РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук

Кафедра прикладной информатики и теории вероятностей

ОТЧЕТ

ПО ЛАБОРАТОРНОЙ РАБОТЕ № 1

дисциплина: Математические основы защиты информации и информационной безопасности

Студент: Пиняева Анна Андреевна

Группа: НПИмд-01-24

МОСКВА

2025

Теоретическое введение

Шифр Цезаря (также является шифром простой замены) - это моноалфавитная подстановка, т.е. каждой букве открытого текста ставится в соответствие одна буква шифртекста. На практике при создании шифра простой замены в качестве шифроалфавита берется исходный алфавит, но с нарушенным порядком букв (алфавитная перестановка). Для запоминания нового порядка букв перемешивание алфавита осуществляется с помощью пароля. В качестве пароля могут выступать слово или несколько слов с неповторяющимися буквами. Шифровальная таблица состоит из двух строк: первой записывается стандартный алфавит открытого текста, во второй - начиная с некоторой позиции размещается пароль (пробелы опускаются), а далее идут в алфавитном порядке оставшиеся буквы, не вошедшие в пароль. В случае несовпадения начала пароля с началом строки процесс после ее завершения циклически продолжается с первой позиции. Ключом шифра служит пароль вместе с числом, указывающим положение начальной буквы пароля.

Шифр Атбаш. Данный шифря является шифром сдвига на всю длину алфавита.

Цель работы

Знакомство и реализация шифра Цезаря и шифра Атбаш.

Ход работы

1. Шифр Цезаря. Создаем функцию, которая будет шифровать текст с помощью шифра Цезаря с произвольным ключом k. Функция имеет атрибуты: text - исходный текст для шифрования, k - ключ (величина сдвига), alphabet - используемый алфавит; возвращает зашифрованный текст (рис. 1). Замена происходит путем сдвига каждой буквы на фиксированное число позиций в алфавите. Дешифрование происходит путем сдвига в обратнуб сторону. Результаты тестирования функции можно увидеть на рис.2.

Рис. 1 Реализация шифра Цезаря:

[1]:
```
function ceasar(text::String, k::Int; alphabet::String="абвгдежзийклмнопрстуфхцчшщъыьэюя")
    alphabet_chars = collect(alphabet)
    text_chars = collect(text)
    result = ""
    for char in text_chars
        idx=findfirst(isequal(char), alphabet_chars)
        if idx !==nothing
            new_idx = mod1(idx+k, length(alphabet_chars))
            result *= string(alphabet_chars[new_idx])
        else
            result *= string(char)
        end
    end
    return result
end

function ceasar_de(de_text::String, k::Int; alphabet::String="абвгдежзийклмнопрстуфхцчшщъыьэюя")
    return ceasar(de_text, -k, alphabet=alphabet)
end
```

[1]:
```
ceasar_de (generic function with 1 method)
```

N|Solid

Рис. 2 Тестирование шифра Цезаря:

```
[3]: text1="привет"
     key1=3
     encrypted1=
     ceasar(text1, key1)
     descrypted1=
     ceasar_de(encrypted1, key1)
     println("Исходный текст'$text1'")
     println("зашифрованный текст'$encrypted1'")
     println("дешифрованный текст'$descrypted1'")

     Исходный текст'привет'
     зашифрованный текст'тулеих'
     дешифрованный текст'привет'
```

N|Solid

2. Шифр Атбаш. Создаем аналогичную функции Цезаря функцию, но без атрибута k. В функции замена происходит путем “переворачивания” алфавита зеркально. Дешиврование и шифрование одинаковы. Реализация представлена на рис.3. Результаты тестирования функции можно увидеть на рис.4.

Рис. 3 Реализация шифра Атбаш:

```
[4]: function atbash(text::String, alphabet::String="абвгдежзийклмнопрстуфхцчшщъыьэюя")
         alphabet_chars = collect(alphabet)
         text_chars = collect(text)
         result = ""
         for char in text_chars
             idx=findfirst(isequal(char), alphabet_chars)
             if idx !==nothing
                 new_idx = length(alphabet_chars)-idx+1
                 result *= string(alphabet_chars[new_idx])
             else
                 result *= string(char)
             end
         end
         return result
     end
     atbash_de = atbash

[4]: atbash (generic function with 2 methods)
```

N|Solid

Рис. 4 Тестирование шифра Атбаш:

[5]:
```
text2="привет"
encrypted2=
atbash(text2)
descrypted2=
atbash_de(encrypted2)
println("Исходный текст'$text2'")
println("зашифрованный текст'$encrypted2'")
println("дешифрованный текст'$descrypted2'")
```

```
Исходный текст'привет'
зашифрованный текст'рпчэън'
дешифрованный текст'привет'
```

N|Solid

Вывод: В ходе данной работы мной были изучены шифры простой замены: шифр Цезаря и шифр Атбаш. Были получены теоретические и практические навыки реализации этих шифров. Написан программный код на языке Julia для шифрования, дешифрования и тестирования каждого метода.