Отчёт по лабораторной работе 2

Тема лабораторной работы: Шрифты перестановки

Студент: Румянцева Александра Сергеевна, 1132223493

Группа: НПМмд-02-22

Преподаватель: Кулябов Дмитрий Сергеевич,

д-р.ф.-м.н., проф.

Москва 2022

Содержание

# Цель работы

Целью данной лабораторной работы является ознакомление с тремя методами шифрования: маршрутным шифрованием, шифрованием с помощью решеток, таблицей Виженера, а так же их реализация на произвольном языке программирования.

# Задание

1. Реализовать метод маршрутного шифрования.
2. Реализовать метод шифрования с помощью решеток.
3. Реализовать метод таблицы Вижера.

# Теоретическое введение

Математическая часть подробно описана в задании к лабораторной работе. Я поставила перед собой задачу найти исторические сведения, факты о методах шифрования.

**Шифр перестановки** — это метод симметричного шифрования, в котором элементы исходного открытого текста меняют местами. Элементами текста могут быть отдельные символы, пары букв, тройки букв, комбинирование этих случаев и так далее. Типичными примерами перестановки являются анаграммы. В классической криптографии шифры перестановки можно разделить на два класса:

1. Шифры одинарной (простой) перестановки — при шифровании символы открытого текста перемещаются с исходных позиций в новые один раз.
2. Шифры множественной (сложной) перестановки — при шифровании символы открытого текста перемещаются с исходных позиций в новые несколько раз.

Метод **маршрутного шифрования** изобрел французский математик и криптограф Франсуа Виет. Этот способ относится к перестановочным шифрам. Шифр называется перестановочным, если все связанные с ним криптограммы получаются из соответствующих открытых текстов перестановкой букв. Способ, каким при шифровании переставляются буквы открытого текста, и является ключом шифра. Такой метод шифрования (столбцовая перестановка) в годы первой мировой войны использовала легендарная немецкая шпионка Мата Хари.

**Шифровальная решётка** — трафарет с прорезями-ячейками (из бумаги, картона или аналогичного материала), использовавшийся для шифрования открытого текста. Текст наносился на лист бумаги через такой трафарет по определённым правилам, и расшифровка текста была возможна только при наличии такого же трафарета.

**Вращающаяся решетка**: Прямоугольные решётки Кардано можно размещать в четырёх позициях. Шифр с сеткой в виде шахматной доски имеет только две позиции, но именно этот вариант вращающейся решётки послужил для разработки более сложной решётки с четырьмя позициями, которую можно вращать в двух направлениях.

**Шифр Виженера** является простой формой многоалфавитной замены. Шифр Виженера изобретался многократно. Впервые этот метод описал Джован Баттиста Беллазо (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, он является недоступным для простых методов криптоанализа.

# Выполнение лабораторной работы

## Маршрутное шифрование

В соответствии с заданием, первой была написана программа для маршрутного шифрования (рис. 1-2). В качестве параметров системы были взяты данные из описательной части лабораторной работы портала ТУИС.

*Примечание:* комментарии по коду рализации маршрутного шифрования представлены на скриншотах.

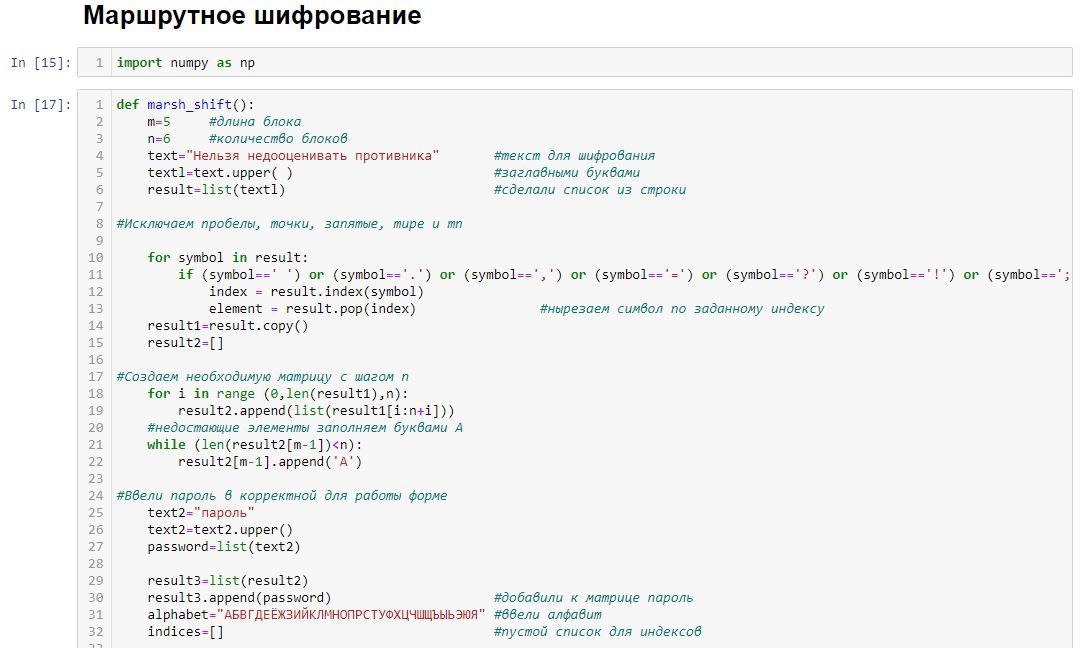


Figure 1: Рис. 1. 1 часть программного кода реализации маршрутного шифрования.

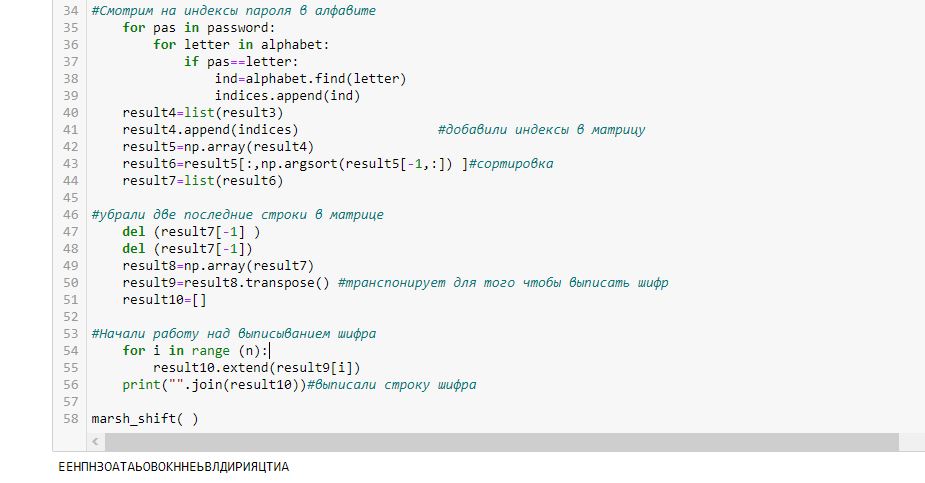


Figure 2: Рис. 2. 2 часть программного кода реализации маршрутного шифрования.

Результат выполнения программы видно на рис. 2. Результат можно назвать успешным, он совпадает с шифрованием из примера в ТУИСе РУДН, при этом само по себе шифрование однозначно, поэтому совпадение результата говорит о правильности выполнения работы.

## Метод решеток

Далее была написана программа релизации шифрования методом решеток (рис. 3-6). В качестве параметров системы были взяты данные из описательной части лабораторной работы портала ТУИС.

*Примечание:* комментарии по коду рализации маршрутного шифрования представлены на скриншотах.



Figure 3: Рис. 3. 1 часть программного кода реализации шифрования с помощью метода решеток.

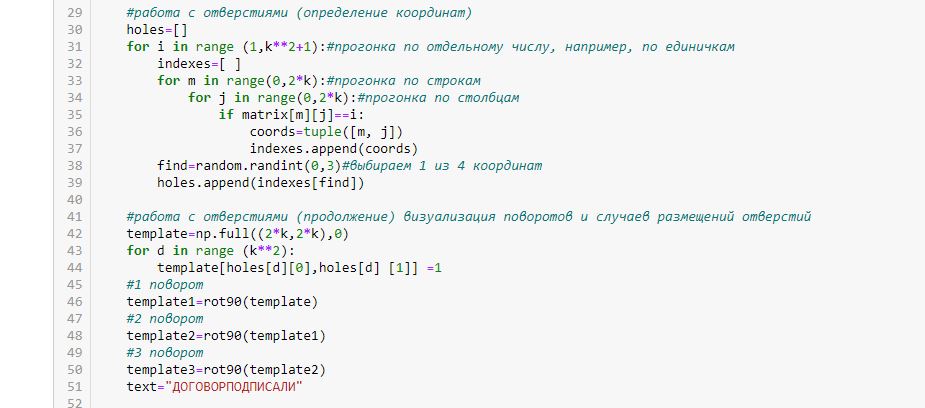


Figure 4: Рис. 4. 2 часть программного кода реализации шифрования с помощью метода решеток.



Figure 5: Рис. 5. 3 часть программного кода реализации шифрования с помощью метода решеток.



Figure 6: Рис. 6. 4 часть программного кода реализации шифрования с помощью метода решеток.

Результат выполнения программы видно на рис. 6. Результат можно назвать успешным, он совпадает с шифрованием из примера в ТУИСе РУДН. При этом само по себе шифрование неоднозначно, поскольку используется модуль рандом для порядка размещения символов, поэтому погли появляться и другие варианты шифрования.

## Метод Виженера

Последним реализованным методом был метод Виженера (рис. 7). В данном методе я шифровала фразы из английского алфавита.

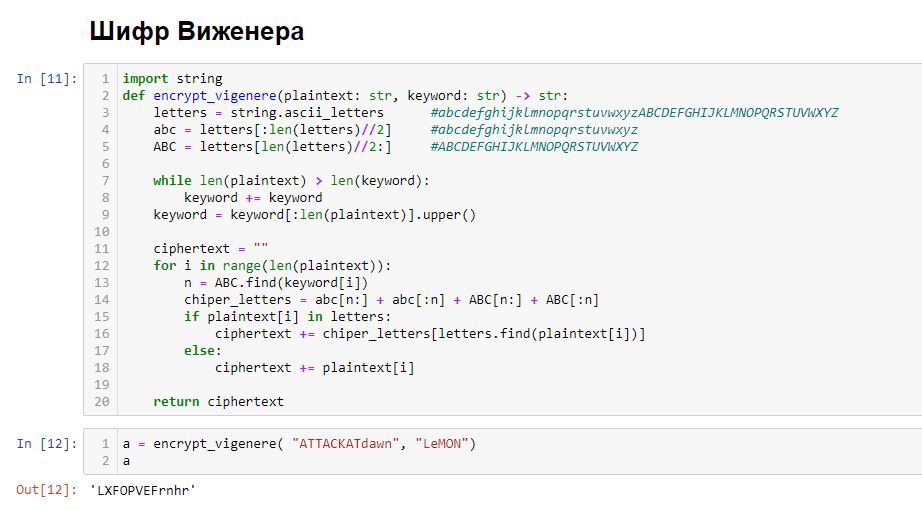


Figure 7: Рис. 7. Программного кода реализации шифра Виженера.

Далее было реализовано дешифрование текста (рис. 8). Важно отметить, что нужно использовать одинаковый ключ (кодовое слово) как для шифровки, так и для шифрования.

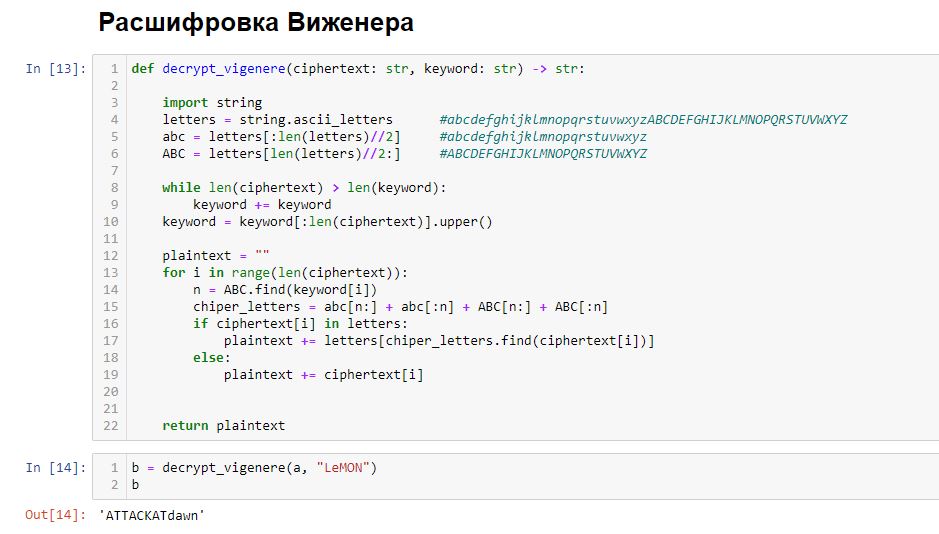


Figure 8: Рис. 8. Программного кода реализации расшифровки шифра Виженера.

Как можно видеть, расшифровка совпадает с изначальным текстом на рис. 7, что говорит об успешной реализации метода.

# Библиография

1. ТУИС РУДН
2. Википедия. Перестановочный шифр [Электронный ресурс]. Википедия, свободная энциклопедия, 2021. URL: <https://en.wikipedia.org/wiki/Transposition_cipher>.
3. VK. Метод маршрутного шифрования [Электронный ресурс]. VK, 2018. URL: <https://vk.com/@cryptandcod-metod-marshrutnogo-shifrovaniya>.
4. Википедия. Шифровальная решетка [Электронный ресурс]. Википедия, свободная энциклопедия, 2021. URL: <https://en.wikipedia.org/wiki/Grille_(cryptography)>.
5. Wix. Криптография [Электронный ресурс]. Wixsite, 2021. URL: <https://en.wikipedia.org/wiki/Grille_(cryptography)>.
6. Википедия. Шифр Виженера [Электронный ресурс]. Википедия, свободная энциклопедия, 2021. URL: <https://en.wikipedia.org/wiki/Vigen%C3%A8re_cipher>.

# Выводы

Таким образом, была достигнута цель, поставленная в начале лабораторной работы: я ознакомилась с тремя методами шифрования – маршрутным шифрованием, шифрованием с помощью решеток, таблицей Виженера, а так же мне удалось реализовать их на языке программирования Python.