Лабораторная работа №2

Шифры перестановки

Якушевич Артём Юрьевич

Содержание

# 1 Цель работы

Ознакомиться с шифрами перестановки и обучиться их программной реализации.

# 2 Задание

* Реализовать шифрование столбцовой перестановки;
* Реализовать таблицу виженера.

# 3 Теоретическое введение

При подготовке использовалась методичка со страницы курса в ТУИС.[1]

Шифрование столбцовой перестановки. Криптограмма получается выписыванием букв из таблицы в соответствии с некоторым маршрутом. Ключом такой криптограммы является марштур и числа m и n. Внизу таблицы приписывается слово из n неповторющихся букв и столбцы нумеруются по алфавитному порядку букв пароля.

Шифрование столбцовой перестановки (рис. 1):



Рис. 1: Шифрование столбцовой перестановки

Таблица Виженера. Его принцип в том, что каждая буква в исходном шифруемом тексте сдвигается по алфавиту не на фиксированное, а переменное количество символов. Величина сдвига каждой буквы задается ключом (паролем) - секретным словом или фразой, которая используется для шифрования и расшифровки. (рис. 2):

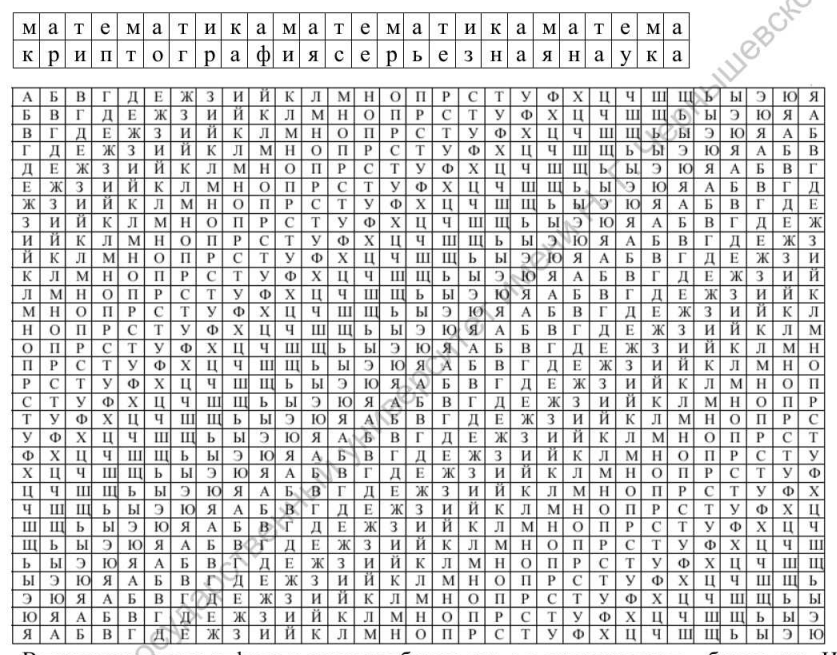


Рис. 2: Таблица Виженера

# 4 Выполнение лабораторной работы

Работа была выполнена на языке программирования Python.

Сначала реализуем шифрование столбцовой перестановки (рис. 3):

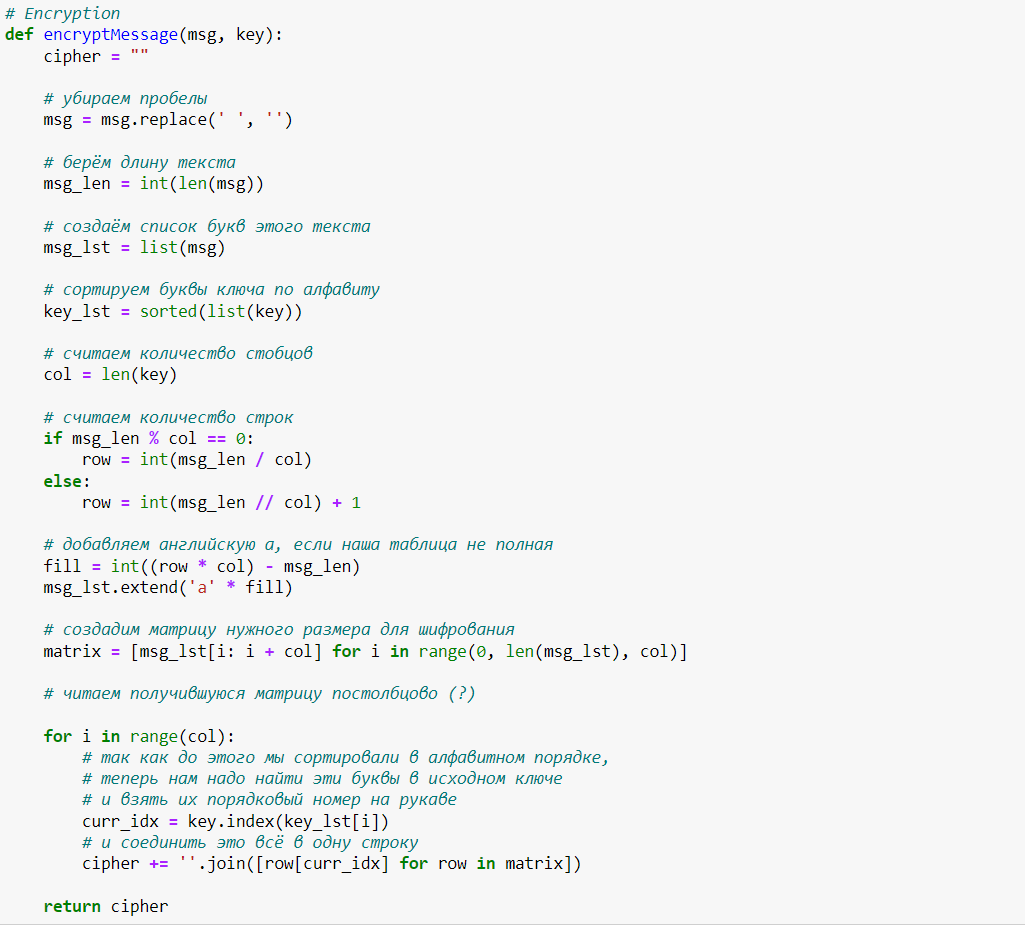


Рис. 3: шифрование столбцовой перестановки

Сначала реализуем шифрование столбцовой перестановки (рис. 4):

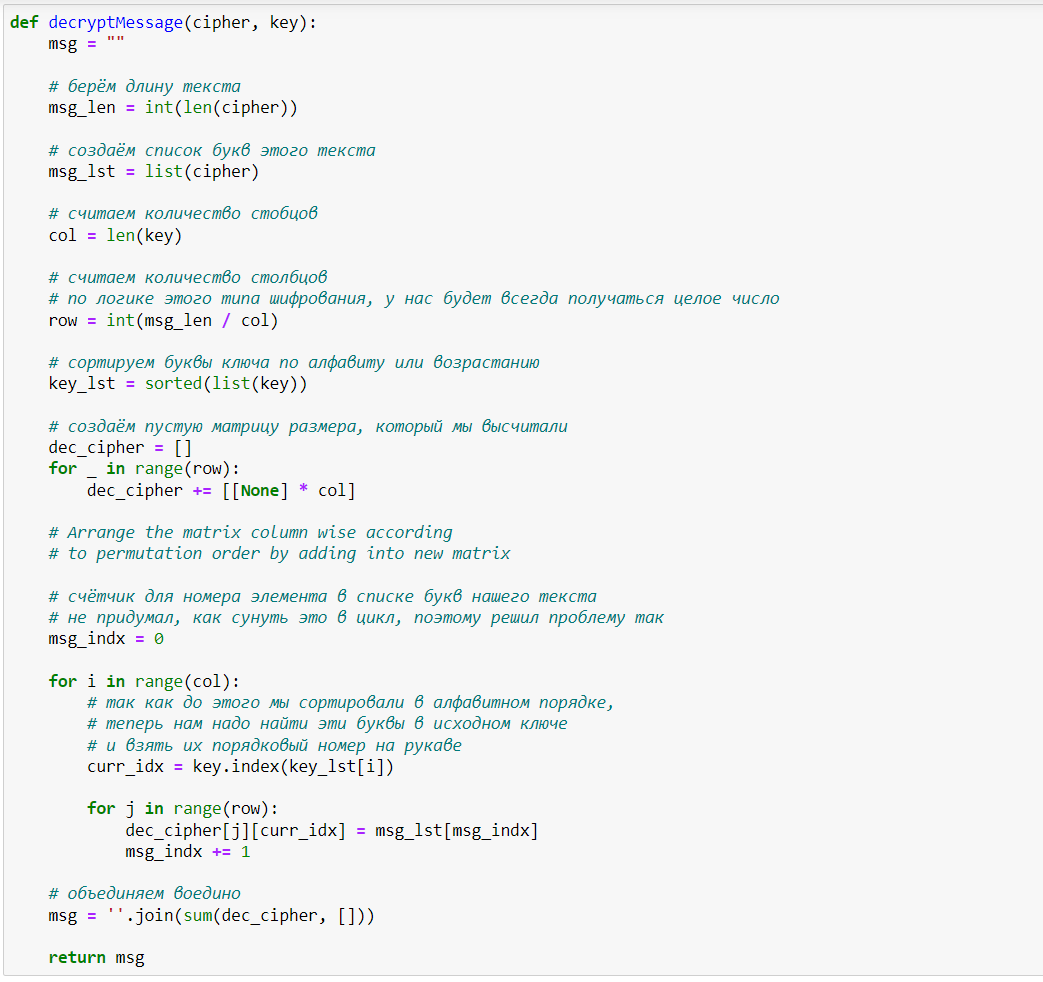


Рис. 4: шифрование столбцовой перестановки

Вывод программы (рис. 5):

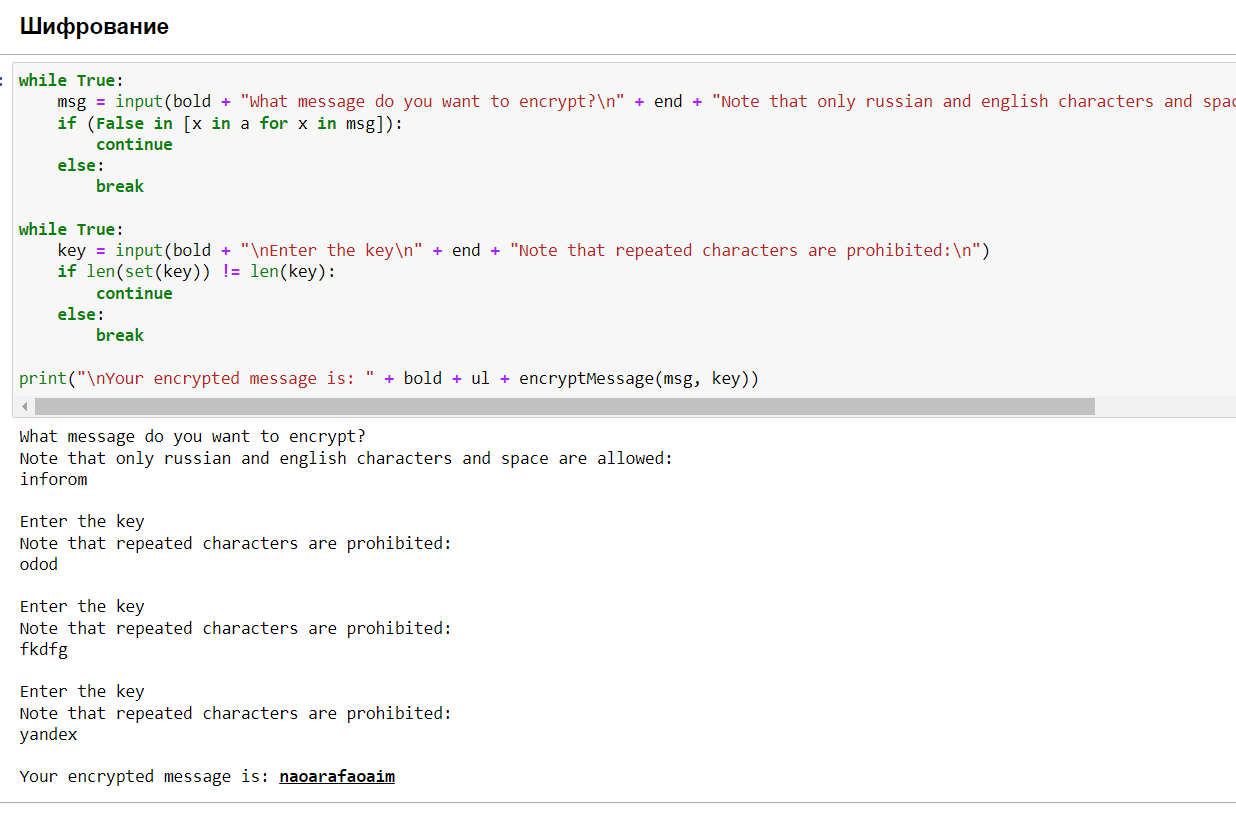


Рис. 5: Вывод программы

Реализация таблицы Виженера (рис. 6):

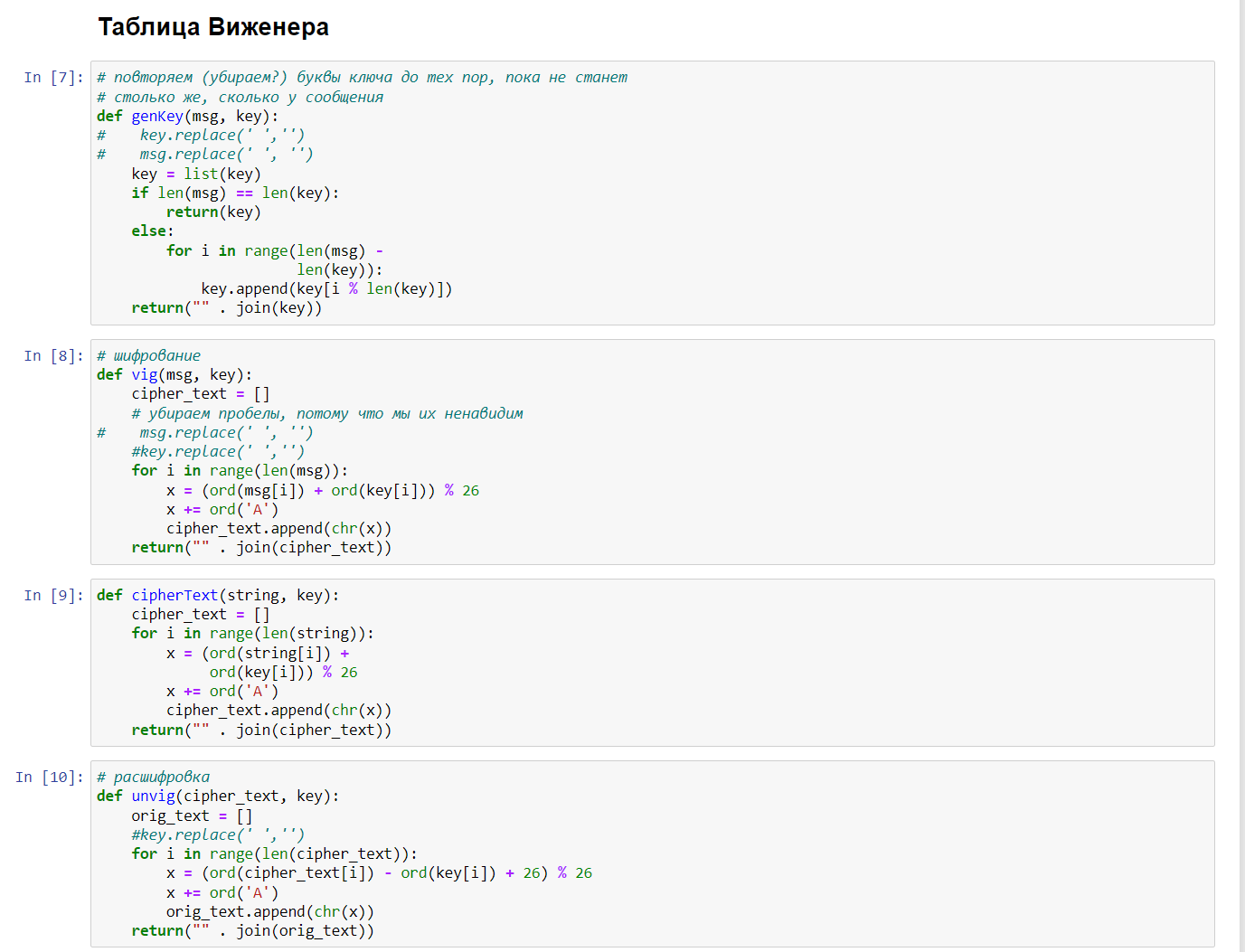


Рис. 6: таблица Виженера

Вывод программы (рис. 7):

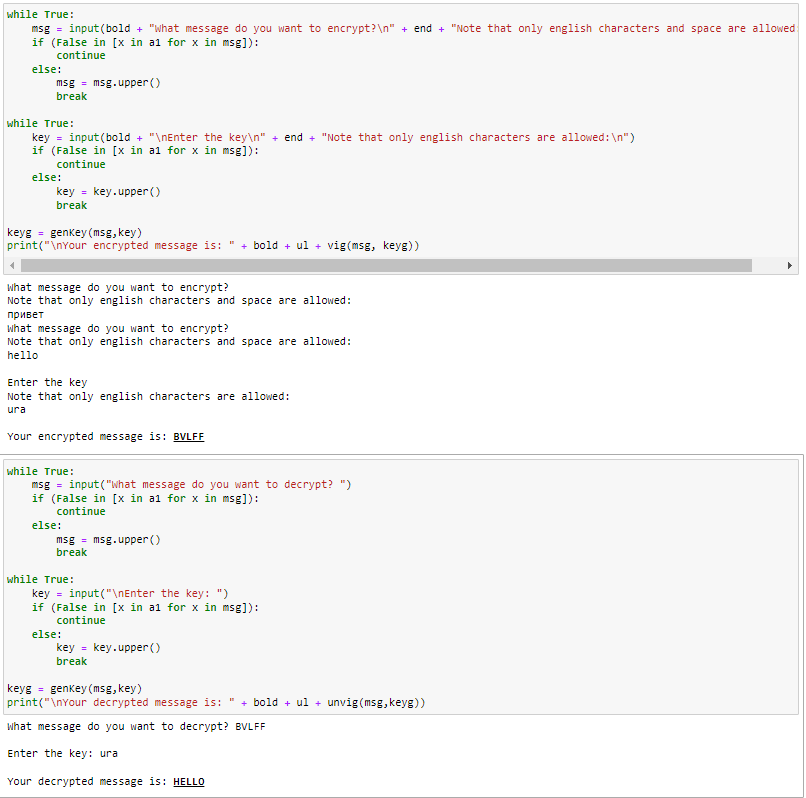


Рис. 7: Вывод программы

# 5 Выводы

Ознакомился с шифрами перестановки и обучился их программной реализации.

# Список литературы

1. ТУИС: Математические основы защиты информации и информационной безопасности (02.04.02) [Электронный ресурс]. РУДН, 2022. URL: <https://esystem.rudn.ru/course/view.php?id=2084>.