Лабораторная работа 2

Шифры перестановки

Греков Максим Сергеевич

Содержание

# Цель работы

* Ознакомиться с шифрами перестановки.
* Реализовать маршрутное шифрование.
* Реализовать шифрование с помощью решеток.
* Реализовать шифрование Таблица Виженера.

# Описание методов

Шифры перестановки преобразуют открытый текст в криптограмму путем перестановки его символов.

Способ, каким при шифровании переставляются буквы открытого текста, и является ключом шифра.

Важным требованием евс является равенство длин ключа и исходного текста.

# Маршрутное шифрование

## Описание

Простейшим примеров перестановочного шифра являются так называемые «маршрутные перестановки», использующие некоторую геометрическую фигуру (плоскую или объемную).

Шифрование заключается в том, что текст записывается в такую фигуру по некоторой траектории, а выписывается по другой траектории. (рис. 1)

## Реализация

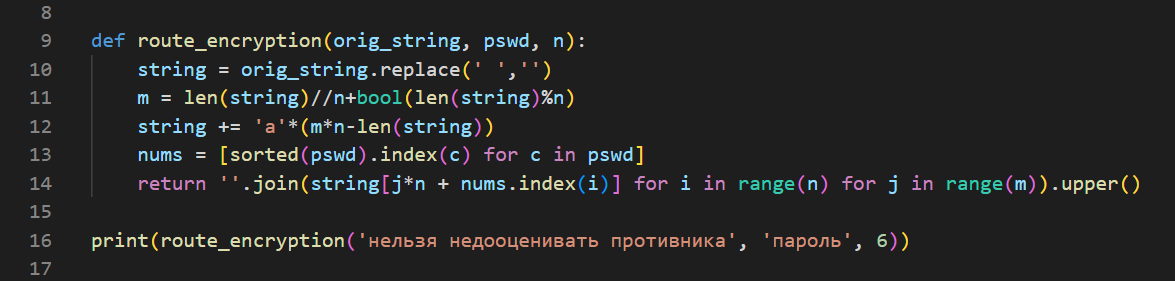


Figure 1: Маршрутное шифрование

Результат: **ЕЕНПНЗОАТАЬОВОКННЕЬВЛДИРИЯЦТИА**

# Шифрование с помощью решеток

## Описание

Выбирается число *k*. Строим квадрат со стороной длины k и заполняем его клетки числами от *1* до *k^2*.

Поворачиваем квадрат на *90* градусов по часовой стрелке и приписываем справа от исходного квадрата.

Поворачивая на *90* градусов по часовой стрелки и добавляя полученный квадрат сначала снизу, а затем слева от предыдущего, получим квадрат со стороной *2k*.

В этом квадрате закрасим произвольным образом все цифры, причем каждая цифра может быть закрашена только один раз.

Это и будет решёткой для шифрования.

Код для шифрования представляет последовательность *k* цифр от *1* до *4*, *i*-тая цифра обозначает в каком подквадрате (нумеруются в порядке создания) закрашивать число *i*.

Открытый текст разбивается на блоки длины *4k^2*.

Каждый блок разбивается на подстроки длины *k^2*.

Решетка накладывается на пустой лист бумаги, закрашиваемые клетки вырезаются.

Для первой подстроки ее *i*-ый символ записывается в вырезанное *i*-ое число решетки.

Повторяем процесс еще *3* раза, поворачивая перед этим решетку на *90* градусов по часовой стрелке.

В результате получаем таблицу, составляющую из символов открытого текста.

Криптограмма из этой таблицы получается путем построчного выписывания символов или применения приемов маршрутного шифрования. (рис. 2)

## Реализация

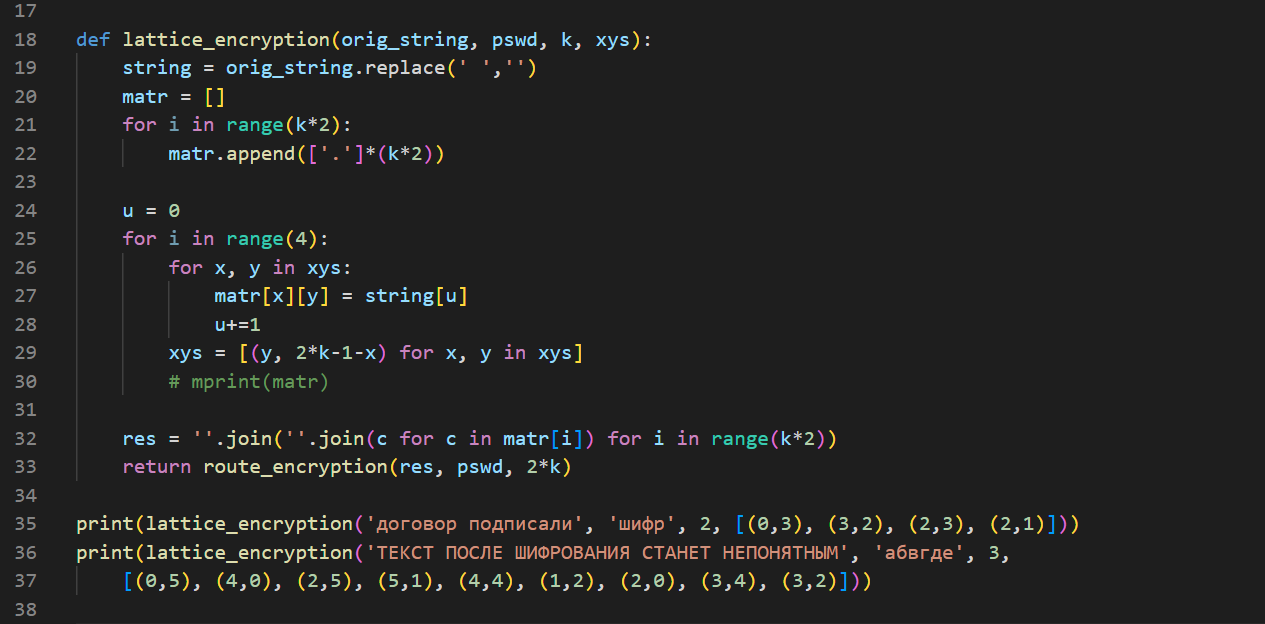


Figure 2: Шифрование с помощью решеток

Результат 1: **ДПОРДАГВЛИИОСПОО**

Результат 2: **ЕФОСЕИШАТТРСОПНЛАНВЫНМНИТЯОСТПТЯКЕНЕ**

# Таблица Виженера

## Описание

Шифр Виженера состоит из последовательности нескольких шифров Цезаря с различными значениями сдвига. (рис. 3)

Для зашифровывания может использоваться таблица алфавитов, называемая *tabula recta* или квадрат (таблица) Виженера.

Применительно к русскому алфавиту таблица Виженера составляется из строк по *33* символов, причём каждая следующая строка сдвигается на несколько позиций.

Таким образом, в таблице получается *33* различных шифров Цезаря.

На каждом этапе шифрования используются различные алфавиты, выбираемые в зависимости от символа ключевого слова.

## Реализация

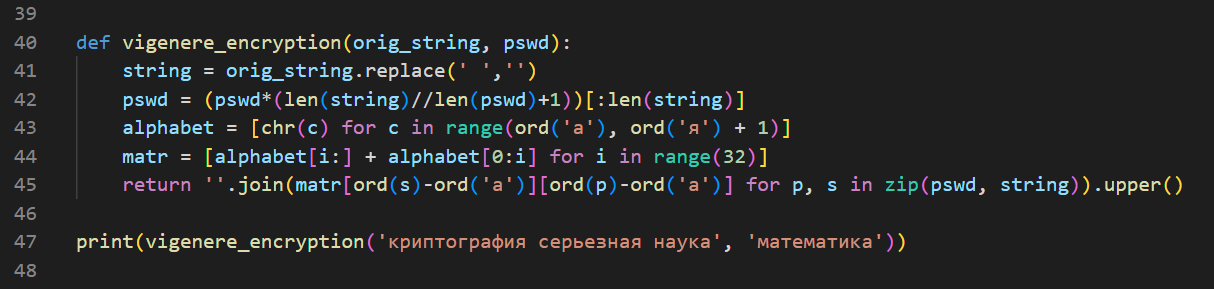


Figure 3: Таблица Виженера

Результат: **ЦРЪФЮОХШКФФЯГКЬЬЧПЧАЛНТШЦА**

# Вывод

* Ознакомились с шифрами перестановки.
* Реализовали маршрутное шифрование.
* Реализовали шифрование с помощью решеток.
* Реализовали шифрование Таблица Виженера.