Лабораторная работа №1

Математические основы защиты информации и информационной безопасности

Николаев Дмитрий Иванович, НПМмд-02-24

6 сентября 2024

Российский университет дружбы народов имени Патриса Лумумбы, Москва, Россия

Прагматика выполнения

Прагматика выполнения

- Освоение шифров простой замены — шифры Цезаря и Атбаша;
- Программная реализация данных шифров на языке Julia.

Цель

Цель

Изучить шифры простой замены, а именно шифр Цезаря и шифр Атбаша. Научиться программной реализации шифра Цезаря с произвольным ключом и шифра Атбаша на языке программирования Julia.

Задачи

Задачи

1. Изучить шифры простой замены — шифры Цезаря и Атбаша.
2. Реализация шифра Цезаря с произвольным ключом на Julia.
3. Реализация шифра Атбаша с произвольным ключом на Julia.

Выполнение работы

Шифр Цезаря 1

```
alphabet = 'a':'z'  # Алфавит
function Caesar_Cipher(Input_Message::String, key::Int)::String
    # Зашифрованное сообщение
    Cipher = String[]
    for char in lowercase(Input_Message)
        if char in alphabet
            position = findfirst(x -> x == char, alphabet)
            # осуществляем сдвиг согласно ключу key
            new_position = mod1(position + key, length(alphabet))
            push!(Cipher, string(alphabet[new_position]))
        else
            # Символ не из алфавита остаётся неизменным
            push!(Cipher, string(char))
        end
```

```
    end
    return join(Cipher)
end
Test_Message = "Veni, vidi, vici"
Test_Key = 3
println("Исходное сообщение: ", Test_Message)
println("Шифр Цезаря с ключом $(Test_Key): ",
        Caesar_Cipher(Test_Message, Test_Key))
println("Обратно расшифрованное сообщение: ",
Caesar_Cipher(Caesar_Cipher(Test_Message, Test_Key), length(alphabet) - Test_
Message_1 = "Si vis pacem, para bellum"
Key_1 = 6
println("\n Исходное сообщение: ", Message_1)
println("Шифр Цезаря с ключом $(Key_1): ",
```

Шифр Цезаря 3

```
PS C:\Users\User\Documents\work\study\2024-2025\Математические
thbase-infosec\labs\lab01\report\report> julia lab1.jl
Исходное сообщение: Veni, vidi, vici
Шифр Цезаря с ключом 3: yhql, ylgl, ylfl
Обратно расшифрованное сообщение: veni, vidi, vici

 Исходное сообщение: Si vis pacem, para bellum
Шифр Цезаря с ключом 6: yo boy vgiks, vgxg hkrras
Обратно расшифрованное сообщение: si vis pacem, para bellum
```

Рис. 1: Результат работы шифра Цезаря

```
function Atbash_Cipher(Input_Message::String)::String
    # Зашифрованное сообщение
    Cipher = String[]
    Reversed_alphabet = reverse(alphabet)
    for char in lowercase(Input_Message)
        if char in alphabet
            position = findfirst(x -> x == char, alphabet)
            # осуществляем сдвиг на весь алфавит
            push!(Cipher, string(Reversed_alphabet[position]))
        else
            # Символ не из алфавита остаётся неизменным
            push!(Cipher, string(char))
        end
    end
```

```
    return join(Cipher)
end
println("\n\nИсходное сообщение: ", Test_Message)
println("Шифр Атбаша: ", Atbash_Cipher(Test_Message))
println("Обратно расшифрованное сообщение: ",
        Atbash_Cipher(Atbash_Cipher(Test_Message)))
Message_1 = "Si vis pacem, para bellum"
Key_1 = 6
println("\n Исходное сообщение: ", Message_1)
println("Шифр Атбаша: ", Atbash_Cipher(Message_1))
println("Обратно расшифрованное сообщение: ",
        Atbash_Cipher(Atbash_Cipher(Message_1)))
```

Шифр Атбаша 3

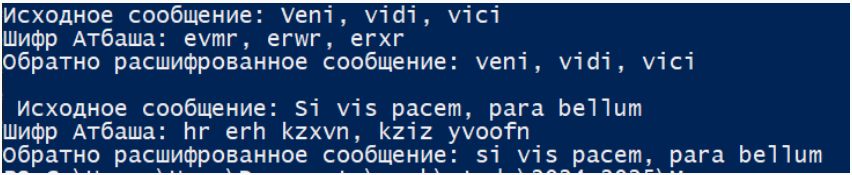

Рис. 2: Результат работы шифра Атбаша

Результаты

Результаты

В ходе работы я изучил шифры простой замены, а именно шифры Цезаря и Атбаша, а также написал программную реализацию шифра Цезаря с произвольным ключом и шифра Атбаша на языке программирования Julia.