Продолжение таблицы

1	2	3	4
21	1101100110001100 0001110000011001 1011100010101000 0011000010110010	1001111111010110 1000011111011110 0100110000010000 1101011010000110	34
45	0110000101110110 0110010101100110 0110011001101101 0110001101110100	1000011100001011 0100100100101010 1111110000011000 1100000110011011	36
10	0110000100110110 0110010101100110 0110011001100101 0110001101110100	0100011111100100 1111001001101010 0000100010000001 0001011001101001	32

Подсчитаем разницу между максимальным значением процента измененных бит и минимальным значением по формуле:

$P_{max} = \frac{36}{64} \times 100 = 56{,}3\ P_{min} = \frac{31}{64} \times 100 = 48{,}4\ P_{max} - P_{min} == 56{,}3 - 48{,}4 = 7{,}9\%$

.

ЛИТЕРАТУРА

1. Vergili I., Yücel M. D. // Turk J ElecEngin. 2001, № 2(9). С. 137–145.

2. Урбанович, П. П. Лабораторный практикум по дисциплинам «Защита информации и надежность информационных систем» и «Криптографические методы защиты информации». В 2 ч. Ч. 1. Кодирование информации: учеб.-метод. пособие для студентов / П. П. Урбанович, Д. В. Шиман, Н. П. Шутько. – Минск: БГТУ, 2019. – 116 с.

3. Урбанович, П. П. Защита информации методами криптографии, стеганографии и обфускации: учеб.-метод. пособие. – Минск: БГТУ, 2016. – 220 с.

УДК [004.056+003.26] (075.8)

Студ. А.Э. Севрюк, Е.В. Гончаревич
Науч. рук. проф. П.П. Урбанович
(Кафедра информационных систем и технологий, БГТУ)

СРАВНЕНИЕ ПРОИЗВОДИТЕЛЬНОСТИ ПРОЦЕССОВ ЗАШИФРОВАНИЯ/РАСШИФРОВАНИЯ ИНФОРМАЦИИ ПО МЕТОДУ ВИЖЕНЕРА С ОДНИМ И ДВУМЯ КЛЮЧАМИ

Шифрование является одним из важных средств обеспечения информационной безопасности [1, 2]. Оно позволяет защитить данные от несанкционированного доступа и использования.

Шифр Виженера является одним из наиболее известных и надежных подстановочных шифров. Он основан на замене каждой буквы в сообщении на другую букву, сдвинутую на определенное количество позиций в алфавите, в зависимости от ключа [3].

Для сравнения метода Виженера с одним и двумя ключами была разработана программа, которая зашифровывает и расшифровывает сообщение длиной в 144586 символов и сравнивает их характеристики, а именно: время шифрования и расшифрования, а также статистику распределения символов. На рис. 1 можно увидеть время, затраченное на зашифрование и расшифрование текста методом Виженера с одним ключом, а также статистику текстов (зашифрованного и расшифрованного), и число используемых символов в исходном тексте и зашифрованном.

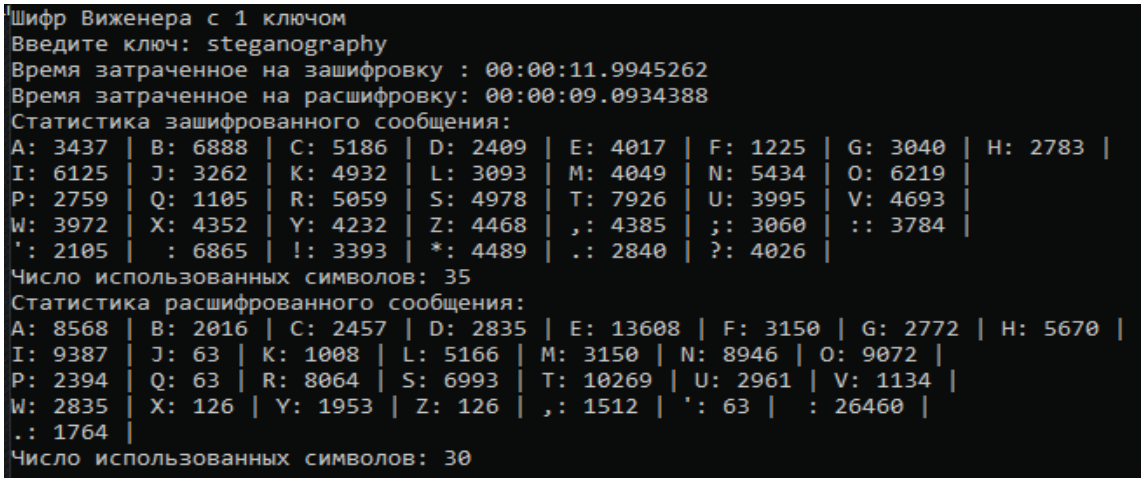

Рисунок 1 – Характеристики шифра Виженера с одним ключом

На рис. 2 изображены характеристики: статистика сообщения, зашифрованного методом с двумя ключами (исходный текст тот же), и затраченное время на шифрование и расшифрование, а также и число используемых символов в зашифрованном сообщении.

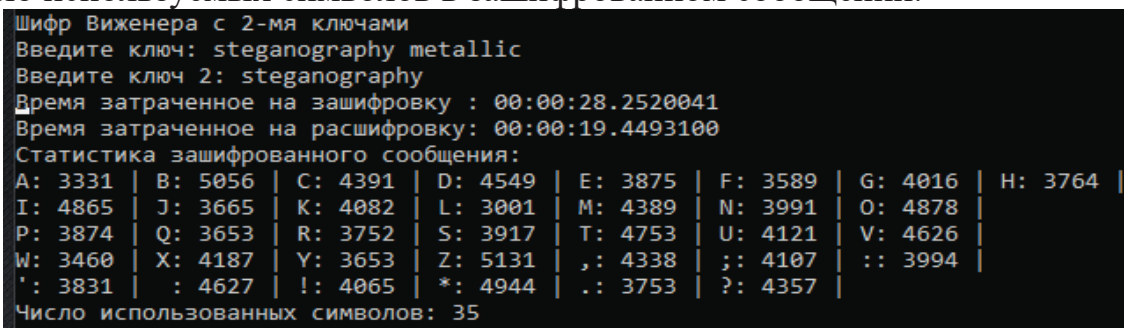

Рисунок 2 – Характеристики шифра Виженера с двумя ключами

Время, затраченное на зашифрование и расшифрование методом Виженера с двумя ключами, больше, чем с одним. Распределение символов по методу Виженера с одним ключом изображено на рис. 3.

Голубой кривой показана статистика символов исходного сообщения, оранжевой – статистика символов зашифрованного сообщения.

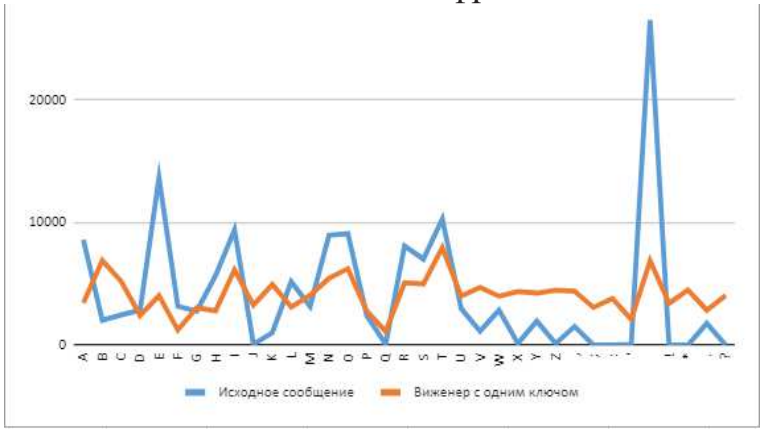

Рисунок 3 – Статистика распределения символов по методу Виженера с одним ключом

Можно сделать вывод, что при использовании шифра с двумя ключами вероятность появления символов становится примерно одинаковой, по сравнению с шифром с одним ключом.

Шифр с двумя ключами выравнивает вероятности лучше, чем с одним ключом, потому что он использует два различных ключа для шифрования сообщения, однако, в обмен требует больше времени на обработку. Это означает, что каждый ключ вносит свой вклад в шифрование, что приводит к более равномерному распределению символов в шифротексте. Если использовать только один ключ, то вероятности символов могут быть смещены в сторону ключа, что может сделать шифрование менее надежным.

Распределение символов по методу с двумя ключом изображено на рис. 4 (цвета линий – как на рис. 3).

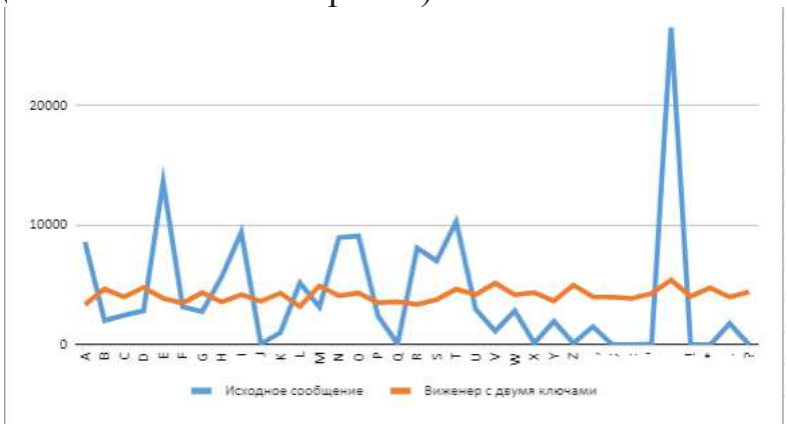

Рисунок 4 – Статистика распределения символов по методу Виженера с двумя ключами

Высокую значимость для выравнивания имеет длина ключей и разнообразие символов в ключах. Большие и неповторяющиеся ключи

будут положительно влиять на выравнивание, но длина шифруемого текста будет больше. Одноключевой шифр Виженера достаточно надежен, но сложнее в использовании, чем одноключевой шифр Цезаря. Двухключевой шифр Виженера намного более безопасен, но гораздо медленнее и сложнее в использовании.

Таким образом, выбор между шифром Виженера с одним ключом и с двумя ключами зависит от конкретных требований безопасности: если безопасность является первостепенной задачей, то можно использовать шифр с двумя ключами, но если удобство использования и экономия ресурсов важнее, то можно выбрать шифр с одним ключом.

ЛИТЕРАТУРА

1. Урбанович, П. П. Защита информации и надежность информационных систем / П. П. Урбанович, Д. В. Шиман. – Минск: БГТУ, 2013. – 90 с.

2. Урбанович, П. П. Защита информации методами криптографии, стеганографии и обфускации: учеб.-метод. пособие. – Минск: БГТУ, 2016. – 220 с.

3. Урбанович, П. П. Лабораторный практикум по дисциплинам «Защита информации и надежность информационных систем» и «Криптографические методы защиты информации». В 2 ч. Ч. 2. Криптографические и стеганографические методы защиты информации: учеб.-метод. пособие для студ. вузов / П. П. Урбанович, Н. П. Шутько. – Минск: БГТУ, 2020. – 226 с.

УДК 004.056.5:004.021

Студ. К.В. Миневич, студ. Н.А**.** Стальмахова
Науч. рук. проф. П.П. Урбанович
(Кафедра информационных систем и технологий, БГТУ)

ОЦЕНКА ПРОИЗВОДИТЕЛЬНОСТИ И КРИПТОСТОЙКОСТИ АЛГОРИТМОВ DES И AES

Шифрование данных является важным инструментом для защиты информ. Алгоритмы DES (Data Encryption Standard) и AES (Advanced Encryption Standard) являются одними из наиболее распространенных и надежных методов шифрования, используемых для защиты конфиденциальных данных [1–4]. Однако, с появлением новых технологий и угроз безопасности, оценка производительности и криптостойкости этих алгоритмов становится все более важной задачей. В этом контексте, наша работа посвящена обсуждению различных аспектов производительности и криптостойкости алгоритмов DES и