ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ

**Федеральное государственное бюджетное образовательное**

**учреждение высшего образования**

**«Санкт-Петербургский государственный университет телекоммуникаций**

**им. проф. М. А. Бонч-Бруевича»**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

Кафедра защищенных систем связи

Дисциплина «Основы криптографии»

# Лабораторная работа № 4

**«Принцип построения подстановочно-перестановочного шифра и его криптоанализ тотальным перебором ключей»**

Выполнила: ст. гр. ИКТЗ-83

Громов Артем

Проверил: Яковлев В. А.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Санкт-Петербург

2021

**Цель работы**

Целью данной работы является изучение структуры и основных свойств блочного шифра, основанного на подстановочно перестановочной сети (Substitution-Permutation Network или SPN), криптоанализа методом тотального перебора ключей и правила принятия решения о правильном ключе при переборе.

**Задание**

1. Изучить схему и принцип действия учебного шифра, используемого в данной работе.

2. Произвести шифрование открытого сообщения, представленного в виде произвольной двоичной последовательности длиной 16-бит (т.е. длиной равной одному блоку шифра), наблюдая результаты на каждом этапе шифрования. Сделать вывод об улучшении качества шифрования с увеличением числа раундов.

3. Произвести дешифрование криптограммы, полученной в п. 2, а также дешифрование этой криптограммы при эмуляции ошибок в канале передачи. Сделать вывод о размножении ошибок в расшифрованном сообщении.

4. Произвести шифрование смыслового текста.

5. Дешифровать полученный шифртекст на правильном и произвольном неправильном ключе.

6. Произвести криптоанализ зашифрованного смыслового текста при помощи метода тотального опробывания ключей.

Ход работы

1. Генерация раундовых ключей.

Выбран управляющий ключ из 7-ми бит: 1110000.

На его основе сгенерированы раундовые ключи:

K1= 1110 0000 0010 1010

K2= 1100 1100 0100 0101

K3= 1010 0111 0010 0001

K4= 0010 1001 0011 0110

K5= 1110 0011 1101 0000

2. Анализ преобразований шифра.

Выбранная двоичная последовательность длиной 16 бит для шифрования («открытый текст»): 0100 0100 0100 0100 (последовательность должна соответствовать номеру варианта, представленному в виде 4-х значного двоичного числа, повторенного 4 раза).

Полученная криптограмма: 1110 0001 0010 1101

Промежуточные результаты:

Раунд 1

подмешивание ключа: 1111 1111 1111 1111

нелинейное преобразование s-box-ов: 0111 0111 0111 0111

перестановка: 0000 1111 1111 1111

Раунд 2

подмешивание ключа: 1111 0000 0000 0000

нелинейное преобразование s-box-ов: 0111 1110 1110 1110

перестановка: 0111 1111 1111 1000

Раунд 3

подмешивание ключа: 1000 0000 0000 0111

нелинейное преобразование s-box-ов: 0011 1110 1110 1000

перестановка: 0111 0110 1110 1000

Раунд 4

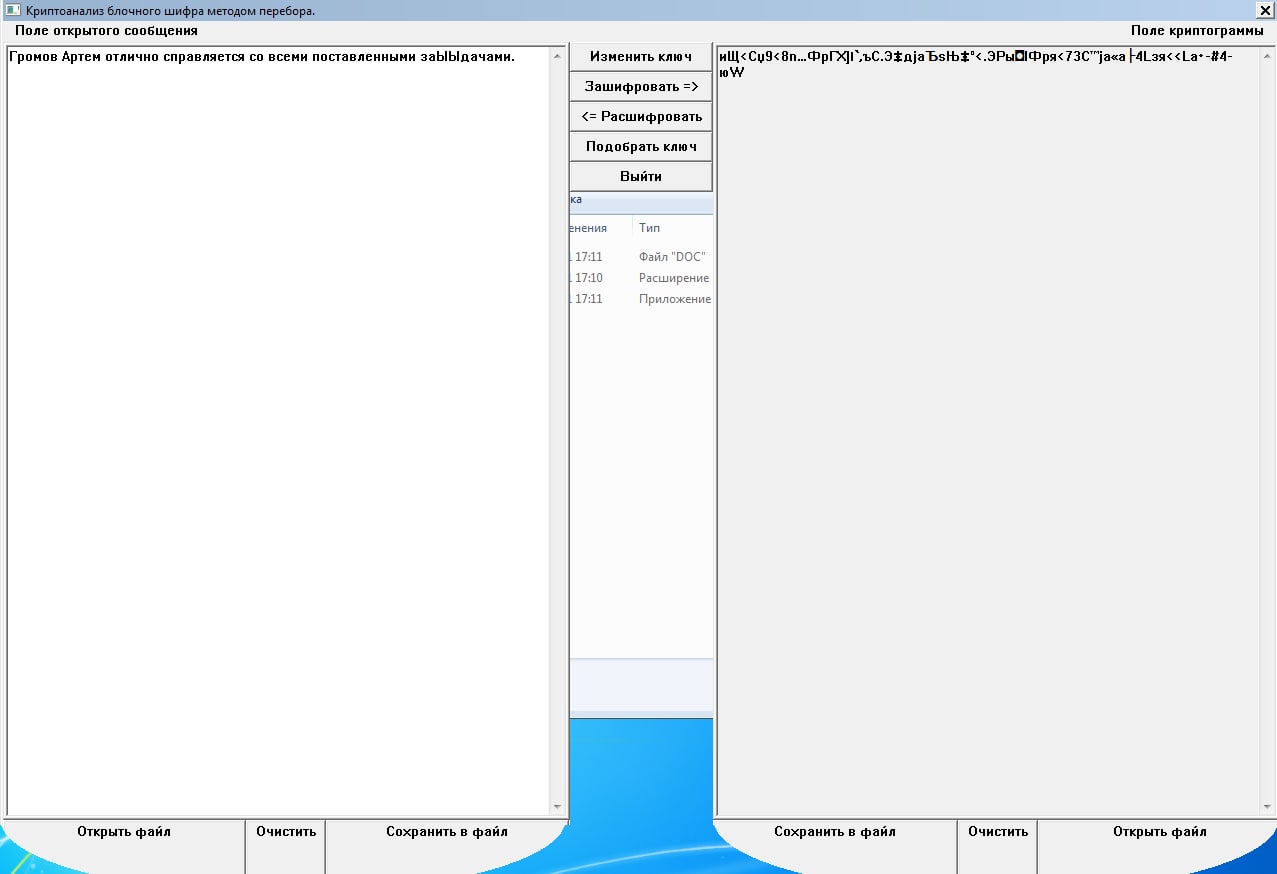
подмешивание ключа: 1000 1001 0001 0111

нелинейное преобразование s-box-ов: 0011 1010 0100 1000

Раунд 5

подмешивание ключа: 1100 0101 1011 0111

3. Криптоанализ перебором всех возможных ключей



При допустимом отклонении в 6% частотные интервалы для букв русского языка равны:

P(«о»)= ( 3 - 15)%

P(«а»)= ( 0.2 - 12.2)%

P(«и»)= (0.2 - 12.2 )%

проверялись ключи:

ключ=0010010 P(«о»)=3% P(«а»)=0% P(«и»)=0%

ключ=0101011 P(«о»)=3% P(«а»)=3% P(«и»)=1,5%

ключ=0101111 P(«о»)=3% P(«а»)=0% P(«и»)=0%

ключ=0110100 P(«о»)=3% P(«а»)=0% P(«и»)=0%

ключ=1001001 P(«о»)=3% P(«а»)=1,5% P(«и»)=0%

ключ=1011101 P(«о»)=3% P(«а»)=0% P(«и»)=0%

ключ=1101001 P(«о»)=4,5% P(«а»)=0% P(«и»)=0%

ключ=1101110 P(«о»)=3% P(«а»)=0% P(«и»)=0%

ключ=1110000 P(«о»)=9,1% P(«а»)=7,5% P(«и»)=6,1%

ключ=1111101 P(«о»)=3% P(«а»)=1,5% P(«и»)=0%

При допустимом отклонении в 5% частотные интервалы для букв русского языка равны::

P(«о»)= ( 4 - 14) %

P(«а»)= ( 1.2 - 11.2) %

P(«и»)= (1.2 - 11.2 ) %

проверялись ключи:

ключ=0101011 P(«о»)=3% P(«а»)=3% P(«и»)=1,5%

ключ=1110000 P(«о»)=9,1% P(«а»)=7,5% P(«и»)=6,1%

Минимальные частотные интервалы, на которых извлекается ключ, соответствуют допустимому отклонению в 1%

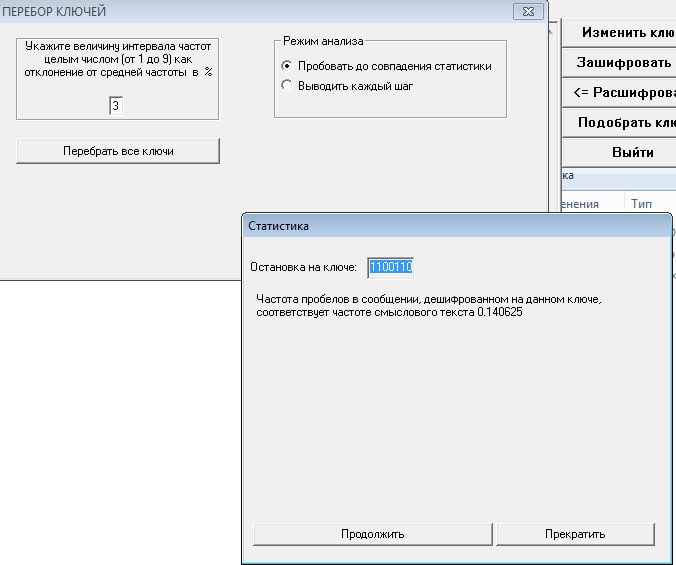
P(«о»)= ( 8 , 10) %

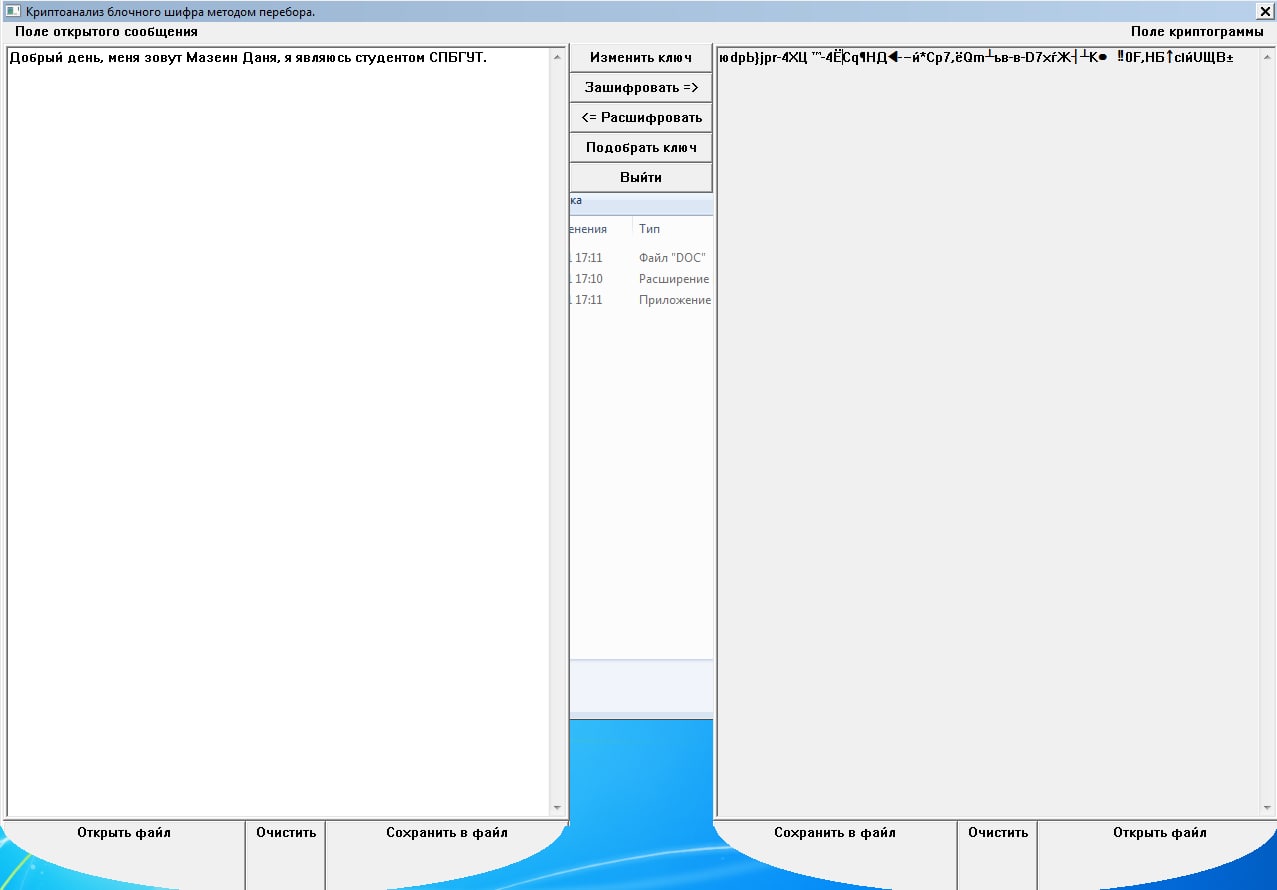
P(«а»)= ( 5.2 , 7.2) %

P(«и»)= (5.2 , 7.2 ) %

При этом вероятности появления контрольных символов в дешифрованном сообщении равны: P(«о»)=9,1% P(«а»)=7,5% P(«и»)=6,1%.

**Расшифровка криптограммы студента Мазеина Д. С.**

От студента Мазеина Д. С. Я получил криптограмму. Программа подобрала ключ для расшифровки при переборе с отклонением 3%.



4. Исследование влияния ошибок в канале передачи.

Исходная криптограмма: 1110 0001 0010 1101

Расшифровка криптограммы: 0100 0100 0100 0100

Расшифровка криптограммы при эмуляции ошибки

в 1-м бите

криптограмма с ошибкой: 0110 0001 0010 1101

расшифровка криптограммы: 1111 1110 0001 0011

количество ошибок в расшифровке: 10

во 2-м бите

криптограмма с ошибкой: 1010 0001 0010 1101

расшифровка криптограммы: 0011 0011 1000 1101

количество ошибок в расшифровке: 10

в 3-м бите

криптограмма с ошибкой: 1100 0001 0010 1101

расшифровка криптограммы: 1101 0110 0011 1101

количество ошибок в расшифровке: 8

в 4-м бите

криптограмма с ошибкой: 1111 0001 0010 1101

расшифровка криптограммы: 0101 0111 0100 0100

количество ошибок в расшифровке: 3

в 5-м бите

криптограмма с ошибкой: 1110 1001 0010 1101

расшифровка криптограммы: 0100 1000 1110 0111

количество ошибок в расшифровке: 6

в 6-м бите

криптограмма с ошибкой: 1110 0101 0010 1101

расшифровка криптограммы: 0001 1101 1101 0001

количество ошибок в расшифровке: 8

в 7-м бите

криптограмма с ошибкой: 1110 0011 0010 1101

расшифровка криптограммы: 1111 1001 1110 1010

количество ошибок в расшифровке: 11

в 8-м бите

криптограмма с ошибкой: 1110 0000 0010 1101

расшифровка криптограммы: 0011 1100 1111 0001

количество ошибок в расшифровке: 9

в 9-м бите

криптограмма с ошибкой: 1110 0001 1010 1101

расшифровка криптограммы: 0001 1001 1010 1100

количество ошибок в расшифровке: 9

в 10-м бите

криптограмма с ошибкой: 1110 0001 0110 1101

расшифровка криптограммы: 0001 0111 1100 0100

количество ошибок в расшифровке: 5

в 11-м бите

криптограмма с ошибкой: 1110 0001 0000 1101

расшифровка криптограммы: 0000 0101 1101 0010

количество ошибок в расшифровке: 6

в 12-м бите

криптограмма с ошибкой: 1110 0001 0011 1101

расшифровка криптограммы: 0111 0101 0000 0111

количество ошибок в расшифровке: 6

в 13-м бите

криптограмма с ошибкой: 1110 0001 0010 0101

расшифровка криптограммы: 0100 0101 0110 0001

количество ошибок в расшифровке: 4

в 14-м бите

криптограмма с ошибкой: 1110 0001 0010 1001

расшифровка криптограммы: 1000 0100 1011 1001

количество ошибок в расшифровке: 9

в 15-м бите

криптограмма с ошибкой: 1110 0001 0010 1111

расшифровка криптограммы: 1010 0110 1010 1001

количество ошибок в расшифровке: 10

в 16-м бите

криптограмма с ошибкой: 1110 0001 0010 1100

расшифровка криптограммы: 1010 1111 1010 1101

количество ошибок в расшифровке: 10

Среднее значение ошибок в дешифрованном сообщении при ошибочном приеме одного бита криптограммы.

Nош.ср. = (10+10+8+3+6+8+11+9+9+5+6+6+4+9+10+10)/16 =7,75

Вывод

Изменение одного бита в криптограмме приводит к изменению всей расшифровки почти на половину.