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

Шифры перестановки

Терентьев Егор Дмитриевич 1132236902

Содержание

# 1 Цель работы

Освоить на практике шифры перестановки.

# 2 Выполнение лабораторной работы

Требуется реализовать:

1. Маршрутное шифрование.
2. Шифрование с помощью решеток.
3. Табоица 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 след. код на python:

1. Функции проверки правильности пароля, значения k
2. Функция берущая столбцы матрицы в виде ключа буквы пароля в алфавитном порядке (был использован словарь для удобства) fig. 1.

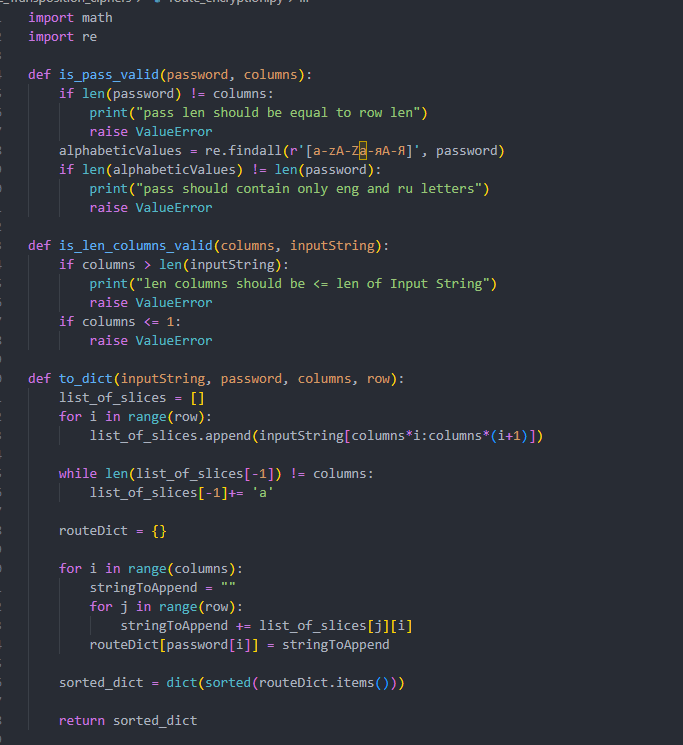


Figure 1: route\_funcs

Main функция в которой вводятся начальные значения, запускаются вышепоказанные функции fig. 2.

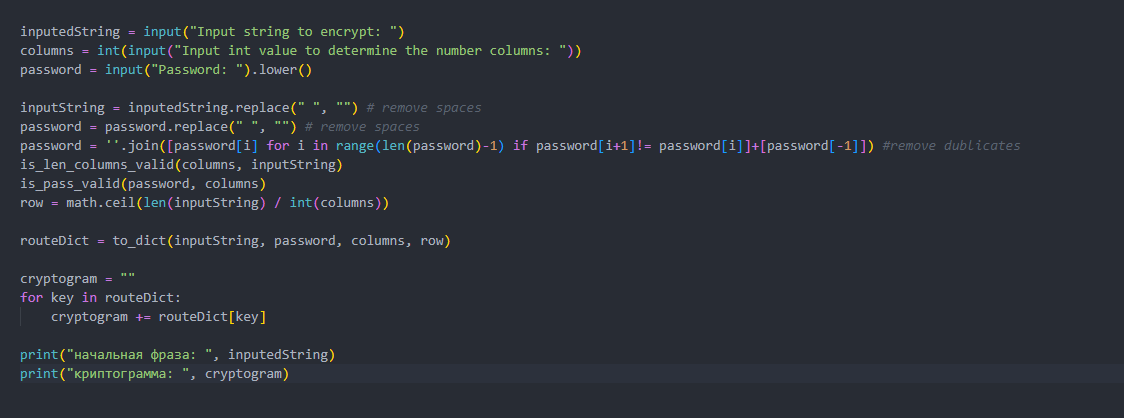


Figure 2: route\_main\_func

Вывод программы (пример как в методических материалах) fig. 3.

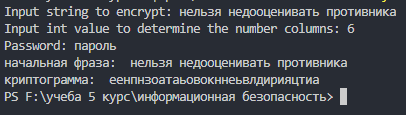


Figure 3: route\_output

## 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 след. код на python:

1. Функция генерирующая сетку (матрицу) (использована библиотека numpy Для удобства) и ее заполнение
2. Функция заполняющая сетку значениями букв из текста и переворачивающая матрицу
3. Функция выбираюшая столбцы в алфавитном порядке пароля
4. Функция объединяющая все вышепоказанные функции и проверки правильности введенных данных fig. 4

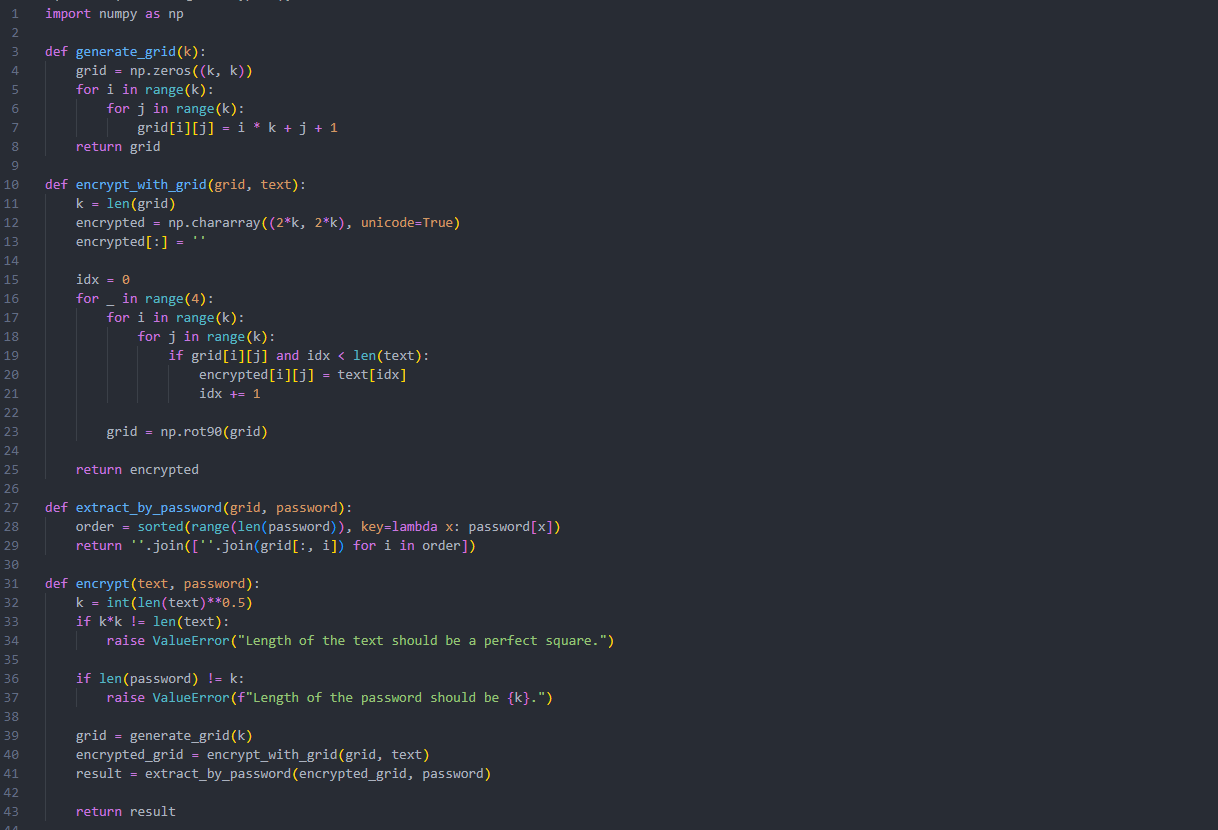


Figure 4: grid\_funcs

Main функция запуска программы fig. 5

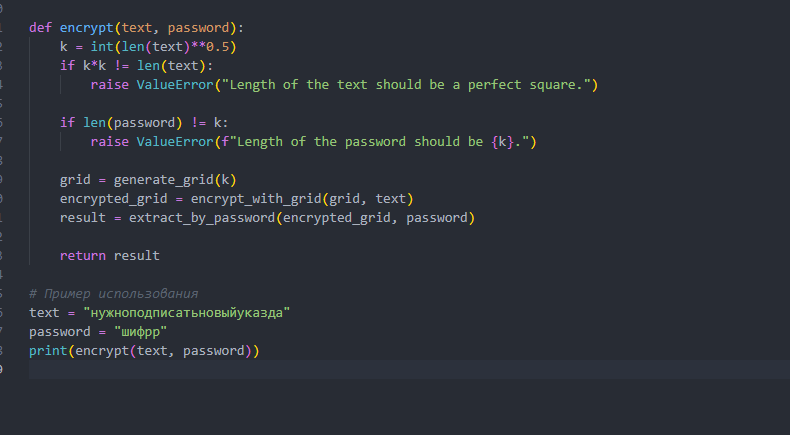


Figure 5: grid\_main\_func

Пример работы программы fig. 6

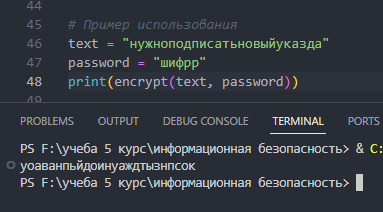


Figure 6: grid\_output

## 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 след. код на python:

1. Функция шифрования (построение таблицы Вижинера)
2. Функция дешифровки fig. 7

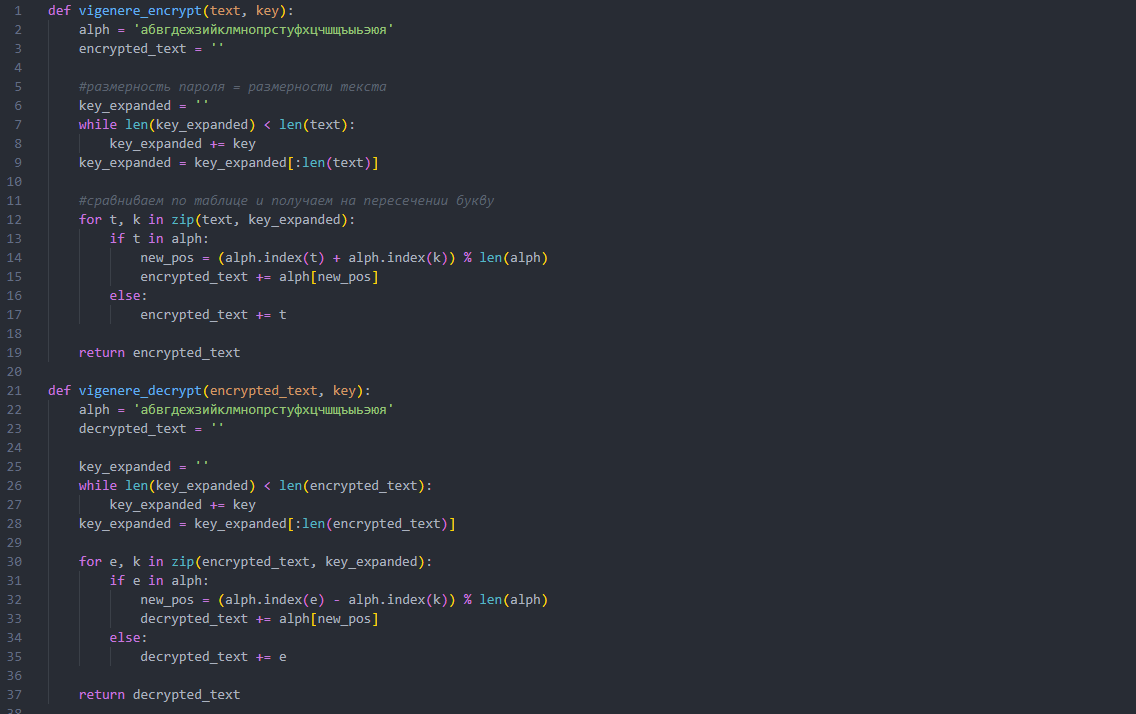


Figure 7: viginere\_funcs

Main функция запуска программы fig. 8

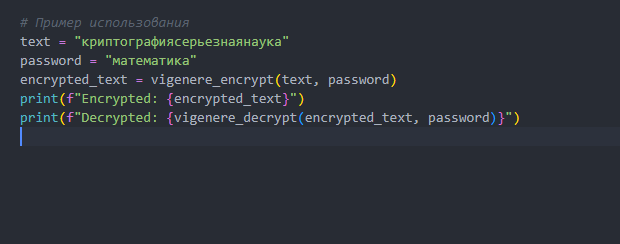


Figure 8: viginere\_main\_func

Пример работы программы (как в методических материалах) fig. 9

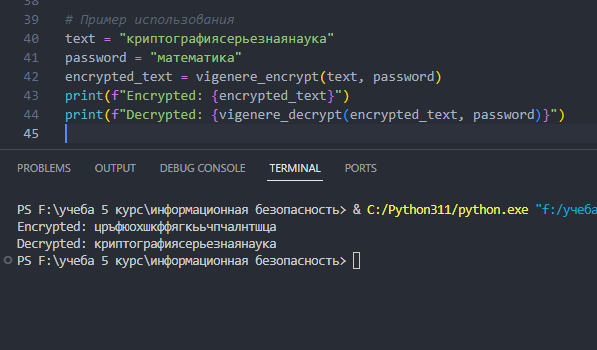


Figure 9: viginere\_output

# 3 Выводы

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

# 4 Список литературы

1. Методические материалы курса