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

КАФЕДРА № 51

ОТЧЁТ ЗАЩИЩЁН С ОЦЕНКОЙ: _____

ПРЕПОДАВАТЕЛЬ:

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

ОТЧЁТ О ЛАБОРАТОРНОЙ РАБОТЕ
ИССЛЕДОВАНИЕ СИММЕТРИЧНЫХ ШИФРОВ

по курсу: Криптографические методы защиты информации

Работу выполнил:

Студент группы 5912 Б. А. Карханин

Санкт-Петербург 2021

Оглавление

1. Цель лабораторной работы:

Инвертируйте вторую половину битов блока, проведите N раундов (N зависит от алгоритма шифрования), затем для первоначальной исходной последовательности инвертируйте каждый четный (каждый второй) 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. Описание алгоритма шифрования

RC5 — это блочный шифр, разработанный Роном Ривестом из компании RSA Security с переменным количеством раундов, длиной блока и длиной ключа. Это расширяет сферу использования и упрощает переход на более сильный вариант алгоритма.

Шифрование по алгоритму RC5 состоит из двух этапов. Процедура расширения ключа и непосредственно шифрование. Все операции сложения и вычитания выполняются по модулю 2^w.

3. Описание тестов

3.1. Тест серий

Определим серию как непрерывную последовательность одного символа, в нашем случае 0 или 1. Длину серии будем считать равной количеству элементов в ней.

Если присутствуют длинные серии одного или другого символа, т.е. число серий мало, то имеет место положительная автокорреляция. Если символы часто меняются, т.е. число серий велико, то имеет место отрицательная автокорреляция.

Рассматривая, как серии ведут себя в абсолютно случайных последовательностях наблюдений, можно вывести тест на проверку случайности серии.

Примем за N общее количество наблюдений, за N1 – количество нулей, за N2 – количество единиц, R – общее количество серий. За нулевую гипотезу примем то, что последовательность абсолютно случайна, при условии, что N1>10 и N2>10, количество серий (асимптотически) нормально распределено с:

Математическим ожиданием: $E(R) = \frac{2N_1N_2}{N} + 1$

Дисперсией: $\sigma_R^2 = \frac{2N_1N_2(2N_1N_2 - N)}{N^2(N-1)}$

3.2. Частотный тест

Суть теста – посчитать количественное соотношение нулей и единиц во всей последовательности. Цель этого теста – определить, будет ли число единиц и нулей в последовательности приблизительно таким же, как в случайной последовательности.

Тест оценивает близость количества единиц к ½ длины всей последовательности, то есть число нулей и единиц в последовательности должно быть примерно одинаковым. Все последующие тесты зависят от прохождения этого теста; нет признака, указывающего на то, что протестированная последовательность неслучайна.

3.3. Автокорреляционный тест

Автокорреляция – явление, встречающееся в основном для временных рядов. При автокорреляции нарушается условие теоремы Гаусса – Маркова о некоррелированности возмущений для различных моментов времени.

В случае, когда в основном после положительных остатков вновь следуют положительные, а после отрицательных вновь следуют отрицательные (т.е. смена знаков остатков происходит редко) – это пример положительной автокорреляции. В случае, когда после положительных остатков чаще всего следуют отрицательные и наоборот – это пример отрицательной автокорреляции.

Для обнаружения корреляции между сдвинутыми копиями исследуемой последовательности. Для этого члены заданной битовой последовательности X_0, X_1, …, X_{n-1} заменяются по правилу: $1 \to 1$, $0 \to -1$. Тогда общий член новой последовательности имеет вид:

$$\alpha_i = (-1)^{1-x_i}$$

Где i = 0, 1,…,n-1

Далее будем находить всплески корреляции по формуле:

$$C_i = \frac{\sum_{i=0}^{n-1} b_i b_{(i+j) mod\, n}}{\sum_{i=0}^{n-1} b_i^2}$$

Для последовательности, близкой к случайной, всплески стремятся к 0 во всех точках, кроме кратных длине последовательности. Если есть много таких всплесков, то следует заподозрить зависимость между членами

4. Примеры работы тестов

4.1. Тест серий

Для первой последовательности:

N1 = 7470 (нули)

N2 = 7506 (единицы)

N = N1+N2 = 14976

R = 7428

$E(R) = \frac{2N_1N_2}{N} + 1 = 7488$

$\sigma_R^2 = \frac{2N_1N_2(2N_1N_2-N)}{N^2(N-1)} = 3739.3$

$\sigma_r = 61.2$

Доверительный интервал 95% для R в нашем примере следующий:

$E(R) - 1.96\sigma R \leq R \leq E(R) + 1.96\sigma R$

$7369.05 \leq R \leq 7608.95$

Интервал включает 7428. На 95% уровне значимости последовательность случайна. Гипотеза об отсутствии автокорреляции не отклоняется.

Для второй последовательности:

N1 = 7525 (нули)

N2 = 7451 (единицы)

N = N1+N2 = 14976

R = 7495

$E(R) = \frac{2N_1N_2}{N} + 1 = 7488$

$\sigma_R^2 = \frac{2N_1N_2(2N_1N_2-N)}{N^2(N-1)} = 3743.6$

$\sigma_r = 61.2$

Доверительный интервал 95% для R в нашем примере следующий:

$E(R) - 1.96\sigma R \leq R \leq E(R) + 1.96\sigma R$

$7368.75 \leq R \leq 7608.65$

Интервал включает 7495. На 95% уровне значимости последовательность случайна. Гипотеза об отсутствии автокорреляции не отклоняется.

4.2. Частотный тест:

Анализируем количество 0 и 1 в каждой из последовательностей: Numbers 0_2: digit one -- 7490 digit zero – 7486

Т.е. Частота повторения 0 в первой последовательности: 7486

Частота повторения 1 в первой последовательности: 7490

Частота повторения 0 во второй последовательности: 7525

Частота повторения 1 во второй последовательности: 7451

Получили, что число 0 и 1 в последовательностях является примерно равным.

```
n1:
frequency test = 0.0208333

n2:
frequency test = 0.520833
```

Рисунок 1. Результат работы программы для частотного теста.

Тест пройден.

4.3. Автокорреляционный тест

Первая последовательность:

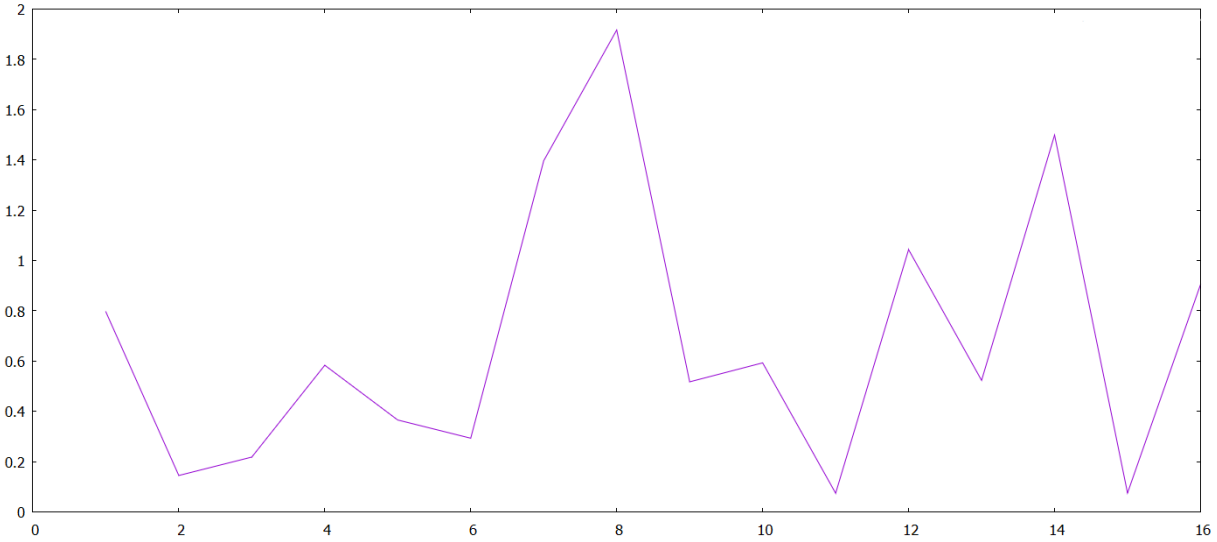

Рисунок 2. График автокорреляционного теста для первой последовательности

Для уровня значимости 0.05 пороговое значение автокорреляционного теста равно 1.96, следовательно, как видно по графику, последовательность проходит автокорреляционный тест (максимальное значение на графике равно 1.92)

Вторая последовательность:

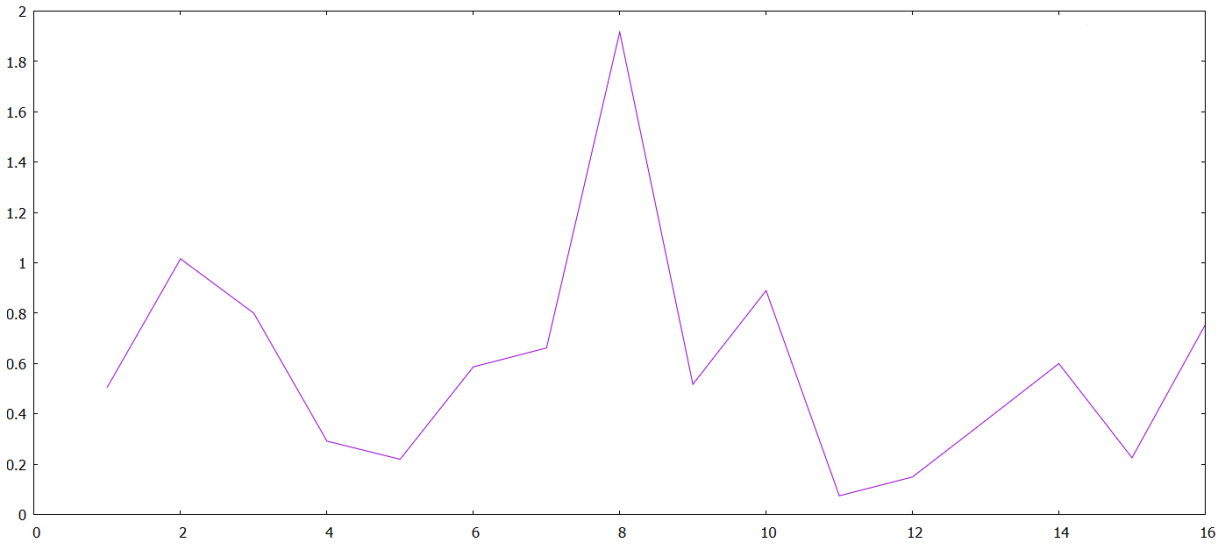

Рисунок 3.График автокорреляционного графика для второй последовательности.

Для уровня значимости 0.05 пороговое значение автокорреляционного теста равно 1.96, следовательно, как видно по графику, последовательность проходит автокорреляционный тест (максимальное значение на графике равно 1.93)

5. Вывод

Таким образом, результатом работы является программа, производящая тесты (частоты, серий и автокорреляционный) над последовательностями, полученными после прохождения алгоритма шифрования RC5. Помимо этого, до прохождения через алгоритм шифрования, входные последовательности были изменены: проинвертирована вторая половина блоков у первой последовательности, проинвертирован каждый четный бит блока у второй последовательности. С помощью произведенных тестов мы могли сделать выводы о случайности полученных последовательностей.

6. Список литературы.

1) Черчхаус. Коды и шифры

2) С.В. Беззатеев, Е.А. Крук, А.А. Овчинников “Блоковые Шифры. Учебное пособие”

3) Чмора, А. (2002). Современная прикладная криптография . Москва: Гелиос АРВ.

4) Шнайер, Б. (2003). Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. ТРИУМФ

5) Menezes, A. J. (1997). Handbook of applied cryptography. Boca Raton : CRC Press.