МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования «САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ АЭРОКОСМИЧЕСКОГО ПРИБОРОСТРОЕНИЯ»

КАФЕДРА № 51

ОТЧЕТ
ЗАЩИЩЕН С ОЦЕНКОЙ

ПРЕПОДАВАТЕЛЬ

ассистент		М.Н. Исаева
должность, уч. степень, звание	подпись, дата	инициалы, фамилия

ОТЧЕТ О ЛАБОРАТОРНОЙ РАБОТЕ №3

Исследование симметричных шифров

по курсу: Криптографические методы защиты информации

РАБОТУ ВЫПОЛНИЛ

СТУДЕНТ ГР. № 5911		К.В. Жук
	подпись, дата	инициалы, фамилия

Санкт-Петербург 2021

1. Цель лабораторной работы

Целью нашего исследования является анализ двух последовательностей, которые формируются с помощью алгоритма шифрования Blowfish. Но в формировании первой последовательности мы инвертируем вторую половину битов блока, а затем инициируем процесс шифрования. А для формирования второй последовательности мы в исходной последовательности инвертируем каждый четный бит блока и также начинаем шифрование.

2. Тесты, используемые для исследования:

- Частотный тест:

Суть теста — определение доли единиц внутри блока длиной m бит. Цель — выяснить действительно ли частота повторения единиц в блоке длиной m бит приблизительно равна m/2, как можно было бы предположить в случае абсолютно случайной последовательности. Вычисленное в ходе теста значение вероятности p должно быть не меньше 0,01. В противном случае ($p < 0,01$), двоичная последовательность не носит истинно случайный характер.

- Тест серий:

Суть теста заключается в анализе количества серий бит, состоящих из одинаковых значений (например, единиц). Например, в битовом потоке: 1011010111011001011010110110110111101010101111010 11 Количество серий из 1-ц составляет 18. Целью теста является сопоставить фактически наблюдаемое количество серий с теоретической оценкой. Он показывает является ли колебание между разными значениями бит слишком быстрым или слишком медленным.

- Автокорреляционный тест:

Суть теста в том, чтобы сдвинуть копию исходной последовательности на n-ное значение относительно оригинала, после этого последовательности XOR-ятся, результат прогоняется через частотный тест. В данном случае p должно быть не меньше значения 0,01. В противном случае тест считается не пройденным.

3. Тестовые примеры:

Для выполнения данного задания была взята и зашифрована картинка lena.bmp

Рис. 1 Исходная картинка

В соответствии с заданием, на исходные последовательности были наложены нужные маски для инверсии определённых бит. После этого производилось шифрование.

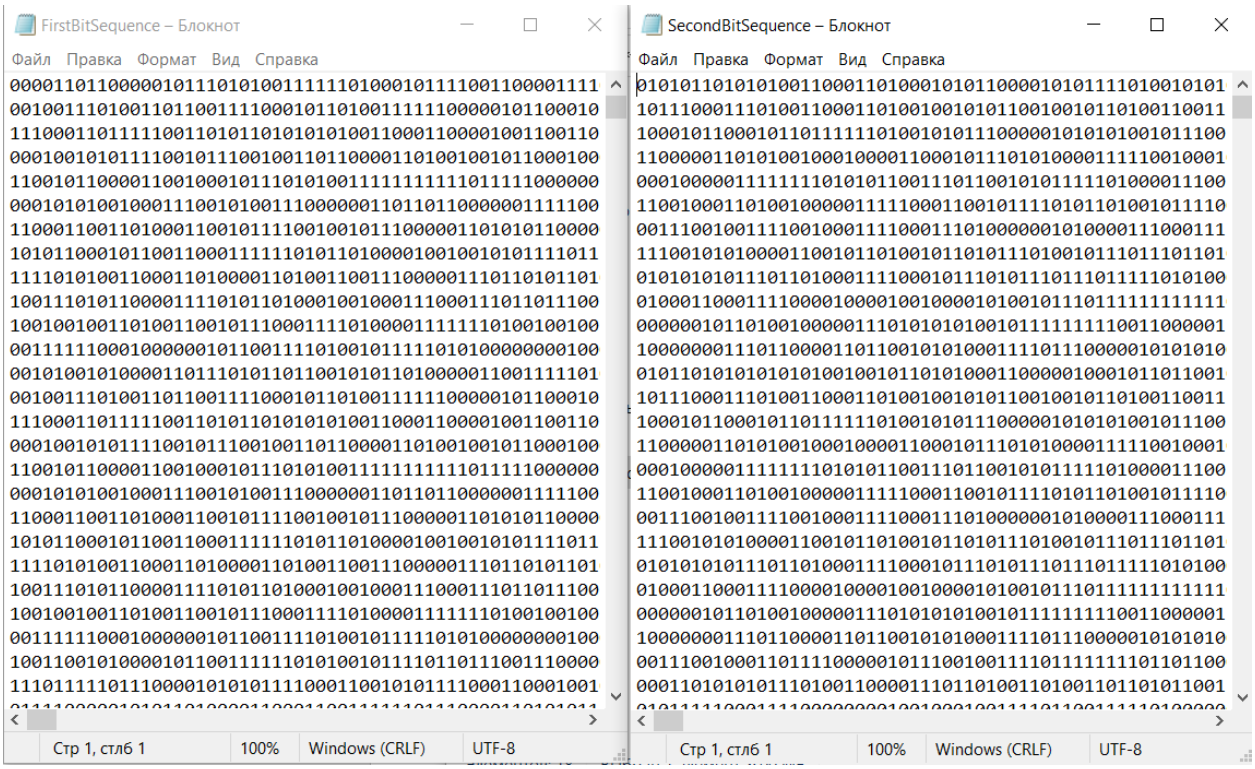

Рис. 2 Битовые последовательности

В результате шифрования были получены последовательности бит, которые в дальнейшем использовались для анализа.

- Частотный тест:

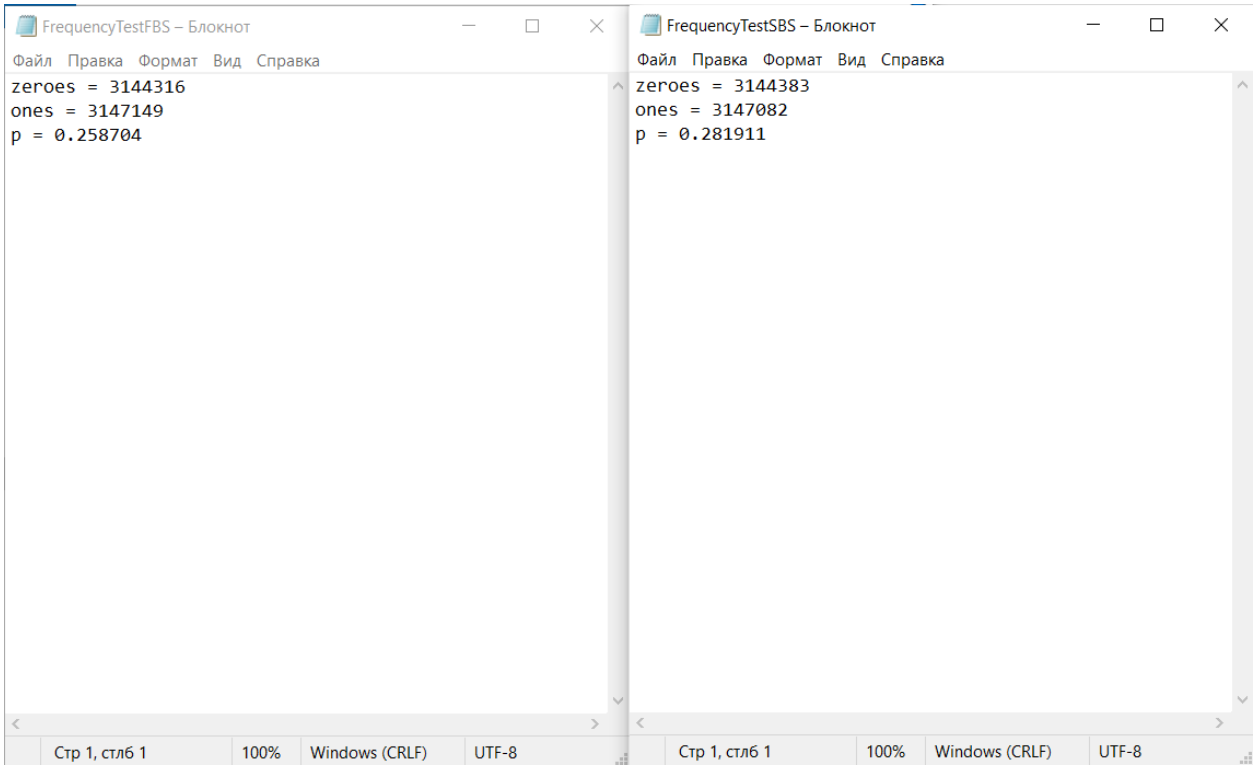

Рис. 3 Результаты частотного теста

Обе последовательности прошли частотный тест, поскольку оба значения p превышают значение 0.01

- Тест серий:

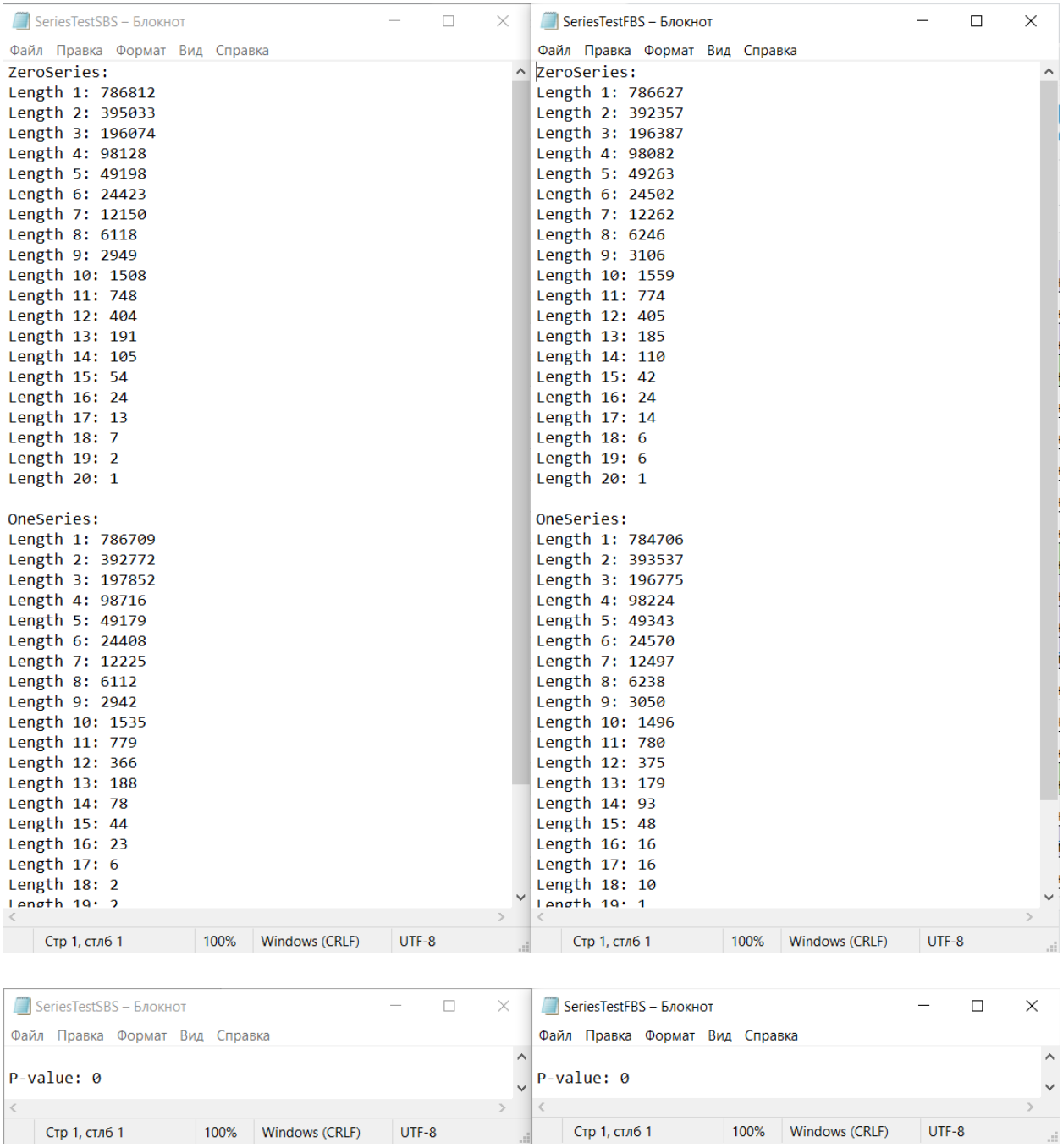

Рис. 4 Результаты теста серий

Обе последовательности не прошли тест серий, поскольку значение p = 0, что меньше 0.01

- Автокорреляционный тест:

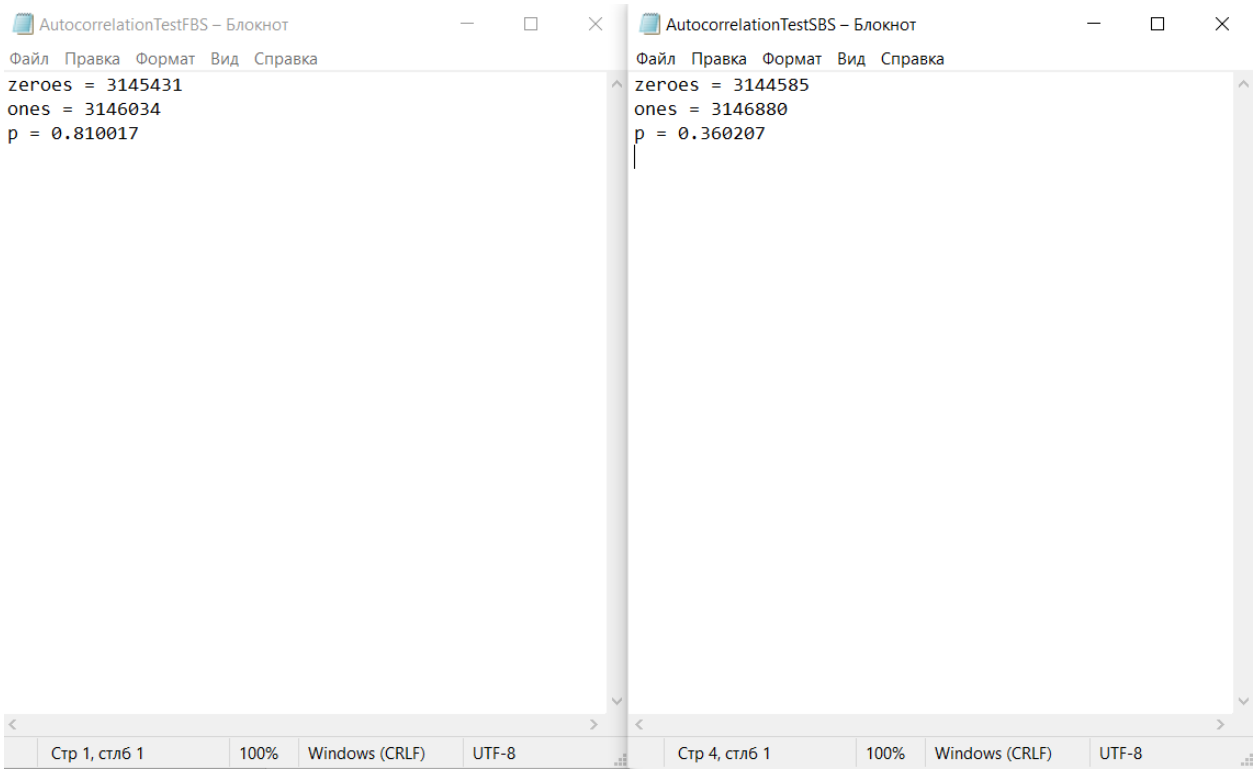

Рис. 5 Результаты автокорреляционного теста

Обе последовательности прошли автокорреляционный тест, поскольку значение p превышает 0.01

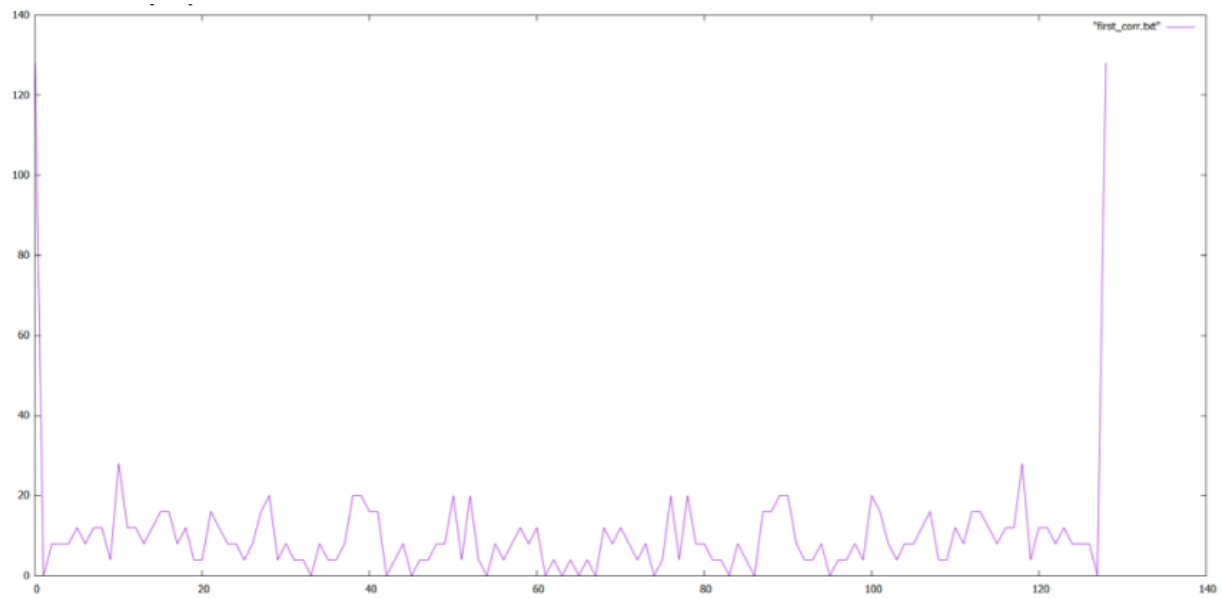

Рис. 6 График автокорреляции для 1 последовательности

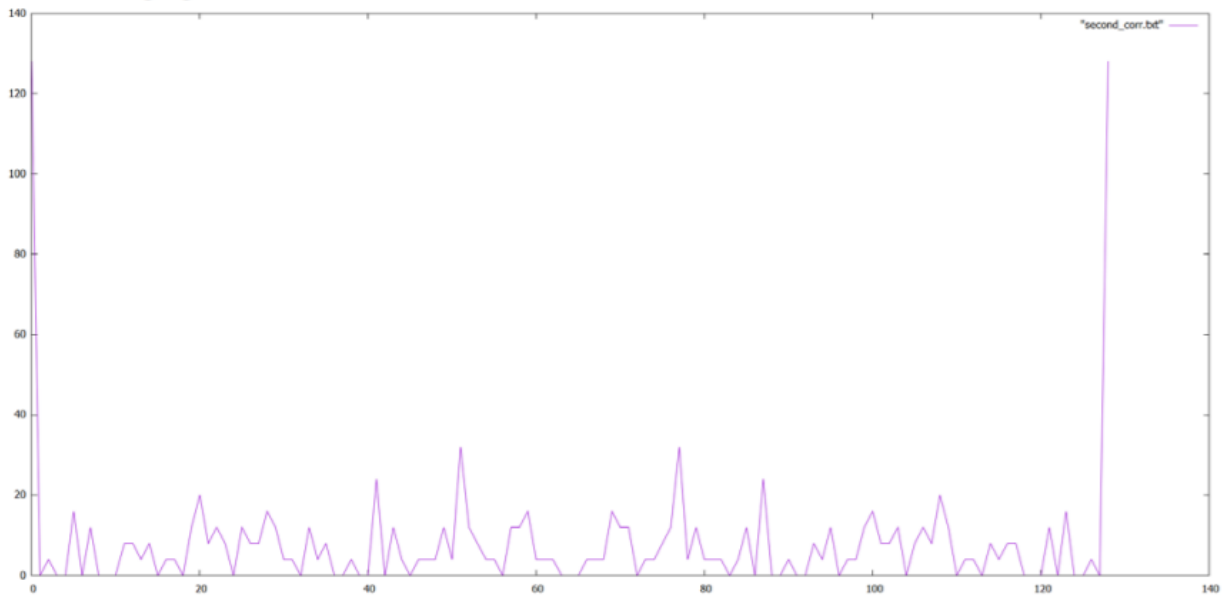

Рис. 7 График автокорреляции для 2 последовательности

4. Вывод:

Результатом работы является программа, генерирующая последовательности в виде битового потока (поток из 0 и 1) с помощью алгоритма Blowfish и инвертирования некоторых битов в соответствии с заданием. Также для каждой из таких последовательностей были проведены тесты: частотный тест, тест серий, автокорреляционный тест. С помощью этих тестов мы могли сделать выводы о случайности получившихся последовательностей.

5. Список литературы:

1. Черчхаус. Коды и шифры

2.Тестирование генераторов псевдослучайных последовательностей - https://cpct.sibsutis.ru/~artpol/downloads/bp/bop-pr8-rand_test_v1.pdf