Лабораторная работа №2

Шифры перестановки

Легиньких Г.А.

Российский университет дружбы народов, Москва, Россия

Информация

Докладчик

- Легиньких Галина Андреевна
- НПМмд-02-25
- Российский университет дружбы народов
- 1032259346@pfur.ru
- https://github.com/galeginkikh

Цель работы

Целью данной работы является изучение алгоритмов шифрования перестановки, принцип его работы, реализация на Julia.

Выполнение лабораторной работы

Маршрутное шифрование

Этот способ шифрования изобрел выдающийся французский математик и криптограф Франсуа Виет (1540-1603).

Пусть m и n – некоторые натуральные (т.е. целые положительные) числа, каждое больше 1. Открытый текст последовательно разбивается на части (блоки) с длиной, равной произведению mn (если в последнем блоке не хватает букв, можно дописать до нужной длины произвольный их набор). Блок вписывается построчно в таблицу размерности m×n (т.е. m строк и n столбцов). Криптограмма получается выписыванием букв из таблицы в соответствии с некоторым маршрутом. Этот маршрут вместе с числами m и n составляет ключ шифра.

Маршрутное шифрование

Выполнение:

```
PS D:\mathsec\labs\lab2\code> julia Маршрутное_шифрование.jl
hamgses!iss_iteetsta

PS D:\mathsec\labs\lab2\code> julia Маршрутное_шифрование.jl
emhrietgeretgertittdmaidbenne_
```

Шифрование с помощью решеток

Этот способ шифрования предложил в 1881 году австрийский криптограф Эдуард Флейснер. Выбирается натуральное число $k > 1$, и квадрат размерности $k \times k$ построчно заполняется числами $1, 2, \ldots, k$. Для примера возьмем $k = 2$.

Квадрат поворачивается по часовой стрелке на 90° и размещается вплотную к предыдущему квадрату. Аналогичные действия совершаются еще два раза, так чтобы в результате из четырех малых квадратов образовался один большой с длиной стороны $2k$.

Шифрование с помощью решеток

Выполнение:

```
PS D:\mathsec\labs\lab2\code> julia Решетки.jl
,lr!HNdwoeolle W

PS D:\mathsec\labs\lab2\code> julia Решетки.jl
s      d    P@r   !w
```

Таблица Вижинера

Шифр Виженера — метод полиалфавитного шифрования буквенного текста с использованием ключевого слова. Изобрёл французский дипломат Блез де Виженер в XVI веке. ru.wikipedia.org* skillbox.ru Принцип работы: под буквами шифруемого текста записывают слово-ключ, многократно его повторяя. Затем заменяют буквы исходного текста их суммами с буквами ключа. При расшифровке вместо сложения приходится выполнять вычитание. foxford.ru Шифр Виженера считался одним из первых методов шифрования, устойчивых к частотному анализу. Однако по

Таблица Вижинера

Выполнение:

```
PS D:\mathsec\labs\lab2\code> julia Виженера.jl
rijvs uyvjn
```

Выводы

В данной лабораторной работе были изучены три шифра перестановки, все алгоритмы были реализованы на языке Julia и работают корректно.