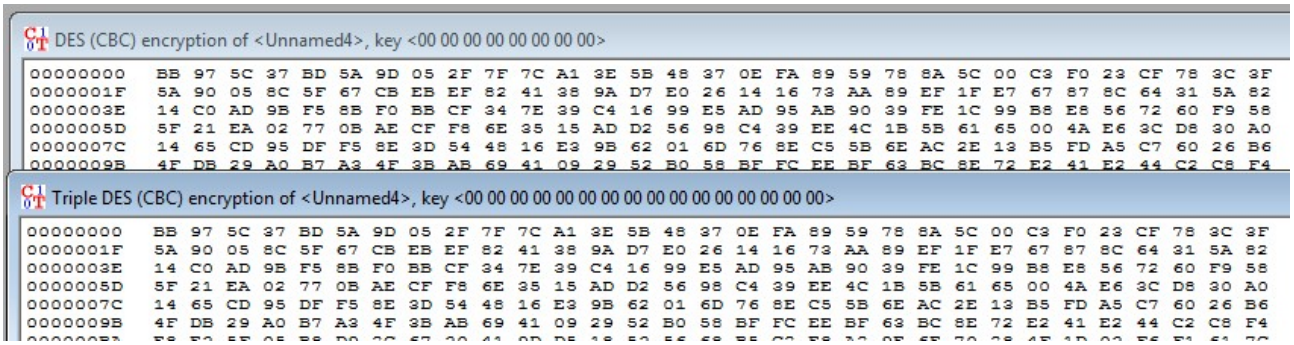


Рисунок 22. Шифрование 3-DES и DES

Совпадение результатов возможно, только если используется DES-EDE2 — в таком случае расшифровка на втором этапе компенсирует зашифровку на 1-м.

4. Исследование модификаций DESX, DESL, DESXL шифра DES

4.1. Описание

Алгоритм DESX используется на входе ключ длиной 184 бита, который делится на 3 56-битные части. Процесс шифрования происходит по следующей схеме:

$$DESX(M) = K_2 \oplus DES_K(M \oplus K_1)$$

Если $K_1 = K_2 = 0$, то это обычный DES.

DESL отказывается от входной и выходной перестановки блока. 8 S-блоков заменяются на один, но более криптостойкий.

DESXL используется оптимизации DESL и производит шифрование по DESX.

4.2. Формулировка задания

- Выбрать случайный текст на английском языке (не менее 1000 знаков).
- Создать бинарный файл с этим текстом, зашифровав и расшифровав его DES на 0-м ключе.
- С помощью CrypTool зашифровать текст с использованием шифров DESX, DESL, DESXL.
- Средствами CrypTool вычислить энтропию исходного текста и шифротекстов, полученных в итоге. Зафиксировать результаты измерений в таблице.
- Средствами CrypTool оцените время проведения атаки «грубой силы» при полном отсутствии информации о секретном ключе

4.3. Ход работы

1. Выбран тот же текст, что и в предыдущем пункте.
2. Описанным образом получен бинарный файл
3. Произведено зашифрование текста с помощью DESX, DESL, DESXL (рисунок 23)

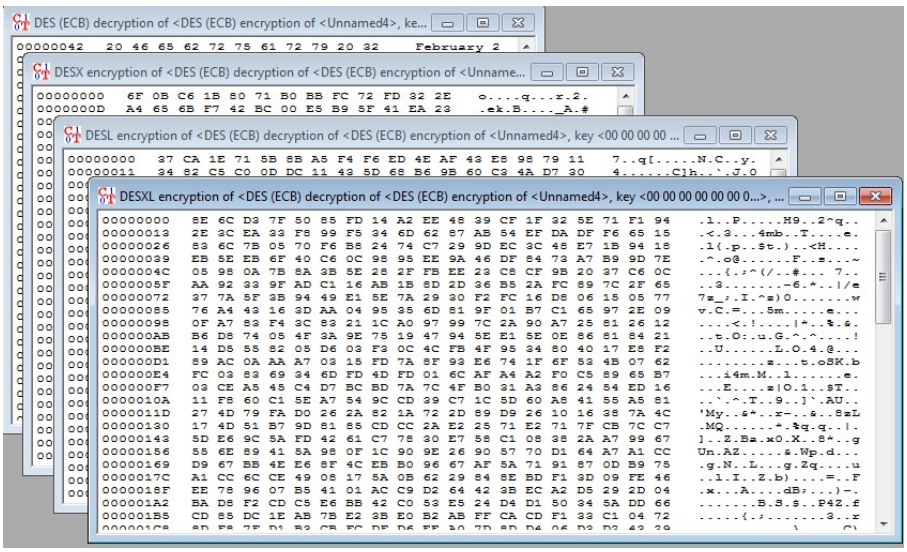


Рисунок 23. Шифрование DESX, DESL, DESXL

4. Определена энтропия исходного текста и шифротекстов:

Текст	**Энтропия**
Исходный	4.46
DESX	7.85
DESL	7.85
DESXL	7.83

5. Произведена оценка времени атаки грубой силы на все шифротексты:

Шифр	**Время атаки грубой силы (лет)**
DESX	$4.8 \cdot 10^{42}$
DESL	$1.1 \cdot 10^{4}$
DESXL	$3.9 \cdot 10^{42}$

Выводы

Шифр	Длина ключа (бит)	Brute force (лет)	Энтропия
DES (EBC)	56	$2 \cdot 10^4$	7.85
DES (CBC)	56	$3.2 \cdot 10^4$	7.84
DES-EDE2 (EBC)	112	$2.6 \cdot 10^{21}$	7.84
DES-EDE2 (CBC)	112	$3 \cdot 10^{21}$	7.85
DESX	184	$4.8 \cdot 10^{42}$	7.85
DESL	64	$1.1 \cdot 10^4$	7.85
DESXL	184	$3.9 \cdot 10^{42}$	7.83

Исследованы разновидности блочного шифра DES. Во всех случая размер блока — 64 бит. Эффективный размер ключа меньше реального из-за битов четности.

Использование шифров в режиме EBC (все блоки независимы) для осмысленной информации (с низкой энтропией) значительно снижает криптостойкость, т.к. одинаковые блоки шифруются одинаково. Режим CBC лишен этого недостатка, но в этом случае невозможно распараллелить зашифрование.

Малая длина ключа — другая проблема оригинального DES. С использованием современного вычислительного оборудования, перебрать 2^{56} вполне возможно.

Использование модификации 3-DES значительно повышает криптостойкость алгоритма; перебор 2^{112} вариантов — гораздо более трудоемкая задача.

Использование DESX — более простой с вычислительной точки зрения способ повысить криптостойкость алгоритма. С точки зрения атаки полного перебора, это даже более эффективно, чем рассмотренный DES-EDE2.

Модификация DESL практически не снижает криптойкость DES, а DESXL — DESX.

Знание части ключа шифрования значительно облегчает дешифровку. Таким образом, если используются слабые ключи (вроде 0630417 из данной л/р), и если это известно криптоаналитику, дешифрование значительно ускорится.