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

ИССЛЕДОВАНИЕ СИММЕТРИЧНЫХ ШИФРОВ

по курсу: КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

РАБОТУ ВЫПОЛНИЛ

СТУДЕНТ ГР. 5912		Нам Д.О.
	подпись, дата	инициалы, фамилия

Санкт-Петербург 2021

1. Цель

Вариант 7.

Инвертируйте каждый четный (каждый второй) бит блока, проведите N раундов (N зависит от алгоритма шифрования), затем для первоначальной исходной последовательности инвертируйте каждый третий бит блока, проведите N раундов (N зависит от алгоритма шифрования), после чего проведите для каждой из двух полученных последовательностей: автокорреляционный тест, тест серий, частотный тест. Проанализируйте частоту изменения битов на позициях блока внутри каждой из полученных последовательностей, приведя результат в виде битового потока (поток из 0 и 1). Сравните полученные результаты. Чтобы было нагляднее, позиции, которые изменяются, можно выделить цветом - цвет выбирать в зависимости от количества изменений.

2. Тестируемый алгоритм

Алгоритм шифрования RC6

RC6 — итеративный блоковый алгоритм с переменной длиной информационного блока, переменным числом циклов и переменной длиной ключа. Алгоритм построен по классической схеме сетей Файстела. В общем случае авторы обозначили свой алгоритм как RC6- w/r/b, где w — размер обрабатываемых алгоритмом блоков, r—число циклов, b — длина ключа.

Алгоритм RC6 – с w = 32, r = 20, b = 128/192/256 бит обозначается просто как RC6

На рисунке 1 изображена схема одного раунда (цикла) алгоритма RC6.

3. Описание статистических тестов

Статистические тесты нужны для измерения качества генератора, предназначенного для генерации случайных бит. При том, что невозможно дать математическое доказательство того, что генератор действительно является генератором случайных бит, тесты, описанные здесь, помогают находить определенные типы недостатков, которыми может обладать генератор. Каждый статистический тест определяет, обладает ли последовательность неким атрибутом, который, вероятно, демонстрировала бы истинно случайная последовательность; заключение каждого тестане точно, а скорее вероятностно.

Частотный тест (однобитный тест)

Цель частотного теста – определить, является ли примерно равным количество 0 и 1 во входной последовательности s, как это ожидается в случайной последовательности. Пусть n_0, n_1 обозначают количество 0 и 1 в s, соответственно. Используется статистика

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

которая примерно следует x^2 распределению с 1 степенью свободы, если n $\geq 10^7$.

Тест серий

Цель теста серий – определить, является ли количество серий (состоящих из нулей, либо единиц) различных длин в последовательности s таким, как ожидается для случайной последовательности. Ожидаемое число разрывов (или блоков) длины i в случайной последовательности длины n оавгл $e_i = (n - i + 3)/2^{i+2}$. Пусть k равен наибольшему целому i, для которого $e_i \geq 5$. Пусть B_i, G_i – количество разрывов и блоков длины i в s, соответственно, для каждого $1 \leq i \leq k$. Используется статистика

$$X_4 = \sum_{i=1}^{k} \frac{(B_i - e_i)^2}{e_i} + \sum_{i=1}^{k} \frac{(G_i - e_i)^2}{e_i},$$

которая примерно следует x^2 распределению с 2k-2 степенями свободы.

Автокорреляционный тест

Цель этого теста – проверить корреляции между последовательностью s и ее (нециклическими) сдивгами. 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

$$X_5 = 2\left(A(d) - \frac{n-d}{2}\right)/\sqrt{n-d},$$

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

4. Примеры

Первая зашифрованная последовательность – S_1:
10011111001111110011001100111010100110111111111000110010100010011001111001011101100110011011011011000100110001110

Вторая зашифрованная последовательность – S_2:
10011111001000001111000111010011011111111100011111000010010101011001011100101110110011001101110101001100010011111 1

Результаты частотного теста

Для последовательности S_1:

$X_1 = 2.8421052$

Для последовательности S_2:

$X_1 = 2.245614$

Для уровня значимости α = 0.05 пороговое значение для X_1 = 3.8415, значит, обе последовательности прошли частотный тест.

Результаты теста серий

Для последовательности S_1:

$X_4 = 11.033171$

Для последовательности S_2:

$X_4 = 2.5726013$

Для уровня значимости α = 0.05 пороговое значение для X_4 = 9.487, значит, только вторая последовательность прошла тест серий.

Результаты автокорреляционного теста

Для последовательности S_1:

$X_5 = 0.76626104$

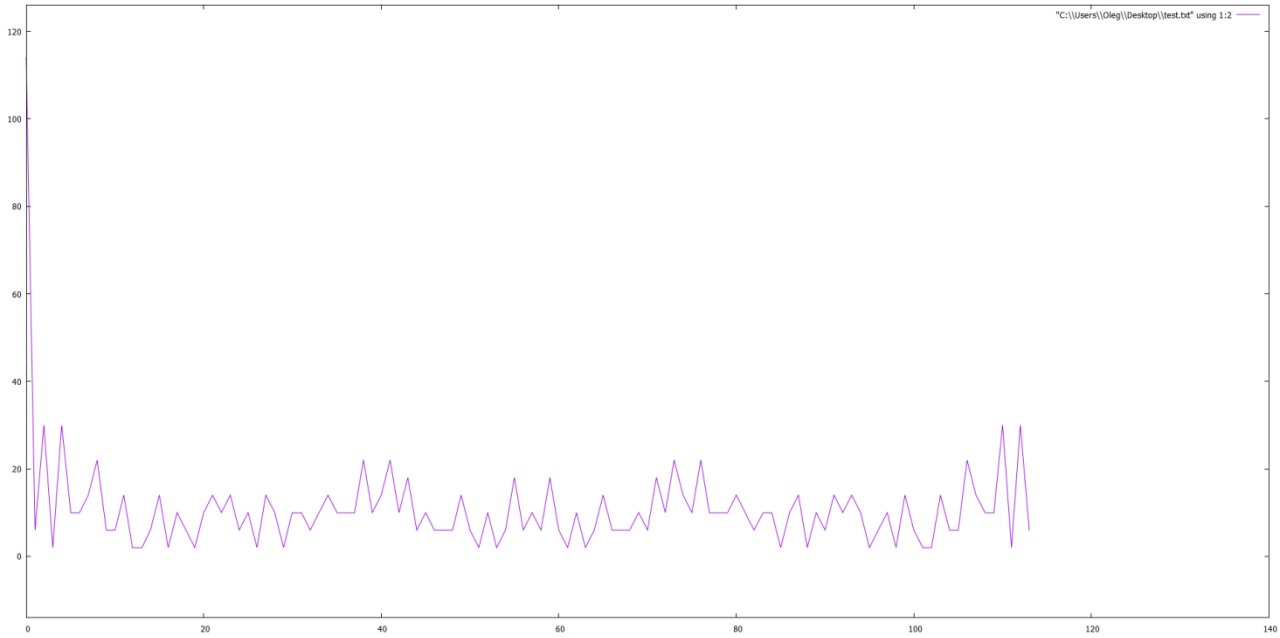

Рисунок 1. График автокорреляционного теста для S_1

Для последовательности S_2:

$X_5 = 2.298783$

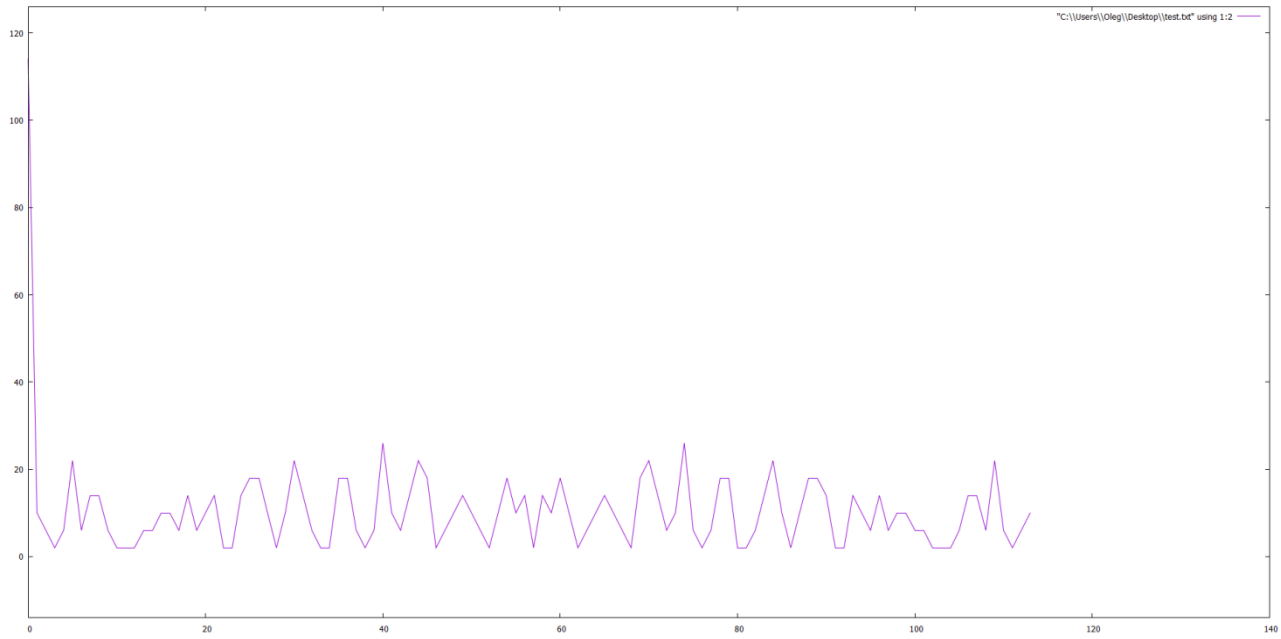

Рисунок 2. График автокорреляционного теста для S_2

Для уровня значимости α = 0.05 пороговое значение для X_5 = 1.96, значит, только первая последовательность прошла автокорреляционный тест.

5. Вывод

Провёл статистические тесты для алгоритма шифрования RC6. Обе рассмотренные последовательности не смогли пройти все три теста: первый провалил тест серий, а второй – автокорреляционный тест. Тем не менее, даже при прохождении последовательностью всех тестов, нет гарантий, что она была произведена генератором случайных бит, так как исход каждого теста является скорее вероятностным. Поэтому нельзя сказать, что алгоритм RC6 является не криптографически стойким из-за того, что данные последовательности провалили тесты.

6. Список литературы

[1] Менезес А., Handbook of applied cryptography, 1965 – 1997, CRC Press

[2] С.В. Беззатеев, Е.А. Крук, А.А. Овчинников, Блоковые Шифры. Учебное пособие, Санкт-Петербург : Издательство Нестор, 2003.