Лабораторная работа №2

Морозова Ульяна

Российский университет дружбы народов, Москва, Россия

Цели

Целью работы является изучение алгоритмов маршрутного шифрования, шифрования с помощью решеток и шифра Виженера и реализация их на языке Julia.

Маршрутное шифрование

Маршрутное шифрование — это способ перестановочного шифрования, который изобрел французский математик и криптограф Франсуа Виет (1540–1603).

Процесс маршрутного шифрования: 1. Открытый текст последовательно разбивается на части (блоки) с длиной, равной произведению двух натуральных чисел m и n, каждое из которых больше 1. Если в последнем блоке не хватает букв, можно дописать до нужной длины произвольный их набор. 2. Блок вписывается построчно в таблицу размерности m×n (т. е. m строк и n столбцов). 3. Криптограмма получается выписыванием букв из таблицы в соответствии с некоторым маршрутом. Этот маршрут вместе с числами m и n составляет ключ шифра.

```
function route_encrypt(message, key, rows, cols)
        message = filter(!isspace, message)
        matrix = fill('_', rows, cols)
        index = 1
        new_message = ""
        for i = 1:rows
                for j = 1:cols
                        if index != rows * cols
                                matrix[i, j] = message[index]
                                index += 1
                        end
                end
        end
        for j in sort(collect(key))
```

Результат работы шифра

```
julia> route_encrypt("WE ARE REBELS IN OUR HEART", "DIVE", 4,5)
"WRSRREOAEEIHABNE"
```

Шифрование с помощью решеток

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 и построчно заполняется числами 1, 2, ..., k^2.

```
function encrypt_grille(text::String, n::Int)
    grille = create_grille(n)
    grid = fill(' ', n, n)
    padded_text = lpad(text, n*n)
    idx = 1
    for _ in 1:4  # четыре поворота
        for i in 1:n
            for j in 1:n
                if grille[i,j]
                    grid[i,j] = padded_text[idx]
                    idx += 1
                end
            end
        end
```

Выполнение работы кода

Выполнение шифрование фразы “WE ARE RUNNING ALL DAY AND NIGHT”:

```
E   A
 RWNED
U NA R
 NANLI
ILN GD
AGYH T
Дешифровка: WE ARE RUNNING ALL DAY AND NIGHT
```

Шифр Виженера

Шифр Виженера — метод полиалфавитного шифрования, разработанный Блезом Виженером в XVI веке. Это более сложный вариант шифра Цезаря, так как использует несколько сдвигов, определяемых символами ключа.

Главный инструмент — таблица Виженера (или квадрат Виженера) — массив, где каждая строка — это сдвинутая версия алфавита. В каждой ячейке таблицы находится буква, которая представляет результат шифрования определённой комбинации букв открытого текста и ключа.

Код

```
function vigenere_encrypt(text, key)
        alphabet = 'a':'z'
        output = ""
        key_index = 1

        for i in text
                if isletter(i)
                        offset = findfirst(isequal(key[key_index]), alphabet)
                        index = findfirst(isequal(i), alphabet) + offset
                        index > 26 && (index -= 26)
                        output *= alphabet[index]
                        key_index += 1
                        key_index > length(key) && (key_index = 1)
                else
```

Выполнение работы кода

```
julia> vigenere_encrypt("i lose my breathe", "waltz")
"e lzld iy mkdwtsx"
```

Выводы

Мы изучили работу алгоритмов маршрутного шифрования, шифрования с помощью решеток и шифра Виженера, а также реализовали их на языке Julia.