

# Лабораторная работа №8

## Информационная безопасность

---

Николаев Д. И.

14 октября 2023

Российский университет дружбы народов, Москва, Россия

## Цели

---

Освоить на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.

## Задачи

---

1. Реализовать режим однократного гаммирования;
2. Найти текст второго сообщения по известным шифротекстам и первому сообщению.

## Выполнение работы

---

Вместо

$$C_1 \oplus C_2 \oplus P_1 = P_1 \oplus P_2 \oplus P_1 = P_2. \quad (1)$$

имеем следующие выражения

$$C_1 + C_2 \equiv P_1 + K + P_2 + K \equiv P_1 + P_2 + 2K \pmod{N}, \quad (2)$$

$$C_i \equiv P_i + K \pmod{N}, \quad i = 1, 2 \quad (3)$$

$$C_1 + C_2 \equiv P_1 + (C_2 - K) + 2K \equiv P_1 + C_2 + K \pmod{N}, \quad (4)$$

$$P_2 \equiv C_2 - K \equiv C_2 - (C_1 + C_2 - P_1 - C_2) \equiv C_2 - (C_1 - P_1) \pmod{N}. \quad (5)$$

В итоге имеем выражение (6)

$$P_2 \equiv C_2 - C_1 + P_1 \pmod{N}. \quad (6)$$

## Получение текста второго сообщения по шифротекстам и первому сообщению 1

```
include("C:/Users/User/Documents/work/study/2022-2023/
Информационная безопасность/infosec/labs/lab07/report/report/gamma.jl")
function Gamma_Hijack_Message(Source_Message_1::String,
Encrypted_Message_1::String, Encrypted_Message_2::String)
    n1 = length(Source_Message_1) # Длина исходного сообщения 1
    n2 = length(Encrypted_Message_1)
    n3 = length(Encrypted_Message_2)
    println("Первое исходное сообщение - ", Source_Message_1)
    println("Первое зашифрованное сообщение - ", Encrypted_Message_1)
    println("Второе зашифрованное сообщение - ", Encrypted_Message_2)
    n1 != n2 != n3 ? println("Несоответствие размерности исходного и зашифров
Source_Code_1 = []
Encrypted_Code_1 = []
Encrypted_Code_2 = []
```



## Получение текста второго сообщения по шифротекстам и первому сообщению 2

```
for i in Source_Message_1
    push!(Source_Code_1, Dictionary[i])
end
for i in Encrypted_Message_1
    push!(Encrypted_Code_1, Dictionary[i])
end
for i in Encrypted_Message_2
    push!(Encrypted_Code_2, Dictionary[i])
end
println("Код первого исходного сообщения - ", Source_Code_1)
println("Код первого зашифрованного сообщения - ", Encrypted_Code_1)
println("Код второго зашифрованного сообщения - ", Encrypted_Code_2)
Source_Code_2 = []    # Код второго исходного сообщения
```

## Получение текста второго сообщения по шифротекстам и первому сообщению 3

```
for i in range(1, n1)
    a = Encrypted_Code_2[i] - Encrypted_Code_1[i] + Source_Code_1[i]
    a <= 0 ? a += N : skip
    a > N ? a %= N : skip
    push!(Source_Code_2, a)
end

println("Код второго исходного сообщения - ", Source_Code_2)
Source_Message_2 = ""
for i in Source_Code_2
    Source_Message_2 *= Dictionary2[i]
end

println("Второе исходное сообщение - ", Source_Message_2)
return Source_Message_2
end
```

```
P1 = "На Ваш исходящий от 1204" # 24 символа
P2 = " в Северный филиал Банка"
Initial_Key = "АБВГДЕжзийклмнопрстуфхцЧ"
println("Находим первое зашифрованное сообщение")
C1 = Gamma_Find_Encrypted_Text(P1, Initial_Key) # тексты зашифрованных сообще
println("Находим второе зашифрованное сообщение")
C2 = Gamma_Find_Encrypted_Text(P2, Initial_Key)
println("Находим второе сообщение по известным шифротекстам и первому сообщен
Hijacked_P2 = Gamma_Hijack_Message(P1, C1, C2)
if P2 == Hijacked_P2
    println("Взлом второго сообщения прошел успешно!")
else
    println("Неудача")
end
```

```
2022-2023\Информационная безопасность\infosec\labs\lab08\report\report> julia gamma.jl
Находим первое зашифрованное сообщение
Исходное сообщение - На Ваш исходящий от 1204
Ключ - АБВГДЕЖИЙКЛМНОПРСТУФХЦ
Код исходного сообщения - Any[48, 1, 79, 36, 1, 26, 79, 10, 19, 23, 16, 5, 33, 27, 10, 11, 79, 16, 20, 79, 68, 69, 67, 71]
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, 57, 58]
Код зашифрованного сообщения - Any[1, 36, 34, 73, 39, 65, 6, 19, 29, 34, 28, 18, 47, 42, 26, 28, 16, 35, 40, 19, 9, 11, 43, 48]
Зашифрованное сообщение - ЗАБАБЕСАХРЗЪВЕСЗЙИН
Код дешифрованного сообщения - Any[48, 1, 79, 36, 1, 26, 79, 10, 19, 23, 16, 5, 33, 27, 10, 11, 79, 16, 20, 79, 68, 69, 67, 71]
Дешифрованное сообщение - На Ваш исходящий от 1204
Находим второе зашифрованное сообщение
Исходное сообщение - в Северный филиал Банка
Ключ - АБВГДЕЖИЙКЛМНОПРСТУФХЦ
Код исходного сообщения - Any[79, 3, 79, 52, 6, 3, 6, 18, 15, 29, 11, 79, 22, 10, 13, 10, 1, 13, 79, 35, 1, 15, 12, 1]
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, 57, 58]
Код зашифрованного сообщения - Any[32, 38, 34, 8, 44, 42, 14, 27, 25, 40, 23, 11, 36, 25, 29, 27, 19, 32, 18, 56, 23, 38, 69, 59]
Зашифрованное сообщение - юдАжИЗмцЕхИвчмськРхХд2Ш
Код дешифрованного сообщения - Any[79, 3, 79, 52, 6, 3, 6, 18, 15, 29, 11, 79, 22, 10, 13, 10, 1, 13, 79, 35, 1, 15, 12, 1]
Дешифрованное сообщение - в Северный филиал Банка
Находим второе сообщение по известным шифротекстам и первому сообщению без использования ключа
Первое исходное сообщение - На Ваш исходящий от 1204
Первое зашифрованное сообщение - ЗАБАБЕСАХРЗЪВЕСЗЙИН
Второе зашифрованное сообщение - юдАжИЗмцЕхИвчмськРхХд2Ш
Код первого исходного сообщения - Any[48, 1, 79, 36, 1, 26, 79, 10, 19, 23, 16, 5, 33, 27, 10, 11, 79, 16, 20, 79, 68, 69, 67, 71]
Код первого зашифрованного сообщения - Any[1, 36, 34, 73, 39, 65, 6, 19, 29, 34, 28, 18, 47, 42, 26, 28, 16, 35, 40, 19, 9, 11, 43, 48]
Код второго зашифрованного сообщения - Any[32, 38, 34, 8, 44, 42, 14, 27, 25, 40, 23, 11, 36, 25, 29, 27, 19, 32, 18, 56, 23, 38, 69, 59]
Код второго исходного сообщения - Any[79, 3, 79, 52, 6, 3, 6, 18, 15, 29, 11, 79, 22, 10, 13, 10, 1, 13, 79, 35, 1, 15, 12, 1]
Второе исходное сообщение - в Северный филиал Банка
Взлом второго сообщения прошел успешно!
PS C:\Users\User\Documents\work\study\2022-2023\Информационная безопасность\infosec\labs\lab08\report\report>
```

Рис. 1: Реализация взлома однократного гаммирования

## Результаты

---

По результатам работы, я освоил на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.