Лабораторна работа №1

Шифры простой замены

Покрас Илья Михайлович

Содержание

Список иллюстраций

1 Цель работы

Ознакомиться с шифрами простой замены. Создать программную реализацию шифров Цезаря и Атбаш.

2 Задание

- Создать алгоритм шифрования Цезаря
- Создать алгоритм шифрования Атбаш

3 Теоретическое введение

- Шифр Цезаря — это один из самых простых и древних методов шифрования. Он заключается в замене каждой буквы исходного текста на другую букву, находящуюся на фиксированное число позиций вперед или назад в алфавите. Он получил своё название в честь Гая Юлия Цезаря, римского полководца и диктатора, который использовал этот метод для шифрования военной корреспонденции. Цезарь применял сдвиг на 3 буквы для шифрования сообщений, чтобы сделать их непонятными для противников. Этот метод использовался около 58 года до н.э. Во времена Цезаря шифр был достаточно эффективным, так как многие противники не знали принципа его работы. Однако сегодня шифр Цезаря считается очень слабым с точки зрения криптографии, поскольку количество возможных ключей ограничено.

- Шифр Атбаш — это моноалфавитный шифр замены, в котором буквы алфавита заменяются на свои зеркальные эквиваленты. Принцип работы основан на том, что первая буква алфавита заменяется на последнюю, вторая — на предпоследнюю и так далее. Это делает шифр симметричным: процесс шифрования и расшифрования одинаков.

4 Выполнение лабораторной работы

4.1 Шифр Цезаря

Я создал функцию шифра Цезаря с входными данными: исходным текстом, ключом шифрования и типом операции(true - шифрование и false - дешифрование). Данная функция возвращает зашифрованный текст (рис. 4.1).

```
function caesar(text, key, encrypt)
    alphabet = join([string(letter) for letter in 'a':'z'])
    new_text = ""

    for char in text
        if char in alphabet
                if encrypt == true
                    new_char = alphabet[mod((findfirst(char, alphabet)) + key - 1, 26) + 1]
                else
                    new_char = alphabet[mod((findfirst(char, alphabet)) - key - 1, 26) + 1]
                end
        else
            # println("Warning! Unknown symbol - ",char)
            new_char = char
        end
        new_text *= string(new_char)
    end

    return new_text
end
```

Рис. 4.1: Функция шифра Цезаря

Далее я инициализировал переменную, которая содержит исходный текст и ключ шифрования, после чего с использую эти данные в вызове функции цезаря. Далее полученный результат записываю в новую переменную, которая будет использована как входной параметр для дешифрования. (рис. 4.2).

```
text = "test"
key = 3
encrypted_text = caesar(text, key, true)
println("encrypted text - ", encrypted_text)
decrypted_text = caesar(encrypted_text, key, false)
println("decrypted text - ", decrypted_text)
```

Рис. 4.2: Инициализация переменных и вызов функций

И получил следующий результат (рис. 4.3).

```
encrypted text - whvw
decrypted text - test
```

Рис. 4.3: Результат программного кода

4.2 Шифр Атбаш

Я создал функцию шифра Цезаря с входными данными: исходным текстом, ключом шифрования и типом операции(true - шифрование и false - дешифрование). Данная функция возвращает зашифрованный текст (рис. 4.4).

```
function atbash(text)
    alphabet = join([string(letter) for letter in 'a':'z'])
    reversed_alphabet = reverse(alphabet)
    new_text = ""

    for char in text
        if char in alphabet
            new_char = reversed_alphabet[findfirst(char, alphabet)]
        else
            new_char = char
        end
        new_text *= string(new_char)
    end

    return new_text
end
```

Рис. 4.4: Функция шифра Атбаш

Далее я инициализировал переменную, которая содержит исходный текст и ключ шифрования, после чего с использую эти данные в вызове функции цезаря. Далее полученный результат записываю в новую переменную, которая будет использована как входной параметр для дешифрования. (рис. 4.5).

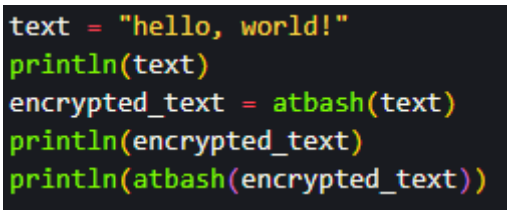

Рис. 4.5: Инициализация переменных и вызов функций

И получил следующий результат (рис. 4.6).

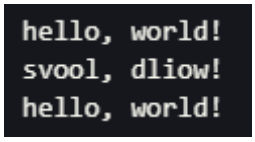

Рис. 4.6: Результат программного кода

5 Выводы

Я ознакомился с шифрами простой замены и создал программную реализацию шифров Цезаря и Атбаш.

Список Литературы

1. Julia - Control Flow
2. Julia - Mathematical Operations
3. Julia - Mathematical Operations
4. Julia - Arrays
5. Julia - Math