Отчёт по лабораторной работе №2  
Математические основы защиты информации и информационной безопасности

Шифры перестановки

Выполнил: Махорин Иван Сергеевич,  
НФИмд-02-21, 1032259380

Содержание

# 1 Цель работы

Изучить шифры перестановки и научиться их реализовывать.

# 2 Выполнение лабораторной работы

## 2.1 Реализация маршрутного шифрования

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.

Выполним реализацию этого шифрования на языке Julia (рис. 1) и (рис. 2):

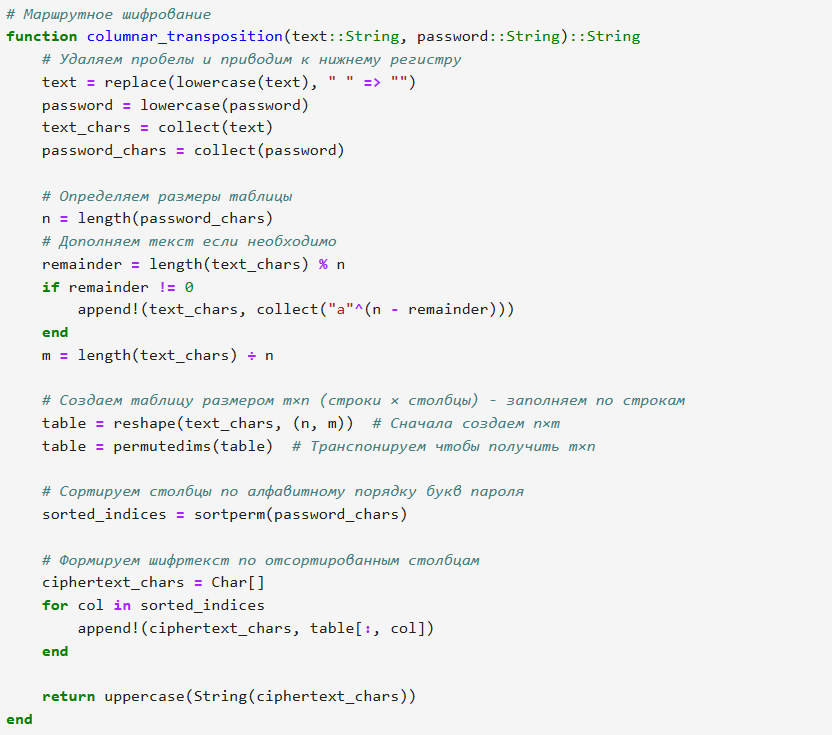


Рис. 1: Реализация маршрутного шифрования

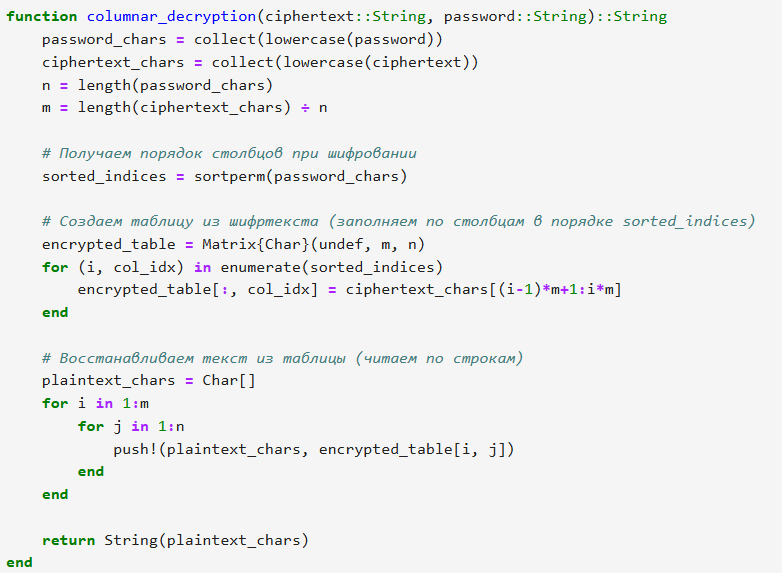


Рис. 2: Реализация маршрутного шифрования

Проверим работу маршрутного шифрования (рис. 3):

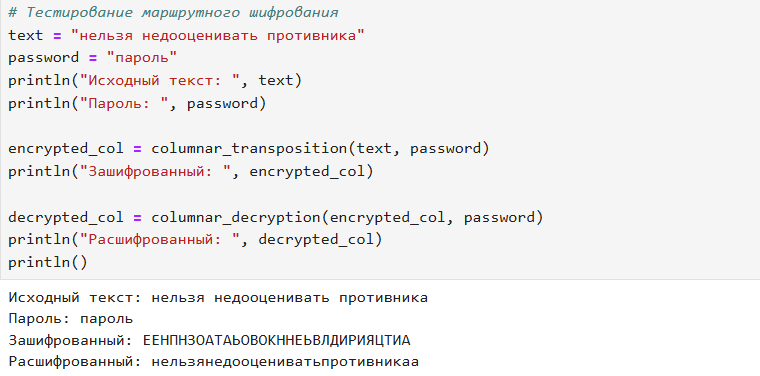


Рис. 3: Проверка

## 2.2 Реализация шифрования 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 и построчно заполняется числами .

Выполним реализацию этого шифрования на языке Julia (рис. 4 - рис. 6):

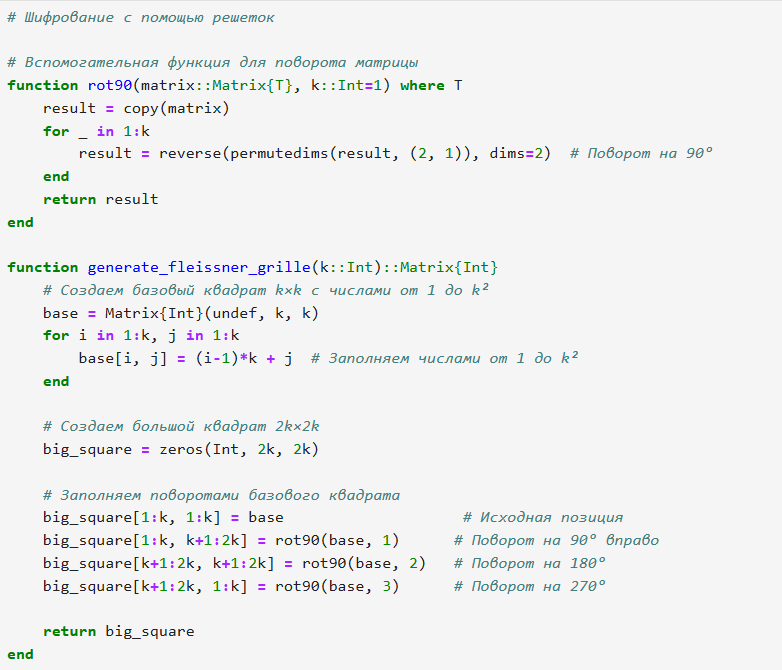


Рис. 4: Реализация шифрования с помощью решеток



Рис. 5: Реализация шифрования с помощью решеток

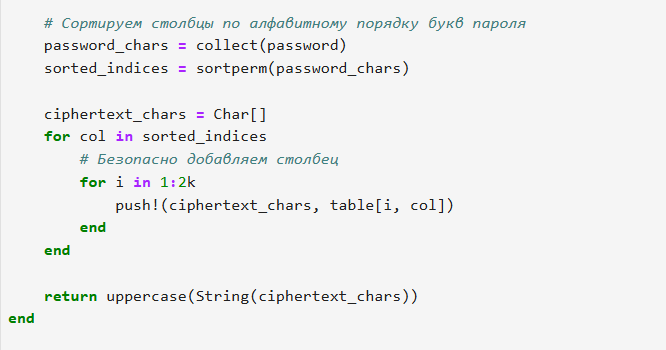


Рис. 6: Реализация шифрования с помощью решеток

Проверим работу шифрования с помощью решеток (рис. 7):

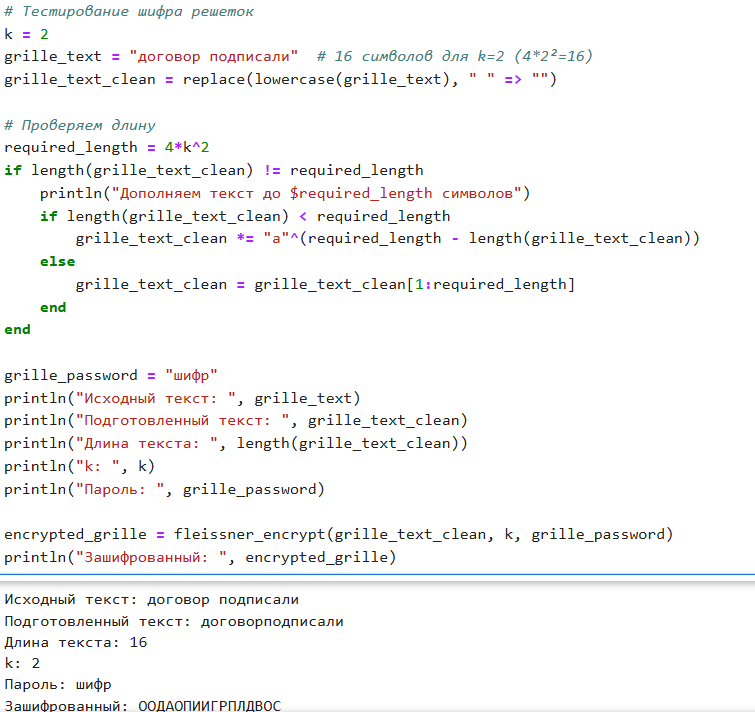


Рис. 7: Проверка

## 2.3 Реализация таблицы 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.

Выполним реализацию этого шифрования на языке Julia (рис. 8) и (рис. 9):

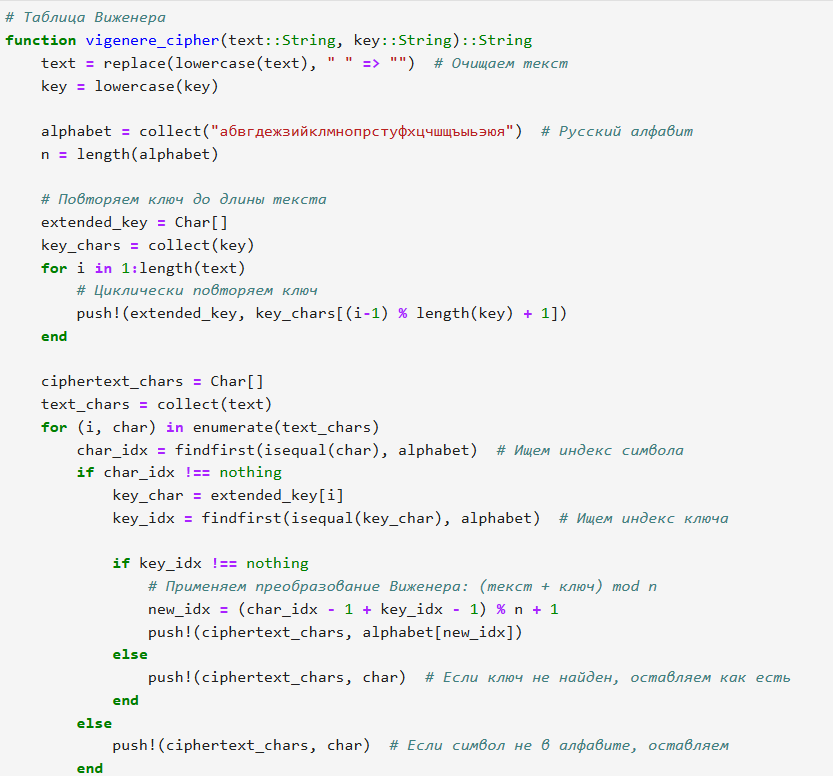


Рис. 8: Реализация таблицы Виженера

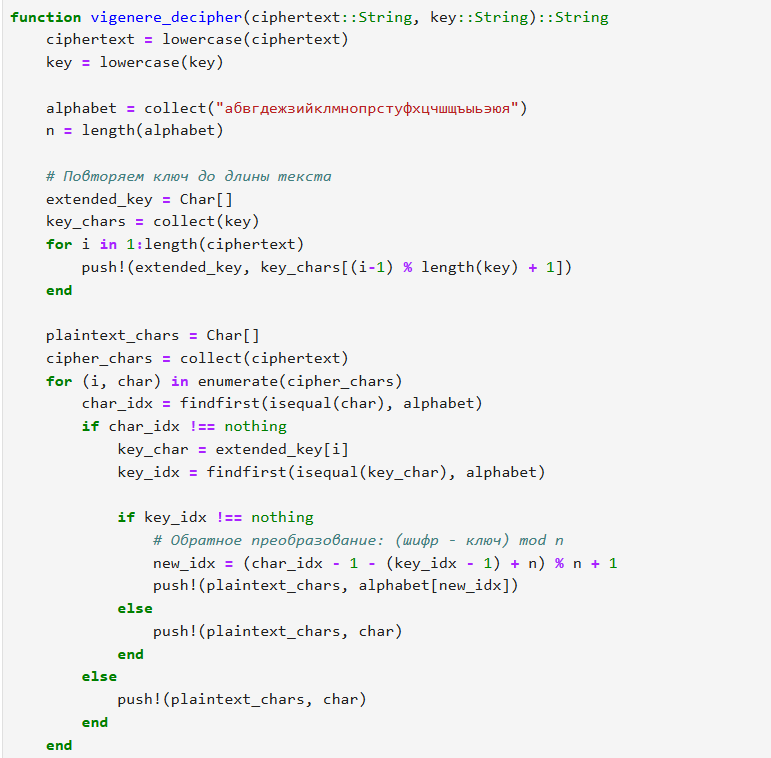


Рис. 9: Реализация таблицы Виженера

Проверим работу таблицы Виженера (рис. 10):

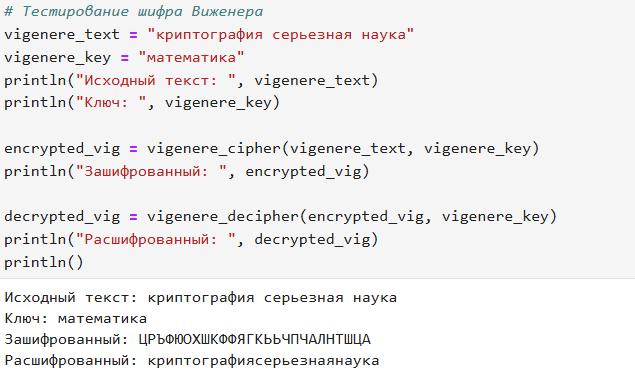


Рис. 10: Проверка

# 3 Список литературы. Библиография

[1] Julia: https://docs.julialang.org/en/v1/