

Презентация к лабораторной работе 1

Математические основы защиты информации и информационной безопасности

Аристова Арина Олеговна

23 сентября 2025

Российский университет дружбы народов, Москва, Россия

- Аристова Арина Олеговна
- студентка группы НФИмд-01-25
- Российский университет дружбы народов
- 1032259382@rudn.ru
- <https://github.com/aoaristova>



Изучить шифрование простой заменой, в частности шифры Цезаря и Атбаш.

- Реализовать шифр Цезаря с произвольным ключом k
- Реализовать шифр Атбаш

Выполнение лабораторной работы

Программа принимает сообщение, которое необходимо закодировать, ключевое слово и размер сдвига.

Код создает алфавит, в котором сначала ключевое слово, затем остальные символы алфавита в алфавитном порядке, и осуществляет необходимый сдвиг:

```
msg = ARGS[1]  
key_word = ARGS[2]  
key_num = parse(Int, ARGS[3])
```

```
function encrypt()  
    result = ""  
    alph = ""  
    for c in key_word  
        if !(c in alph)  
            alph = alph * c  
        end  
    end
```

Код шифрования шифром Цезаря

```
first_char = msg[1]
if first_char in "абвгдеёжзийклмнопрстуфхцчшщъыьэюя"
for i in "абвгдеёжзийклмнопрстуфхцчшщъыьэюя"
    if !(i in alph)
        alph = alph * i
    end
end
else
for i in "abcdefghijklmnopqrstuvwxyz"
    if !(i in alph)
        alph = alph * i
    end
end
end
end
```

```
alph_vec = collect(alph)    # преобразуем строку в массив символов для рус
for char in msg
    ind = findfirst(char, alph)
    result = result * alph_vec[(ind + key_num - 1) % length(alph_vec) + 1]
end
result
end
a = encrypt()
println(a)
```

Проверяю работу кода, получаю результат, идентичный тому, что был получен мною в результате шифрования вручную:

```
PS C:\Users\arist\Github\study_2025-2026_mathsec\labs\lab01> julia Cezar.jl "hello" "elephant" 2
e1phantbcdfgijkmoqrsuvwxyz
nphhr
PS C:\Users\arist\Github\study_2025-2026_mathsec\labs\lab01> julia Cezar.jl "year" "elephant" 2
e1phantbcdfgijkmoqrsuvwxyz
eptu
```

Рис. 1: Проверка работы шифрования шифром Цезаря

Данная программа принимает на вход сообщение для шифрования и алфавит, переворачивает алфавит и задает результат шифрования теми же индексами

```
msg = ARGS[1]
alph = ARGS[2]
rev = reverse(alph)
function atbash()
    result = ""
    for c in msg
        result = result * rev[findfirst(c, alph)]
    end
    result
end
a = atbash()
println(a)
```

Проверяю работу кода, получаю результат, идентичный тому, что был получен мною в результате шифрования вручную:

```
PS C:\Users\arist\Github\study_2025-2026_mathsec\labs\lab01> julia .\Atbash.jl "abc" "abcdefghij"
jih
PS C:\Users\arist\Github\study_2025-2026_mathsec\labs\lab01> julia .\Atbash.jl "абв" "абвгдеёжи"
изж
PS C:\Users\arist\Github\study_2025-2026_mathsec\labs\lab01> _
```

Рис. 2: Проверка работы шифрования шифром Атбаш

В ходе выполнения данной лабораторной работы мною были получены знания о шифрах простой замены, а также навыки по реализации шифрования простой заменой, а именно шифрами Цезаря и Атбаш.