Задача

Вариант 5.

Инвертировать каждый четвертый бит блока, провести 16 раундов, затем для первоначальной исходной последовательности инвертировать каждый восьмой бит блока, провести 16 раундов, после чего провести для каждой из двух полученных последовательностей:

- Частотный тест;
- Тест серий;
- Автокорреляционный тест.

Проанализировать частоту изменения битов на позициях блока внутри каждой из полученных последовательностей, приведя результат в виде битового потока (поток из 0 и 1). Сравнить полученные результаты.

Тестируемый алгоритм

Twofish представляет собой алгоритм шифрования 128-битных блоков данных ключами по 128, 192 или 256 бит.

Описание статистических 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.

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 $n \geq 10^7$.

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.

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.

Примеры использования тестов

Исходный блок:

0110 1111 0110 1100 0010 0000 0100 0001 0111 0111 0010 0000 0110 0101 0110 1110 0110 0101 0111 0100 0110 1001 0110 1000 0110 1001 0110 0001 0111 0011 0010 0000

Рассмотрим последовательность бит S_1, получившуюся после инвертирования каждого четвертого бита блока и проведенных 16 раундов, и последовательность S_2, получившуюся после инвертирования каждого восьмого бита блока и проведенных 16 раундов.

Последовательность S_1 до шифрования:

0111 1110 0111 1101 0011 0001 0101 0000 0110 0110 0011 0001 0111 0100 0111 1111 0111 0100 0110 0101 0111 1000 0111 1001 0111 1000 0111 0000 0110 0010 0011 0001

Последовательность S_2 до шифрования:

0110 1110 0110 1101 0010 0001 0100 0000 0111 0110 0010 0001 0110 0100 0110 1111 0110 0100 0111 0101 0110 1000 0110 1001 0110 1000 0110 0000 0111 0010 0010 0001

Последовательность S_1 после шифрования:

1000 1001 1111 0001 0010 1100 1000 1100 1010 0110 0011 1100 1011 1011 0100 0110 1000 1011 0111 0010 0101 0111 0001 0001 1000 0010 0011 1100 0010 0001 0000 1010

Последовательность S_2 после шифрования:

0011 1111 1010 1011 0000 1110 1001 0000 0011 1100 1111 1100 1001 0100 1010 1011 1100 0001 0010 0100 0011 0110 0101 0011 0111 0000 1110 0010 0000 0100 1001 0110

Частотный тест

Оценим количество единиц и количество нулей.

Для первой последовательности S_1:

Количество единиц - $n_1 = 56$;

количество нулей - $n_0 = 72$;

всего бит - $n = 128$

По формуле (1) получаем:

$$X_1 = \frac{(72-56)^2}{128} = 2$$

Для второй последовательности S_2:

Количество единиц - $n_1 = 59$;

количество нулей - $n_0 = 69$;

всего бит - $n = 128$.

По формуле (1) получаем:

$$X_1 = \frac{(69-59)^2}{128} = 0.78125$$

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

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_2 = 16.25;

длины 2 – e_2 = 8.0625;

длины 3 – e_3 < 5, следовательно, k = 2;

количество разрывов длины 1 – G_1 = 32;

количество разрывов длины 2 – G_2 = 11;

количество блоков длины 1 – B_1 = 33;

количество блоков длины 1 – B_2 = 9.

По формуле (2) получаем:

$$X_2 = \sum_{i=1}^{2} \frac{(B_i - e_i)^2}{e_i} + \sum_{i=1}^{2} \frac{(G_i - e_i)^2}{e_i} = 33.71$$

Для второй последовательности S_2:

Ожидаемое число разрывов или блоков длины 1 – e_2 = 16.25;

длины 2 – e_2 = 8.0625;

длины 3 – e_3 < 5, следовательно k = 2;

количество разрывов длины 1 – G_1 = 31;

количество разрывов длины 2 – G_2 = 17;

количество блоков длины 1 – B_1 = 31;

количество блоков длины 1 – B_2 = 8.

По формуле (2) получаем:

$$X_2 = \sum_{i=1}^{2} \frac{(B_i - e_i)^2}{e_i} + \sum_{i=1}^{2} \frac{(G_i - e_i)^2}{e_i} = 36.6849$$

Для уровня значимости α = 0.05, пороговое значение для X_2 = 9.4877, следовательно, обе последовательности провалили тест серий.

Автокорреляционный тест

По формуле (3) для последовательности S_2 получаем(рис.1):

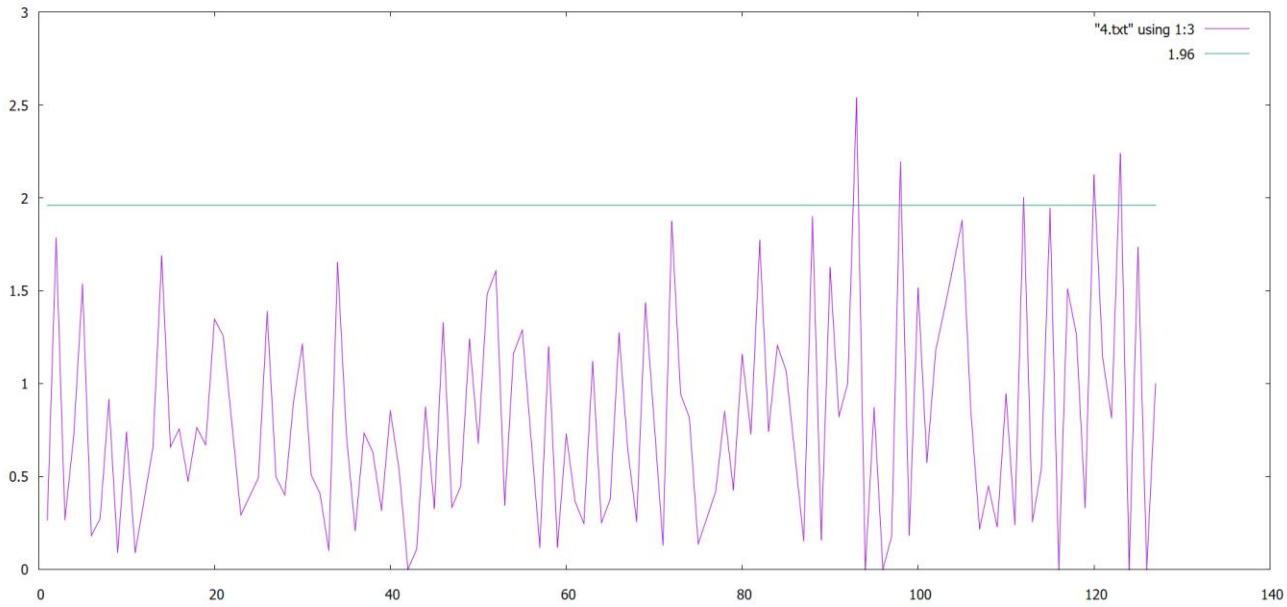

Рисунок 1.Автокорреляционный тест первой последовательности

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

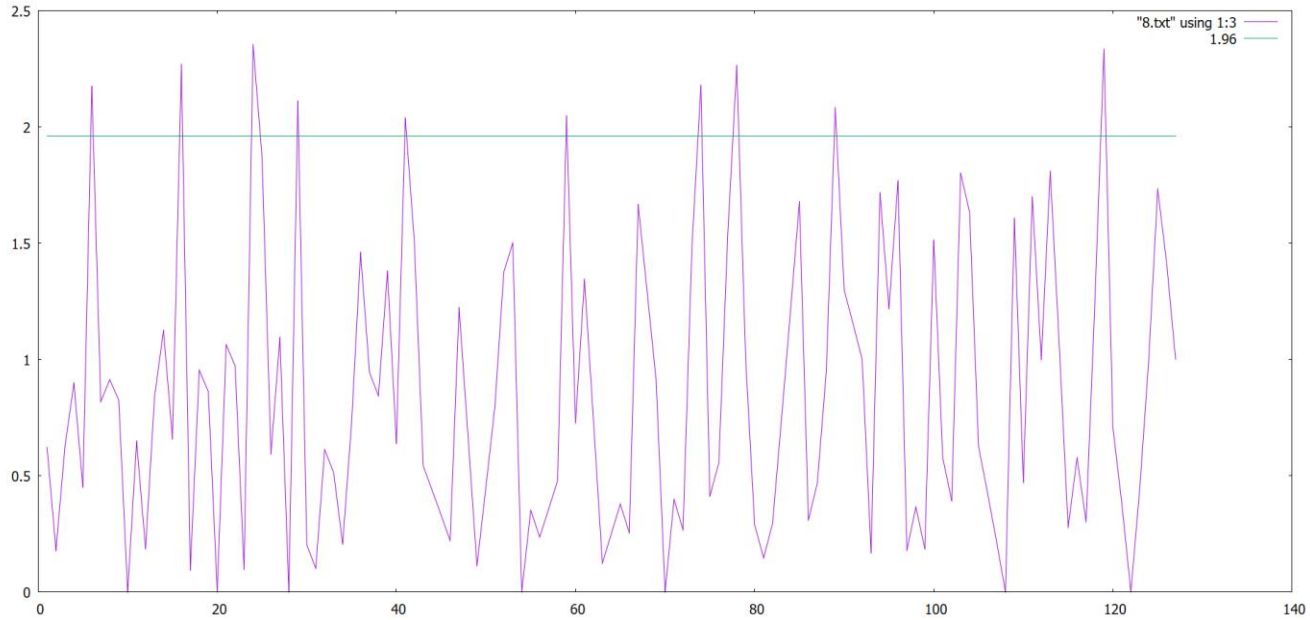

Рисунок 2. Автокорреляционный тест второй последовательности

Для уровня значимости $\alpha = 0.05$, пороговое значение для $X_3 = 1.96$, следовательно обе 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:

1000 1001 1111 0001 0010 1100 1000 1100 1010 0110 0011 1100 1011 1011 0100 0110 1000 1011 0111 0010 0101 0111 0001 0001 1000 0010 0011 1100 0010 0001 0000 1010

Изменения битов на соответствующих позициях:

5 9 5 10 9 9 7 7 5 10 9 8 9 8 12 5 8 7 13 12 13 5 6 9 7 8 11 6 9 8 7 11 8 8 9 10 6 6 9 7 5 9 9 12 4 12 10 10 10 11 10 14 10 7 9 11 9 10 10 10 10 8 7 9 4 8 4 9 11 9 8 7 5 10 8 7 9 9 11 5 6 8 13 11 14 4 6 10 8 9 11 6 9 9 7 8 9 8 9 11 7 6 9 7 6 7 8 11 5 12 12 10 9 11 11 12 10 8 9 10 8 10 10 10 9 8 9 8

Всего изменений: 1108

Последовательность S_2:

0011 1111 1010 1011 0000 1110 1001 0000 0011 1100 1111 1100 1001 0100 1010 1011 1100 0001 0010 0100 0011 0110 0101 0011 0111 0000 1110 0010 0000 0100 1001 0110

Изменения битов на соответствующих позициях:

9 10 11 12 9 9 9 11 12 10 8 11 10 6 8 7 8 5 7 14 11 11 11 10 10 8 10 9 5 9 7 13 13 10 8 8 9 7 6 10 8 10 5 11 5 7 10 11 10 11 10 11 9 11 8 10 7 10 7 10 8 6 11 7 9 9 11 12 11 9 10 10 12 10 8 10 10 7 8 6 6 6 10 13 11 10 11 11 8 9 10 8 5 7 6 10 11 10 7 9 9 7 7 10 10 9 4 10 6 6 11 11 10 10 8 9 8 12 9 10 7 11 7 9 7 7 10 7

Всего изменений: 1155

Из полученной оценки изменения битов можно сделать вывод, что при инвертировании каждого восьмого бита последовательность терпит больше изменений, чем при инвертировании каждого четвертого бита.

Вывод

В данной работе были проведены статистические тесты для алгоритма шифрования Twofish. 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 Twofish не является не криптографически стойким из-за того, что провалил тест серий и автокорреляционный тест.
Также было выяснено, что при инвертировании каждого восьмого бита последовательность терпит больше изменений, чем при инвертировании каждого четвертого бита.

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