Лабораторная работа № 2

Шифры перестановки

Овениязов Артур НФИмд-02-22 1032225418

Содержание

Лабораторная работа №2

[TOC]

Цель работы

Освоить на практике написание шифров перестановки. Таких как маршрутное шифрование и шифр методом Виженера

Задание

1. Реализовать маршрутное шифрование.
2) Реализовать шифр Виженера.

Теоретическое введение

Шифр перестано́вки — 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 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**.

Шифр Виженера (фр. Chiffre de Vigenère) — метод полиалфавитного шифрования буквенного текста с использованием ключевого слова.[1]

Этот метод является простой формой многоалфавитной замены. Шифр Виженера изобретался многократно. Впервые этот метод описал Джовани Баттиста Белласо (итал. Giovan Battista Bellaso) в книге La cifra del. Sig. Giovan Battista Bellaso в 1553 году[2], однако в XIX веке получил имя Блеза Виженера[3], французского дипломата. Метод прост для понимания и реализации, но является недоступным для простых методов криптоанализа.[4]

Хотя шифр легко понять и реализовать, на протяжении трех столетий он противостоял всем попыткам его сломать; чем и заработал имя le chiffre indéchiffrable (фр. неразгаданный шифр). Многие люди пытались реализовать схемы шифрования, которые по сути являлись шифрами Виженера.[5]

Оборудование

Лабораторная работа выполнялась дома со следующими характеристиками техники:

– Ryzen 5600X CPU – ОС Майкрософт Windows 10 – VirtualBox верс. 6.1.26

Код был написан на языке Python3.

Демонстрация работы кода проводилась в продукте Google Colaboratory.

Выполнение лабораторной работы

Шифр Маршрутной перестановки

1. Реализовал Шифр Маршрутной перестановки. Показала создание нового шифровочного алфавита. В качестве ключа использовал использованные в примере слова

   (рис. -@fig:001) Программа

2. Получил следующую криптограмму.

   (рис. -@fig:002) Вывод

Шифр Виженера

1. Реализовал Шифр Виженера. Код будет представлен отдельно, он довольно громоздкий для отчета.

2. Вывод программы шифрования Виженера.

(рис. -@fig:001) Вывод

Получили вывод в виде исходного слова, шифра и дешифра

Выводы

В ходе данной лабораторной работы, написал 2 программы для шифров перестановки Поняла принцип шифрования и освоила написание шифров маршрута и Вижинера на языке Python.

Список литературы

1. Лабораторная работа 2. Шифры перестановки. // Туис URL: https://esystem.rudn.ru/pluginfile.php/1198312/mod_resource/content/2/007-lab_crypto-gamma.pdf (дата обращения: 12.09.2022).