

Лабораторна работа №2 - Шифры перестановки

Покрас Илья Михайлович НФИмд-01-24

28 сентября, 2024, Москва, Россия

Российский Университет Дружбы Народов Имени Патриса Лумумбы

Ознакомиться с шифрами перестановки и реализовать программный код маршрутного шифрования, шифрования решеток и шифрования Виженера.

- Создать алгоритм маршрутного шифрования
- Создать алгоритм шифрования с помощью решеток
- Создать алгоритм шифрования Виженера

Маршрутное шифрование

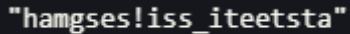
Маршрутное шифрование - код

```
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
```

Рис. 1: Функция маршрутного шифрования

```
message = "this is a test message!"
rows, cols = 4, 5
key = "water"
route_encrypt(message, key, rows, cols)
```

Рис. 2: Инициализация переменных и вызов функции 1



```
"hamgses!iss_iteetsta"
```

Рис. 3: Результат программного кода 1

Шифрование с помощью решеток

Шифрование с помощью решеток - код

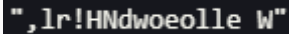
```
def rails_encrypt(text, key, k):
    grid = [[None] * len(text), None]
    rows = [None] * k
    cols = [None] * k
    row = 0
    col = 0
    for i in range(len(text)):
        if row == 0:
            row = k
        elif row == k:
            row = 0
        grid[i][row] = text[i]
        row = row - 1 if row > 0 else k
        col = col + 1 if col < k - 1 else 0
    result = ''
    for i in range(k):
        for j in range(len(text)):
            if grid[j][i] is not None:
                result += grid[j][i]
    return result

def rails_decrypt(text, key, k):
    grid = [[None] * len(text), None]
    rows = [None] * k
    cols = [None] * k
    row = 0
    col = 0
    for i in range(len(text)):
        if row == 0:
            row = k
        elif row == k:
            row = 0
        grid[i][row] = text[i]
        row = row - 1 if row > 0 else k
        col = col + 1 if col < k - 1 else 0
    result = ''
    for i in range(k):
        for j in range(len(text)):
            if grid[j][i] is not None:
                result += grid[j][i]
    return result
```

Рис. 4: Функция шифровани с помощью решеток

```
text = "Hello, New World!"
key = "keys"
k = 2
rails_encrypt(text, key, k)
```

Рис. 5: Инициализация переменных и вызов функций 2



```
“,lr!HNdwoeolle w”
```

Рис. 6: Результат программного кода 2

Шифрование Виженера

Шифрование Виженера - код

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

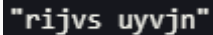
    for i in text
        if isletter(i)
            offset = findfirst(isequal(key[key_index]), alphabet) - 1
            index = findfirst(isequal(i), alphabet) + offset
            index > 26 && (index -= 26)
            output *= alphabet[index]
            key_index += 1
            key_index > length(key)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

    return new_message
end
```

Рис. 7: Функция шифрования Виженера

```
text = "hello world"
key = "key"
encrypted_text = vigenere_encrypt(text, key)
```

Рис. 8: Инициализация переменных и вызов функций 3



"rijvs uyvjn"

Рис. 9: Результат программного кода 3

Я ознакомился с шифрами перестановки и реализовал программный код маршрутного шифрования, шифрования решеток и шифрования Виженера.

Спасибо за внимание
