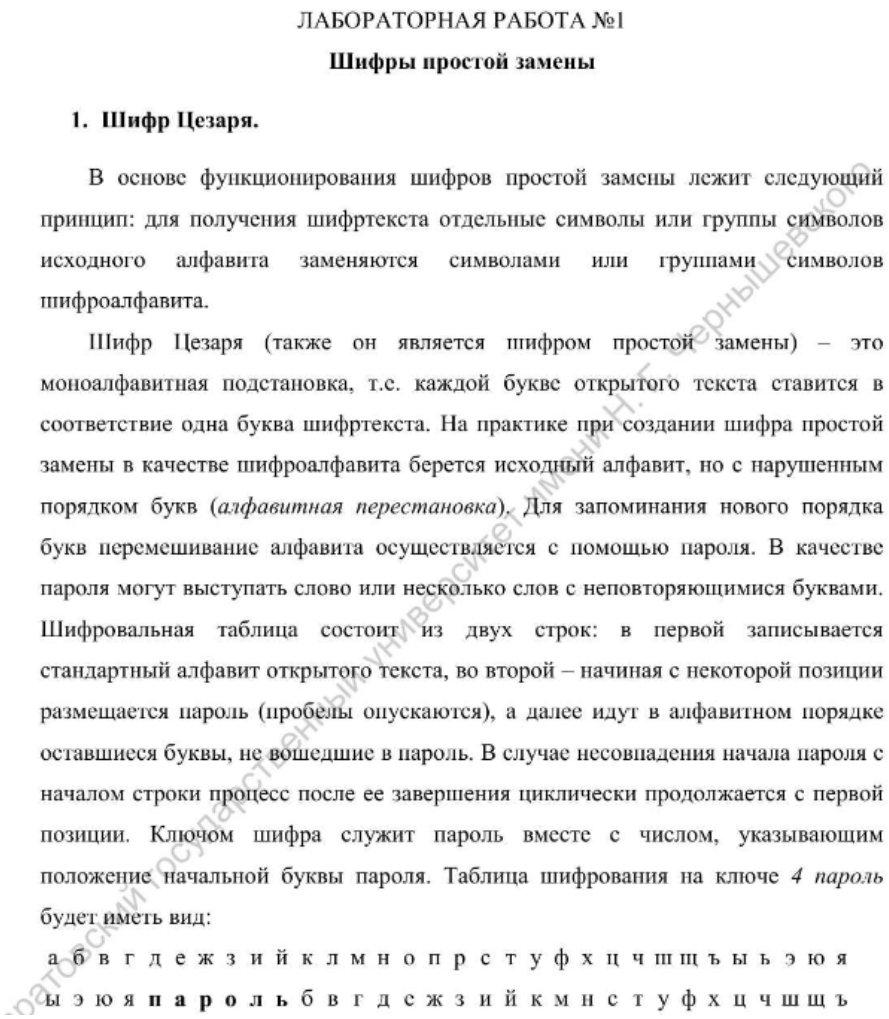
Цель работы

1. Изучить шифры простой замены.
2. Реализовать шифр Цезаря с произвольным ключом k.
3. Реализовать шифр Атбаш.

Выполнение лабораторной работы

1. Изучим файл лабороторной работы №1.



ЛАБОРАТОРНАЯ РАБОТА №1

Шифры простой замены

1. Шифр Цезаря.

В основе функционирования шифров простой замены лежит следующий принцип: для получения шифртекста отдельные символы или группы символов исходного алфавита заменяются символами или группами символов шифроалфавита.

Шифр Цезаря (также он 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: в 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. Таблица шифрования на ключе *4 пароль* будет иметь вид:

а б в г д е ж з и й к л м н о п р с т у ф х ц ч ш щ ъ ы ь э ю я

ы э ю я **п а р о л ь** б в г д е ж з и й к м н с т у ф х ц ч ш щ ъ

Файл лабороторной работы № 1

2. Используя язык программирования Julia приступим к реализации кода для шифра Цезаря с произвольным ключом k.

MathSec > lab1 > lab1.jl > caesar_cipher_encrypt

```julia
function caesar_cipher_encrypt(text::String, k::Int)
    encrypted_text = String[]
    for char in text
        if isletter(char)
            base = isuppercase(char) ? 'A' : 'a'
            shift = k % 26
            encrypted_char = Char((Int(char) - Int(base) + shift) % 26 +
            push!(encrypted_text, string(encrypted_char))
        else
            push!(encrypted_text, string(char))
        end
    end
    return join(encrypted_text)
end

println("Введите фразу для шифрования: ")
text = readline()
println("Введите ключ(сдвиг): ")
k = parse(Int, readline())

encrypted_message = caesar_cipher_encrypt(text, k)
println("Зашифрованное сообщение: $encrypted_message")
```

Реализация кода для шифра Цезаря

3. Запустим написанный код и введем с клавиатуры сначала сообщение, которое нужно зашифровать, а затем ключ(сдвиг), на который будем сдвигать символы по алфавиту.

```
C:\Users\TemaPC\YandexDisk\Учеба\MathSec\lab1>julia lab1.jl
Введите фразу для шифрования:
Hello, world!
Введите ключ(сдвиг):
3
Зашифрованное сообщение: Khoor, zruog!

C:\Users\TemaPC\YandexDisk\Учеба\MathSec\lab1>julia lab1.jl
Введите фразу для шифрования:
Hello
Введите ключ(сдвиг):
27
Зашифрованное сообщение: Ifmmp

C:\Users\TemaPC\YandexDisk\Учеба\MathSec\lab1>julia lab1.jl
Введите фразу для шифрования:
hello
Введите ключ(сдвиг):
26
Зашифрованное сообщение: hello
```

Пример работы шифра Цезаря на языке Julia

4. Приступим к реализации шифра атбаш на языке Julia.

```
MathSec > lab1 > lab12.jl > ...
function atbash_cipher(text::String)
    encrypted_text = String[]


    for char in text
        if isuppercase(char)
            push!(encrypted_text, string(Char('Z' - (char - 'A'))))
        elseif islowercase(char)
            push!(encrypted_text, string(Char('z' - (char - 'a'))))
        else
            push!(encrypted_text, string(char))
        end
    end

    return join(encrypted_text)
end

println("Введите фразу для шифрования: ")
text = readline()

encrypted_message = atbash_cipher(text)
println("Зашифрованное сообщение: $encrypted_message")

```

Реализация кода для шифра Атбаш

5. Запустим написанный код и введем с клавиатуры сообщение, которое нужно зашифровать.

```
C:\Users\TemaPC\YandexDisk\Учеба\MathSec\lab1>julia lab12.jl
Введите фразу для шифрования:
Hello
Зашифрованное сообщение: Svool

C:\Users\TemaPC\YandexDisk\Учеба\MathSec\lab1>julia lab12.jl
Введите фразу для шифрования:
AbC
Зашифрованное сообщение: ZyX

C:\Users\TemaPC\YandexDisk\Учеба\MathSec\lab1>
```

Пример работы шифра Атбаш на языке Julia

Выводы

В рамках данной лабораторной работы были получены практические навыки в написании простых методов шифрования на языке Julia.