

# Лабораторная работа №1. Шифры простой замены

Выполнила: Лебедева Ольга Андреевна

РУДН, Москва, Россия

2025

Изучить и реализовать на языке Julia[1] классические методы символьного шифрования - шифр Цезаря[2] и шифр Атбаш[3]. Получить практические навыки программирования функций шифрования, обработки строк и работы с символьными данными.

- 1 Ознакомиться с принципами работы символьных подстановочных шифров.
- 2 Реализовать функцию для шифра Цезаря с параметром сдвига  $k$ .
- 3 Реализовать функцию для шифра Атбаш, основанного на зеркальной замене символов.
- 4 Провести тестирование алгоритмов.

Объект исследования: классические методы шифрования текста.

Предмет исследования: алгоритмы шифрования Цезаря и Атбаш, их реализация средствами Julia.

Шифр Цезаря - моноалфавитный шифр подстановки, в котором каждая буква заменяется на букву, сдвинутую на фиксированное число позиций.

Шифр Атбаш - простой шифр, в котором зеркально заменяются буквы алфавита: А <-> Z, В <-> Y, С <-> X и т.д.

Программное обеспечение:

- Язык программирования Julia.
- Среда разработки JupyterLab / VS Code.

Методы:

- Обработка строковых данных посимвольно.
- Использование арифметики по модулю для циклического сдвига символов.

Шифры подстановки являются одними из древнейших методов защиты информации.

Цезарь впервые использовал сдвиг символов в своих военных сообщениях. Несмотря на простоту, этот метод иллюстрирует базовые принципы символьной криптографии.

Атбаш — древнееврейский шифр, где алфавит полностью отражается: первая буква меняется на последнюю, вторая на предпоследнюю и т. д.

- 1 Реализовать шифр Цезаря с произвольным ключом  $k$ .
- 2 Реализовать шифр Атбаш.



Выполним задание 1 с помощью языка Julia:

```
function ceasar_encrypt(text:: String, k::Int)
    result = IOBuffer()
    for c in text
        if 'a' <= c <= 'z'
            base =Int('a')
            enc = Char((Int(c) - base + k) % 26 + base)
            print(result, enc)
        elseif 'A'<= c <= 'Z'
            base =Int('A')
            enc = Char((Int(c) - base + k) % 26 + base)
            print(result, enc)
        else
            print(result,c)
        end
    end
    return String(take!(result))
end

println(ceasar_encrypt("Hello World", 3))
println(ceasar_encrypt("Hello World", 5))
println(ceasar_encrypt("Hello World", 15))
```

Проверим результат работы кода: См. рис. 1

```
[15]: function caesar_encrypt(text:: String, k::Int)
      result = IOBuffer()
      for c in text
          if 'a' <= c <= 'z'
              base = Int('a')
              enc = Char((Int(c) - base + k) % 26 + base)
              print(result, enc)
          elseif 'A' <= c <= 'Z'
              base = Int('A')
              enc = Char((Int(c) - base + k) % 26 + base)
              print(result, enc)
          else
              print(result, c)
          end
      end
      return String(take!(result))
end

println(caesar_encrypt("Hello World", 3))
println(caesar_encrypt("Hello World", 5))
println(caesar_encrypt("Hello World", 15))

Khoor Zruog
Mjqqt Btwqi
Wtaad Ldgas
```

Рис. 1: Шифр Цезаря

Принцип работы заключается в том, что каждая буква текста заменяется на букву, расположенную в алфавите на фиксированное число позиций вправо (или влево). Например, при сдвиге на 3 буква А превращается в D, В — в Е и так далее. При выходе за пределы алфавита используется циклический переход. Этот метод иллюстрирует идею моноалфавитной подстановки.

Выполним задание 2 с помощью языка Julia:

```
function atbash_encrypt(text:: String)
    result = IOBuffer()
    for c in text
        if 'a' <= c <= 'z'
            base =Int('a')
            enc = Char(base + (25 - (Int(c) - base)))
            print(result, enc)
        elseif 'A'<= c <= 'Z'
            base =Int('A')
            enc = Char(base + (25 - (Int(c) - base)))
            print(result, enc)
        else
            print(result,c)
        end
    end
    return String(take!(result))
end
println(atbash_encrypt("Hello World"))
```

Проверим результат работы кода: См. рис. 2

```
[19]: function atbash_encrypt(text:: String)
      result = IOBuffer()
      for c in text
          if 'a' <= c <= 'z'
              base = Int('a')
              enc = Char(base + (25 - (Int(c) - base)))
              print(result, enc)
          elseif 'A' <= c <= 'Z'
              base = Int('A')
              enc = Char(base + (25 - (Int(c) - base)))
              print(result, enc)
          else
              print(result, c)
          end
      end
      return String(take!(result))
end

println(atbash_encrypt("Hello World"))

Svool Dliow
```

Рис. 2: Шифр Атбаш

Здесь используется зеркальное преобразование алфавита: первая буква заменяется на последнюю, вторая — на предпоследнюю, третья — на предпредпоследнюю и так далее. Таким образом,  $A \leftrightarrow Z$ ,  $B \leftrightarrow Y$ ,  $C \leftrightarrow X$ . Применение алгоритма дважды возвращает исходный текст. Шифр относится к простейшим видам моноалфавитной замены.

- 1 Реализованы функции для шифра Цезаря и Атбаш.
- 2 Проверена корректность работы алгоритмов на тестовых строках.

В ходе работы были изучены два классических шифра — Цезаря и Атбаш. Обе реализации продемонстрировали принципы символьного шифрования — использование циклического сдвига и зеркального отражения алфавита. Получены навыки обработки строк в Julia и закрепились основы криптографии.



- [illegible]