Лабораторная работа №1: Шифры простой замены

Дисциплина: Математические основы защиты информации и информационной безопасности

Манаева Варвара Евгеньевна, НФИмд-01-24, 1132249514

14 сентября 2024

Российский университет дружбы народов, Москва, Россия

Цель работы

Ознакомиться с классическими примерами шифров простой замены.

Задание

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

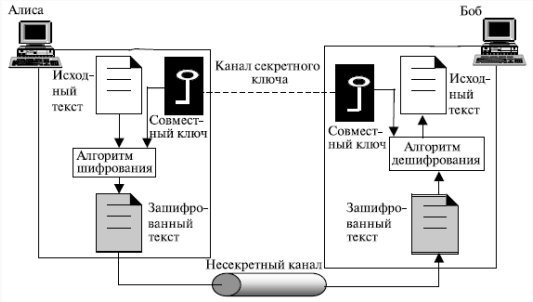
Теоретическое введение

Виды шифров

Шифры подразделяются на:

- Симметричные;
- Асимметричные.

Виды симметричных шифров



Среди симметричных шифров выделяют:

- Шифры перестановки;
- Шифры подстановки.

Шифры подстановки

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
```

Результат выполнения пункта 1

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

```
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)
```

```
Text sent to be encoded:
TEXT to be coded!!!! αβγ and some innocent letters
Text to be encoded:
TEXT to be coded!!!!  and some innocent letters
The result of encoding:
WH[W#wr#eh#frghg$$$$##dqg#vrph#lqqrfhqw#ohwwhuv


Text sent to be encoded:
WH[W#wr#eh#frghg$$$$##dqg#vrph#lqqrfhqw#ohwwhuv
Text to be encoded:
WH[W#wr#eh#frghg$$$$##dqg#vrph#lqqrfhqw#ohwwhuv
The result of decoding:
TEXT to be coded!!!!  and some innocent letters
```

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)
```

]:
```
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)
```

```
Text sent to be encoded:
TEXT to be coded!!!! αβγ and some innocent letters
Text to be encoded:
TEXT to be coded!!!!  and some innocent letters
The result of encoding:
:'+_∂┼_↔→_└┼↔←^^^^__▲◀←_┼↕→_┬◀╫└→◀∂_‼→∂∂→


Text sent to be encoded:
:'+_∂┼_↔→_└┼↔←^^^^__▲◀←_┼↕→_┬◀╫└→◀∂_‼→∂∂→
Text to be encoded:
:'+_∂┼_↔→_└┼↔←^^^^__▲◀←_┼↕→_┬◀╫└→◀∂_‼→∂∂→
The result of decoding:
TEXT to be coded!!!!  and some innocent letters
```

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.