

# Отчёт по лабораторной работе №2

---

Дарижапов Тимур Андреевич

28 Сентября 2024

РУДН, Москва, Россия

## Отчет по лабораторной работе №2

---

Цель работы: Изучить маршрутное шифрование, шифрование с помощью решёток и таблицу Виженера, научиться реализации данных шифров программным путём.

# Маршрутное шифрование

```
julia> function route_encryption(text, row_length, password)
    text = replace(text, " " => "")

    while length(text) % row_length != 0
        text *= 'a'
    end

    num_rows = div(length(text), row_length)
    table = [collect(text)[i * row_length + 1:(i + 1) * row_length] for i in 0:num_rows-1]
    password_indices = sortperm(collect(password)) # Преобразуем строку в массив символов

    encrypted_text = ""
    for col in password_indices
        for row in 1:num_rows
            encrypted_text *= table[row][col]
        end
    end

    return encrypted_text
end
route_encryption (generic function with 1 method)
```

Рис. 1: Код функции для маршрутного шифрования

## Маршрутное шифрование 2

```
julia> text = "нельзя недооценивать противника"  
"нельзя недооценивать противника"  
  
julia> password = "пароль"  
"пароль"  
  
julia> row_length = 6  
6  
  
julia> println(route_encryption(text, row_length, password))  
еенпнзоатаьовокнеьвдиряцтиа
```

Рис. 2: Начальные данные и результат

# Шифрование с помощью решёток

```
julia> function lattices(text::String, word::String)
    result = ""
    text = replace(text, " " => "")
    matrix = fill(' ', 4, 4) # Создаем двумерный массив (Matrix{Char})

    # Правильная индексация для работы с многобайтовыми символами
    index = 1
    matrix[1, 4] = text[index]
    index = nextind(text, index)

    matrix[3, 2] = text[index]
    index = nextind(text, index)

    matrix[3, 4] = text[index]
    index = nextind(text, index)

    matrix[4, 3] = text[index]
    index = nextind(text, index)

    matrix = rotate90(matrix)

    matrix[3, 2] = text[index]
    index = nextind(text, index)

    matrix[4, 3] = text[index]
    index = nextind(text, index)

    matrix[3, 4] = text[index]
    index = nextind(text, index)

    matrix[1, 4] = text[index]
    index = nextind(text, index)

    matrix = rotate90(matrix)

    matrix[4, 3] = text[index]
    index = nextind(text, index)
```

Рис. 3: Функция заполнения матрицы 1

```
julia> text = "договор подписали"  
"договор подписали"  
  
julia> word = "шифр"  
"шифр"  
  
julia> println(lattices(text, word))  
овордлгпапиосдои
```

Рис. 4: Начальные данные и результат

## Таблица Виженера

```
def vigenere_table(text, keyword):
    alphabet = 'АБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ'
    keyword = keyword.upper()
    text = text.upper().replace(' ', '')
    result = ''

    keyword_repeated = ''
    while len(keyword_repeated) < len(text):
        keyword_repeated += keyword
    keyword_repeated = keyword_repeated[:len(text)]

    for i in range(len(text)):
        if text[i] in alphabet:
            p_index = alphabet.index(text[i])
            k_index = alphabet.index(keyword_repeated[i])
            c_index = (p_index + k_index) % len(alphabet)
            result += alphabet[c_index]
        else:
            text += text[i]
    return result

text = 'криптография серьезная наука'
keyword = 'математика'
print(vigenere_table(text, keyword))
```

Рис. 5: Функция шифрования таблицей Виженера



```
C:\Users\tidaa\PycharmProjects\InfoBez\venv\Scripts\python.exe C:/Users/tidaa/PycharmProjects/InfoBez/venv\Scripts\python.exe C:/Users/tidaa/PycharmProjects/InfoBez/venv\Scripts\python.exe C:/Users/tidaa/PycharmProjects/InfoBez/venv\Scripts\python.exe  
ЦРЬФЯОХШКФЯДКЗЪЧПЧЛНТЩА
```

Рис. 6: Результат вывода

- Я изучил маршрутное шифрование, шифрование с помощью решёток и таблицу Виженера, научился реализации данных шифров программным путём.