# РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

### Факультет физико-математических и естественных наук

### Кафедра прикладной информатики и теории вероятностей

# ОТЧЕТ

# ПО ЛАБОРАТОРНОЙ РАБОТЕ № 2

### дисциплина: Математические основы защиты информации и информационной безопасности

### Студент: Пиняева Анна Андреевна

### Группа: НПИмд-01-24

### МОСКВА

### 2025

# Теоретическое введение

**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 шифртекст. Пусть m и n - целые положительные числа, большие 1. Открытый текст разбивается на блоки равной длины, состоящие из числа символов, равному произведению mn. Если последний блок получится меньше остальных, то в него следует дописать требуемое количество произвольных символов. Составляется таблица размерности mn. Блоки вписывается построчно в таблицу. Криптограмма получается выписыванием букв из таблицы в соответствии с некоторым маршрутом. Ключом такой криптограммы является маршрут и числа m и n . Обычно буквы выписывают по столбцам, которые упорядочивают согласно паролю: внизу таблицы приписывается слово из n неповторяющихся букв и столбцы нумеруются по алфавитному порядку букв пароля.

**Шифрование с помощью решеток**

Данный способ шифрования предложил австрийский криптограф Эдуард Флейснер в 1881 году. Суть этого способа заключается в следующем. Выбирается натуральное число k > 1, строится квадрат размерности k и построчно заполняется числами 1,2,…,k^2.

Важно отметить, что число k подбирается в соответствии с количеством букв N исходного теста. В идеальном случае k^2 = N. Если такого равенства достичь невозможно, то можно либо дописать произвольную букву k последнему слову открытого текста, либо убрать ее.

**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 n. Ключ представляет собой последовательность из n натуральных чисел: а1, а2,…, аn. Далее в каждом блоке первая буква циклически сдвигается вправо по алфавиту на а1 позиций, вторая буква - на а2 позиций, последняя - на аn, позиций. Для лучшего запоминания в качестве ключа можно взять осмысленное слово, а алфавитные номера входящих в него букв использовать для осуществления сдвигов. ———–

# Цель работы

Изучение и реализация маршрутного шифрования, шифрования с помощью решеток и таблицы Виженера.

# Ход работы

1. Маршрутное шифрование.

Алгоритм:

* Удаление пробелов и приведение к верхнему регистру.
* Разбиение на блоки длиной пароля.
* Создание таблицы m\*n.
* Сортировка столбцов по алфавитному порядку пароля.
* Чтение по стобцам в новом порядке.

Код реализации представлен на рис.1, тестирование - рис.2.

*Рис. 1 Реализация маршрутного шифрования:*



*Рис. 2 Тестирование маршрутного шифрования:*



1. Шифрование с помощью решеток.

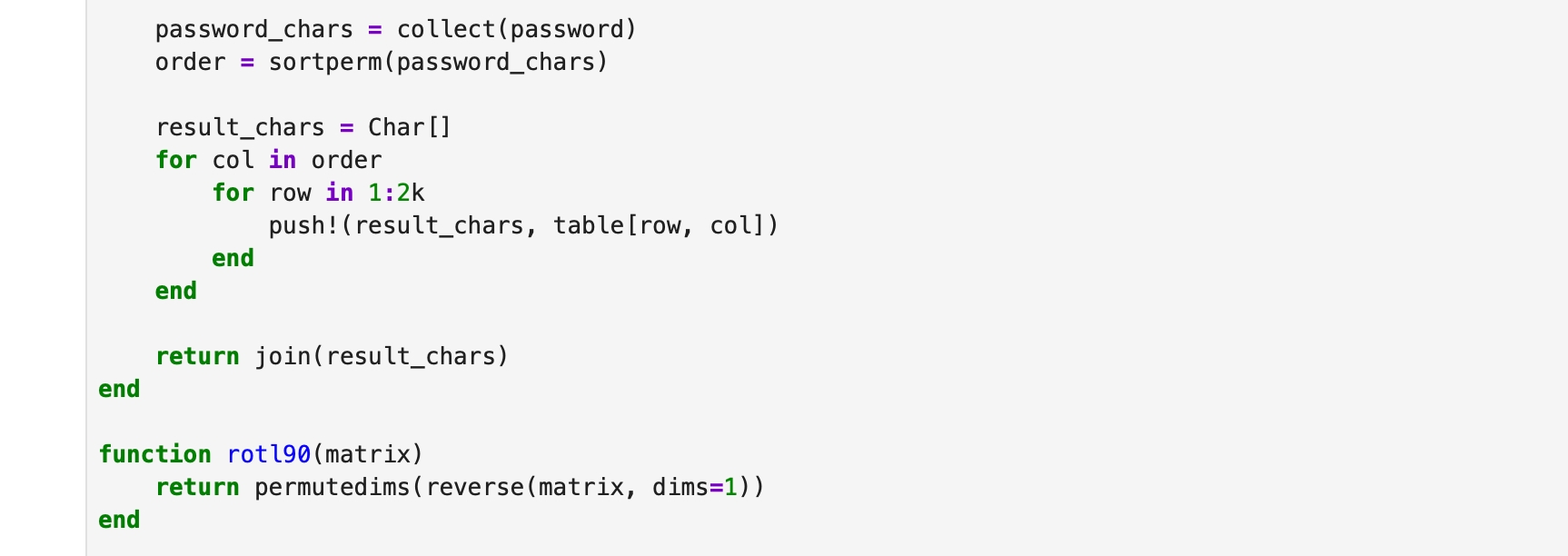
Алгоритм:

* Удаление пробелов и приведение к верхнему регистру.
* Дополнить количество символов при необходимости.
* Создание решетки 2k\*2k с последовательной нумерацией.
* Определение отверстий.
* Для каждого поаворота решетки на 90: -записать символы текста в отверстия; -повернуть решетку.
* Прочитать заполненную таблицу по столбцан согласно паролю.

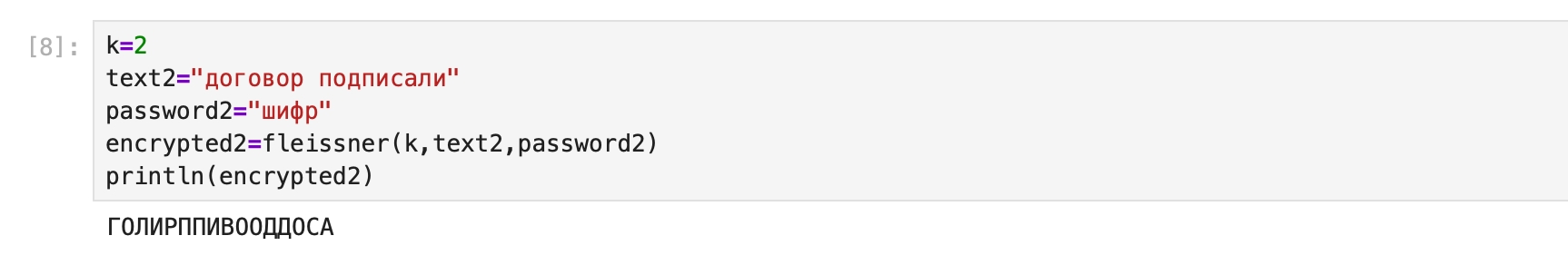
Код реализации представлен на рис.3, тестирование - рис.4.

*Рис. 3 Реализация шифрования с помощью решеток:*





*Рис. 4 Тестирование шифрования с помощью решеток:*



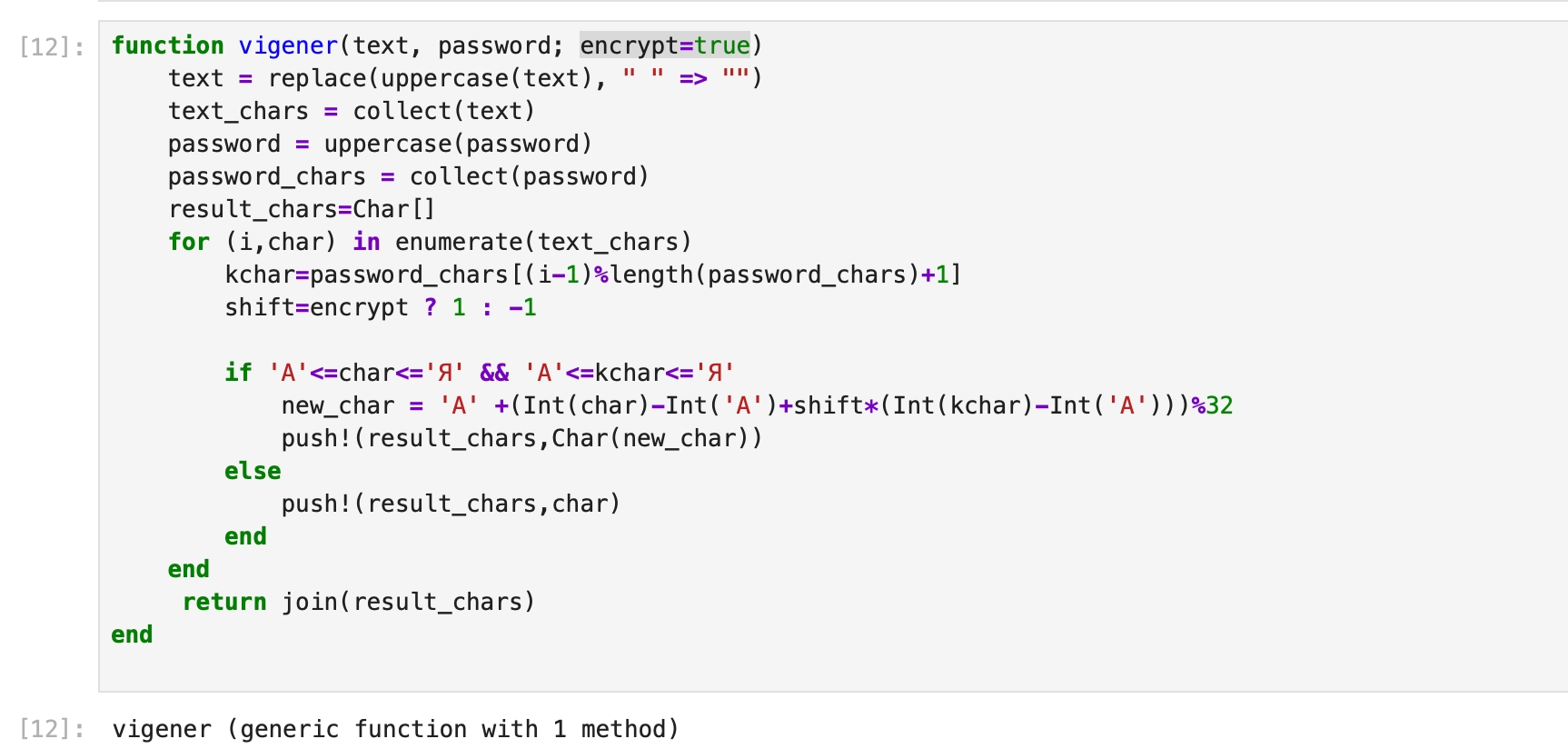
1. Таблица Виженера.

Алгоритм:

* Удаление пробелов и приведение к верхнему регистру.
* Для каждого символа текста: -взять соответствующий символ ключа; - вычислить сдвиг; - применить модуль 32; -получить новый символ.

Код реализации представлен на рис.5, тестирование - рис.6.

*Рис. 5 Реализация таблицы Виженера:*



*Рис. 6 Тестирование таблицы Виженера:*



Вывод: В ходе данной работы мной были изучены и реализованы методы маршрутного шифрования, шифрования с помощью решеток и таблицы Виженера. Написан программный код на языке Julia и протестирован.