Отчёт по лабораторной работе №2.  
Шифры перестановки

Студент: Лапшенкова Любовь Олеговна, 10322127633

Группа: НФИмд-02-21

Преподаватель: Кулябов Дмитрий Сергеевич,

д-р.ф.-м.н., проф.

Москва 2021

Содержание

# 1 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.

# 2 Задание

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

# 3 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 [1]. 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[2].

**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[3].

**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[4].

**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[5].

# 4 Выполнение лабораторной работы

**Примечание:** комментарии по коду представлены на скриншотах к каждому из проделанных заданий.

## 4.1 Маршрутное шифрование

В соответствии с заданием, первой была написана программа для маршрутного шифрования. Программный код представлен ниже.



Figure 1: 1 часть программного кода реализации маршрутного шифрования

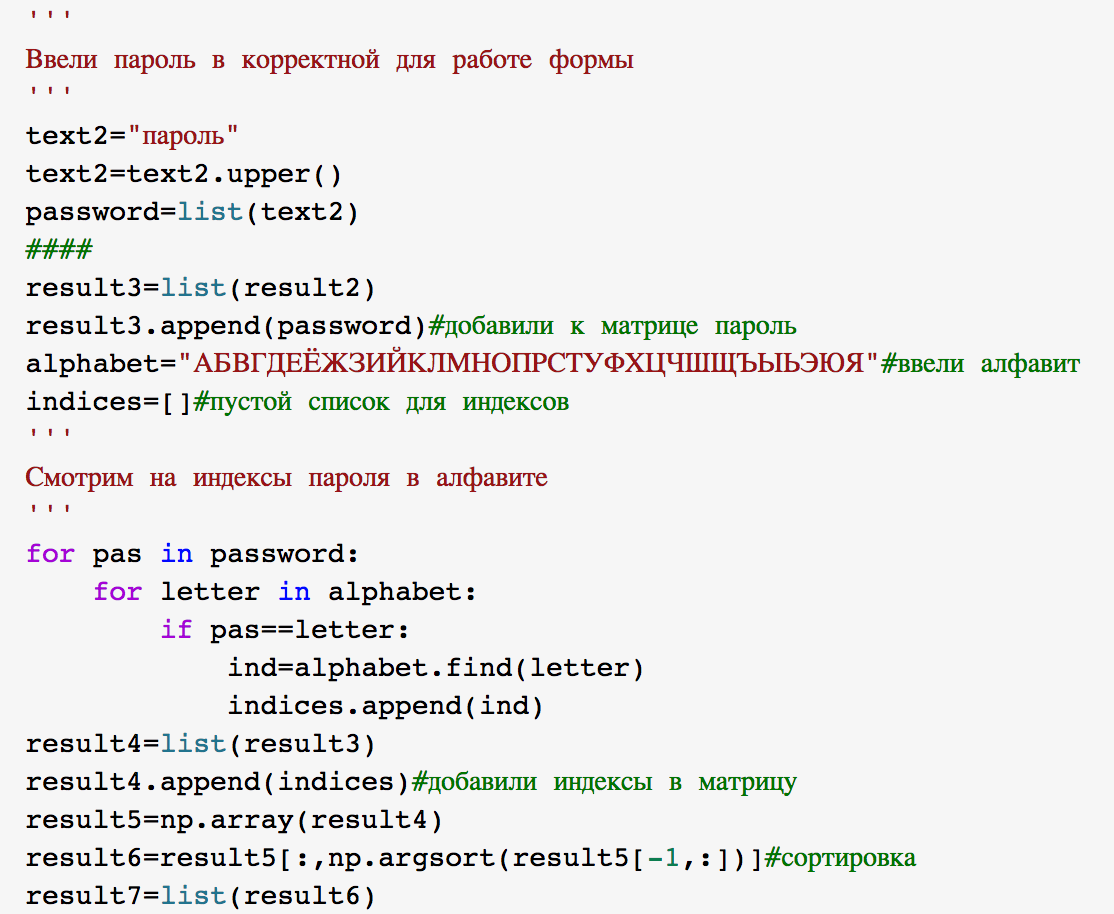


Figure 2: 2 часть программного кода реализации маршрутного шифрования

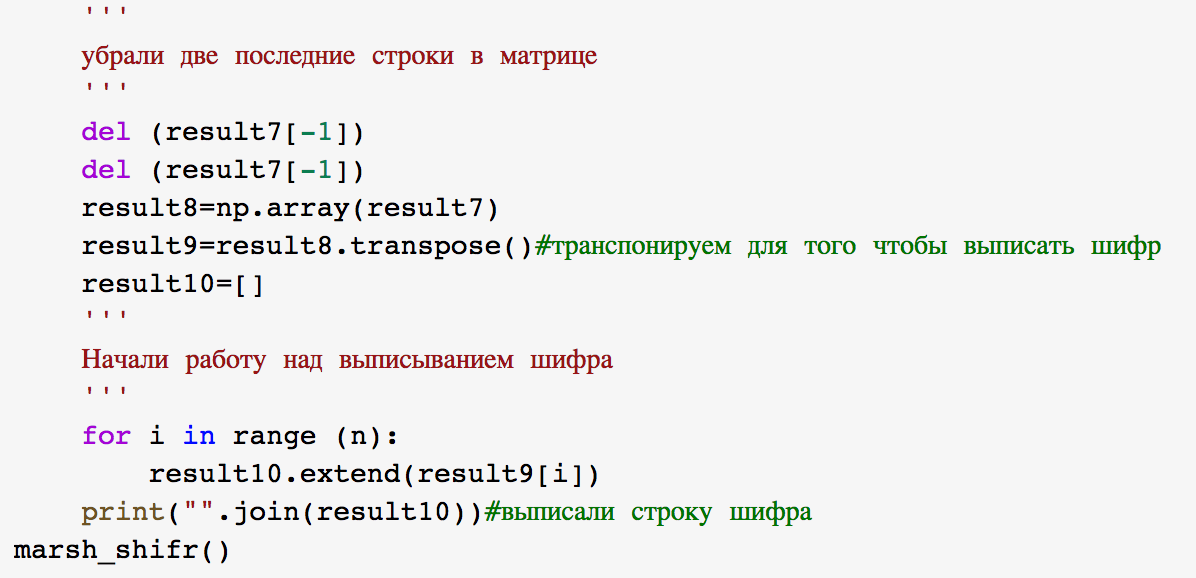


Figure 3: 3 часть программного кода реализации маршрутного шифрования

Результаты выполнения программы представлены ниже (см. рис. 4). В качестве параметров системы были взяты данные из описательной части лабораторной работы портала ТУИС.

Figure 4: Результат шифрования сообщений с использованием маршрутного шифрования

Figure 4: Результат шифрования сообщений с использованием маршрутного шифрования

## 4.2 Метод решеток

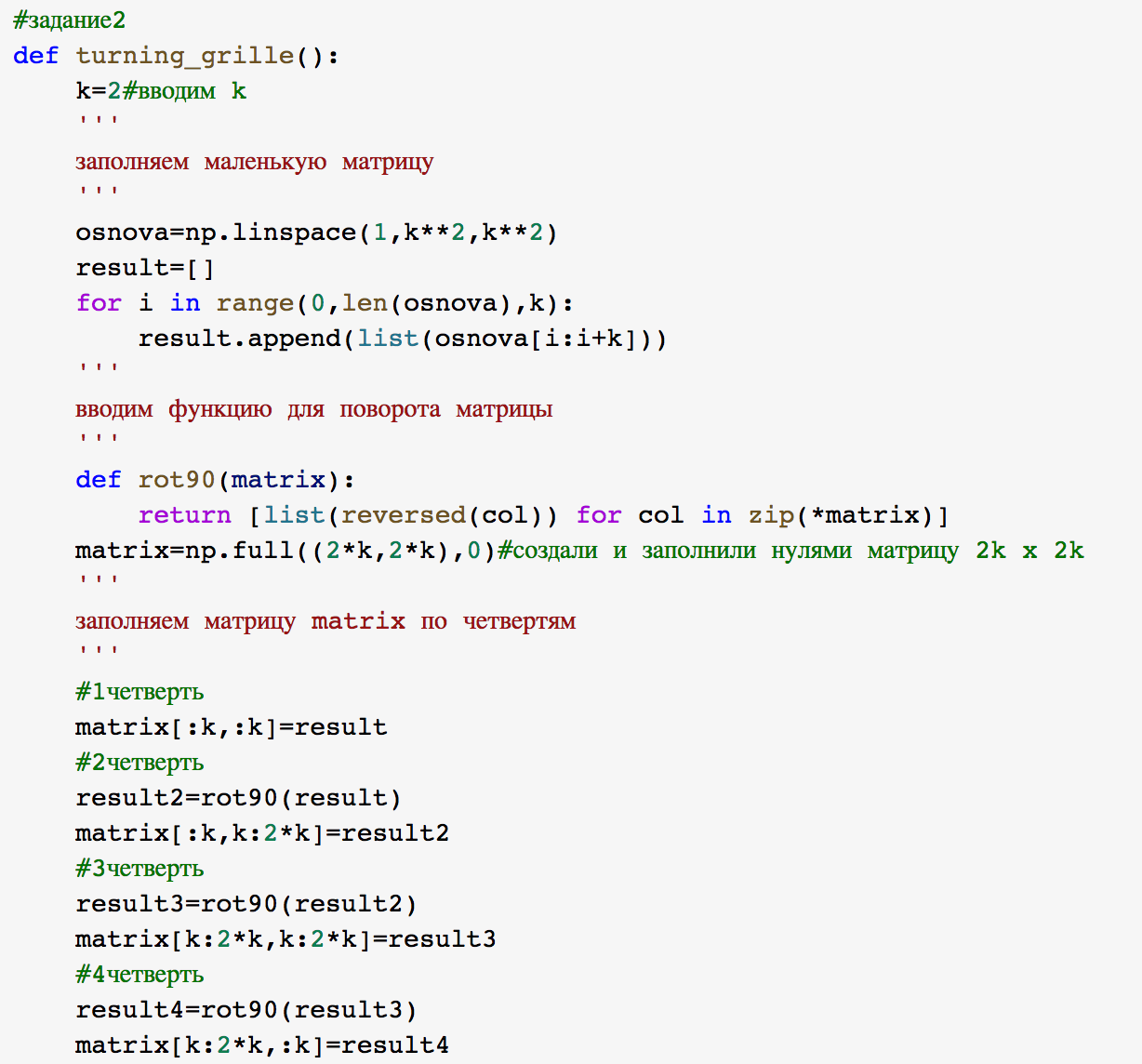


Figure 5: 1 часть программного кода реализации шифрования с помощью решеток

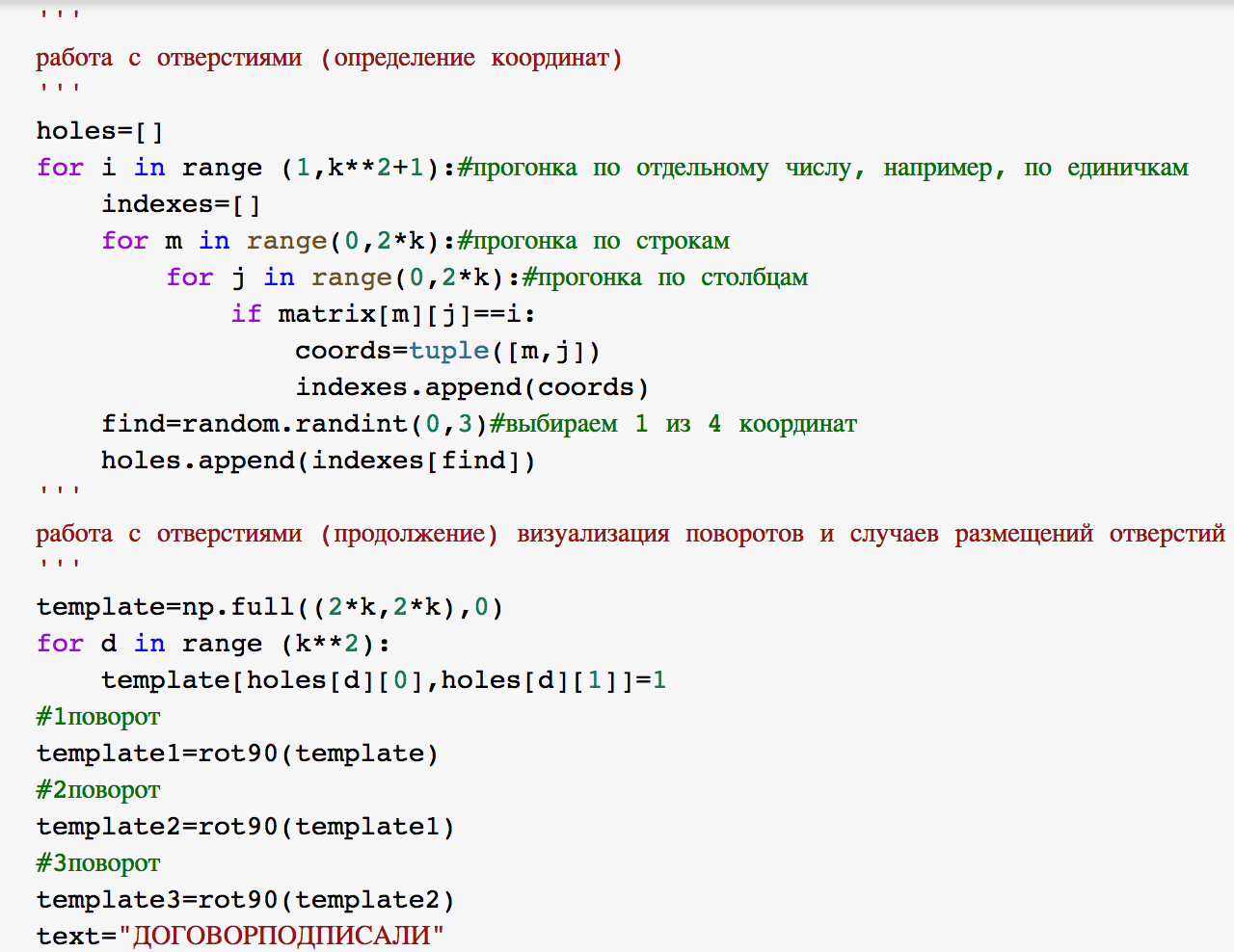


Figure 6: 2 часть программного кода реализации шифрования с помощью решеток

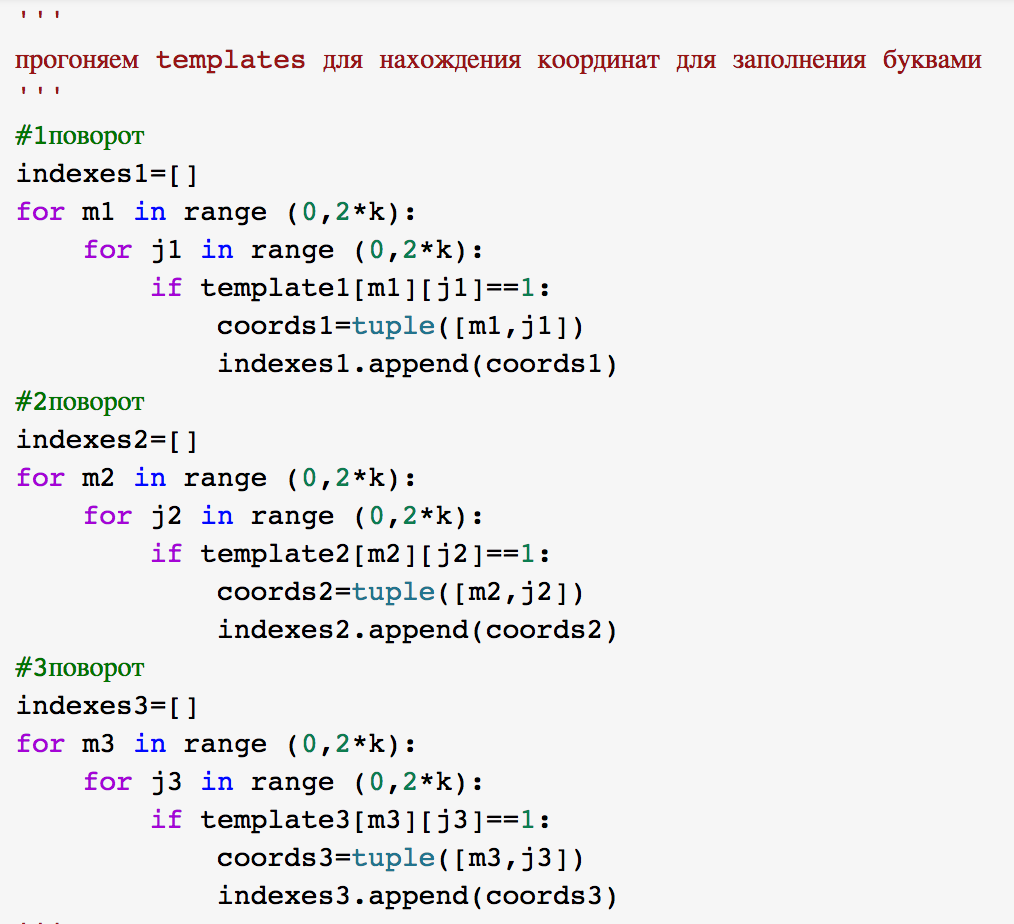


Figure 7: 3 часть программного кода реализации шифрования с помощью решеток

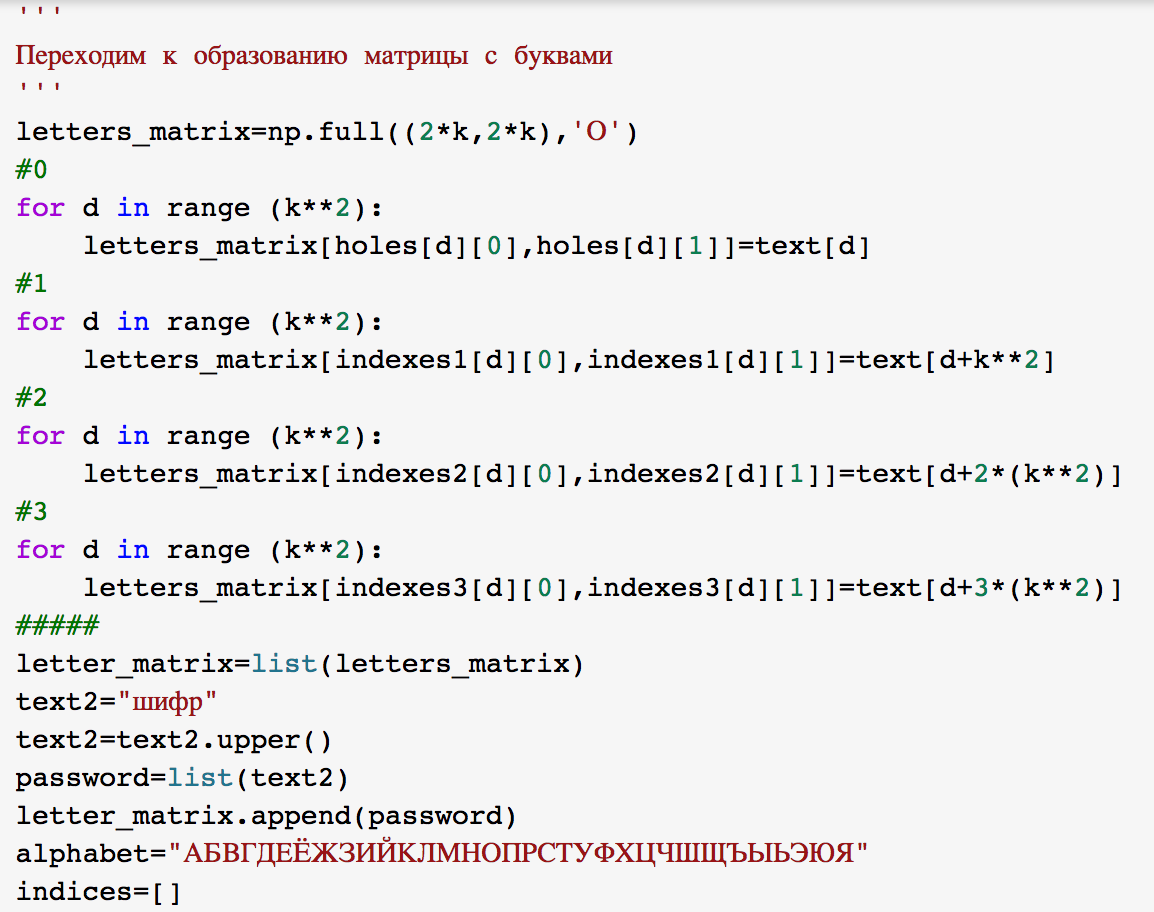


Figure 8: 4 часть программного кода реализации шифрования с помощью решеток

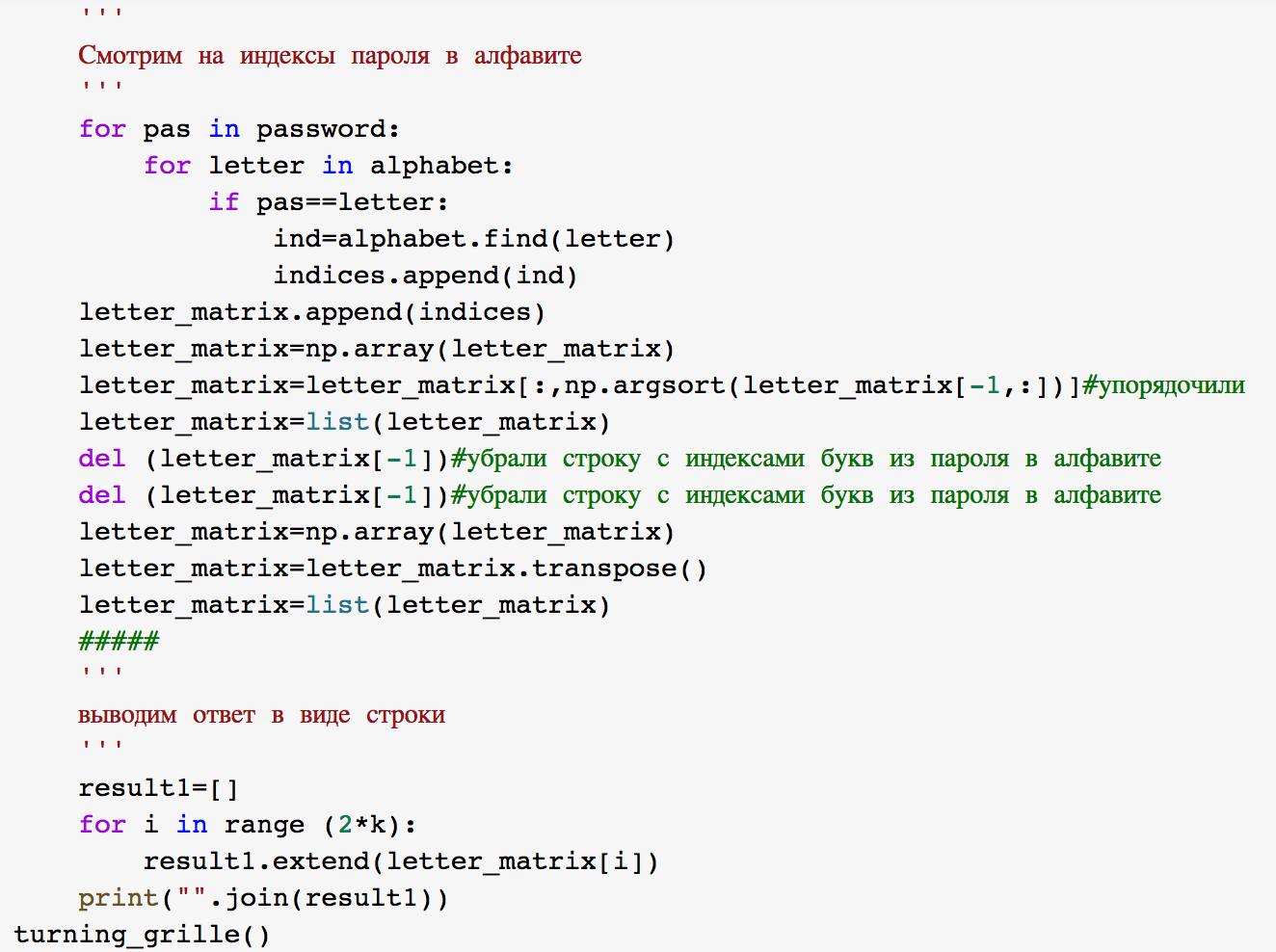


Figure 9: 5 часть программного кода реализации шифрования с помощью решеток

Результаты выполнения программы представлены ниже (см. рис. 10). В качестве параметров системы были взяты данные из описательной части лабораторной работы портала ТУИС.



Figure 10: Результат шифрования сообщений с использованием шифрования с помощью решеток

## 4.3 Таблица Виженера

Ну и наконец мы перешли к шифрованию при помощи таблицы Виженера. Программный код представлен ниже.



Figure 11: 1 часть программного кода реализации шифрования с помощью Таблица Виженера

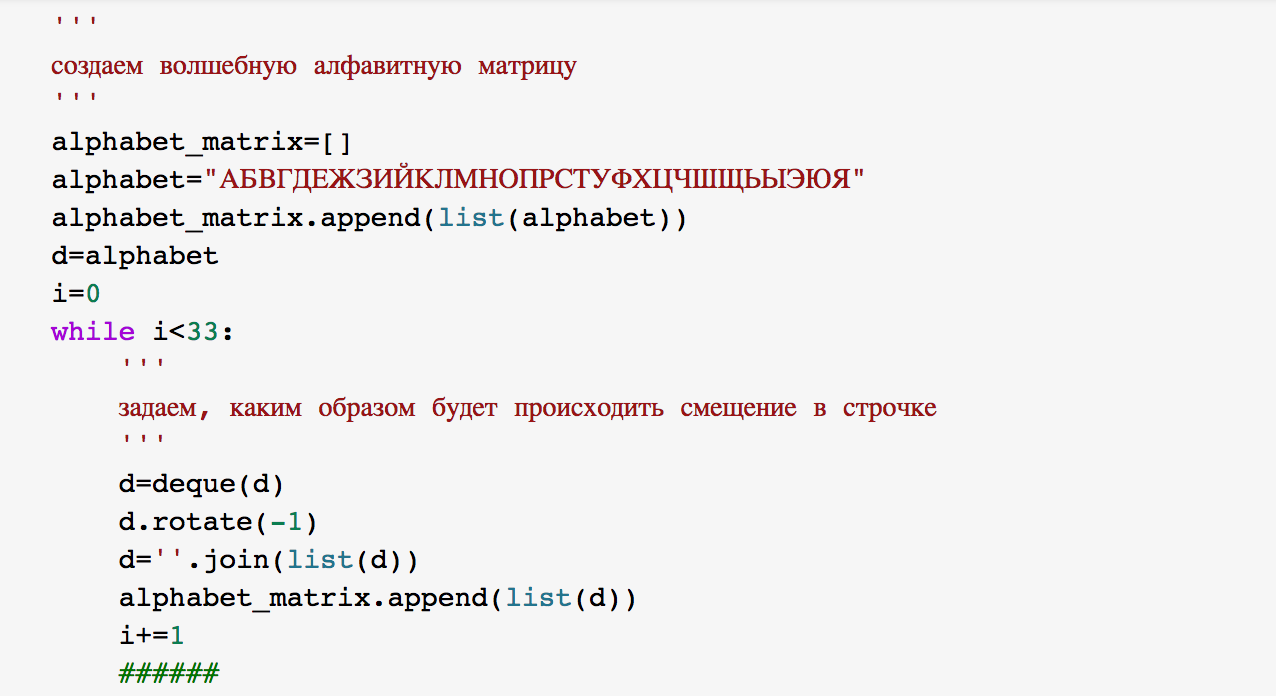


Figure 12: 2 часть программного кода реализации шифрования с помощью Таблица Виженера

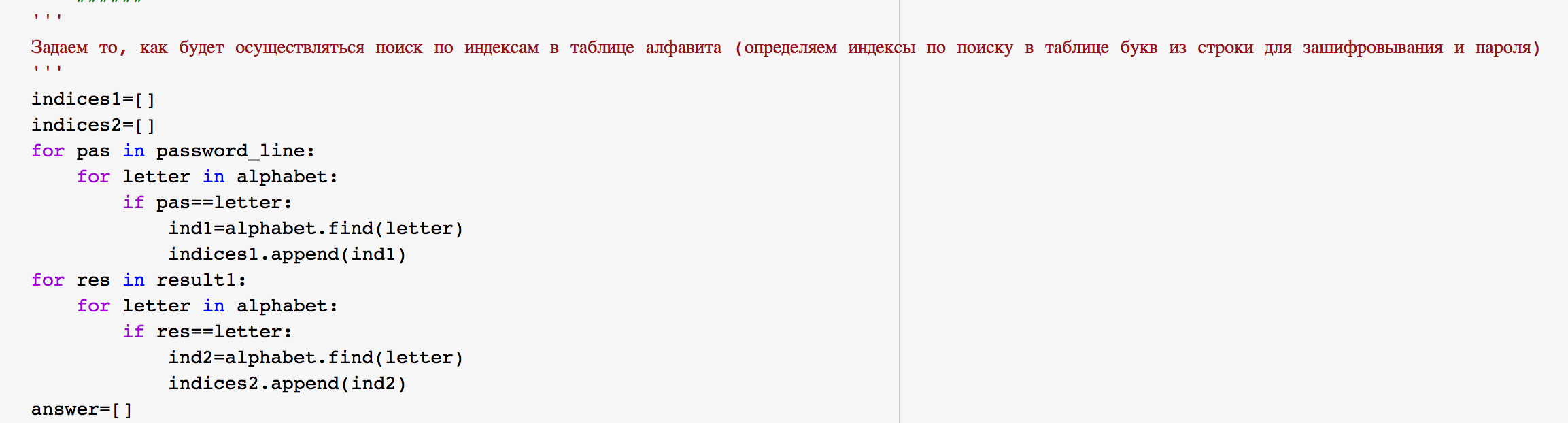


Figure 13: 3 часть программного кода реализации шифрования с помощью Таблица Виженера

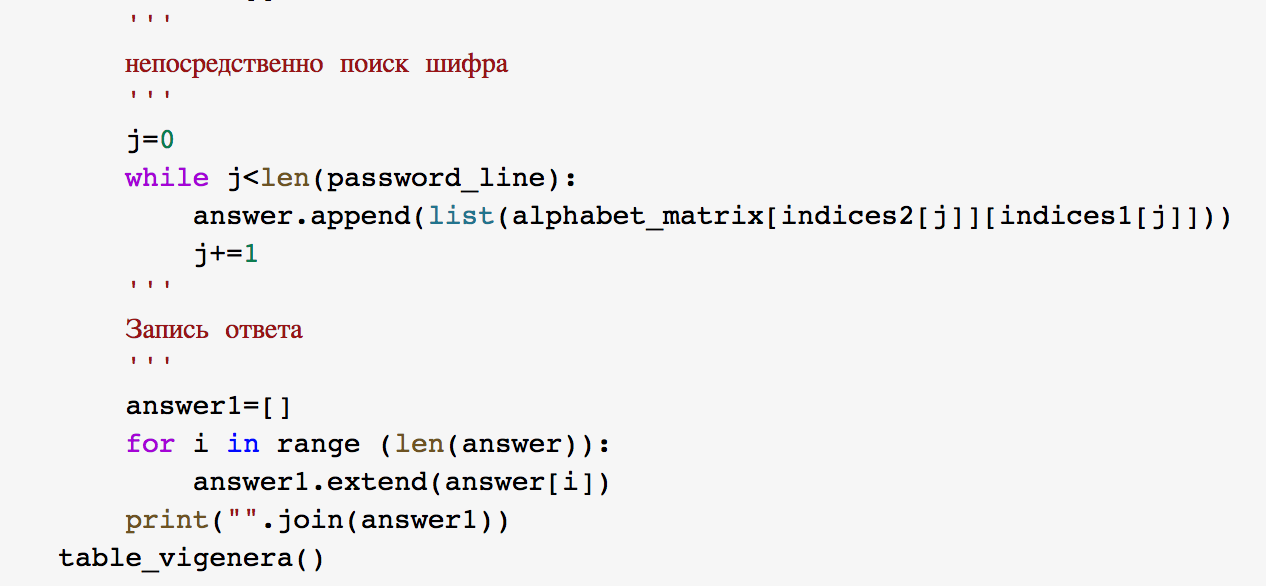


Figure 14: 4 часть программного кода реализации шифрования с помощью Таблица Виженера

Результаты выполнения программы представлены ниже (см. рис. 15). В качестве параметров системы были взяты данные из описательной части лабораторной работы портала ТУИС.

Figure 15: Результат шифрования сообщений с использованием шифрования с помощью Таблица Виженера

Figure 15: Результат шифрования сообщений с использованием шифрования с помощью Таблица Виженера

# 5 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.

# Список литературы

1. Википедия. Перестановочный шифр [Электронный ресурс]. Википедия, свободная энциклопедия, 2021. URL: <https://en.wikipedia.org/wiki/Transposition_cipher> (дата обращения: 19.11.2021).

2. VK. Метод маршрутного шифрования [Электронный ресурс]. VK, 2018. URL: <https://vk.com/@cryptandcod-metod-marshrutnogo-shifrovaniya> (дата обращения: 19.11.2021).

3. Википедия. Шифровальная решетка [Электронный ресурс]. Википедия, свободная энциклопедия, 2021. URL: <https://en.wikipedia.org/wiki/Grille_(cryptography)> (дата обращения: 19.11.2021).

4. Wix. Криптография [Электронный ресурс]. Wixsite, 2021. URL: <https://en.wikipedia.org/wiki/Grille_(cryptography)> (дата обращения: 19.11.2021).

5. Википедия. Шифр Виженера [Электронный ресурс]. Википедия, свободная энциклопедия, 2021. URL: <https://en.wikipedia.org/wiki/Vigen%C3%A8re_cipher> (дата обращения: 19.11.2021).