Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Криптографические шифры на основе подстановки символов

Студент: Вайсера Р.Л.

ФИТ 3 курс 4 группа

Преподаватель: Сазонова

Минск 2023

# Моноалфавитный подстановочный шифр

Одним из самых простых шифров является моноалфавитный шифр подстановки. В данных шифрах каждый символ исходного алфавита заменяется на один и тот же символ также из этого алфавита.

Для наглядной демонстрации шифра простой замены достаточно выписать под заданным алфавитом тот же алфавит, но в другом порядке или, например, со смещением. Записанный таким образом алфавит называют алфавитом замены.

Максимальное количество ключей для любого шифра этого вида не превышает *N!*, где *N* – количество символов в алфавите. Для математического описания криптографического преобразования предполагаем, что зашифрованная буква *ay* (*ay* ∈ *Ci*), соответствующая символу *ax* (*ax* ∈ *Mi*), находится на позиции

(2.1)

где *x*, *y* – индекс (порядковый номер, начиная с 0) символа в используемом алфавите; *k* – ключ. Для расшифрования сообщения *Ci* необходимо произвести расчеты, обратные выражению (1.1), т. е.

(2.2)

Ключом в моноалфавитном подстановочном шифре является число *k*.

# Зашифрование моноалфавитным шифром

В качестве алфавита выбран английский язык, а в качестве ключа *k* в формуле (1.1) выбрано число *k* = 5. В качестве открытого текста на исходном языке используется текстовый документ text.txt длиной более 5000 символов, представленный на рисунке 1.1.

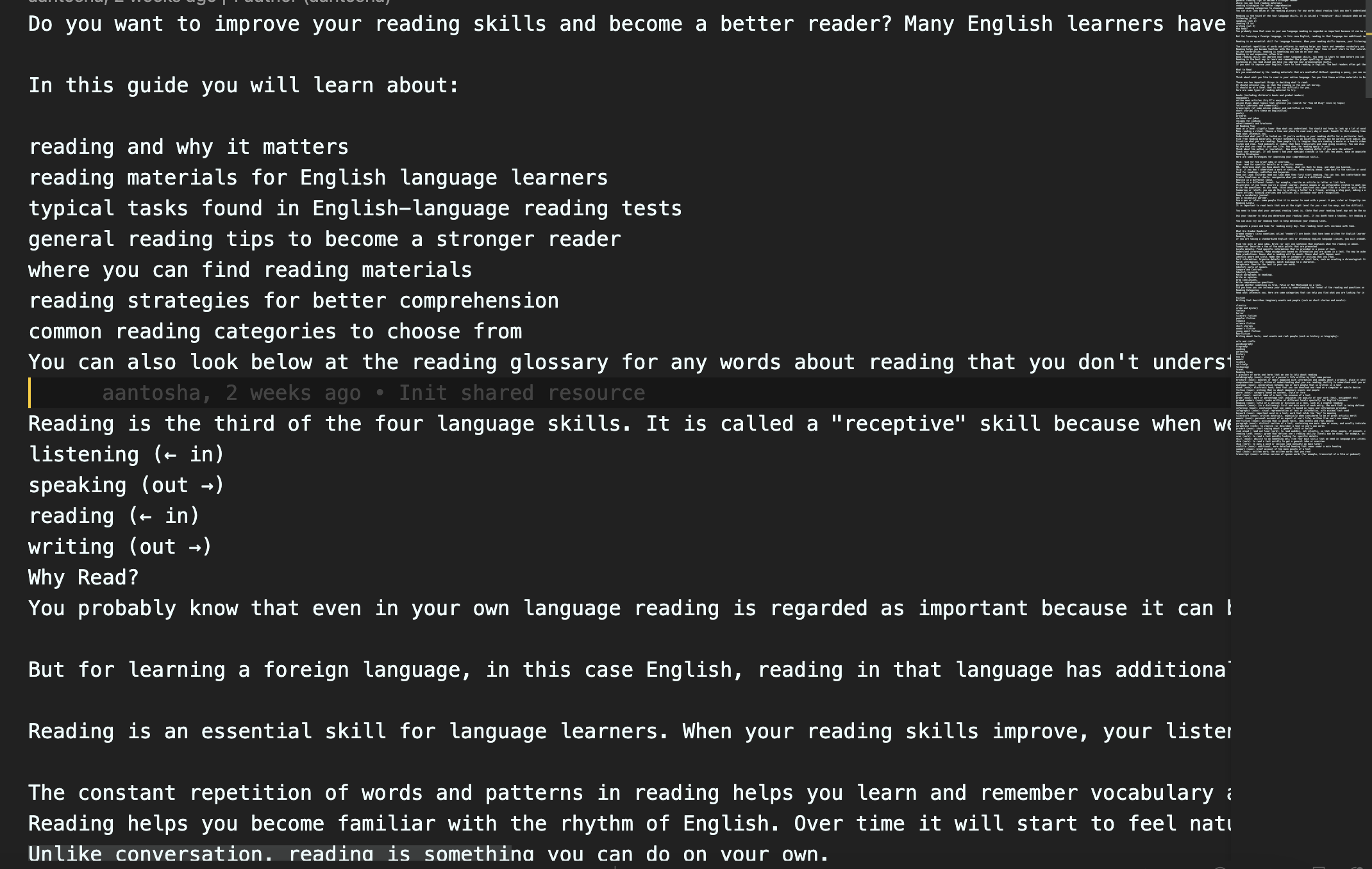


Рисунок 1.1 – Текстовый документ на исходном английском языке

Далее для зашифрования необходимо получить индексы всех символов исходного текста и подставить индекс символа *x*, ключ *k* = 5 и мощность алфавита *N* = 26 в формулу (2.1). Для зашифрования текста с помощью моноалфавитного подстановочного шифра реализована следующая функция, представленная на рисунке 1.2

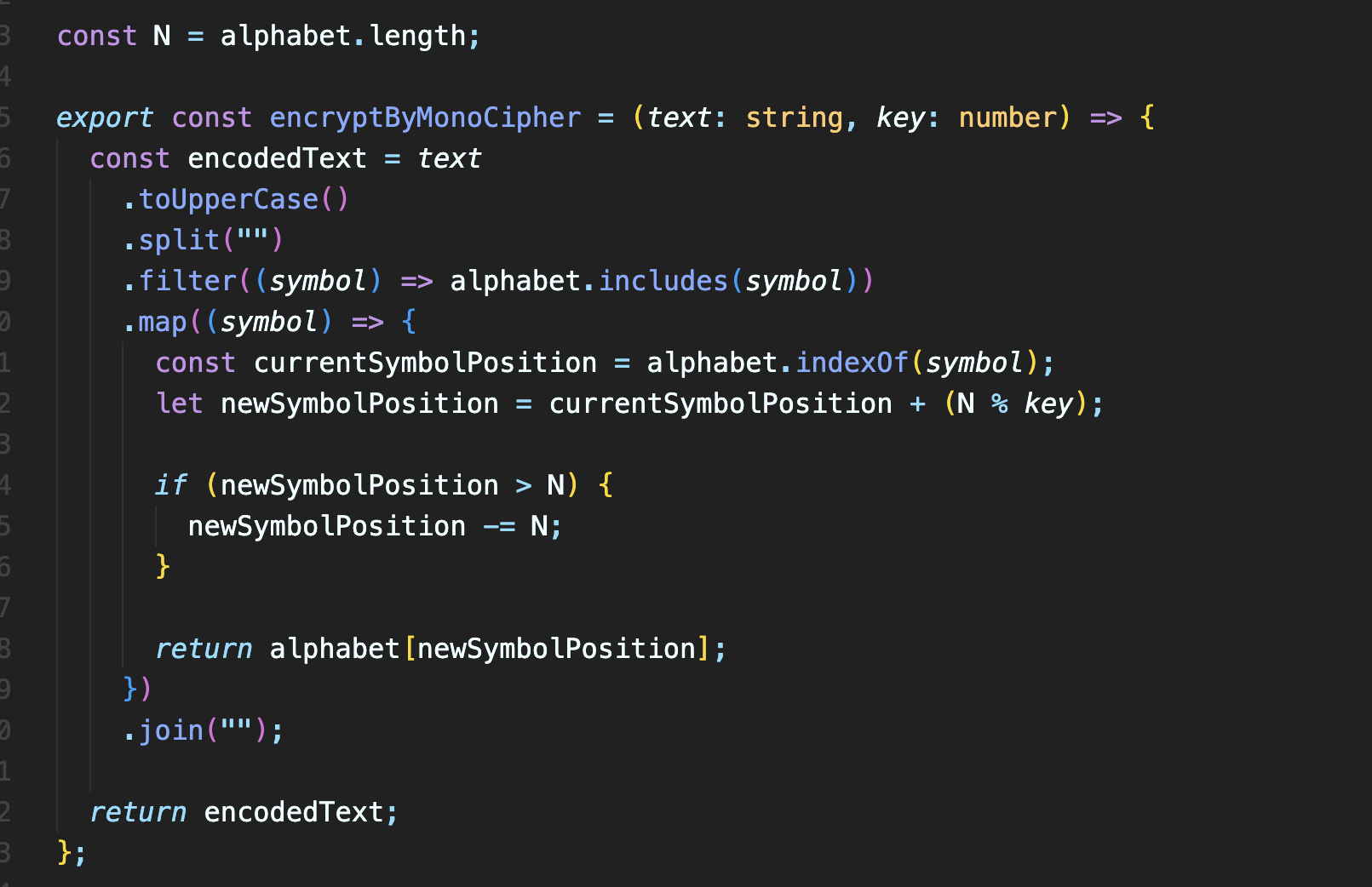


Рисунок 1.2 – Функция зашифрования моноалфавитным шифром

# Расшифрование моноалфавитным шифром

Для расшифрования текста, зашифрованного моноалфавитным подстановочным шифром, необходима аналогичная функция, в которой единственным изменением является использование формулы (2.2) вместо формулы (2.1). Для расшифрования текста с помощью моноалфавитного подстановочного шифра реализована следующая функция, представленная на рисунке 1.3

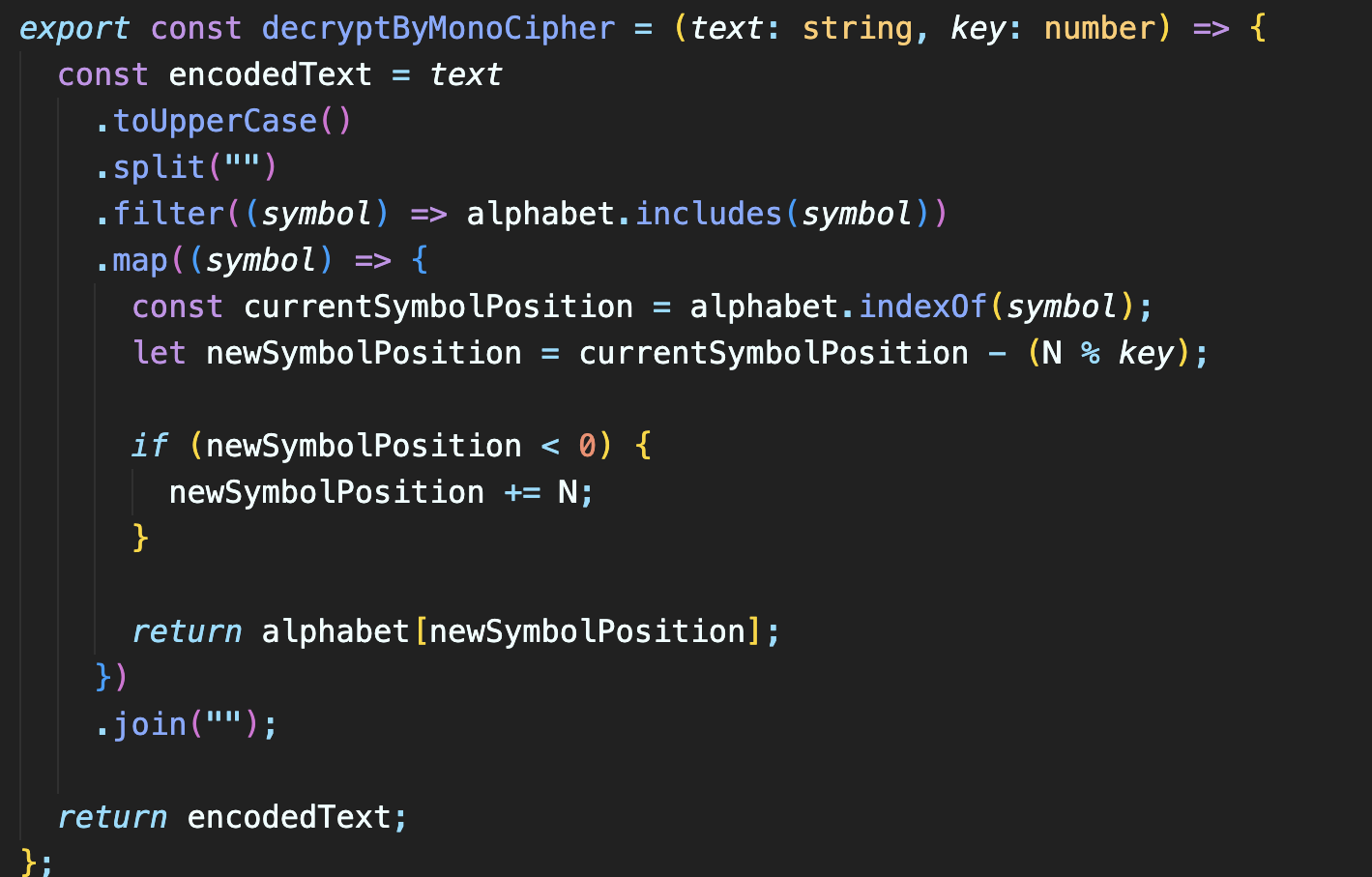


Рисунок 1.3 – Функция расшифрования моноалфавитного шифра

# Шифр Виженера

В этом шифре мы имеем дело с последовательностью сдвигов, циклически повторяющейся. Основная идея заключается в следую- щем. Создается таблица (таблица Виженера) размером *NN* (*N* – число знаков в используемом алфавите).

# Зашифрование шифром Виженера

Создается таблица (таблица Виженера) размером *NN* (*N* – число знаков в используемом алфавите). Эти знаки могут включать не только буквы, но и, например, пробел или иные знаки. В первой строке таблицы записывается весь используемый алфавит. Каждая последующая строка получается из предыдущего циклического сдвига последней на 1 символ влево. Таким образом, при мощности алфавита (английского языка), равной 26, необходимо выполнить последовательно 25 сдвигов для формирования всей таблицы. Для зашифрования текста с помощью шифра Виженера реализована следующая функция, представленная на рисунке 1.3

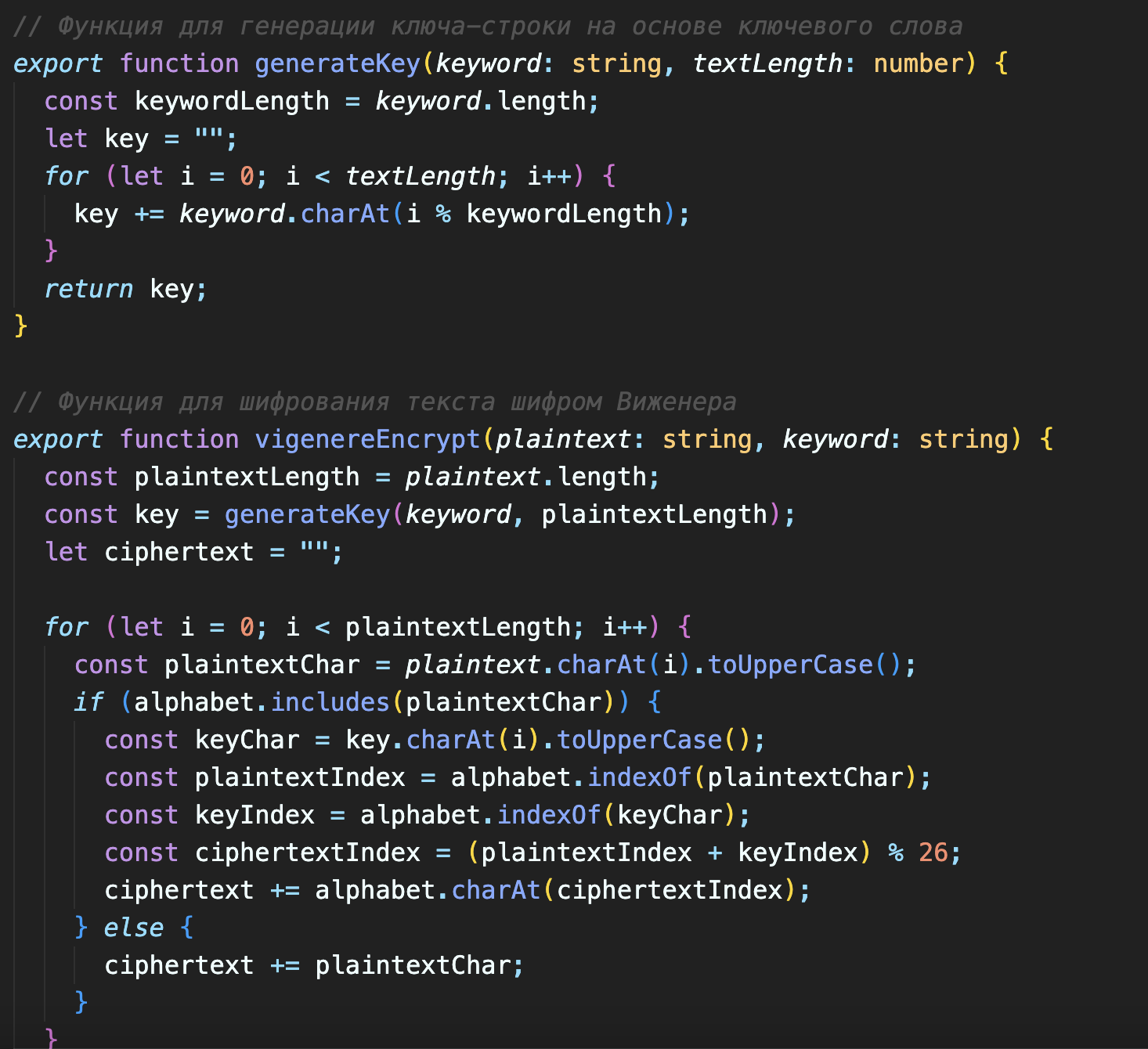


Рисунок 1.3 – Функция зашифрования таблицей Виженера

# Расшифрование таблицы Виженера

Для расшифрования текста с помощью шифра Виженера необходимо выполнить те же действия, но в обратном порядке:найти ряд, обозначенный первой буквой ключевого слова, затем найти в нем первую букву зашифрованной фразы. Посмотреть, в какой колонке она находится: буква, которой обозначена эта колонка, и будет первой буквой расшифрованного сообщения.

Для реализации расшифрования создана следующая функция, представленная на рисунке 1.4.

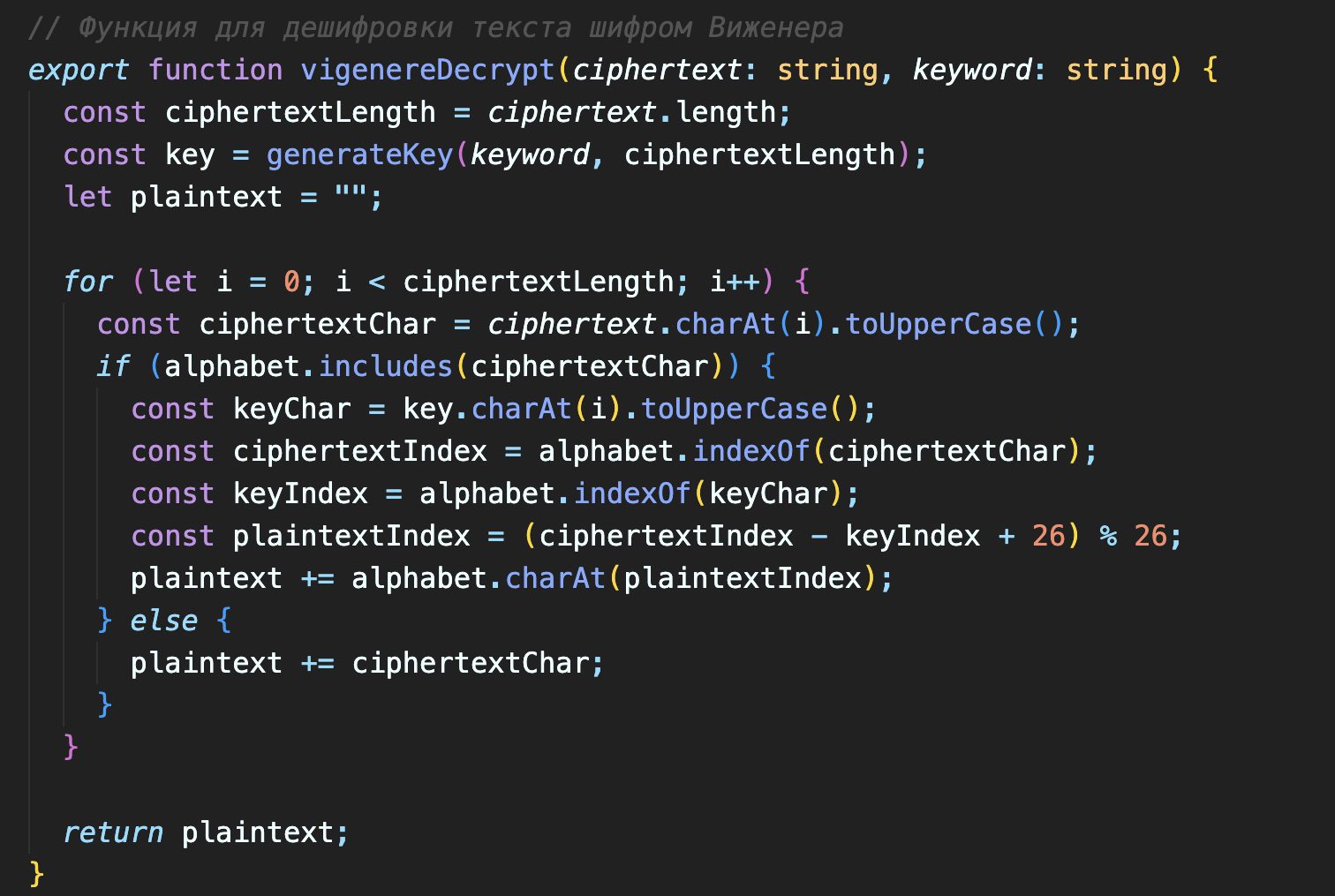


Рисунок 1.4 – Функция расшифрования таблицы Виженера

# Частоты появления символов.

Для вычисления количества появлений символов в тексте используется функция, представленной на рисунке 3.1.

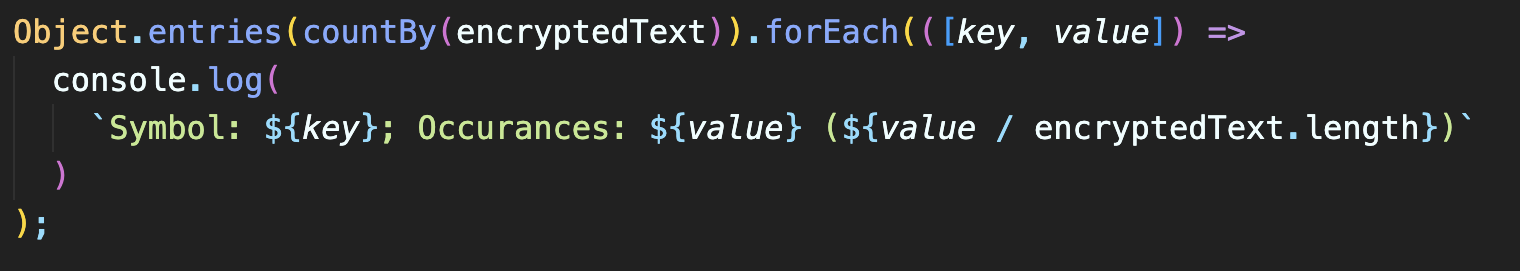


Рисунок 1.5 – Функция подсчёта количества символов

Результат работы функции представлен на рисунке 1.6

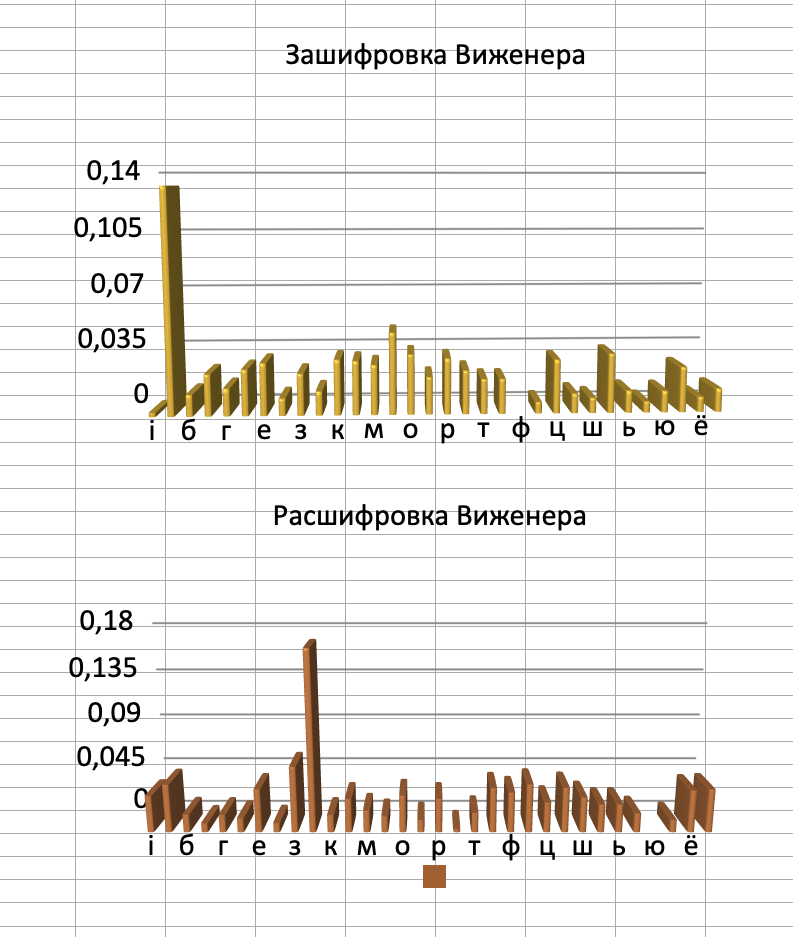


Рисунок 1.6 – Гистограмма частотности букв

# Производительность

График зависимости времени шифрования и расшифрования от количества символом для шифров по варианту представлен на рисунке 1.7

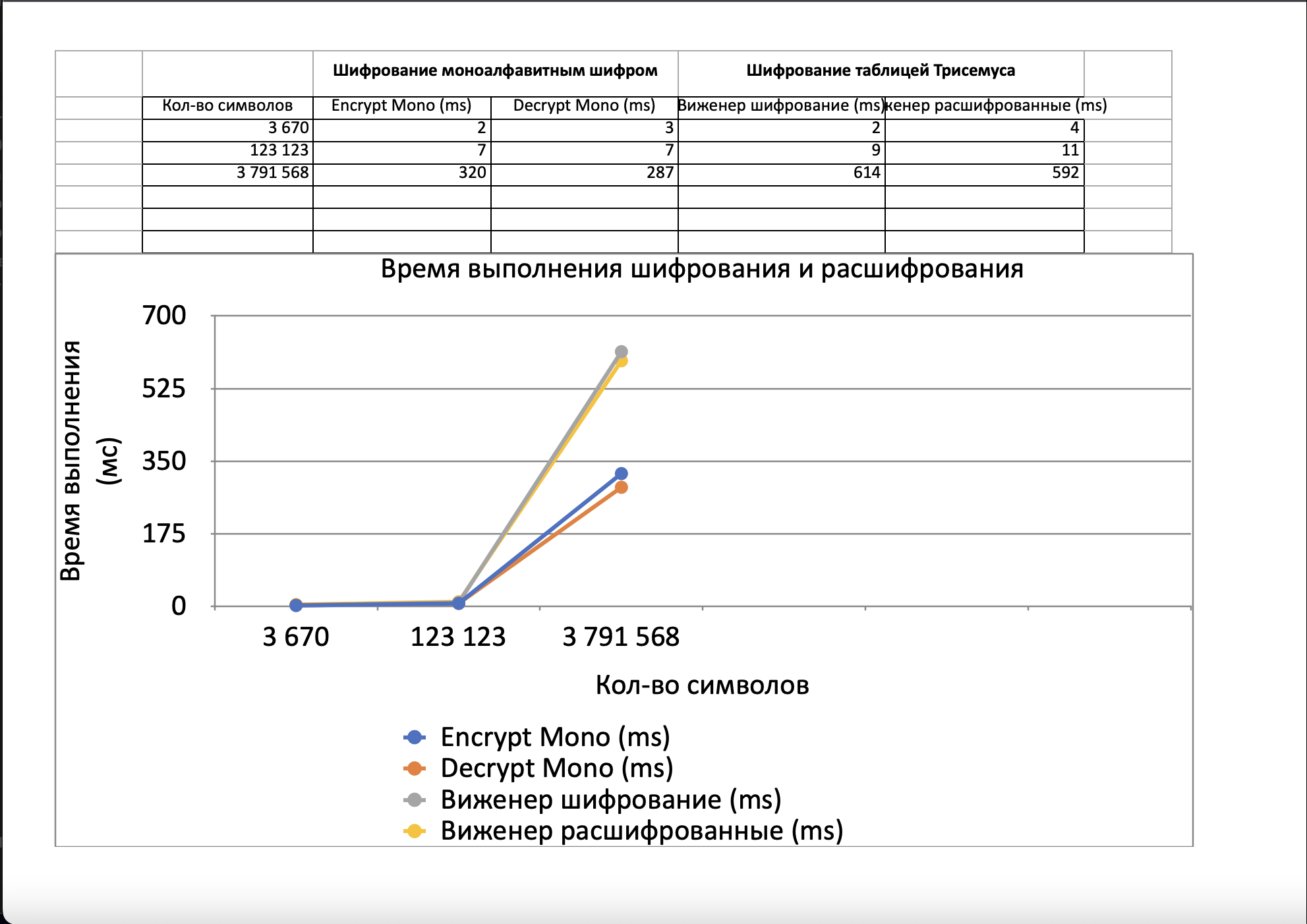


Рисунок 1.7 – Время выполнения операций шифрования расшифрования

# Вывод

Были рассмотрены два подстановочных шифра – моноалфавитный шифр и полиалфавитный шифр таблицей Виженера. С точки зрения криптоанализа, оба шифра не являются криптостойкими, так как уязвимы к частотному анализу ввиду того, что каждому символу исходного текста всегда соответствует только один символ шифротекста.

При сравнении времени выполнения операций зашифрования и расшифрования для обоих шифров выясняется, что зашифрование таблицей Виженера быстрее зашифрования моноалфавитным шифром примерно в 5-10 раз при входных документах не длиннее 1 миллиона символов, но начинает замедляться при увеличении количества входных символов. Аналогично, расшифрование таблицы Виженера быстрее только при количестве символов, примерно равном 100 миллионам.

По результатам гистограмм можно заметить, что частоты сохранились, но сместились относительно положения в исходном тексте, что говорит о том, что шифр подвержен частотному анализу, т. к., видно, что, например символ «i» исходного алфавита по частоте встречаемости соотствествует символу «k» шифртекста.

Следовательно, таблицу Виженера целесообразно использовать для небольших документов (менее 1 миллиона символов).