Лабораторная работа №7

Информационная безопасность

Николаев Д. И.

13 октября 2023

Российский университет дружбы народов, Москва, Россия

Цели

Цели

Освоить на практике применение режима однократного гаммирования.

Задачи

Задачи

1. Реализовать режим однократного гаммирования;
2. Найти зашифрованный текст по известному исходному тексту и ключу;
3. Найти ключ по известному зашифрованному и исходному тексту.

Выполнение работы

Создание словаря

```
const S = """абвгдеёжзийклмнопрстуфхцчшщъыьэюяАБВГДЕЁЖЗИЙКЛМНОПР
СТУФХЦЧШЩЪЫЬЭЮЯ0123456789., !-"""
const N = length(S)

Dictionary = Dict(zip(S, 1:length(S)))
# Сделаем словарь с ключом и значением наоборот
Dictionary2 = Dict(zip(values(Dictionary), keys(Dictionary)))
```

Получение шифротекста по известному исходному тексту и ключу 1

```
function Gamma_Find_Encrypted_Text(Source_Message::String, Key::String)::Stri
    n = length(Source_Message)  # Длина исходного сообщения
    println("Исходное сообщение - ", Source_Message)
    println("Ключ - ", Key)
    n != length(Key) ? println("Размерности ключа и сообщения не равны") : sk
    Source_Code = []
    Key_Code = []
    for i in Source_Message
        push!(Source_Code, Dictionary[i])
    end
    for i in Key
        push!(Key_Code, Dictionary[i])
    end
    println("Код исходного сообщения - ", Source_Code)
```

Получение шифротекста по известному исходному тексту и ключу 2

```
println("Код ключа - ", Key_Code)
Encrypted_Code = []   # Код зашифрованного сообщения
for i in range(1, n)
    a = Source_Code[i] + Key_Code[i]
    a > N ? a %= N : skip
    push!(Encrypted_Code, a)
end
println("Код зашифрованного сообщения - ", Encrypted_Code)
Encrypted_Message = ""
for i in Encrypted_Code
    Encrypted_Message *= Dictionary2[i]
end
println("Зашифрованное сообщение - ", Encrypted_Message)
```

Получение шифротекста по известному исходному тексту и ключу 3

```
Decrypted_Code = []   # Код зашифрованного сообщения
for i in range(1, n)
    a = Encrypted_Code[i] - Key_Code[i]
    a <= 0 ? a += N : skip
    push!(Decrypted_Code, a)
end
println("Код дешифрованного сообщения - ", Decrypted_Code)
Decrypted_Message = ""
for i in Decrypted_Code
    Decrypted_Message *= Dictionary2[i]
end
println("Дешифрованное сообщение - ", Decrypted_Message)
return Encrypted_Message
```

Получение ключа по известному исходному тексту и шифротексту 1

```
function Gamma_Find_Key_Text(Source_Message::String, Encrypted_Message::Strin
    n = length(Source_Message)  # Длина исходного сообщения
    println("Исходное сообщение - ", Source_Message)
    println("Зашифрованное сообщение - ", Encrypted_Message)
    n != length(Encrypted_Message) ? println("Несоответсвие размерности исход
    Source_Code = []
    Encrypted_Code = []
    for i in Source_Message
        push!(Source_Code, Dictionary[i])
    end
    for i in Encrypted_Message
        push!(Encrypted_Code, Dictionary[i])
    end
    println("Код исходного сообщения - ", Source_Code)
```

Получение ключа по известному исходному тексту и шифротексту 2

```
println("Код зашифрованного сообщения - ", Encrypted_Code)
Key_Code = []   # Код ключа
for i in range(1, n)
    a = Encrypted_Code[i] - Source_Code[i]
    a <= 0 ? a += N : skip
    push!(Key_Code, a)
end
println("Код ключа - ", Key_Code)
Key = ""
for i in Key_Code
    Key *= Dictionary2[i]
end
println("Ключ - ", Key)
return Key
```

Вызов функций

```
Source_Text = "С Новым Годом, друзья!"
Given_Key = "АБВГДЕжзийклмнопрстуфх"

Result_Encrypted_Message = Gamma_Find_Encrypted_Text(Source_Text, Given_Key)
println("Зашифрованное сообщение, имея исходный текст и ключ - ", Result_Encr

Result_Key = Gamma_Find_Key_Text(Source_Text, Result_Encrypted_Message)
println("Ключ, имея исходный текст и зашифрованное сообщение - ", Result_Key)

if Given_Key == Result_Key
    println("Однократное гаммирование работает - успех!")
else
    println("Неудача")
end
```

Результат

```
PS C:\Users\User\Documents\work\study\2022-2023\Информационная безопасность\infosec\labs\lab07\report\report> julia gamma.jl
Исходное сообщение - С Новым Годом, друзья!
Ключ - АБВГДЕжзийклмнопрстуфх
Код исходного сообщения - Any[52, 79, 48, 16, 3, 29, 14, 79, 37, 16, 5, 16, 14, 78, 79, 5, 18, 21, 9, 30, 33, 80]
Код ключа - Any[34, 35, 36, 37, 38, 39, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23]
Код зашифрованного сообщения - Any[5, 33, 3, 53, 41, 68, 22, 7, 47, 27, 17, 29, 28, 12, 14, 22, 36, 40, 29, 51, 55, 22]
Зашифрованное сообщение - дявТЖЦфЁМщпыЪкмфВЁыРФф
Код дешифрованного сообщения - Any[52, 79, 48, 16, 3, 29, 14, 79, 37, 16, 5, 16, 14, 78, 79, 5, 18, 21, 9, 30, 33, 80]
Дешифрованное сообщение - С Новым Годом, друзья!
Зашифрованное сообщение, имея исходный текст и ключ - дявТЖЦфЁМщпыЪкмфВЁыРФф
Исходное сообщение - С Новым Годом, друзья!
Зашифрованное сообщение - дявТЖЦфЁМщпыЪкмфВЁыРФф
Код исходного сообщения - Any[52, 79, 48, 16, 3, 29, 14, 79, 37, 16, 5, 16, 14, 78, 79, 5, 18, 21, 9, 30, 33, 80]
Код зашифрованного сообщения - Any[5, 33, 3, 53, 41, 68, 22, 7, 47, 27, 17, 29, 28, 12, 14, 22, 36, 40, 29, 51, 55, 22]
Код ключа - Any[34, 35, 36, 37, 38, 39, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23]
Ключ - АБВГДЕжзийклмнопрстуфх
Ключ, имея исходный текст и зашифрованное сообщение - АБВГДЕжзийклмнопрстуфх
Однократное гаммирование работает - успех!
PS C:\Users\User\Documents\work\study\2022-2023\Информационная безопасность\infosec\labs\lab07\report\report>
```

Рис. 1: Реализация однократного гаммирования

Результаты

Результаты

По результатам работы, я освоил на практике применение режима однократного гаммирования.