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

Шифры перестановки

Попова Юлия Дмитриевна

Содержание

# Цель работы

Освоить на практике шифры перестановки.

# Выполнение лабораторной работы

Требуется реализовать:

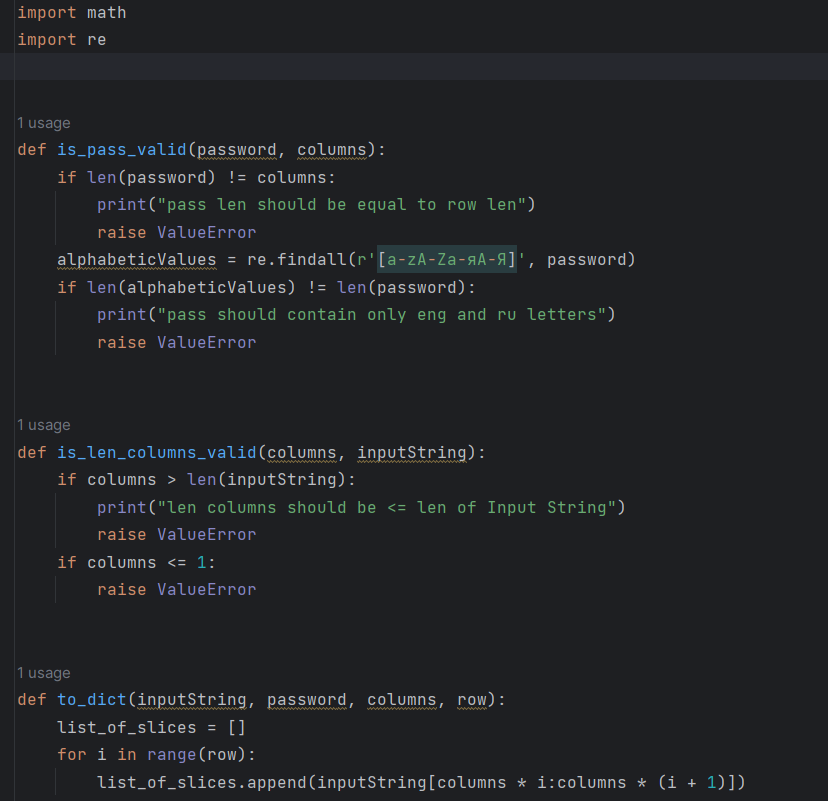
1. Маршрутное шифрование.
2. Шифрование с помощью решеток.
3. Табоица Виженера

## Маршрутное шифрование

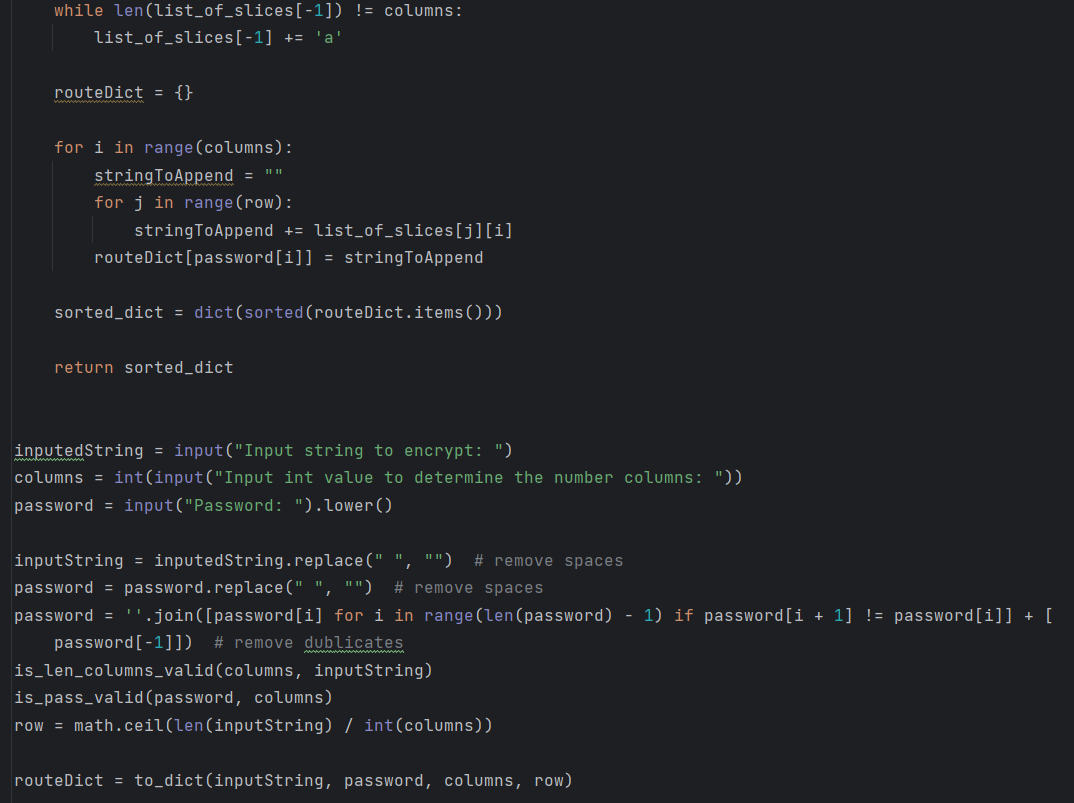
Текст разбивается на равные блоки N длиной M. Если в конце не хватает букв, то они добавляются в конец. Блоки записываются построчно в таблицу. Затем буквы выписываются по столбцам, которые упорядываются согласно паролю: внизу таблицы приписывается слово из n неповторяющихся букв и столбы нумеруются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

Чтобы реализовать программу был написан код на python:

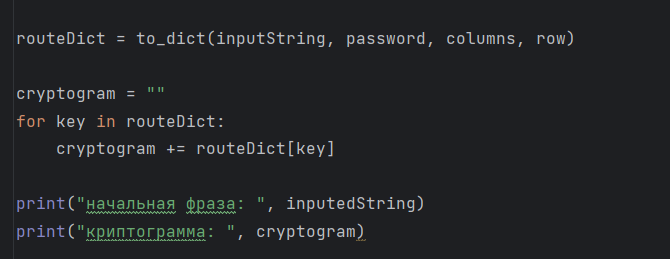
1. Функции заполнения матрицы текстом
2. Функция, шифрующая матрицу



route\_funcs

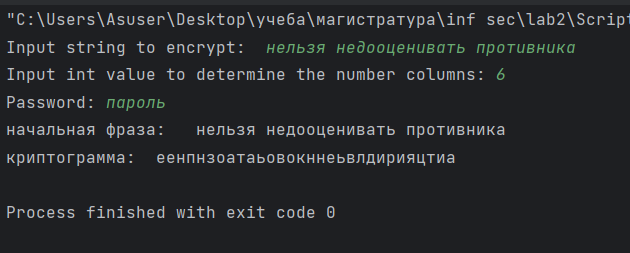


route\_funcs2



route\_funcs3

Вывод программы (пример как в методических материалах).



route\_output

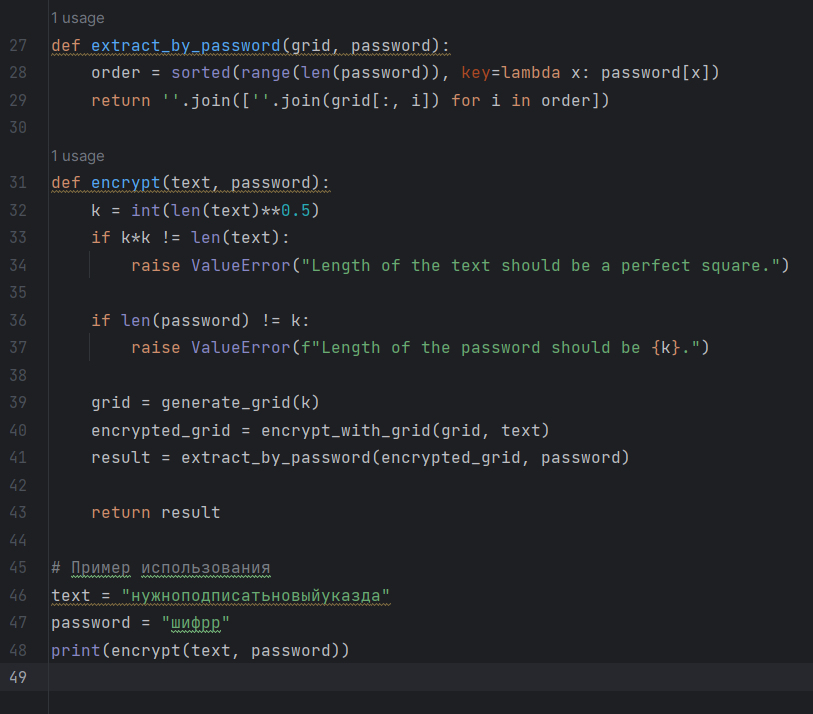
## Шифрование с помощью решеток

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:

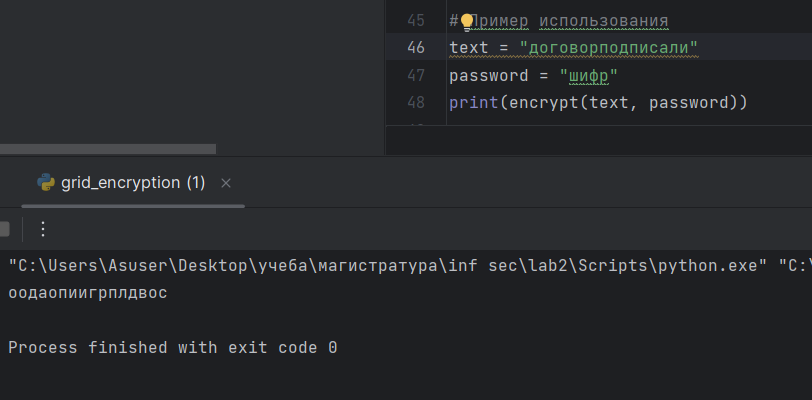


grid\_funcs\_1



grid\_funcs\_2

Пример работы программы

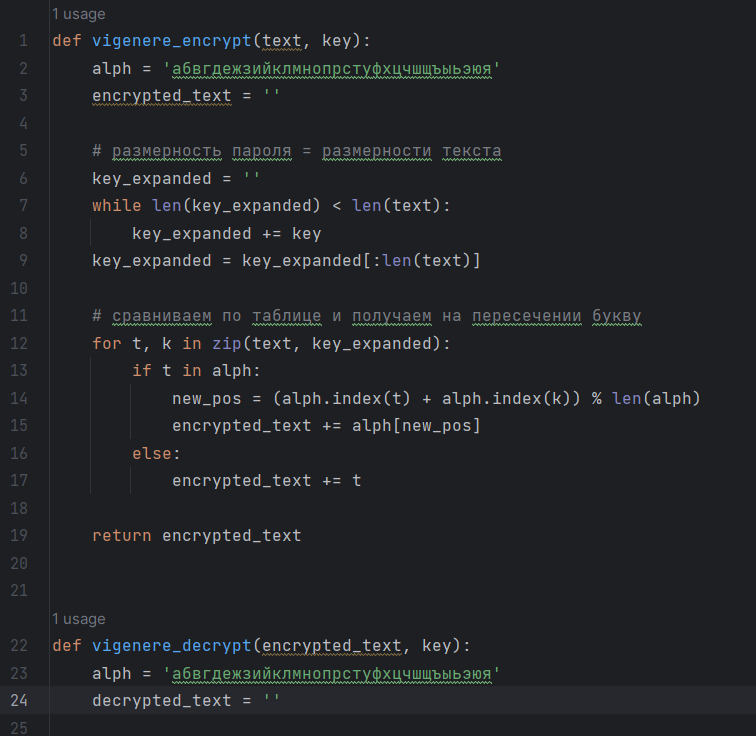


grid\_output

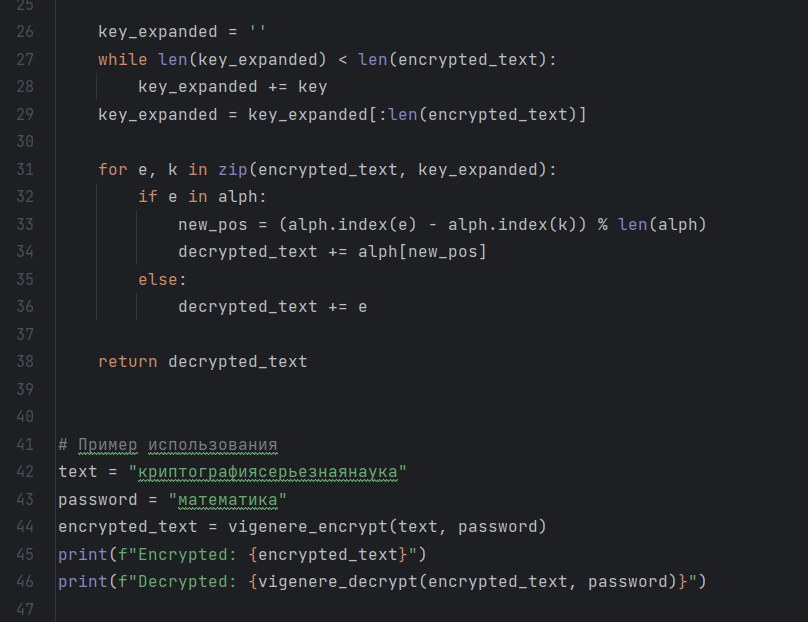
## Таблица Виженера

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 буква.

Чтобы реализовать программу был написал след. код на python:

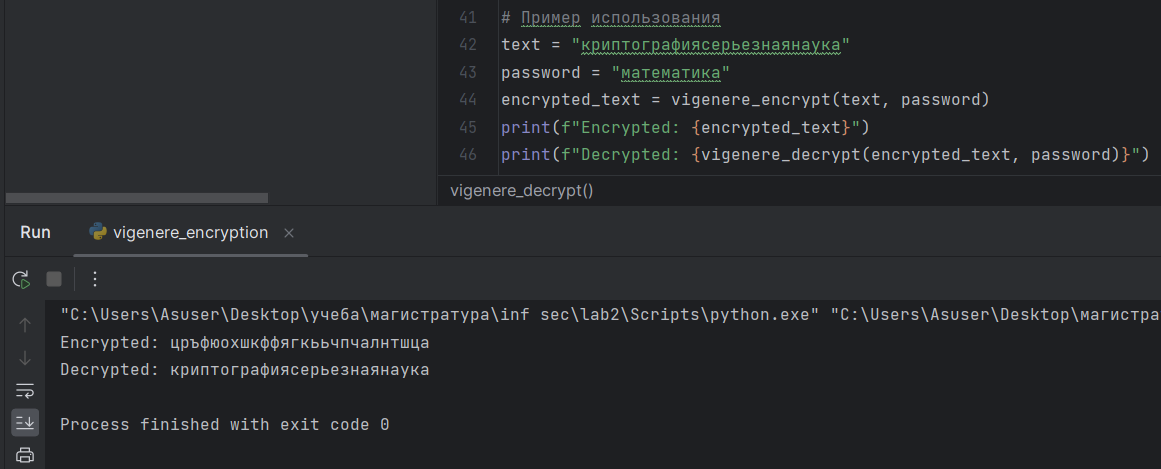


viginere\_funcs



viginere\_funcs2

Пример работы программы (как в методических материалах)



viginere\_output

# Выводы

В результате выполнения работы освоили на практике применение шифров перестановки.

# Список литературы

1. Методические материалы курса