Лабораторная работа №2: Шифры перестановки"

Дисциплина: Математические основы защиты информации и информационной безопасности"

Савченко Елизавета Николаевна, НПИмд-01-24, 1132249569 **Российский университет дружбы народов, Москва, Россия**

27 сентября 20251

Цель работы

Ознакомиться с классическими примерами шифров простой замены.

Задание

1. Реализовать шифр Цезаря с произвольным ключом k;
2. Реализовать шифр Атбаш.

Теоретическое введение

Виды шифров

Шифры подразделяются на:

- Симметричные;
- Асимметричные.

Виды симметричных шифров

Среди симметричных шифров выделяют:

- Шифры перестановки;
- Шифры подстановки.

Шифры подстановки

:::::::::::::: {.columns align=center} ::: {.column width="50%"}

Шифры подстановки подразделяются на:

- Моноалфавитные шифры;
- Многоалфавитные шифры.

Шифр Цезаря и шифр Атбаш в сравнении

Сходства:

- Моноалфавитные шифры.

Различия:

- Шифр Цезаря использует смещение по кольцу;
- Шифр Атбаш использует зеркальное отражение алфавита.

Выполнение лабораторной работы

1. Реализация шифра Цезаря для произвольного ключа k

```
function shifrCezarya(k::Integer, text::AbstractString)::AbstractString
    k = mod(k, 128)
    println("Text sent to be encoded:\n", text)
    t = filter(isascii,text)
    println("Text to be encoded:\n", t)
    temp = only.(split(t,""))
    for i in 1:length(temp)
        temp[i] = Char(mod(k+Int(temp[i]), 128))
    end
    t = ""
    for i in 1:length(temp)
        t *= string(temp[i])
    end
    return t
end
```

Результат выполнения пункта 1

```
coded_text = shifrCezarya(3, "TEXT to be coded!!!! αβγ and some innocent letters")
println("The result of encoding:\n", coded_text, "\n\n")
decoded_text = shifrCezarya(-131, coded_text)
println("The result of decoding:\n", decoded_text)
```

```
julia> function Cesar_cipher(text::String, k::Int)
          result = IOBuffer()
              for ch in text
              if 'A' <= ch <= 'Я'  # Заглавные русские буквы
                  shifted = Char(mod(Int(ch) - Int('A') + k, 32) + Int('A'))                    print(result, shifted)
                                    elseif 'a' <= ch <= 'я'  # Строчные русские буквы
                  shifted = Char(mod(Int(ch) - Int('a') + k, 32) + Int('a'))                    print(result, shifted)
                                    else
                  # Все другие символы без изменений
                              print(result, ch)
              end
          end
julia> println(caesar_cipher("Молодец!", 2))
Орнржзш!
```

2. Реализация шифра Атбаш

```
function shifrAtbash(text::AbstractString)::AbstractString
    println("Text sent to be encoded:\n", text)
    t = filter(isascii,text)
    println("Text to be encoded:\n", t)
    temp = only.(split(t,""))
    for i in 1:length(temp)
        temp[i] = Char(127-Int(temp[i]))
    end
    t = ""
    for i in 1:length(temp)
        t *= string(temp[i])
    end
    return t
end
```

Результат выполнения пункта 2

```
coded_text = shifrAtbash("TEXT to be coded!!!! αβγ and some innocent letters")
println("The result of encoding:\n", coded_text, "\n\n")
decoded_text = shifrAtbash(coded_text)
println("The result of decoding:\n", decoded_text)
```

```
julia> function atbash_cipher(text::String, k::Int=0)
          # В атбаш обычный ключ не используется, это фиксированное отражение
              # Но если нужен ключ k — реализуем модифицированный атбаш:
          # сначала отражаем буквы, затем сдвигаем результат на k

          function reflect_russian(ch)
                  if 'А' <= ch <= 'Я'
                  return Char(Int('А') + (Int('Я') - Int(ch)))
                          elseif 'а' <= ch <= 'я'
                  return Char(Int('а') + (Int('я') - Int(ch)))
                          else
                  return ch
              end
          end
          function shift_russian(ch, k)
              if 'А' <= ch <= 'Я'
                  return Char(mod(Int(ch) - Int('А') + k, 32) + Int('А'))
                          elseif 'а' <= ch <= 'я'
                  return Char(mod(Int(ch) - Int('а') + k, 32) + Int('а'))
                          else
                  return ch
              end
          end

                  result = IOBuffer()
                      for ch in text
              reflected = reflect_russian(ch)
                          shifted = shift_russian(reflected, k)
              print(result, shifted)
                  end
                      return String(take!(result))
                      end
atbash_cipher (generic function with 2 methods)

julia> println(atbash_cipher("Молодец!", 2))
Хуцуэьл!
```

Выводы по проделанной работе

Вывод

В результате работы мы ознакомились с традиционными моноалфавитными шрифтами простой замены, а именно:

- Шифром Цезаря;
- Шифром Атбаш.

Были записаны скринкасты:

- выполнения лабораторной работы;

- создания отчёта по результатам выполения лабораторной работы;
- создания презентации по результатам выполнения лабораторной работы;
- защиты лабораторной работы.