Лабораторная работа 2

Шифры перестановки

Пологов Владислав Александрович

Содержание

# Цель работы

Реализовать метод маршрутного шифрования.

Реализовать метод шифрования с помощью решёток.

Реализовать метод шифрования с помощью таблицы Виженера.

# Описание реализации

Для реализации алгоритмов использовались средства языка Python.

Каждый метод был реализован отдельной функцией с соответствующим названием. (рис. 1)

Каждая функция принимала в качестве входных параметров строку и пароль для её шифрования. Помимо этого в методе машрутного шифрования необходимо было сообщать функции о длине блока n. А в методе шифрования с помощью решёток на вход ещё подавались сторона изначального квадрата k и координаты прорезей решётки.

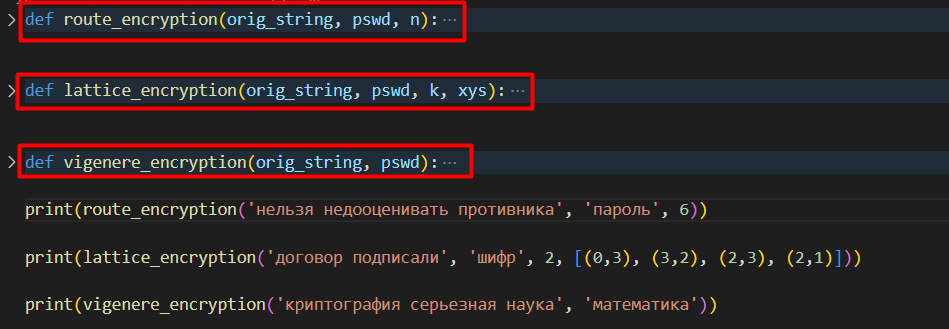


Figure 1: Функции методов шифрования

# Реализация

## Маршрутное шифрование

Данный способ шифрования разработал фанцунзский математик Франсуа Виет. Его суть заключалась в записи исходного текста в некоторую геометрическую форму(обычно прямоугольник) по некоторому пути, а затем, выписывая символы по другому пути, можно было получить шифртекст. (рис. 2)

В данном способе можно обойтись без составления матрицы. Доступ к строке и её шифрования осуществлялось следующим образом:

где — номер строки, — длина одного модуля или количество столбцов, — функция, вовзращающая индекс буквы пароля в соответствие с алфавитным порядком.

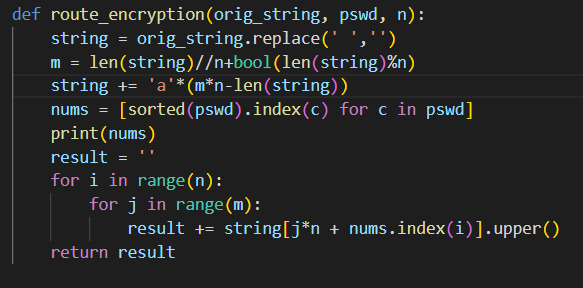


Figure 2: Код маршрутного шифрования

## Шифрование с помощью решёток

Данный способ шифрования предложил австрийский криптограф Эдуард Флейснер в 1881 году. Суть заключается в том, что строится матрица размерности 2\*k. Далее в матрице вырезаются клетки, содержащие числа от 1 до . Получается решето, которое мы накладываем на наш исходный текст. Алгоритм является иттерационнным и каждая иттерация сопровождается поворотом решётки на 90 градусов. Число выбирается в соответствии с количеством букв исходного текста. (рис. 3)

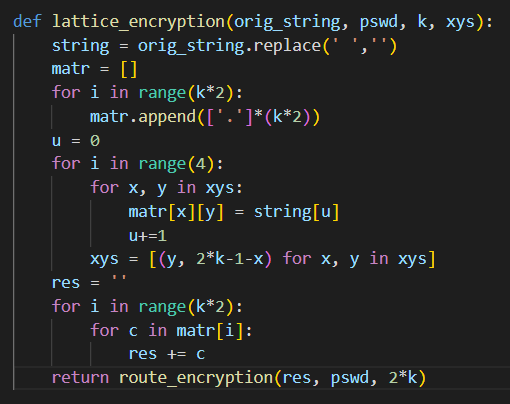


Figure 3: Код шифрования с помощью решёток

## Таблица Виженера

Суть этого метода заключается в том, что имеется таблица, составленная при помощи циклического сдвига букв русского алфавита на одну позицию влево. Для составления шифра используется пароль, который продлевается до конца исходной строки. После, в соответствии с паролем, находится буква в таблице Виженера для шифрования соответствующей буквы исходного текста. (рис. 4)

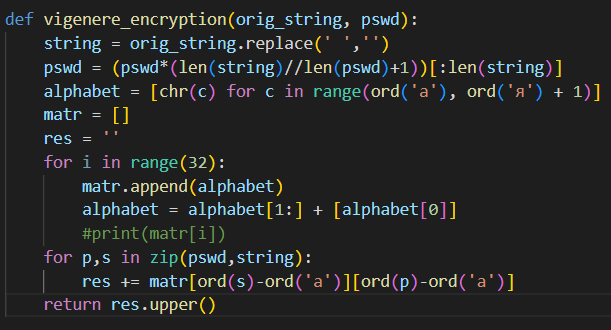


Figure 4: Код шифрования с помощью таблицы Виженера

# Вывод

Ознакомились с шифрами перестановок.

Реализовали метод маршрутного шифрования.

Реализовали метод шифрования с помощтю решёток.

Реализовали метод шифрования с помощью таблицы Виженера.