Отчет по лабораторной работе №2

дисциплина: Математические основы защиты информации и информационной безопасности

Морозова Ульяна Константиновна

Содержание

1 Цель работы

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

2 Выполнение лабораторной работы

2.1 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.

Далее приведена реализация шифра на языке Julia.

```
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))
            for i = 1:rows
                new_message *= (matrix[i, (findfirst(j, key))])
            end
        end
        return new_message
end
```

На вход функция принимает слово, которое нужно (де)шифровать, ключ шифра, а также размеры таблицы, куда будет записываться текст.

Результат работы шифра:

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

2.2 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.

Его реализация:

```
function create_grille(n::Int)
    # создаем пустую решетку n x n с отверстиями (true) и не отверстиями (false)
    grille = falses(n, n)
    holes = div(n*n, 4)  # половина отверстий (четверть площади, 4 прохода)
    count = 0
```

```
    for i in 1:n
        for j in 1:n
            if (i + j) % 2 == 1 && count < holes
                grille[i,j] = true
                count += 1
            end
        end
    end
    return grille
end

function rotate_grille(grille)
    # Поворот решетки на 90 градусов по часовой стрелке
    return reverse(transpose(grille), dims=1)
end

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
        grille = rotate_grille(grille)
    end
    return grid
end

function decrypt_grille(grid, n::Int)
    grille = create_grille(n)
    decrypted = ""
    for _ in 1:4
        for i in 1:n
            for j in 1:n
                if grille[i,j]
                    decrypted *= string(grid[i,j])
                end
            end
        end
        grille = rotate_grille(grille)
    end
    return strip(decrypted)
end

n = 6
text = "WE ARE RUNNING ALL DAY AND NIGHT"
encrypted = encrypt_grille(text, n)
for i in 1:n
    println(String(encrypted[i, :]))
end
```

```
decrypted = decrypt_grille(encrypted, n)
println("Дешифровка: ", decrypted)
```

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
```

2.3 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.

```
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) - 1
```

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

        return output
end
```

Результат работы шифра:

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

3 Выводы

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