

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.

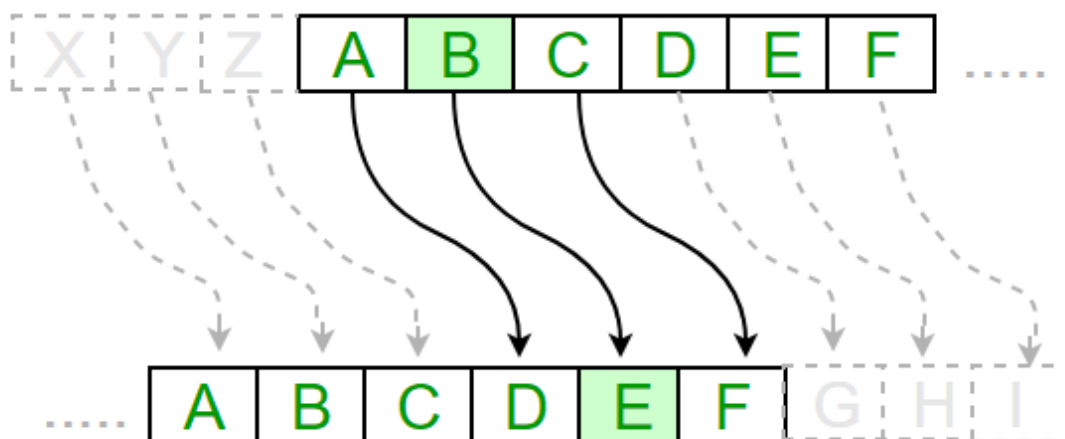


Рис. 1: Ceasar CIPHER

Шифр Цезаря (также он является шифром простой замены) - это моноалфавитная подстановка, т.е. каждой букве открытого текста ставится в соответствие одна буква шифротекста. 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.

Шифр “Атбаш”

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

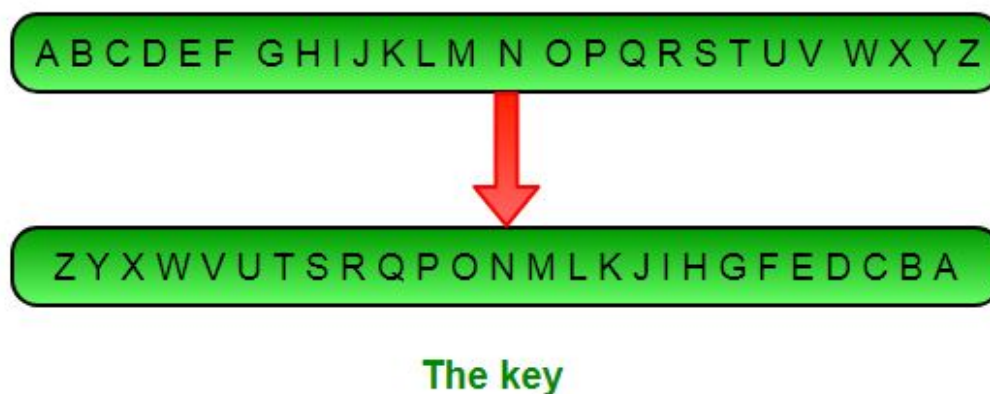


Рис. 2: Atbash cipher

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

A screenshot of a code editor with a dark background and light-colored text. The code is written in Ruby and implements the Caesar cipher. It defines a function 'cesar' that takes 'text' and 'shift' as arguments. The function initializes an 'alphabet' array with uppercase and lowercase letters, and an 'encrypted_text' array. It then iterates over each character in the text. If the character is in the alphabet, it determines if it's uppercase or lowercase, calculates its new position based on the shift, and pushes the encrypted character to the 'encrypted_text' array. If the character is not in the alphabet, it is pushed as-is. Finally, the function returns the 'encrypted_text' as a string. A test call is made at the bottom: 'println(cesar("Hello, world", 2))'.

```
1 function cesar(text, shift)
2   alphabet = ['A':'Z'; 'a':'z']
3   encrypted_text = Char[]
4
5   for char in text
6     if char in alphabet
7       is_upper = isuppercase(char)
8       base = is_upper ? 'A' : 'a'
9       encrypted_char = base + ((char - base + shift) % 26)
10      push!(encrypted_text, Char(encrypted_char))
11    else
12      push!(encrypted_text, char)
13    end
14  end
15
16  return String(encrypted_text)
17 end
18
19 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)



```
1  function atbash(message)
2    alph_uppercase = ['A':'Z'];
3    alph_lowercase = ['a':'z'];
4
5    str = Char[];
6
7    for letter in message
8      if letter in alph_uppercase
9        index = findfirst(x -> x == letter, alph_uppercase);
10       push!(str, alph_uppercase[end - index + 1]);
11     elseif letter in alph_lowercase
12       index = findfirst(x -> x == letter, alph_lowercase);
13       push!(str, alph_lowercase[end - index + 1]);
14     else
15       push!(str, letter);
16     end
17   end
18
19   return String(str);
20 end
21
22 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”.