Лабораторная работа №2.

Студенка: Царитова Нина Аведиковна

Группа: НФИмд-02-23

Москва 2023

Содержание

# 1 Цель работы

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

# 2 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.

Точное время появления шифра перестановки не известно. Вполне возможно, что писцы в древности переставляли буквы в имени своего царя ради того, чтобы скрыть его подлинное имя или в ритуальных целях. Одно из древнейших известных нам шифровальных устройств — Скитала. Бесспорно известно, что скитала использовалась в войне Спарты против Афин в конце V века до н. э.

Прародителем анаграммы считают поэта и грамматика Ликофрона, который жил в Древней Греции в III веке до н. э. Как сообщал византийский автор Иоанн Цец, из имени царя Птоломея он составил первую из известных нам анаграмм: Ptolemaios — Аро Melitos, что в переводе означает «из мёда», а из имени царицы Арсинои — как «Ion Eras» (фиалка Геры). 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.

# 3 Ход лабораторной работы

## 3.1 Маршрутное шифрование

Программный код реализации маршрутного шифрования представлен ниже.

Реализации маршрутного шифрования

Реализации маршрутного шифрования

Реализации маршрутного шифрования

Результаты выполнения программы представлены ниже.

Результат маршрутного шифрования

## 3.2 Метод решеток

Реализации шифрования с помощью решеток

Реализации шифрования с помощью решеток

Реализации шифрования с помощью решеток

Реализации шифрования с помощью решеток

Реализации шифрования с помощью решеток

Результаты выполнения программы представлены ниже.

Результат шифрования с помощью решеток

## 3.3 Таблица Виженера

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

Реализация Таблицы Виженера

Реализация Таблицы Виженера

Реализация Таблицы Виженера

Реализация Таблицы Виженера

Результаты выполнения программы представлены ниже.

Результат шифрования с помощью Таблица Виженера

# 4 Выводы

Таким образом, я ознакомилась с тремя методами шифрования – маршрутным шифрованием, шифрованием с помощью решеток, таблицей Виженера, – а так же реализовала 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.
2. Википедия. Шифровальная решетка [Электронный ресурс]. Википедия, свободная энциклопедия, 2021. URL: https://en.wikipedia.org/wiki/Grille\_(cryptography).
3. Википедия. Шифр Виженера [Электронный ресурс]. Википедия, свободная энциклопедия, 2021. URL: https://en.wikipedia.org/wiki/Vigen%C3%A8re\_cipher.