Лабораторная работа №1

Шифры простой замены

Коняева Марина Александровна
НФИмд-01-25
Студ. билет: 1032259383

2025

RUDN

Теоретическое введение

Шифр Цезаря — один из древнейших и наиболее известных алгоритмов шифрования, относящийся к классу моноалфавитных подстановочных шифров. Исторически использовался Юлием Цезарем для защиты военной переписки.

Каждая буква открытого текста заменяется другой буквой, находящейся на фиксированное число позиций (ключ k) дальше в алфавите.

Шифр Атбаш — это древний моноалфавитный шифр подстановки, происходящий из еврейской криптографической традиции. Название “Атбаш” образовано от первых и последних букв еврейского алфавита: Алеф (первая), Тав (последняя), Бет (вторая), Шин (предпоследняя).

Алфавит записывается в прямом порядке, а затем под ним записывается в обратном порядке. Каждая буква открытого текста заменяется на соответствующую букву из обратного алфавита.

Цель работы

Целью данной работы является изучение алгоритмов шифрования Цезарь и Атбаш, принцип его работы, реализация на Julia.

Задание

1. Реализовать шифр Цезаря с произвольным ключем k.
2. Реализовать шифр Атбаш.

Выполнение лабораторной работы

Суть шифра Цезаря заключается в том, что происходит смещение всех букв по алфавиту в сообщении на некоторый коеффициент k. Декодирование происходим путем смещения в обратную сторону.

Далее приведена реализация как для русского так и для английского алфавита одновременно

```
function caesar_cipher(text::String, k::Int)
    ...
    for char in lowercase(text)
      if char in alphabet
       idx = (findfirst(isequal(char),alphabet) - 1
        result *= alphabet[idx + 1]
       else
        result *= char
       end
    end
    return result
end
```

Выполнение лабораторной работы

```
Исходный текст: привет
Зашифрованный:  тулеих
Расшифрованный: привет
```

В качестве параметров скрипт принимает:

- ‘e’ (encrypt) зашифровать сообщение
- ‘d’ (decrypt) расшифровать сообщение
- (Тип: String) Сообщение, с которым нужно произвести действие. Сообщение может содержать буквы русского алфавита, пробелы и знаки препинания.
- (Тип: Int) Значение сдвига в шифре Цезаря. Для русского алфавита должен находиться в промежутке [0, 31], для английского алфавита - в промежутке [0, 26]. При значениях за пределами этих диапазонов применяется операция взятия по модулю.

Выполнение лабораторной работы

Шифр Атбаш, отчасти, похож на шифр Цезаря, но в данном алгоритме разворачивается весь алфавит, а не происходит сдвиг.

```
function atbash_cipher(text::String)
    ...
    result = ""
    for char in lowercase(text)
        if char in alphabet
            result *= dict[char]
        else
            result *= char
        end
    end
    return result
end
```

Выполнение лабораторной работы

```
Исходный текст: шифр
Зашифрованный:  зчлп
Расшифрованный: шифр
```

В качестве параметров скрипт принимает:

- (Тип: Char) Режим работы: расшифровать или зашифровать сообщение. Возможные значения: ‘d’, ‘e’. Для шифра Атбаш оба режима эквивалентны из-за свойства самодвойственности.

  - (Тип: String) Сообщение, с которым нужно произвести действие.
  - (Тип: String) Алфавит, используемый для шифрования. Позволяет указать, какой алфавит использовать для данного сообщения (например, русский или английский).

Вывод

В данной лабораторной работе были изучены два алгоритма шифрования: Цезарь и Атбаш, оба алгоритма были реализованы на языке Julia и работают корректно.

Список литературы. Библиография

[1] Методические материалы курса.

[2] Wikipedia: Caesar cipher (URL: https://en.wikipedia.org/wiki/Caesar_cipher)

[3] Официальная документация по языку Julia (URL: https://docs.julialang.org/).