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

КАФЕДРА № 51

ОТЧЕТ
ЗАЩИЩЕН С ОЦЕНКОЙ

ПРЕПОДАВАТЕЛЬ

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

ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №3

ИССЛЕДОВАНИЕ СИММЕТРИЧНЫХ ШИФРОВ

по курсу: КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

РАБОТУ ВЫПОЛНИЛ

СТУДЕНТ ГР. 5912		Льдокова С.В.
	подпись, дата	инициалы, фамилия

Санкт-Петербург 2021

1. Цель

Вариант 8.

Исследовать влияние различных ключей на результаты шифрования для одного блока. Провести N (N зависит от алгоритма шифрования) раундов шифрования на ключах, например, из всех нулей/единиц, с сериями нулей и единиц. Провести N раундов шифрования с использованием псевдослучайных ключей. Провести для полученных шифртекстов: автокорреляционный тест, тест серий, частотный тест. Проанализируйте частоту изменения битов внутри блока в процессе шифрования для обоих вариантов ключей внутри, продемонстрировать частоту изменения битов. Сравнить полученные результаты. Чтобы было нагляднее, позиции, которые изменяются, можно выделить цветом - цвет выбирать в зависимости от количества изменений.

2. Тестируемый алгоритм

Blowfish — алгоритм 64-битного блочного шифра с ключом переменной длины. Размер ключа алгоритма от 32 до 448 битов.

3. Описание статистический тестов

Для определения, обладает ли двоичная последовательность некоторыми специфическими характеристиками, которые, скорее всего, демонстрировала бы истинно случайная последовательность, существуют статистические тесты. Однако, исход каждого теста является не точным, а скорее вероятностным. Если последовательность прошла все тесты, нет гарантии, что она действительно произведена генератором случайных бит.

3.1 Частотный тест (однобитный тест)

Цель этого теста — определить, является ли примерно равным количество 0 и 1 в последовательности s, как это ожидается для случайной последовательности. Пусть n_0, n_1 обозначают количество 0 и 1 в s, соответственно. Используется статистика:

$$X_1 = \frac{(n_0 - n_1)^2}{n}, \quad (1)$$

которая примерно следует χ^2 распределению с 1 степенью свободы, если n ≥ 10^7.

3.2 Тест серий

Цель теста серий — определить, является ли количество серий (состоящих либо из нулей, либо из единиц) различных длин в последовательности s таким, как ожидается для случайной последовательности.

Ожидаемое число разрывов (или блоков) длины i в случайной последовательности длины n равно $e_i = \frac{(n-i+3)}{2^{i+2}}$. Пусть k равен наибольшему целому i, для которого $e_i \geq 5$. Пусть B_i, G_i — количество блоков и разрывов длины i в s соответственно для каждого $1 \leq i \leq k$.

Используется статистика:

$$X_2 = \sum_{i=1}^{k} \frac{(B_i - e_i)^2}{e_i} + \sum_{i=1}^{k} \frac{(G_i - e_i)^2}{e_i}, \quad (2)$$

которая примерно следует χ^2 распределению с 2k - 2 степенью свободы.

3.3 Автокорреляционный тест

Цель этого теста — проверить корреляции между последовательностью s и ее (нециклическими) сдвигами. Пусть d — фиксированное целое число, $1 \leq d \leq \lfloor n/2 \rfloor$. Число бит в s, не равных их d-сдвигам, есть $A(d) = \sum_{i=0}^{n-d-1} s_i \oplus s_{i+d}$, где $\oplus$ обозначает операцию XOR.

Используется статистика:

$$X_3 = 2\left(A(d) - \frac{n-d}{2}\right) / \sqrt{n-d}, \quad (3)$$

которая примерно следует распределению N (0,1), если $n - d \geq 10$. Так как малые значения A(d) столь же мало ожидаемы, как и большие значения A(d), должен быть использован двусторонний тест.

4. Примеры использования тестов

Первый блок исходного текста (последовательность S):

0100100100100000011101000111001001111001001000000111010001101111

Различные ключи:

Ключ K_1 (ключ из всех единиц)

1111111111111111111111111111111111111111111111111111111111111111

Ключ K_2 (ключ из серии нулей и единиц)

0000000000000000000000000000000011111111111111111111111111111111

Ключ K_3 (псевдослучайный ключ)

0100111001000100010100000011100001000001010001100011000001010110

Первый блок исходного текста после шифрования различными ключами:

После шифрования ключом K_1 (последовательность S_1)

1011010011011010000010111100100001011011001101011110101000111001

После шифрования ключом K_2 (последовательность S_2)

1010101111000001111100010000100000010101011101001111000110011110

После шифрования ключом K_3 (последовательность S_3)

0001000011111011101001101101100010011001110101001011011111100000

4.1 Частотный тест

Оценим количество единиц и количество нулей.

Для первой последовательности S_1:

Количество единиц — 33;

Количество нулей — 31;

Всего бит — 64.

По формуле (1) получаем:

$$X_1 = \frac{(31-33)^2}{64} = 0.0625$$

Для второй последовательности S_2:

Количество единиц — 31;

Количество нулей — 33;

Всего бит — 64.

По формуле (1) получаем:

$$X_1 = \frac{(33-31)^2}{64} = 0.0625$$

Для третьей последовательности S_3:

Количество единиц — 37;

Количество нулей — 27;

Всего бит — 64.

По формуле (1) получаем:

$$X_1 = \frac{(27-37)^2}{64} = 1.5625$$

Для уровня значимости $\alpha = 0.05$ пороговое значение для $X_1 = 3.8415$, следовательно, все последовательности прошли частотный тест.

4.2 Тест серий

Для каждой последовательности оценим ожидаемое число разрывов или блоков, найдем значение k и реальные количества разрывов и блоков.

Для первой последовательности S_1:

Ожидаемое число разрывов или блоков длины 1 – $e_1 = 8.25$, длины 2 – $e_2 < 5$, следовательно, $k = 1$;

Количество разрывов длины 1 – $G_1 = 11$;

Количество блоков длины 1 – $B_1 = 10$;

По формуле (2) получаем:

$$X_2 = \sum_{i=1}^{1} \frac{(B_i - e_i)^2}{e_i} + \sum_{i=1}^{1} \frac{(G_i - e_i)^2}{e_i} = 1.287$$

Для второй последовательности S_2:

Ожидаемое число разрывов или блоков длины 1 – $e_1 = 8.25$, длины 2 – $e_2 < 5$, следовательно, k = 1;

Количество разрывов длины 1 – $G_1 = 8$;

Количество блоков длины 1 – $B_1 = 9$;

По формуле (2) получаем:

$$X_2 = \sum_{i=1}^{1} \frac{(B_i - e_i)^2}{e_i} + \sum_{i=1}^{1} \frac{(G_i - e_i)^2}{e_i} = 0.075$$

Для третьей последовательности S_3:

Ожидаемое число разрывов или блоков длины 1 – $e_1 = 8.25$, длины 2 – $e_2 < 5$, следовательно, k = 1;

Количество разрывов длины 1 – $G_1 = 8$;

Количество блоков длины 1 – $B_1 = 6$;

По формуле (2) получаем:

$$X_2 = \sum_{i=1}^{1} \frac{(B_i - e_i)^2}{e_i} + \sum_{i=1}^{1} \frac{(G_i - e_i)^2}{e_i} = 0.621$$

Для уровня значимости $\alpha = 0.05$, пороговое значение для $X_2 = 9.4877$, следовательно, все последовательности прошли тест серий.

4.3 Автокорреляционный тест

По формуле (3) для последовательности S_1 получаем(рис.1):

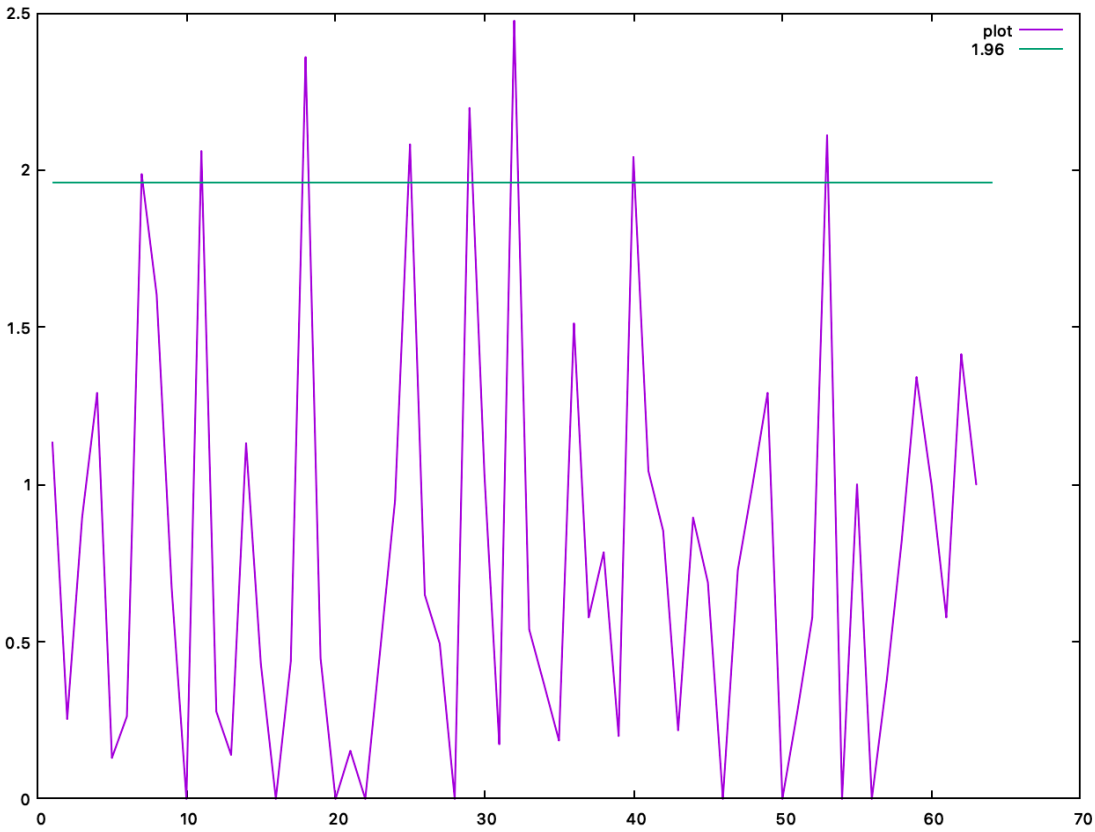

Рисунок 1 - Автокорреляционный тест первой последовательности

По формуле (3) для последовательности S_2 получаем(рис.2):

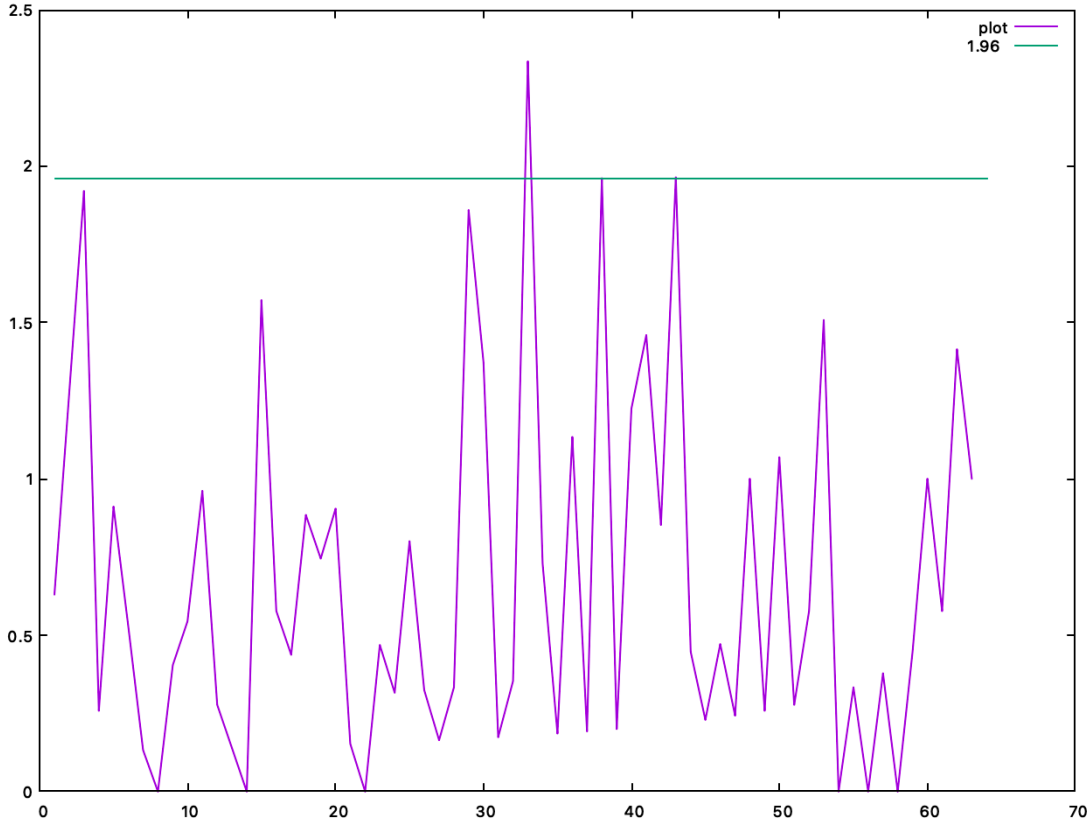

Рисунок 2 - Автокорреляционный тест второй последовательности

По формуле (3) для последовательности S_3 получаем(рис.3):

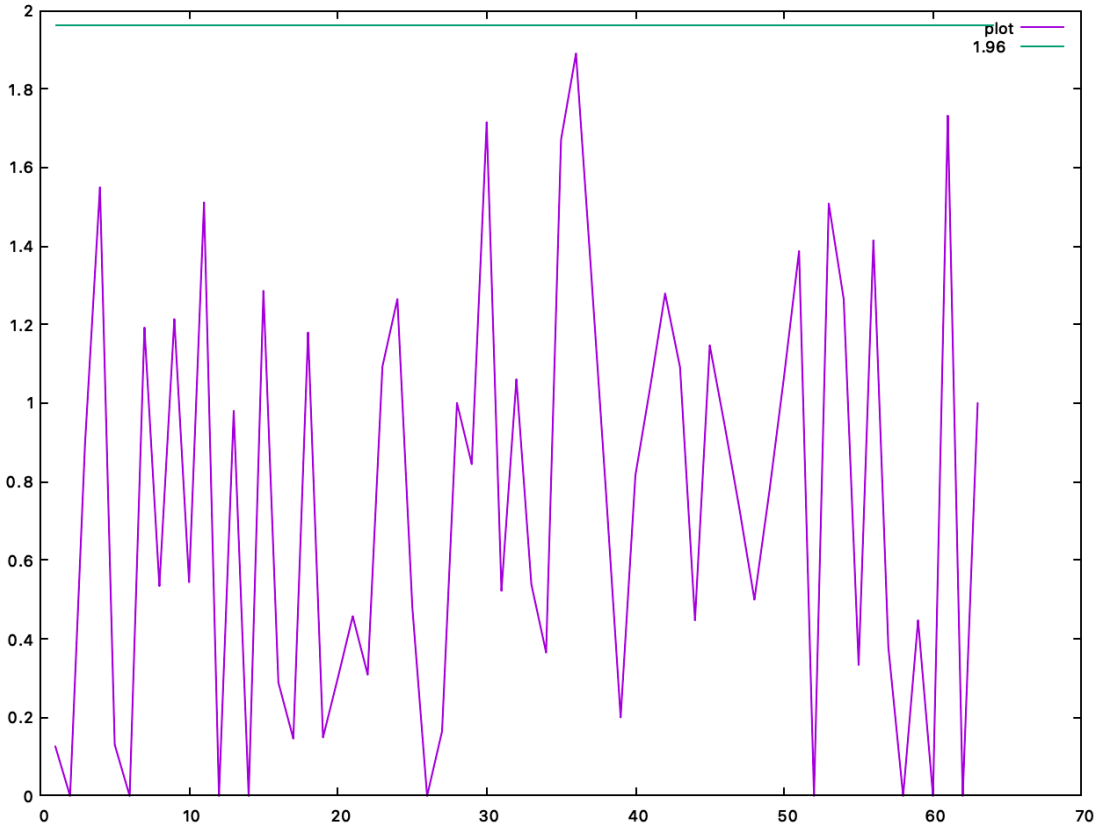

Рисунок 3 - Автокорреляционный тест третьей последовательности

Для уровня значимости $\alpha = 0.05$, пороговое значение для $X_3 = 1.96$, следовательно первая и вторая последовательности не прошли автокорреляционный тест.

Частота изменения битов внутри последовательностей

Возвращаясь к полученным последовательностям, определим частоту изменения битов внутри каждой из последовательностей.

Последовательность S_1:

10110100110110100000101111001000010110110011010111101010001110 01

Изменения битов на соответствующих позициях:

11 9 7 8 9 8 5 2 4 4 10 2 7 7 7 8 6 11 6 9 8 7 8 11 8 7 6 10 9 4 5 7 11 6 7 6 10 9 10 7 11 11 8 3 8 7 8 6 5 10 8 10 8 5 10 5 9 10 9 10 9 9 9 9

Всего изменений: 493

Последовательность S_2:

10101011110000011111000100001000000101010111010011110001100111 10

Изменения битов на соответствующих позициях:

11 7 11 4 10 9 9 9 8 7 6 10 6 9 5 7 7 8 5 9 7 9 8 9 6 9 4 7 7 10 6 7 8 10 8 6 8 10 11 11 7 8 5 8 6 10 10 7 11 11 7 9 5 7 8 7 5 7 6 10 8 9 4 10

Всего изменений: 503

Последовательность S_3:

00010000111110111010011011011000100110011101010010110111111 00000

Изменения битов на соответствующих позициях:

8 8 8 8 9 9 11 7 9 6 8 6 9 6 9 7 9 8 7 7 9 8 11 8 10 7 9 8 10 9 12 7 10 12 10 7 9 9 9 9 7 7 10 11 9 9 11 7 9 9 10 5 9 10 10 6 6 9 7 6 7 10 6 9

Всего изменений: 541

9. Вывод

В данной работе были проведены статистические тесты для алгоритма шифрования Blowfish. Было выяснено, что алгоритм проходит частотный тест, но проваливает тест серий и автокорреляционный тест. Однако, даже если последовательность прошла все тесты, нет гарантии, что она действительно произведена генератором случайных бит. Ведь исход каждого теста является не точным, а скорее вероятностным. Поэтому алгоритм Blowfish не является не криптографически стойким из-за того, что провалил автокорреляционный тест.

Также было выяснено, что при использовании рандомного ключа последовательность терпит больше изменений, чем при использовании ключей из единиц или ключей из серий нулей и единиц.

10. Список литературы

1. Менезес А., Handbook of applied cryptography, 1965 - 1997, CRC Press
2. Лидл Р., Нидеррайтер Г. Конечные поля. В 2-х томах. -Москва: Мир, 1988