Лабораторная работа №2

Математические основы защиты информации и информационной безопасности

Леонтьева Ксения Андреевна | НПМмд-02-23

Содержание

# 1 Цель работы

Реализовать на языке программирования маршрутное шифрование, шифрование с помощью решеток и таблицу Виженера.

# 2 Теоретическое введение

**Шифры перестановки** преобразуют открытый текст в криптограмму путем перестановки его символов.

**Маршрутное шифрование** разработал французский математик Франсуа Виет. Открытый текст записывают в некоторую геометрическую фигуру, например, прямоугольник, разбив предварительно текст на блоки, длина которых равна количеству букв в пароле (при необходимости дописывают произвольные буквы для достижения нужного количества). Блоки располагаются друг под другом. Затем выписывают столбцы в порядке следования букв в пароле по алфавиту (пароль записывается под прямоугольником).

Более подробно см. в [1].

**Шифрование с помощью решеток** предложил австрийский криптограф Эдуард Флейснер в 1881 году. Формируется решетка, заполненная цифрами от 1 до 4, из которой удаляются некоторые ячейки так, чтобы при последовательных поворотах этой решетки на 90 градусов и записи букв в удаленные ячейки буквы не накладывались друг на друга и можно было записать весь текст (в идеальном случае , где - длина стороны квадрата решетки, а - количество букв в исходном тексте). Затем полученная решетка накладывается на аналогичную, но пустую, и, когда заполняются все прорези буквами исходного текста по порядку их следования, решетка поворачивается на 90 градусов и вписывание букв продолжается. Далее подбирается подходящий пароль (число букв пароля должно равняться и они не должны повторяться), выписываются буквы по столбцами. Очередность столбцов определяется алфавитным порядком букв пароля как в маршрутном шифровании.

Более подробно см. в [2].

**Шифр Виженера** опубликовал в 1585 году французский криптограф Блез Виженер в “Трактате о шифрах”. Он считался нераскрываемым до 1863 года, когда австриец Фридрих Казиски взломал его. Опишем одну из схем построения данного шифра. Формируется таблица, где в строчках записаны буквы русского алфавита (рис. 1). При переходе от одной строке к другой происходит циклический сдвиг на одну позицию. Пароль же записывается с повторениями над буквами сообщения. Далее в горизонтальном алфавите находим букву из исходного текста, в вертикальном - из пароля. На пересечении столбца и строки в таблице распологается нужная буква. Продолжаем так с остальными буквами.

Более подробно см. в [3].

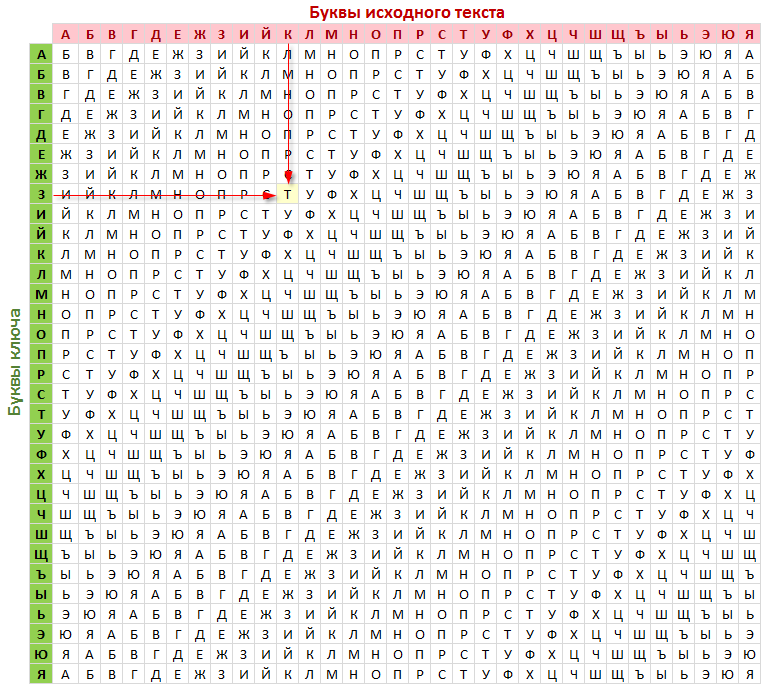


Рис. 1: Таблица Виженера для русского алфавита

# 3 Выполнение лабораторной работы

Начнем с реализации маршрутного шифрования. Переменные phrase и key содержат открытый текст и пароль соответственно. Проверим необходимость добавления в открытый текст дополнительных букв, чтобы текст можно было разбить на равные блоки. Если остаток от деления количества символов в открытом тексте на количество символов в пароле меньше количества символов в пароле, то добавляем в конец текста нужное количество букв. Список block представляет собой список, состоящий из блоков, на которые мы разбили наш открытый текст. Размер каждого блока соответствует количеству символов в пароле.

В список alphabet внесем коды ASCII для букв в пароле. Затем в список new\_alphabet внесем индексы букв из пароля в алфавитном порядке. Список word представляет собой зашифрованную последовательность: сначала выбираем индекс буквы в подсписке blocks в соответствии с алфавитным порядком букв в пароле, а затем выписываем буквы с таким индексом последовательно из каждого подсписка. Наконец, выводим полученную последовательность.

Код программы (рис. 2).



Рис. 2: Маршрутное шифрование

В шифровании с помощью решеток начнем с создания решетки, которая впоследствии будет накладываться на пустую для заполнения. Создаем начальный массив a\_1 и поворачиваем его три раза подряд на 90 градусов. Затем объединяем соответствующие полученные массивы, чтобы получить решетку 4x4. Далее запоминаем в переменные i\_1, i\_2, i\_3, i\_4 индексы цифр 1, 2, 3, 4 и, выбрав, для каждой цифры произвольный индекс, заменяем ее на -1 (“удаляем”). Оставшиеся цифры для удобства заменяем на 0. Делим полученный массив на блоки по 4 цифры в каждом для дальнейшей работы.

Переменная m содержит полученный разделенный на блоки массив, переменная k - пустой список, куда будут записываться буквы. В phrase и key записываем исходный текст и пароль. В indices сохраняем индексы из m, на месте которых стоят -1. Пока список k не будет заполнен полностью повторяем алгоритм: сохраняем текущие индексы с -1 в indices, далее на место этих -1 записываем последовательно буквы из phrase, удаляя после записи каждой буквы ее из phrase, поворачиваем решетку m на 90 градусов, список indices делаем пустым для дальнейшего заполнения. Выводим итоговую табличку k.

Далее код представляет собой аналогичный маршрутному шифрованию и вывод зашифрованного текста.

Код программы (рис. 3 и рис. 4).



Рис. 3: Шифрование с помощью решеток



Рис. 4: Шифрование с помощью решеток

В шифре Виженера аналогично в переменные phrase и key записываем исходную последовательность и пароль. В alphabet - русский алфавит без буквы “ё”. Создаем таблицу (table) из повторения алфавита со сдвигом на одну позицию влево, так называемую таблицу Виженера. В k вычисляем количество повторений пароля целиком и записываем его k раз в key\_list. На оставшиеся свободные места (длина key\_list равна длине исходной фразы) дописываем только часть пароля. Далее печатаем зашифрованную последовательность следующим образом: из таблицы выбираем строку с буквой из исходной фразы phrase и столбец с буквой из key\_list. С помощью цикла последовательно проходимся по соответствующим спискам. Выводим полученную последовательность.

Код программы (рис. 5).



Рис. 5: Таблица Виженера

# 4 Выводы

В ходе выполнения данной лабораторной работы были реализованы маршрутное шифрование, шифрование с помощью решеток и таблица Виженера.

# Список литературы

1. Маршрутное шифрование [Электронный ресурс]. 2021. URL: <https://teletype.in/@hackersacademy/-YilCBTU7Mk>.

2. Шифрование с помощью решеток [Электронный ресурс]. URL: <https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B0%D0%BB%D1%8C%D0%BD%D0%B0%D1%8F_%D1%80%D0%B5%D1%88%D1%91%D1%82%D0%BA%D0%B0>.

3. Таблица Виженера [Электронный ресурс]. URL: <https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80_%D0%92%D0%B8%D0%B6%D0%B5%D0%BD%D0%B5%D1%80%D0%B0>.