Лабораторная работа №2

Математические основы защиты информации и информационной безопасности

Николаев Дмитрий Иванович, НПМмд-02-24

Содержание

# 1 Цель работы

Изучить работу шифров перестановки — маршрутного шифрования, шифрования с помощью решёток и таблицы Вижинёра, а также реализовать их программно.

# 2 Теоретическое введение

Шифры перестановки преобразуют открытый текст в криптограмму путем перестановки его символов. Способ, каким при шифровании переставляются буквы открытого текста, и является ключом шифра. Важным требованием является равенство длин ключа и исходного текста.

Существует два широко распространенных метода перестановок: маршрутное шифрование и шифрование с помощью решеток.

## 2.1 Маршрутное шифрование

Данный способ шифрования разработал французский математик Франсуа Виет. Открытый текст записывают в некоторую геометрическую фигуру (обычно прямоугольник) по некоторому пути, а затем, выписывая символы по другому пути, получают шифротекст. Пусть и — целые положительные числа, большие 1. Открытый текст разбивается на блоки равной длины, состоящие из числа символов, равного произведению . Если последний блок получится меньше остальных, то в него следует дописать требуемое количество произвольных символов. Составляется таблица размерности . Блоки вписываются построчно в таблицу. Криптограмма получается выписыванием букв из таблицы в соответствии с некоторым маршрутом. Ключом такой криптограммы является маршрут и числа и . Обычно буквы выписывают по столбцам, которые упорядочивают согласно паролю: внизу таблицы приписывается слово из неповторяющихся букв и столбцы нумеруются по алфавитному порядку букв пароля.

Например, для шифрования текста “нельзя недооценивать противника”, разобьем его на блоки длины . Блоков получится . К последнему блоку припишем букву “а”. В качестве пароля выберем слово “пароль”. Теперь будем выписывать буквы по столбцам в соответствии с алфавитным порядком букв пароля и получим следующую криптограмму: ЕЕНПНЗОАТАЬОВОКННЕЬВЯЦТИА.

Рассмотренный способ шифрования (столбцовая перестановка) в годы первой мировой войны использовала легендарная немецкая шпионка Мата Хари.

## 2.2 Шифрование с помощью решеток

Данный способ шифрования предложил австрийский криптограф Эдуард Флейснер в 1881 году. Суть этого способа заключается в следующем. Выбирается натуральное число , строится квадрат размерности , который построчно заполняется числами . В качестве примера рассмотрим квадрат размерности :

Повернем его по часовой стрелке на 90° и присоединим к исходному квадрату справа:

Проделаем такую процедуру еще дважды и припишем получившиеся квадраты снизу. Получился большой квадрат размерности .

Далее из большого квадрата вырезаются клетки, содержащие числа от 1 до . В каждой клетке должно быть только одно число. Получается своего рода решето. Шифрование осуществляется следующим образом. Решето накладывается на чистый квадрат , и в прорези вписываются буквы исходного текста по порядку их следования. Когда заполнятся все прорези, решето поворачивается на 90° и вписывание букв продолжается. После третьего поворота все клетки большого квадрата окажутся заполненными. Подобрав подходящий пароль (число букв пароля должно равняться , и они не должны повторяться), выпишем буквы по столбцам. Очередность столбцов определяется алфавитным порядком букв пароля.

Пример. Исходный текст — “договор подписали”, пароль — “шифр”.



Шифрование с помощью решеток

С применением вышеуказанной ([??]) решетки за пять шагов получаем следующую криптограмму: ОВОРДЛГПАПИОСДОИ.

Важно отметить, что число подбирается в соответствии с количеством букв исходного текста. В идеальном случае . Если такого равенства достичь невозможно, то можно либо дописать произвольную букву к последнему слову открытого текста, либо убрать её.

## 2.3 Таблица Виженера

В 1585 году французский криптограф Блез Виженер опубликовал свой метод шифрования в “Трактате о шифрах”. Шифр считался нераскрываемым до 1863 года, когда австриец Фридрих Казиски взломал его.

Открытый текст разбивается на блоки длины . Ключ представляет собой последовательность из натуральных чисел: . Далее в каждом блоке первая буква циклически сдвигается вправо по алфавиту на позиций, вторая буква — на позиций, последняя — на позиций. Для лучшего запоминания в качестве ключа можно взять осмысленное слово, а алфавитные номера входящих в него букв использовать для осуществления сдвигов. Рассмотрим еще одну схему построения шифра Виженера. В таблице в строчках записаны буквы русского алфавита смещённые на соответсвующий номер строки (первая — исходный алфавит). При переходе от одной строке к другой происходит циклический сдвиг на одну позицию.

Пример. Исходный текст – “криптография серьезная наука”, пароль – “математика”. Пароль записывается с повторениями над буквами сообщения ([??]):

Соответствия в шифровании с помощью таблицы Вижинёра

Соответствия в шифровании с помощью таблицы Вижинёра

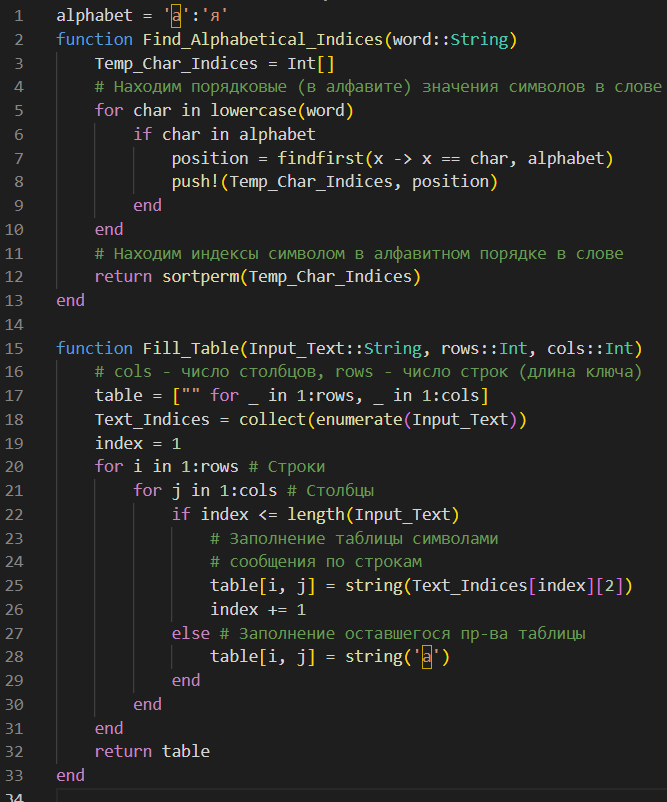
В итоге получается следующая криптограмма: ЦРЬФЯОХШКФФЯДКЭЬЧПЧАЛНТШЦА.

# 3 Ход работы

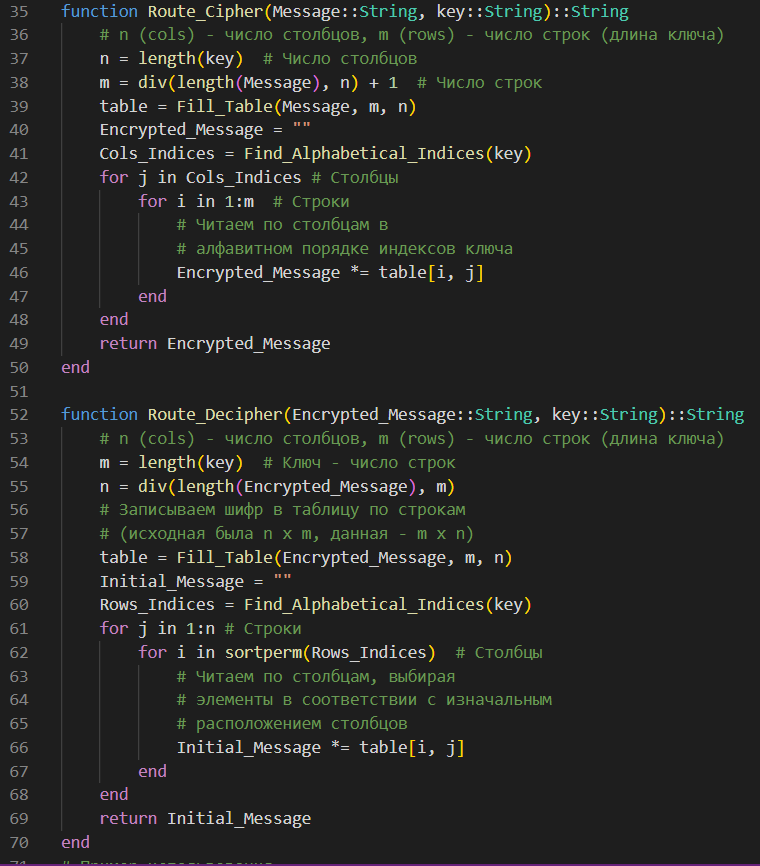
Следуем указаниям из [1].

## 3.1 Маршрутное шифрование

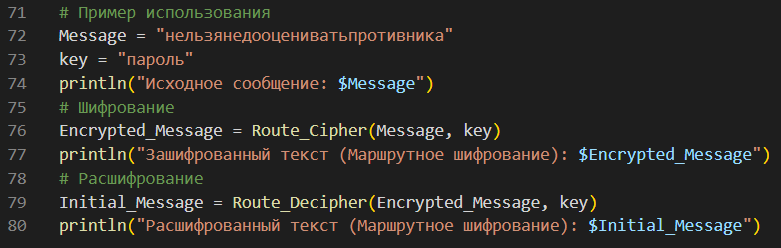
Реализуем алгоритм маршрутного шифрования и его расшифрование на Julia ([??-??]), в результате получим следующий вывод ([??]).



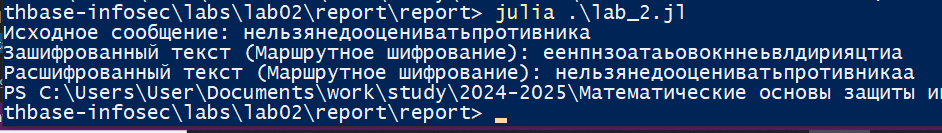
Код реализации алгоритма маршрутного шифрования на Julia (1/3)



Код реализации алгоритма маршрутного шифрования на Julia (2/3)



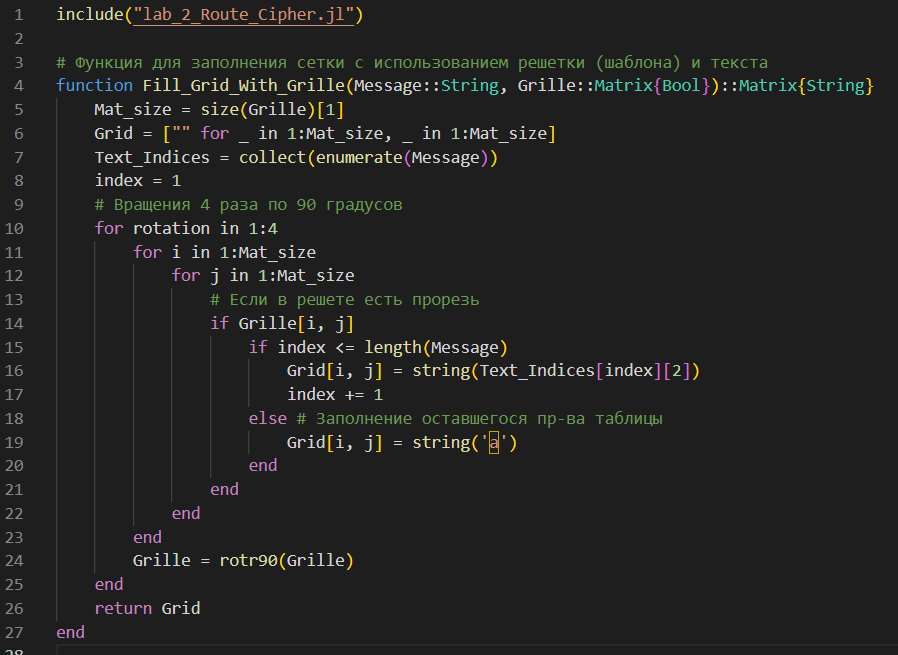
Код реализации алгоритма маршрутного шифрования на Julia (3/3)



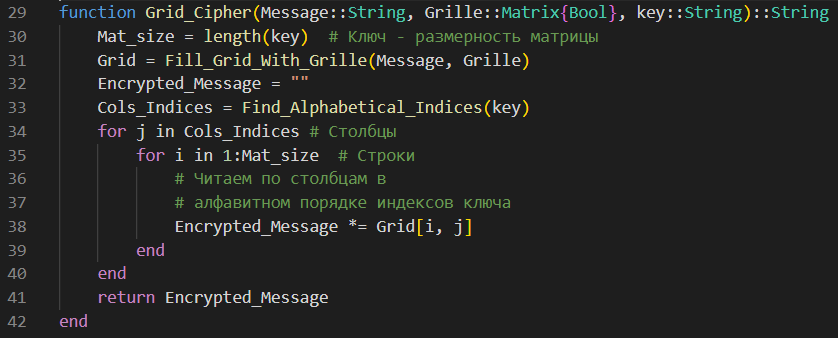
Результат кода реализации алгоритма маршрутного шифрования на Julia

## 3.2 Шифрование с помощью решеток

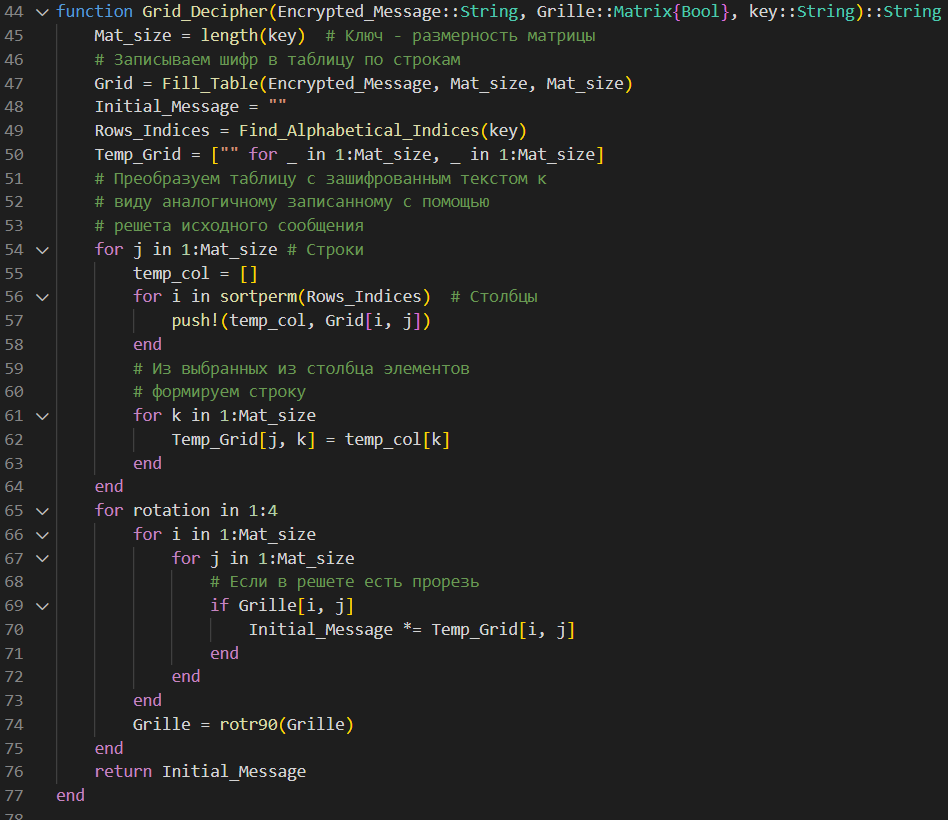
Реализуем алгоритм шифрования с помощью решёток и его расшифрование на Julia ([??-??]), в результате получим следующий вывод ([??]).



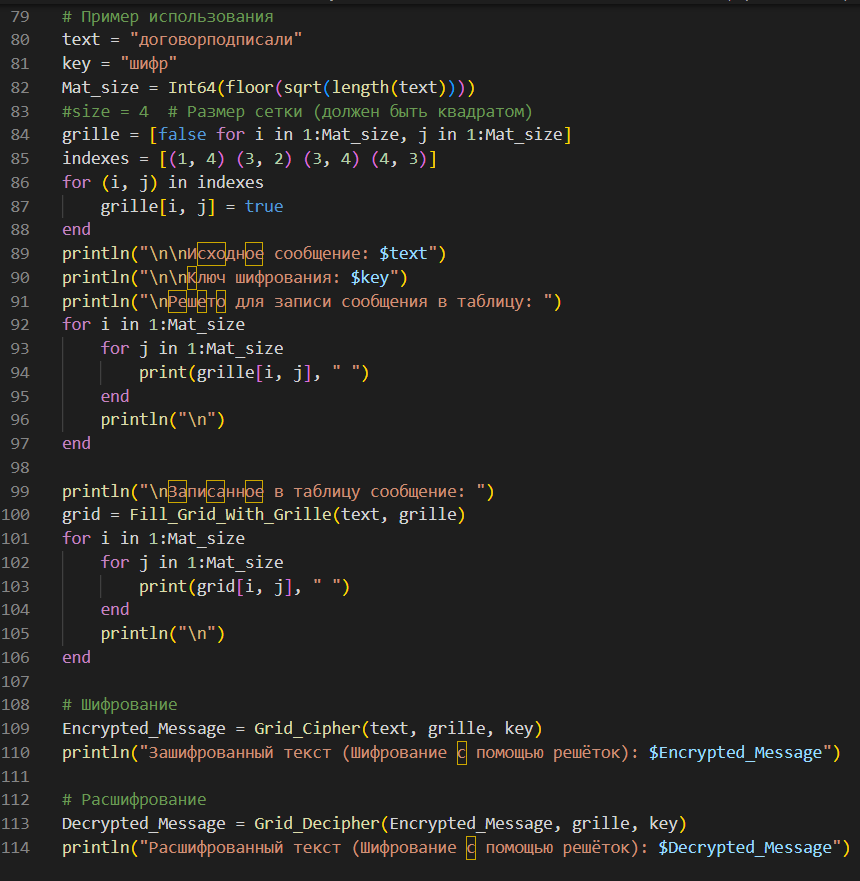
Код реализации алгоритма шифрования с помощью решёток на Julia (1/4)



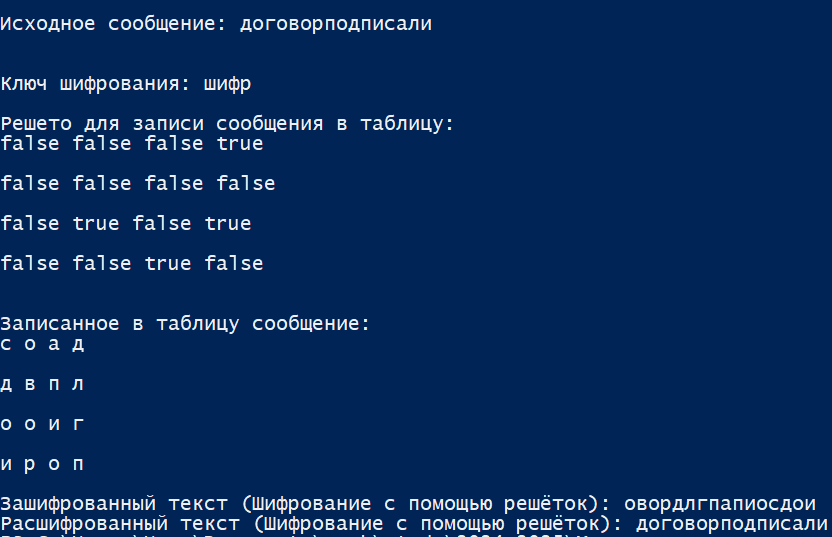
Код реализации алгоритма шифрования с помощью решёток на Julia (2/4)



Код реализации алгоритма шифрования с помощью решёток на Julia (3/4)



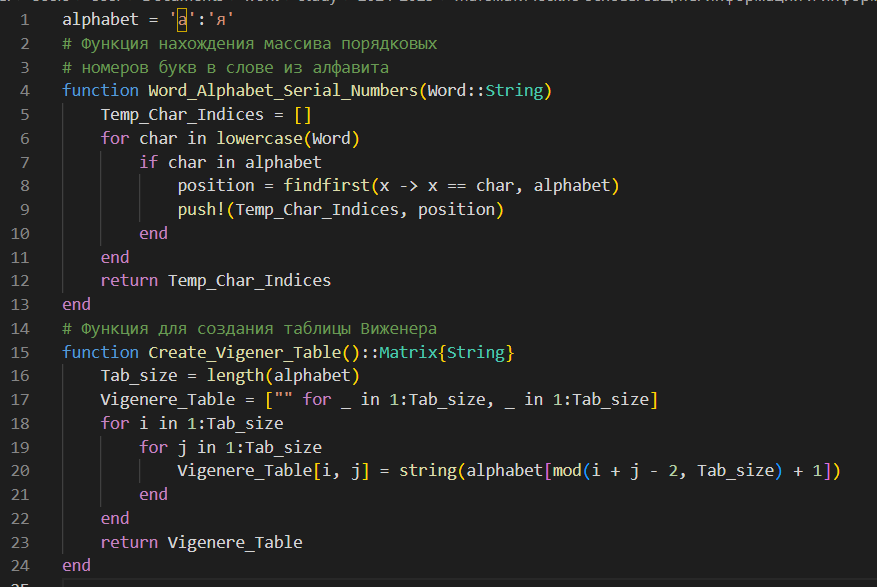
Код реализации алгоритма шифрования с помощью решёток на Julia (4/4)



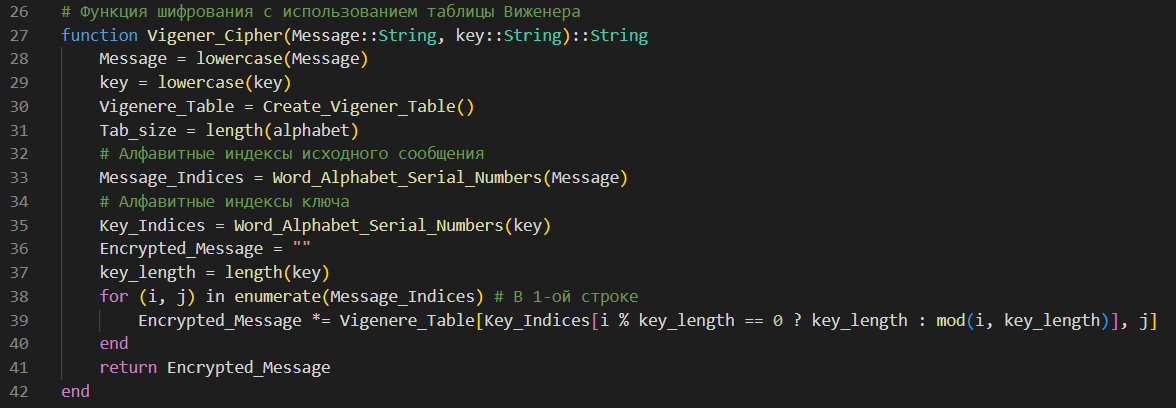
Результат кода реализации алгоритма шифрования с помощью решёток на Julia

## 3.3 Таблица Виженера

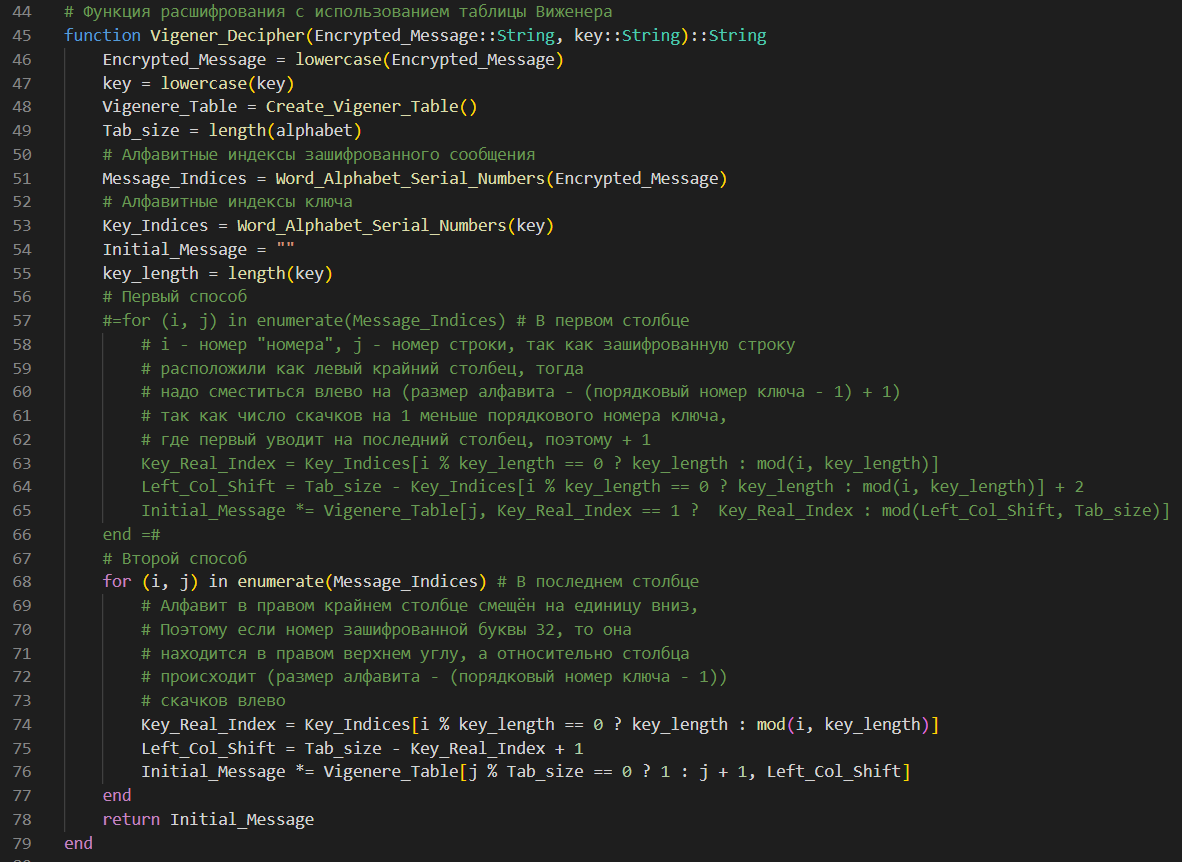
Реализуем алгоритм шифрования с помощью таблицы Вижинёра и его расшифрование на Julia ([??-??]), в результате получим следующий вывод ([??]).



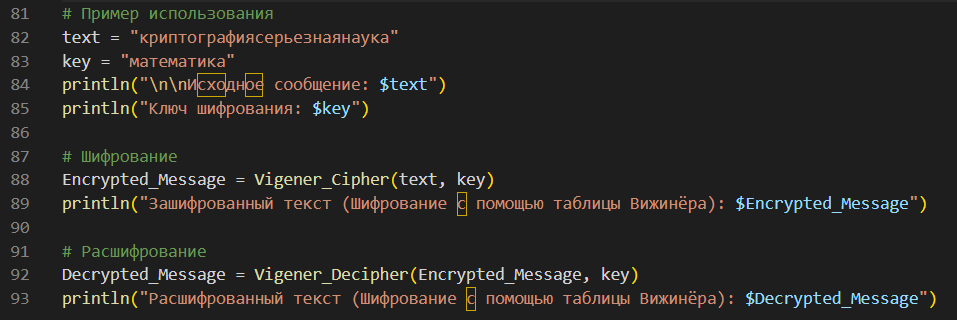
Код реализации алгоритма шифрования с помощью таблицы Вижинёра на Julia (1/4)



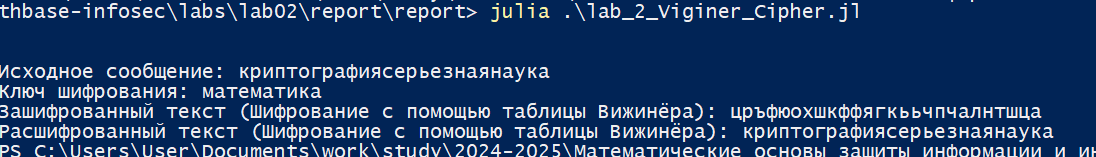
Код реализации алгоритма шифрования с помощью таблицы Вижинёра на Julia (2/4)



Код реализации алгоритма шифрования с помощью таблицы Вижинёра на Julia (3/4)



Код реализации алгоритма шифрования с помощью таблицы Вижинёра на Julia (4/4)



Результат кода реализации алгоритма шифрования с помощью таблицы Вижинёра на Julia

# 4 Выводы

В ходе выполнения лабораторной работы я изучил работу перестановочных шифров — маршрутного шифрования, шифрования с помощью решёток и таблицы Вижинёра, а также реализовать их программно на языке Julia.

# Список литературы

1. Лабораторная работа № 2. Шифры перестановки [Электронный ресурс]. Саратовский государственный университет имени Н.Г. Чернышевского, 2024.