

Лабораторная работа №2

Шифры перестановки

Баулин Егор Александрович, НФИмд-02-22

29 сентября 2022

Российский университет дружбы народов, Москва, Россия

Цели и задачи

Знакомство с шифрами перестановки: маршрутным шифрование, шифрованием с помощью решеток, шифрованием при помощи таблицы Виженера.

1. Релизовать маршрутное шифрование.
2. Реализовать шифрование с помощью решеток.
3. Реализовать шифрование при помощи таблицы Виженера.

Выполнение лабораторной работы

Шифры перестановки преобразуют открытый текст в криптограмму путем перестановки его символов. Способ, каким при шифровании переставляются буквы открытого текста, и является ключом шифра. Важным требованием является равенство длин ключа и исходного текста.

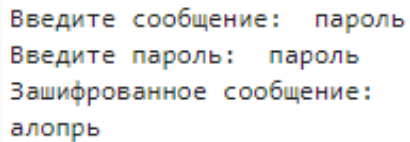
Широкое распространение получили так называемые маршрутные перестановки, использующие некоторую геометрическую фигуру (плоскую или объемную). Преобразования состоят в том, что отрезок открытого текста записывается в такую фигуру по некоторой траектории, а выписывается по другой траектории.

Данный способ шифрования предложил австрийский криптограф Эдуард Флейснер в 1881 году. Суть этого способа заключается в следующем. Выбирается натуральное число $k > 1$, строится квадрат размерности k и построчно заполняется числами $1, 2, \dots, k^2$.

Шифр Виженера — метод полиалфавитного шифрования буквенного текста с использованием ключевого слова.

Этот метод является простой формой многоалфавитной замены. Шифр Виженера изобретался многократно.

Полученные результаты



The diagram illustrates the process of route-based encryption. It consists of four lines of text: 'Введите сообщение: пароль' (Enter message: password), 'Введите пароль: пароль' (Enter password: password), 'Зашифрованное сообщение:' (Encrypted message:), and 'алопрь' (alopry). The text is displayed in a monospaced font with a light blue background.

Введите сообщение: пароль
Введите пароль: пароль
Зашифрованное сообщение:
алопрь

Figure 1: Маршрутное шифрование

Шифрование решетками

```
Введите сообщение: пароль
Сообщение с учетом добавления произвольных символов:
парольюкфяйдщцб
Исходная матрица:
[1, 2]
[3, 4]
Образованная большая таблица k*2:
[1, 2, 3, 1]
[3, 4, 4, 2]
[2, 4, 4, 3]
[1, 3, 2, 1]
Зашифрованное сообщение в списке представлении:
['щ', 'а', 'й', 'п']
['ю', 'к', 'о', 'я']
['ь', 'д', 'б', 'ц']
['л', 'р', 'ч', 'ф']

Введите ключ (длина ключа = 4): абвг
Зашифрованное сообщение в виде словаря до сортировки:
{'а': ['щ', 'а', 'й', 'п'], 'б': ['ю', 'к', 'о', 'я'], 'в': ['ь', 'д', 'б', 'ц'], 'г': ['л', 'р', 'ч', 'ф']}
Зашифрованное сообщение в виде словаря после сортировки:
OrderedDict([('а', ['щ', 'а', 'й', 'п']), ('б', ['ю', 'к', 'о', 'я']), ('в', ['ь', 'д', 'б', 'ц']), ('г', ['л', 'р', 'ч', 'ф'])])
```

Figure 2: Шифрование решетками

Шифрование шифром Виженера

Введите сообщение: пароль

Форматированное сообщение:

пароль

Введите пароль (не превышающий длину сообщения): пароль

Дополненный пароль до длины сообщения:

пароль

Таблица:

абвгдежзийклмнопрстуфхцчщъыьэюя

бвгдежзийклмнопрстуфхцчщъыьэюяа

вгдежзийклмнопрстуфхцчщъыьэюяаб

...

...

эюяабвгдежзийклмнопрстуфхцчщъыь

юяабвгдежзийклмнопрстуфхцчщъыьэ

яабвгдежзийклмнопрстуфхцчщъыьэю

Зашифрованное сообщение:

юааьцш

Figure 3: Шифр Виженера

Выводы

Таким образом в процессе лабораторной работы были изучены реализованы следующие методы шифрования:

- Маршрутное шифрование.
- Шифрование с помощью решеток.
- Шифрование при помощи таблицы Виженера.