Лабораторна работа №2

Шифры перестановки

Покрас Илья Михайлович

Содержание

# 1 Цель работы

Ознакомиться с шифрами перестановки и реализовать программный код маршрутного шифрования, шифрования решеток и шифрования Виженера.

# 2 Задание

* Создать алгоритм маршрутного шифрования
* Создать алгоритм шифрования с помощью решеток
* Создать алгоритм шифрования Виженера

# 3 Теоретическое введение

* Маршрутное шифрование - это метод шифрования, при котором символы сообщения переставляются или перестраиваются в соответствии с определенным правилом. Каждый символ сообщения заменяется другим символом или перемещается на определенное количество позиций в алфавите.
* Шифрование с помощью решеток - это метод шифрования, при котором сообщение записывается в ячейки решетки, а затем символы выбираются в определенном порядке для формирования зашифрованного текста. Расшифровка происходит путем восстановления исходного текста из решетки.
* Шифрование Виженера - это метод шифрования, основанный на использовании повторяющегося ключа. Каждая буква ключа соответствует определенной букве алфавита, и при шифровании каждая буква сообщения сдвигается на соответствующее значение ключа. Для расшифровки используется обратная операция сдвига.

# 4 Выполнение лабораторной работы

## 4.1 Маршрутное шифрования

Я создал функцию маршрутного шифрования с входными данными: исходным текстом, ключом шифрования и параметрами матрицы - количество строк и столбцов. Данная функция возвращает зашифрованный текст (рис. 1).

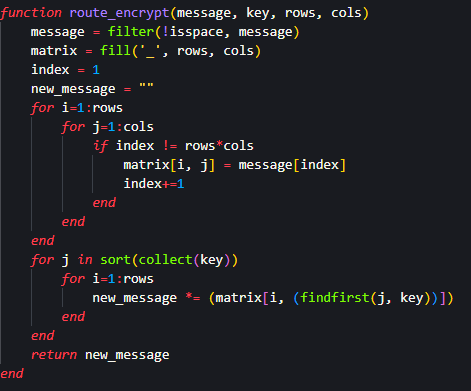


Рис. 1: Функция маршутного шифровани

Далее я инициализировал переменные, которые содержат исходный текст, ключ шифрования и данные матрицы(строки, столбцы), после чего использовал эти данные в вызове функции маршутного шифрования. (рис. 2).

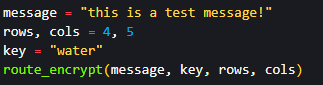


Рис. 2: Инициализация переменных и вызов функций 1

И получил следующий результат (рис. 3).

Результат программного кода 1

Рис. 3: Результат программного кода 1

## 4.2 Шифрование с помощью решеток

Я создал функцию шифрования с помощью решеток принимающую исходный текст, натуральное число k и ключ шифрования, которая создает матрицу c элементами, принимающие значения от 1 до k^2. Далее c помощью циклов я заменил эти числовые значения на символы, содержащиеся в сообщении(кроме пробелов - они удаляются). Далее с помощью ключа я составил новый зашифрованный текст, заменяя те числовые значения, которые остались, на пробелы (рис. 4).

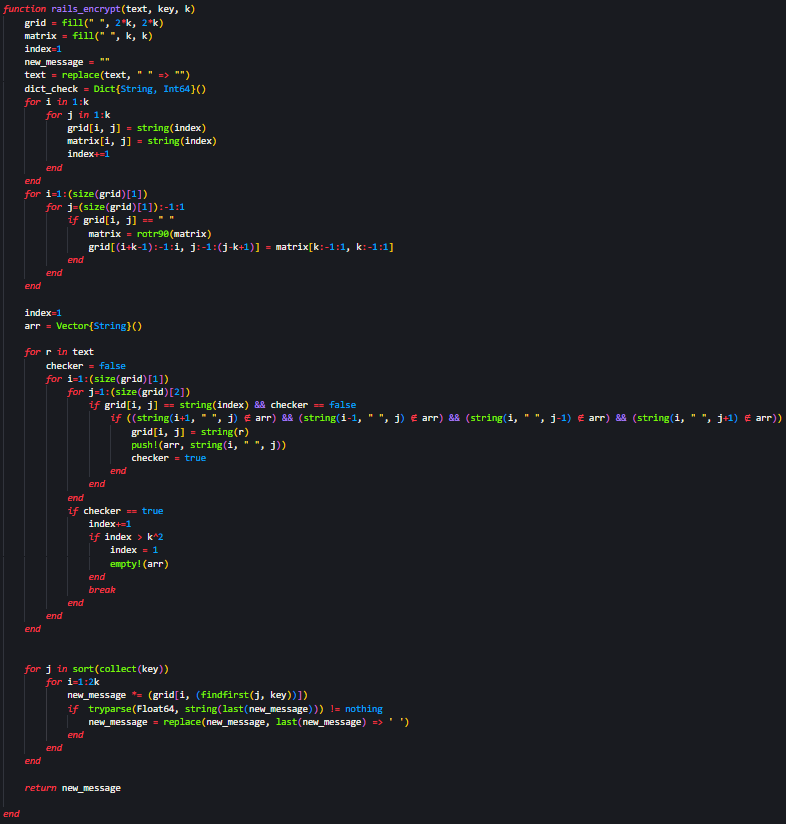


Рис. 4: Функция шифровани с помощью решеток

Далее я инициализировал переменные, которые содержат исходный текст, натуральное число и ключ шифрования, после чего использовал эти данные в вызове функции шифрования решеток. (рис. 5).

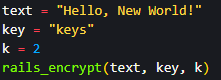


Рис. 5: Инициализация переменных и вызов функций 2

И получил следующий результат (рис. 6).

Результат программного кода 2

Рис. 6: Результат программного кода 2

## 4.3 Шифрование Виженера

Я создал функцию шифрования Виженера, которая принимает текст и ключ шифрования, и возвращает зашифрованный текст (рис. 7).



Рис. 7: Функция шифровани Виженера

Далее я инициализировал переменные, которые содержат исходный текст, ключ шифрования, после чего использовал эти данные в вызове функции шифрования Виженера. (рис. 8).

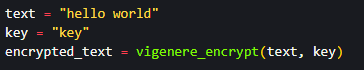


Рис. 8: Инициализация переменных и вызов функций 3

И получил следующий результат (рис. 9).

Результат программного кода 3

Рис. 9: Результат программного кода 3

# 5 Выводы

Я ознакомился с шифрами перестановки и реализовал программный код маршрутного шифрования, шифрования решеток и шифрования Виженера.

# Список Литературы

1. [Julia - Control Flow](https://docs.julialang.org/en/v1/manual/control-flow/)
2. [Julia - Mathematical Operations](https://docs.julialang.org/en/v1/manual/mathematical-operations/)
3. [Julia - Strings](https://docs.julialang.org/en/v1/manual/strings/)
4. [Julia - Arrays](https://docs.julialang.org/en/v1/base/arrays/)
5. [Julia - Collections and Data Structures](https://docs.julialang.org/en/v1/base/collections/)