Лабораторная работа 2

Попов Дмитрий Павлович, НФИмд-01-23

Содержание

РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук

Кафедра математического моделирования и искусственного интеллекта

ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №2

дисциплина: Математические основы защиты информации и информационной безопасности

Преподователь: Кулябов Дмитрий Сергеевич

Студент: Попов Дмитрий Павлович

Группа: НФИмд-01-23

МОСКВА

2023 г.

# 1 Цель работы

Целью данной работы является приобретение практических навыков в шифрах перестановки.[1]

# 2 Выполнение лабораторной работы

Требуется реализовать:

1. Маршрутное шифрование.
2. Шифрование с помощью решеток.
3. Таблица Виженера

## 2.1 Маршрутное шифрование

Текст разбивается на равные блоки N длиной M. Если в конце не хватает букв, то они добавляются в конец. Блоки записываются построчно в таблицу. Затем буквы выписываются по столбцам, которые упорядываются согласно паролю: внизу таблицы приписывается слово из n неповторяющихся букв и столбы нумеруются по алфавитному порядку букв пароля

Чтобы реализовать программу был написал код на Python(fig. 1)(fig. 2):

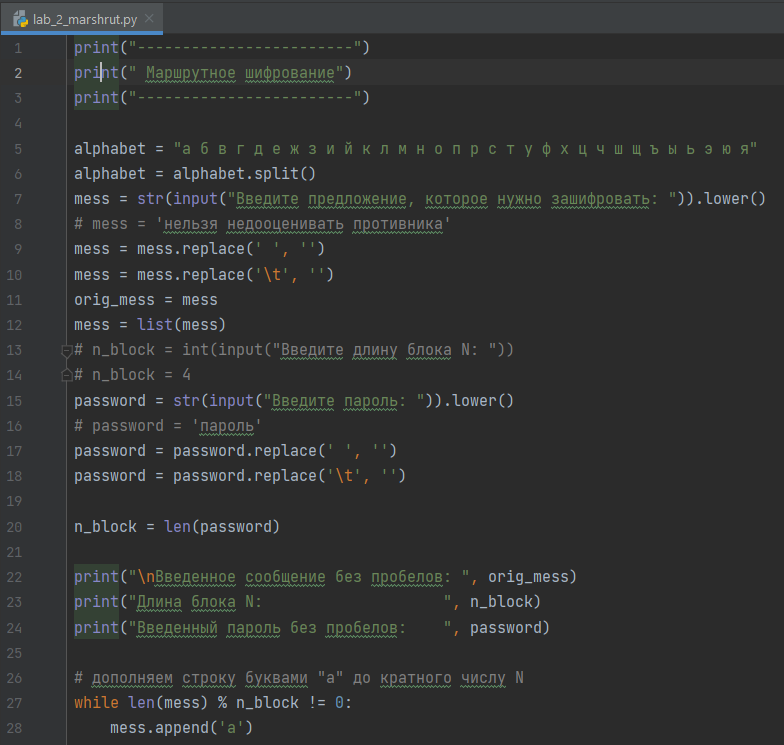


Figure 1: route1

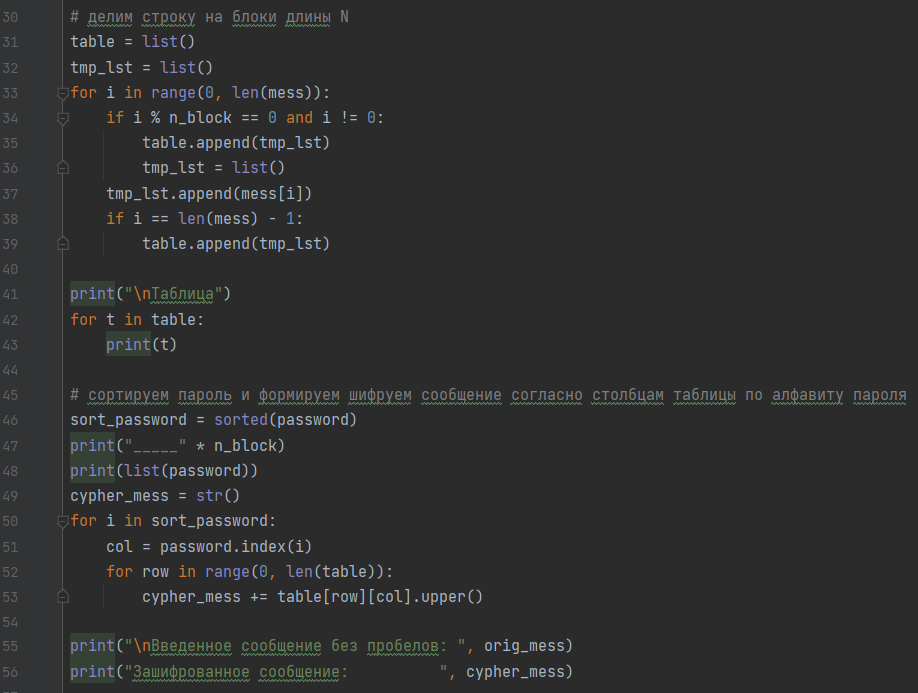


Figure 2: route2

Затем я запустил программу, ввел пароль и исходное сообщение. Получил таблицу шифрования, далее получил зашифрованное сообщение. Вывод работы программы (fig. 3)

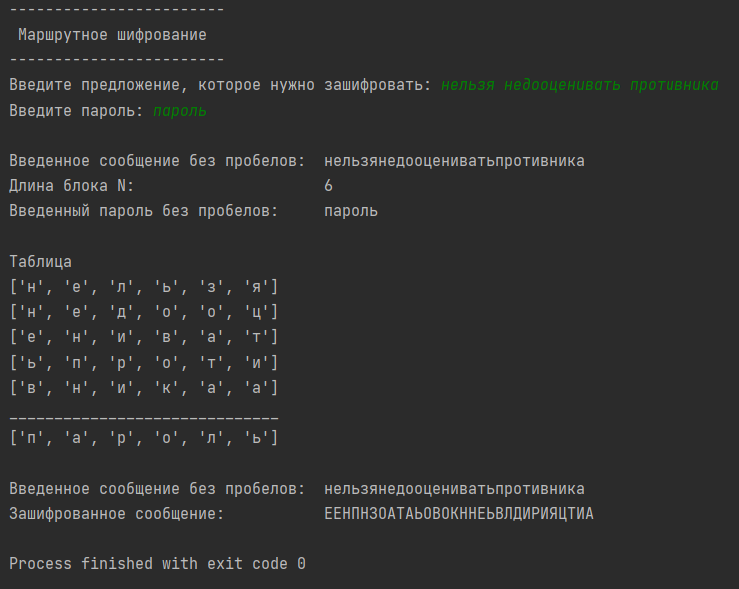


Figure 3: route\_out

## 2.2 Шифрование с помощью решеток

Строится квадрат из k чисел. Затем к нему добавляются еще 3 квадрата, которые поворачиваются на 90 градусов и получается большой квадрат 2k размерностью. Дальше из большого квадрата вырезаются клетки и прорези записываются буквы. Когда заполнятся все прорези решето поворачивается на 90 градусов. И так продолжается пока не заполнится вся таблица. И буквы выписываются по алфивитному порядку пароля.

Чтобы реализовать программу был написал код на Python(fig. 4)(fig. 5)(fig. 6):

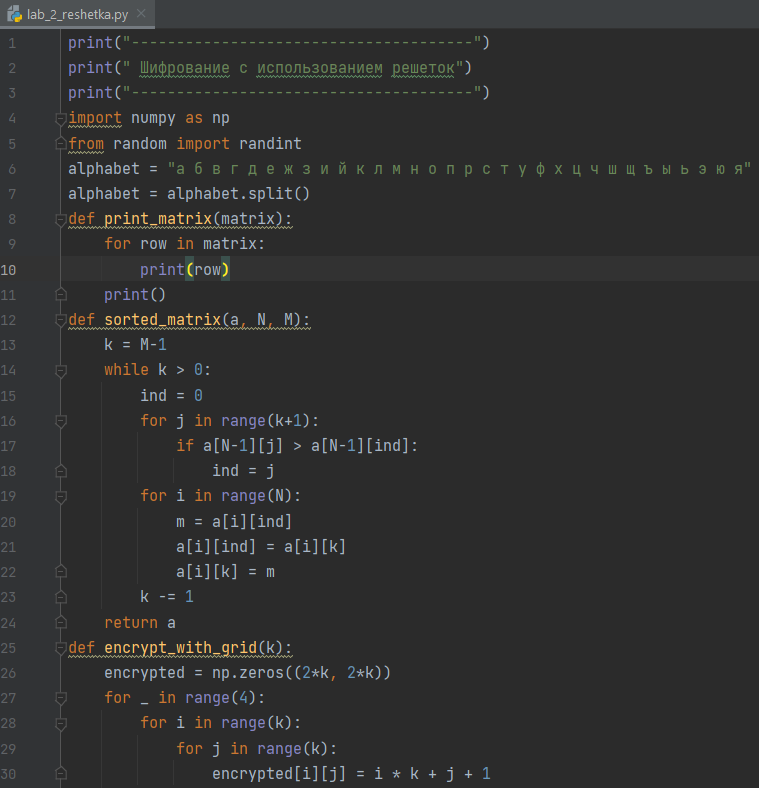


Figure 4: grid1



Figure 5: grid2

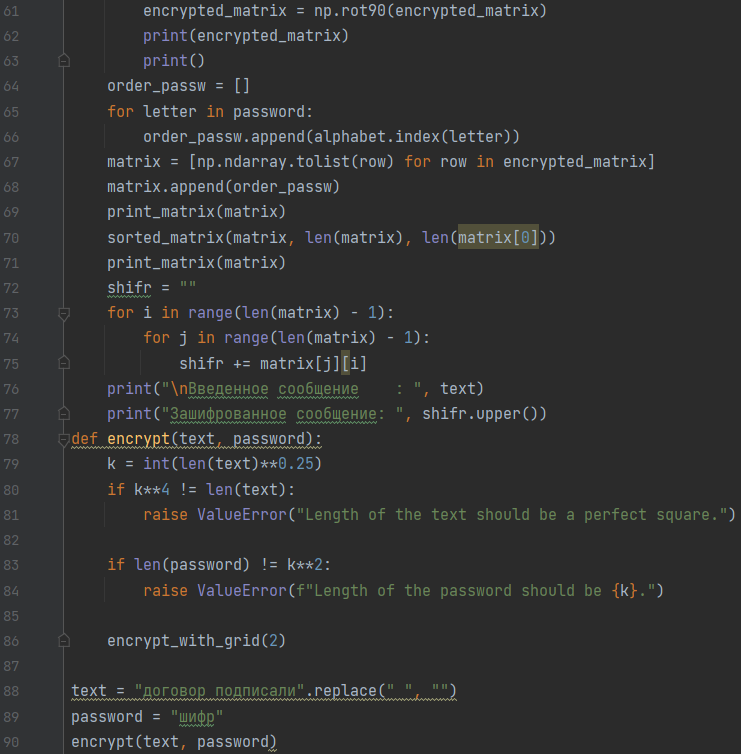


Figure 6: grid3

Затем я запустил программу. Получил матрицы шифрования, далее получил зашифрованное сообщение. Вывод работы программы (fig. 7)(fig. 8)(fig. 9)

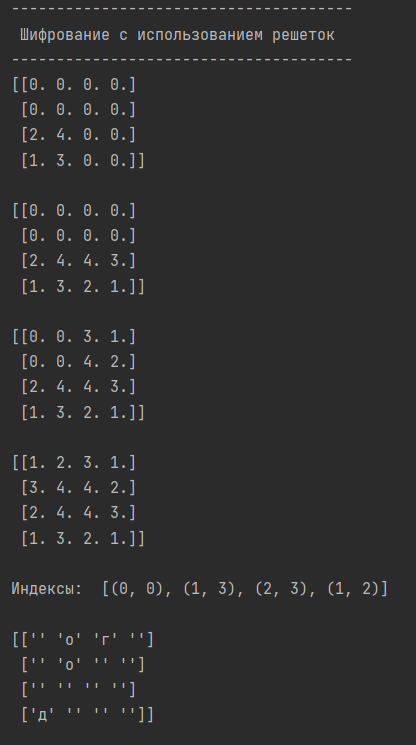


Figure 7: grid\_out1

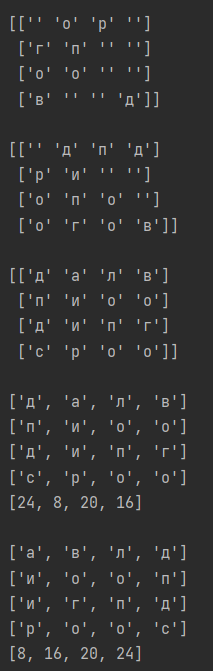


Figure 8: grid\_out2

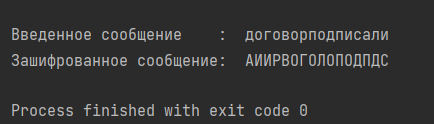


Figure 9: grid\_out3

## 2.3 Таблица Виженера

В таблице записаны буквы русского алфавита. При переходе от одной строке к другой происходит циклический сдвиг на одну позицию. Пароль записывается с повторениями над буквами сообщения. В горизонтальном алфавите ищем букву нашего текста, а в вертикальном букву пароля и на их пересечении будет нужная нам буква.

Чтобы реализовать программу был написал код на Python(fig. 10)(fig. 11):

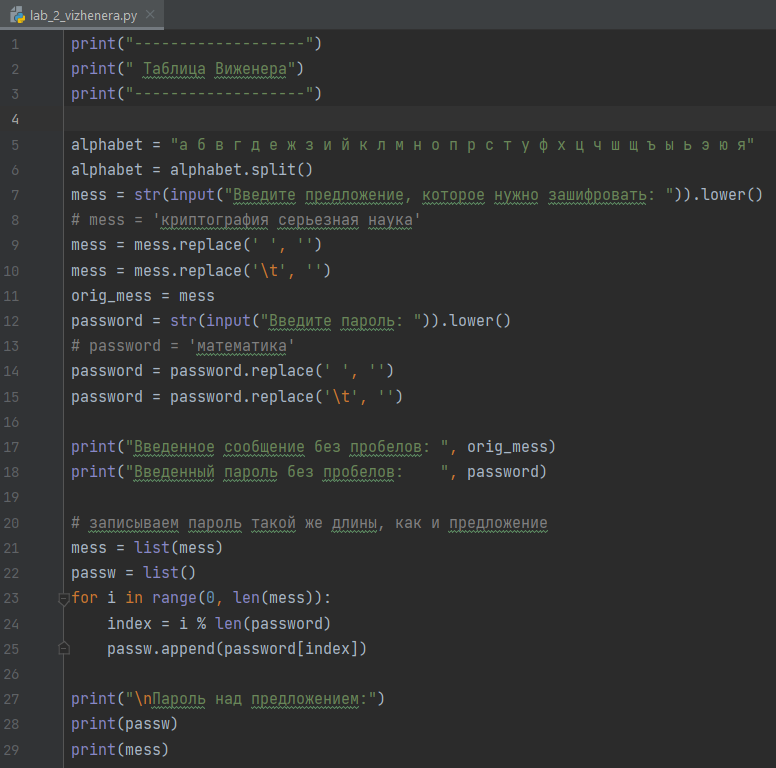


Figure 10: viginere1

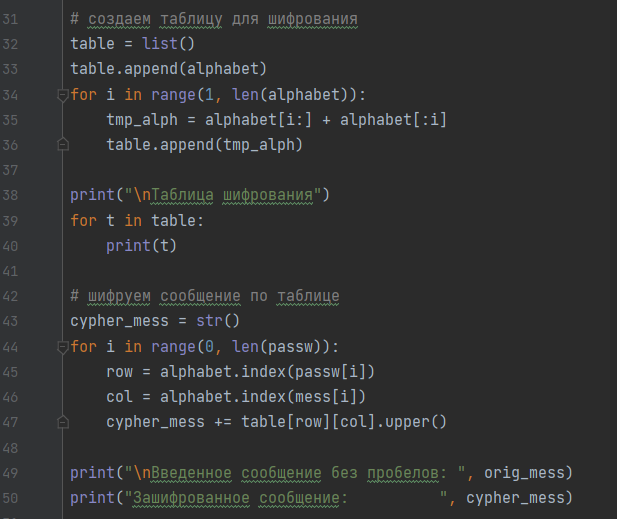


Figure 11: viginere2

Затем я запустил программу, ввел пароль и исходное сообщение. Получил пароль над предложением, таблицу шифрования (алфавит), далее получил зашифрованное сообщение. Вывод работы программы (fig. 12)(fig. 13)(fig. 14)

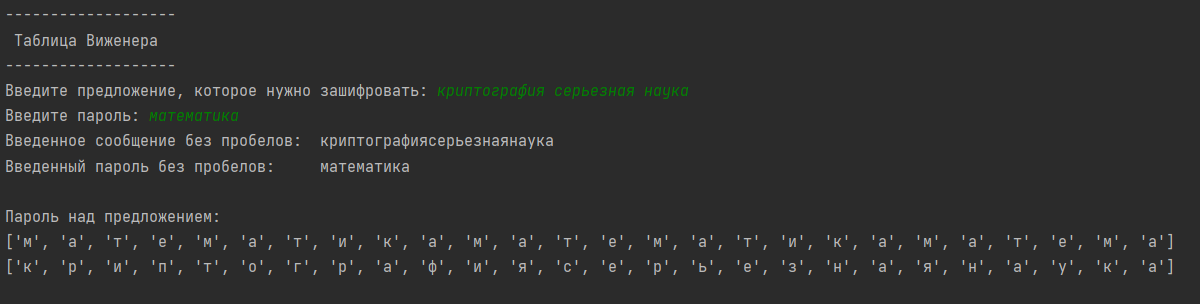


Figure 12: viginere\_out1



Figure 13: viginere\_out2

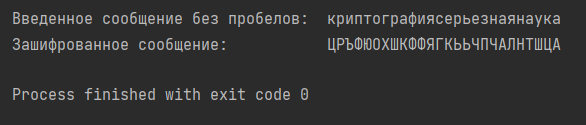


Figure 14: viginere\_out3

# 3 Выводы

В результате выполнения работы я освоил на практике применение шифров перестановки.

# 4 Список литературы

1. Методические материалы курса