Лабораторная работа № 1

Математические основы защиты информации и информационной безопасности

Кузнецов Юрий Владимирович

Содержание

Введение **3**
Основные темы 3

Теоретическое введение **4**
Шифр “Цезаря” 4
Шифр “Атбаш” 5

Ход работы **6**

Заключение **8**

Введение

В данной лабораторной работе будут описаны и реализованы на языке Julia основные концепции шифров “Цезаря” и “Атбаш”

Основные темы

- Шифр “Цезаря”
- Шифр “Атбаш”

Теоретическое введение

Шифр “Цезаря”

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

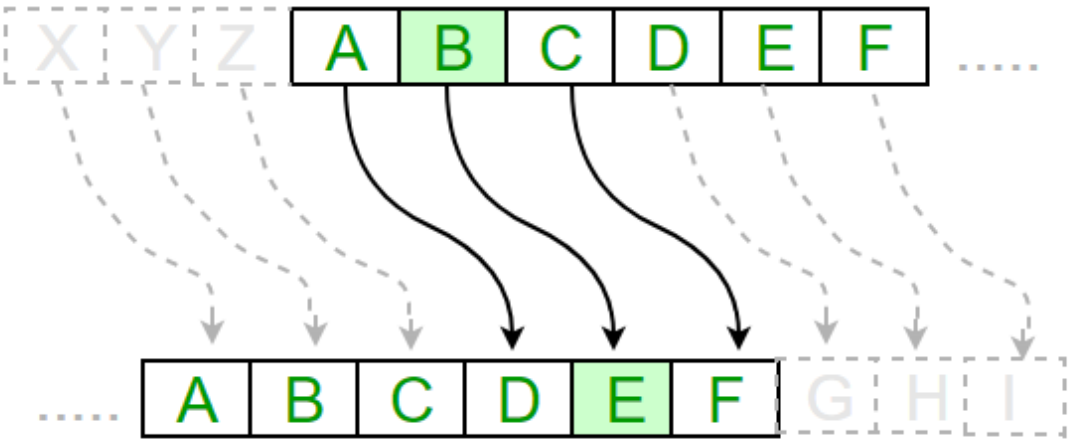

Рис. 1: Ceasar Cipher

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 впароль. Вслучае 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 шифр является шифром сдвига на всю длину алфавита. Для алфавита, состоящего только из русских букв и пробела.

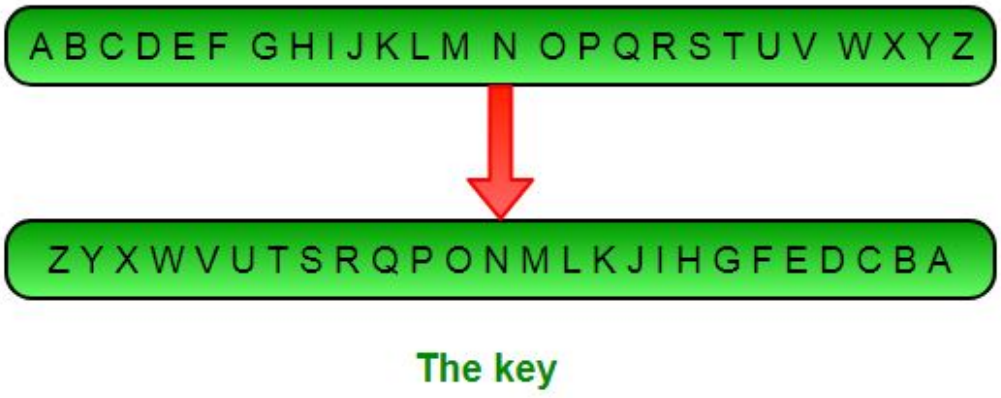

Рис. 2: Atbash cipher

Ход работы

Программная реализация шифра “Цезаря”

В ходе реализации шифра была создана функция, которая принимает такие аргументы как: сообщение, которое требуется зашифровать, а также ключ, по которому будет осуществлено шифрование

```
function cesar(text, shift)
    alphabet = ['A':'Z'; 'a':'z']
    encrypted_text = Char[]

    for char in text
        if char in alphabet
            is_upper = isuppercase(char)
            base = is_upper ? 'A' : 'a'
            encrypted_char = base + ((char - base + shift) % 26)
            push!(encrypted_text, Char(encrypted_char))
        else
            push!(encrypted_text, char)
        end
    end

    return String(encrypted_text)
end

println(cesar("Hello, world", 2));
```

Рис. 1: Ceasar cipher code

Программная реализация шифра “Атбаш”

В отличие от шифра цезаря, шифр “Атбаш” не требует ключа для шифрования строки, соответственно, ниже также была описана функция, принимающая в

себя 1 аргумент (строку)

```
function atbash(message)
  alph_uppercase = ['A':'Z';];
  alph_lowercase = ['a':'z';];

  str = Char[];

  for letter in message
    if letter in alph_uppercase
      index = findfirst(x -> x == letter, alph_uppercase);
      push!(str, alph_uppercase[end - index + 1]);
    elseif letter in alph_lowercase
      index = findfirst(x -> x == letter, alph_lowercase);
      push!(str, alph_lowercase[end - index + 1]);
    else
      push!(str, letter);
    end
  end

  return String(str);
end

println(atbash("Hello, world!"));
```

Рис. 2: Atbash cipher code

Заключение

В ходе выполнения лабораторной работы были закреплены навыки программирования на языке Julia, а также реализованы на ранее упомянутом языке программирования шифры “Цезаря” и “Атбаш”.