Лабораторная работа №2. Шифры перестановки.

Предмет: Математические основы защиты информации и информационной безопасности

Александр Сергеевич Баклашов

Содержание

# 1 Цель работы

Рассмотреть шифры перестановки, а именно:

Маршрутное шифрование

Шифрование с помощью решеток

Таблица Виженера

# 2 Задание

1. Реализовать маршрутное шифрование.
2. Реализовать шифрование с помощью решеток.
3. Реализовать шифрование с помощью таблицы Виженера.

# 3 Теоретическое введение

## 3.1 Маршрутное шифрование

Этот способ шифрования изобрел выдающийся французский математик и криптограф Франсуа Виет (1540-1603).

Пусть m и n – некоторые натуральные (т.е. целые положительные) числа, каждое больше 1. Открытый текст последовательно разбивается на части (блоки) с длиной, равной произведению mn (если в последнем блоке не хватает букв, можно дописать до нужной длины произвольный их набор). Блок вписывается построчно в таблицу размерности m×n (т.е. m строк и n столбцов). Криптограмма получается выписыванием букв из таблицы в соответствии с некоторым маршрутом. Этот маршрут вместе с числами m и n составляет ключ шифра.

## 3.2 Шифрование с помощью решеток

Шифрование с использованием решеток (или квадратных сеток) - это метод шифрования, который предлагает различные способы организации текста внутри квадратной сетки и затем извлечения информации из этой сетки с помощью ключа или другой инструкции. Этот метод шифрования обеспечивает некоторую степень защиты данных, особенно когда криптографический ключ сложно угадать или определить без знания специфических правил.

## 3.3 Шифрование с помощью таблицы Виженера

Шифр Виженера (фр. Chiffre de Vigenère) — метод полиалфавитного шифрования буквенного текста с использованием ключевого слова.

Этот метод является простой формой многоалфавитной замены. Шифр Виженера изобретался многократно. Впервые этот метод описал Джовани Баттиста Белласо (итал. Giovan Battista Bellaso) в книге La cifra del. Sig. Giovan Battista Bellasо в 1553 году, однако в XIX веке получил имя Блеза Виженера, французского дипломата. Метод прост для понимания и реализации, но является недоступным для простых методов криптоанализа.

Хотя шифр легко понять и реализовать, на протяжении трех столетий он противостоял всем попыткам его сломать; чем и заработал имя le chiffre indéchiffrable (фр. неразгаданный шифр). Многие люди пытались реализовать схемы шифрования, которые по сути являлись шифрами Виженера.

# 4 Выполнение лабораторной работы

## 4.1 Маршрутное шифрование

### 4.1.1 Задача

Реализовать маршрутное шифрование.

#### 4.1.1.1 Решение

Запросим длину блоков и разобьем текст на них (рис. [1](#fig:001))

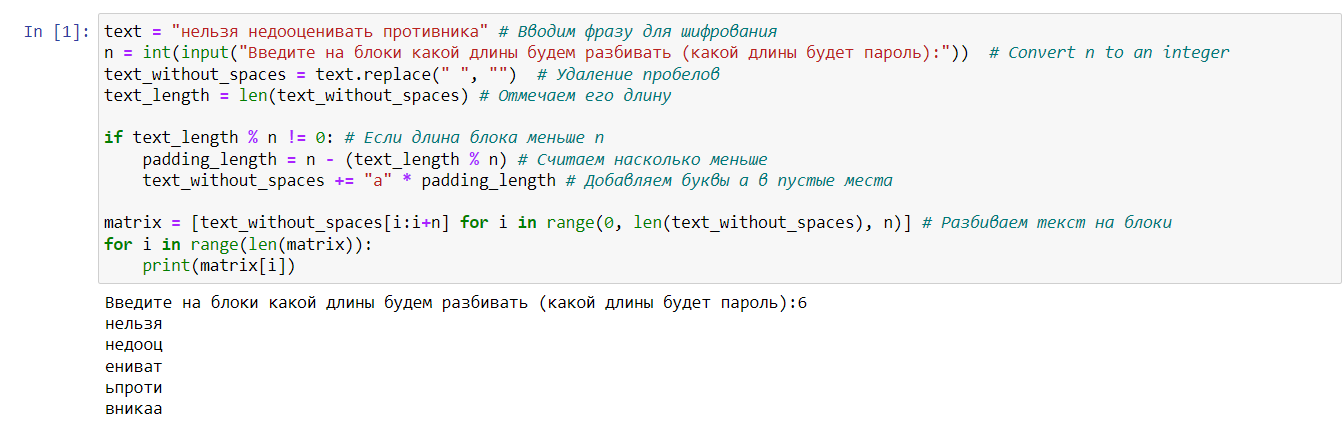


Figure 1: Маршрутное шифрование (1)

Запросим пароль и построим столбцы в соотв. с алф. порядком букв в пароле (рис. [2](#fig:002))

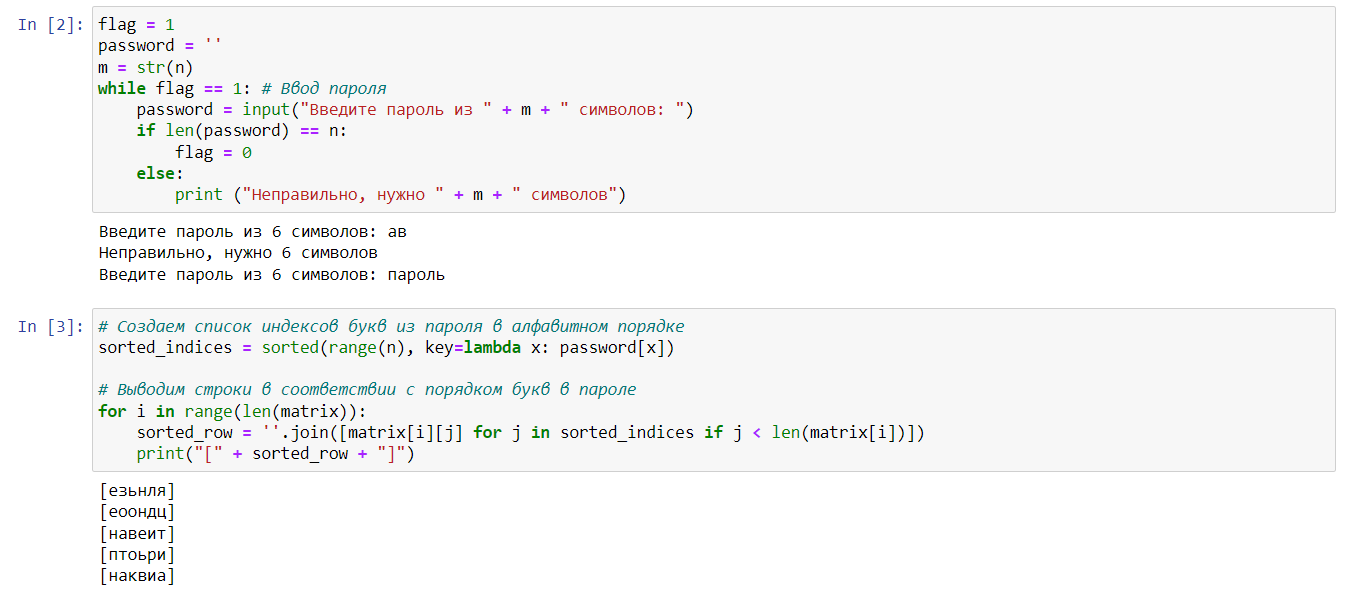


Figure 2: Маршрутное шифрование (2)

Выведем результат (рис. [3](#fig:003))

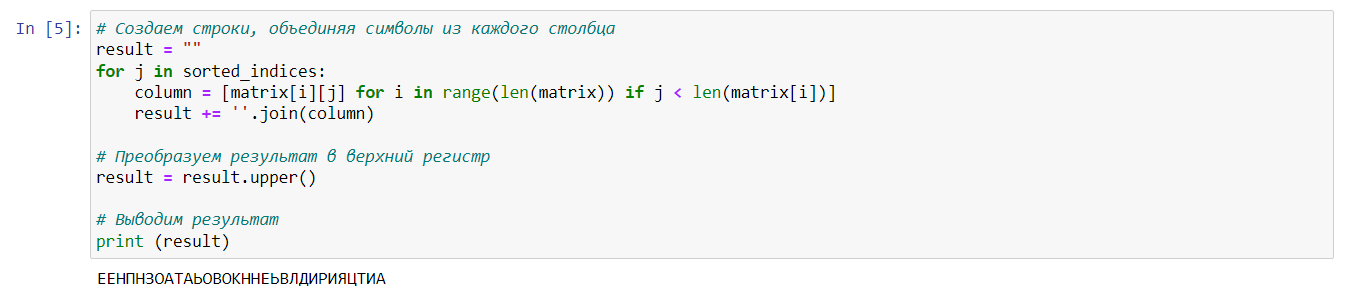


Figure 3: Маршрутное шифрование (3)

## 4.2 Шифрование с помощью решеток

### 4.2.1 Задача

Реализовать шифрование с помощью решеток.

#### 4.2.1.1 Решение

Заполним исх. матрицу и выявим ячейки, числа в которых будем вырезать (рис. [4](#fig:004))



Figure 4: Шифрование с помощью решеток (1)

Зададим шифротекст и ключ и выведем результат, поворачивая матрицу против часовой стрелки и вставляя соотв. буквы (рис. [5](#fig:005))



Figure 5: Шифрование с помощью решеток (2)

## 4.3 Шифрование с помощью таблицы Виженера

### 4.3.1 Задача

Реализовать шифрование с помощью таблицы Виженера.

#### 4.3.1.1 Решение

Создадим функцию для шифрования (рис. [6](#fig:006))



Figure 6: Шифрование с помощью таблицы Виженера (1)

Создадим функцию для дешифрования (рис. [7](#fig:007))



Figure 7: Шифрование с помощью таблицы Виженера (2)

Зададим шифротекст и ключ и выведем результат (рис. [8](#fig:008))

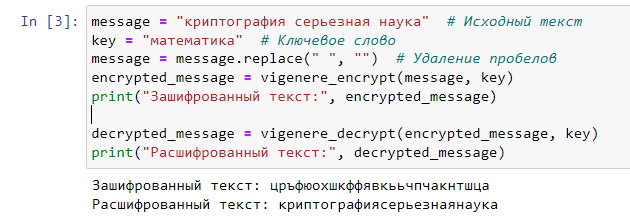


Figure 8: Шифрование с помощью таблицы Виженера (3)

# 5 Выводы

В ходе данной лабораторной работы я рассмотрел и реализовал такие шифры перестановки, как маршрутное шифрование, шифрование с помощью решеток и таблица Виженера.

# 6 Библиография

1. Python documentation. [Электронный ресурс]. М. URL: [Python documentation](https://docs.python.org/3/index.html) (Дата обращения: 28.09.2023).
2. Лабораторная работа №1. Задача о погоне. - 4 с. [Электронный ресурс]. М. URL: [Лабораторная работа №2. Шифры перестановки.](https://esystem.rudn.ru/pluginfile.php/2089789/mod_folder/content/0/lab02.pdf) (Дата обращения: 28.09.2023).