Отчёт по лабораторной работе №2

Шифры перестановки

Артур Арменович Давтян

Содержание

# 1 Цель работы

Ознакомиться с шифрами перестановки и обучиться их программной реализации.

# 2 Задание

* Реализовать маршрутное шифрование;
* Реализовать шифрование с помощью решёток;
* Реализовать таблицу виженера.

# 3 Теоретическое введение

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

Шифрование перестановкой заключается в том, что текста переставляются по определенному правилу. 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. Пример — маршрутные шифры перестановки, основанные на прямоугольниках (таблицах). Шифруемое сообщение в этом случае записывается в прямоугольную таблицу по маршруту: по горизонтали, начиная с верхнего левого угла, поочередно слева направо.

Представим, что у нас есть зашифрованное сообщение (рис. 1)

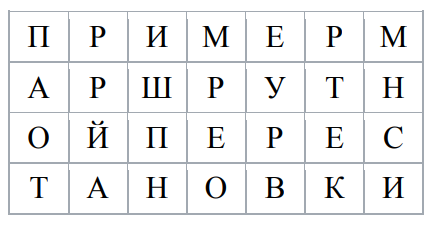


Рис. 1: Пример шифрования перестановкой

Тогда наше зашифрованное сообщение: ПАОТРРЙАИШПНМРЕОЕУРВРТЕКМНСИ.

Шифрование с помощью решёток применяется для защиты информации, представляющую ценность в течение ограниченного времени (несколько часов). Этот шифр также является перестановочным, т.е. криптограммы этого шифра представляют собой анаграммы открытого текста. Данный метод шифрования активно применялся во время второй мировой войны, и до сих пор используется в качестве армейского шифра.

Алгоритм шифрования следующий (рис. 2):

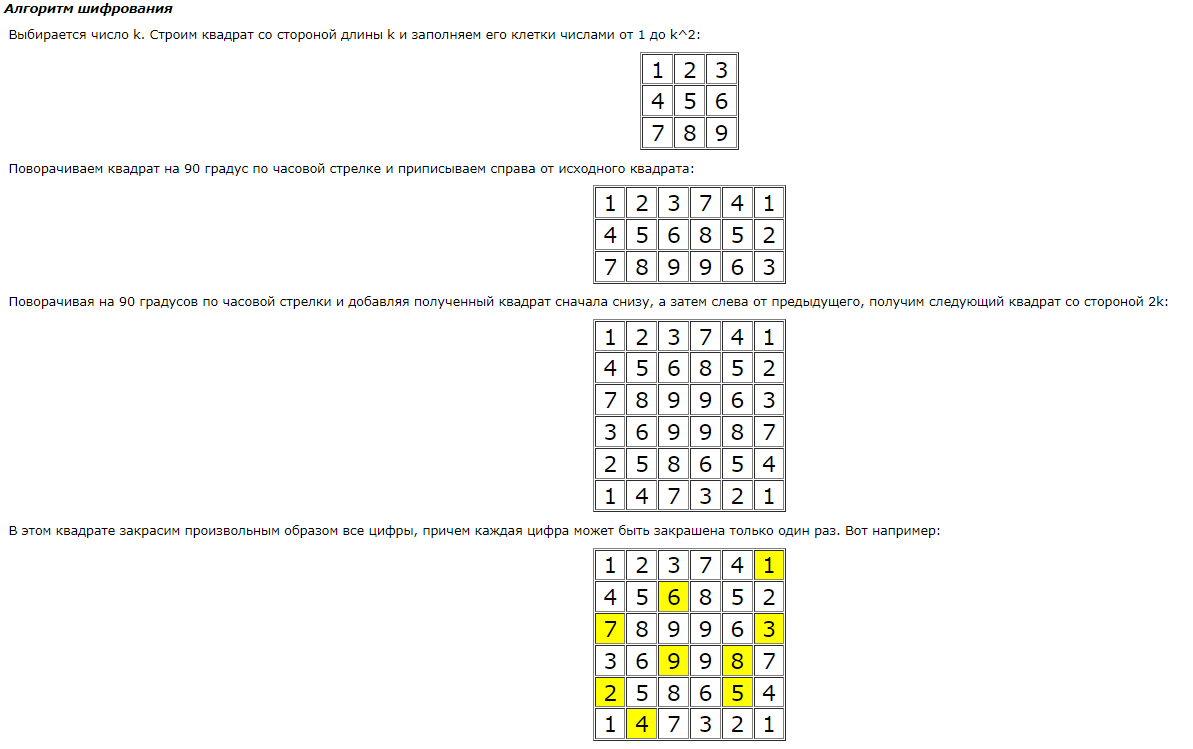


Рис. 2: Алгоритм шифрования с помощью решеток

Шифр Виженера — метод полиалфавитного шифрования буквенного текста с использованием ключевого слова. Этот метод является простой формой многоалфавитной замены. Метод прост для понимания и реализации, он является недоступным для простых методов криптоанализа.

Алгоритм следующий: у нас есть сообщение, которое мы хотим зашифровать, и кодовое слово. Кодовое слово надо повторять до тех пор, пока количество букв не станет равным количеству букв нашего сообщения. Тогда, если буквы A-Z соответствуют числам 0-25, то шифрование Виженера можно записать в виде формулы:

А расшифровку:

# 4 Выполнение лабораторной работы

Работа была выполнена на языке программирования Python.

Реализуем маршрутное шифрование (рис. 3):



Рис. 3: Программная реализация маршрутного шифрования

И расшифровку (рис. 4):

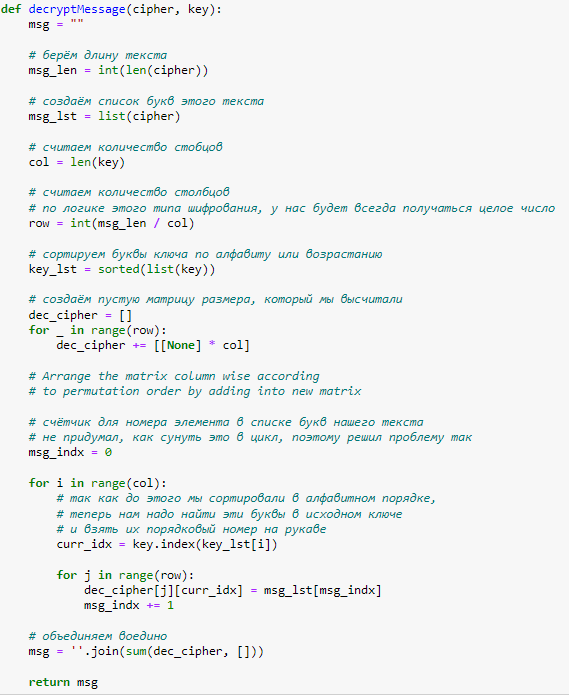


Рис. 4: Программная реализация расшифровки маршрутного шифрования

Сам процесс шифрования и расшифровки (рис. 5):

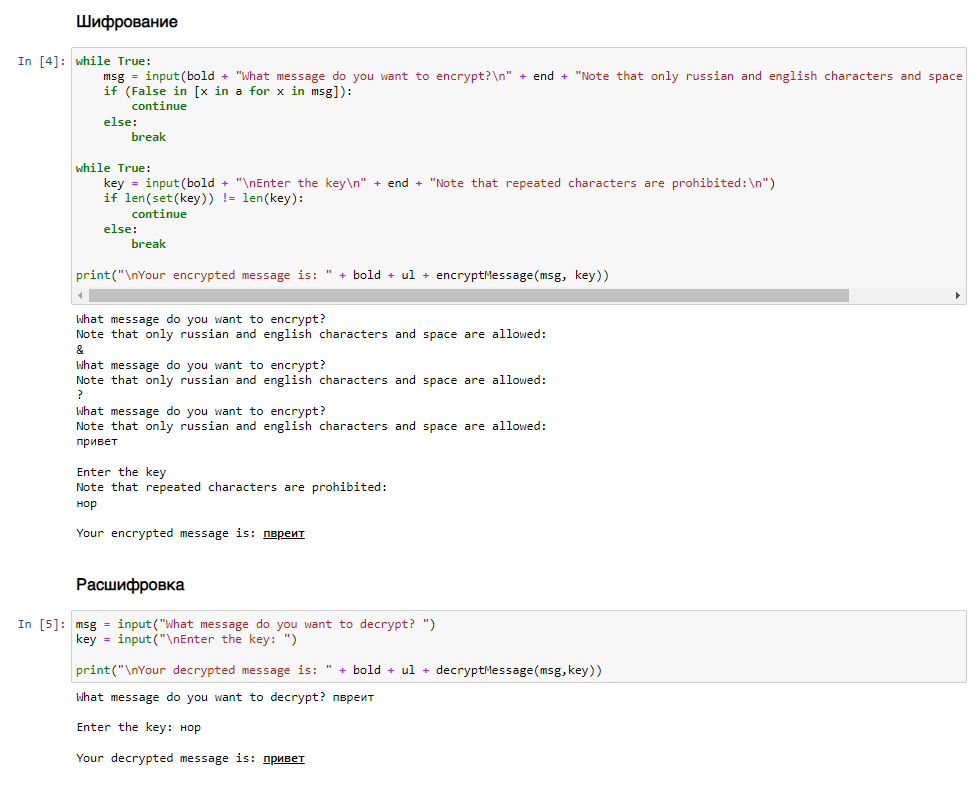


Рис. 5: Шифрование и расшифровка методом маршрутного шифрования

Шифрование методом таблицы Виженера (рис. 6):

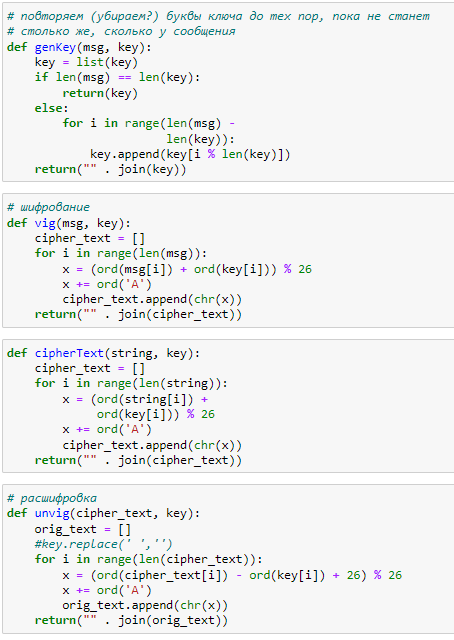


Рис. 6: Программная реализация шифрования методом таблицы Виженера

Сам процесс шифрования и расшифровки (рис. 7):

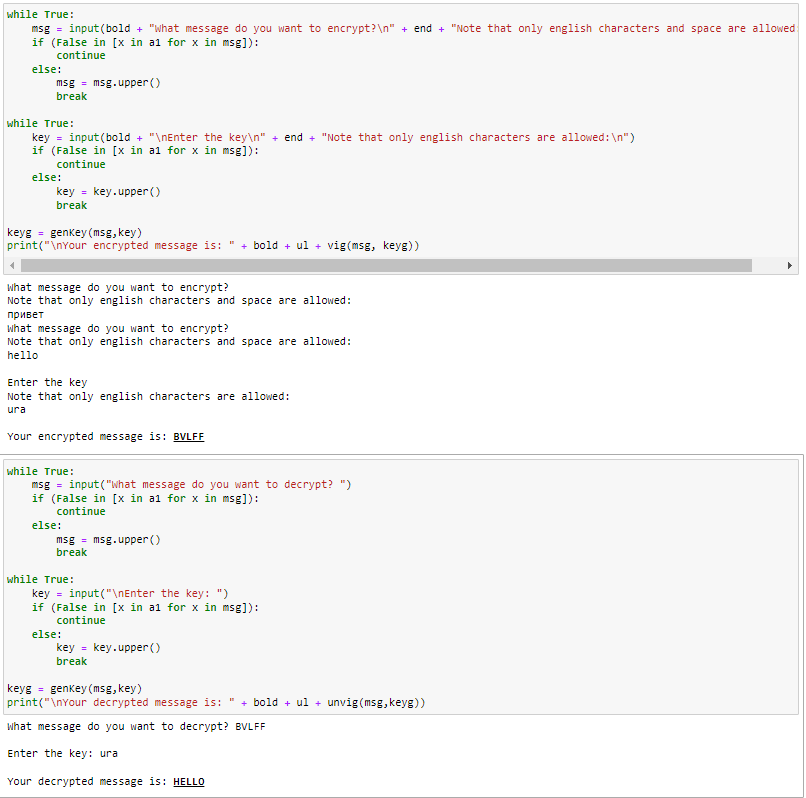


Рис. 7: Шифрование и расшифровка методом таблицы Виженера

# 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>.