

Отчет по лабораторной работе №1

Математические основы защиты информации и информационной безопасности

КОНЕ СИРИКИ

2024 Sep 14th

Содержание

1	Цель работы	1
1.1	Реализовать шифр Цезаря произвольным ключом k	1
1.2	Реализовать шифр Атбаш	2
1.3	Результат выполнения шифр Цезаря произвольным ключом k	3
1.4	Результат выполнения шифр Атбаш	4
1.11	Вывод	4

1 Цель работы

Познакомиться с шифры простой замены.

1.1 Реализовать шифр Цезаря произвольным ключом k.

```
2  # Функция шифрования Цезаря
3  function caesar_cipher(text::String, k::Int)
4      encrypted_text = ""
5      for char in text
6          if isletter(char)
7              base = isuppercase(char) ? 'A' : 'a' # Определяем, прописная
              или строчная буква
8              new_char = base + mod((char - base + k), 26) # Вычисляем сдвиг
9              encrypted_text *= Char(new_char)
10         else
11             encrypted_text *= char # Оставляем символы, не являющиеся
              буквами
12         end
13     end
14     return encrypted_text
15 end
16
```

```

17  # Использование:
18  plaintext = "Hello, World!"
19  key = 3 # Произвольный ключ
20  ciphertext = caesar_cipher(plaintext, key)
21  println("Зашифрованный текст: ", ciphertext)
22

```

1.2 Реализовать шифр Атбаш.

```

# Функция шифрования Атбаш
function atbash_cipher(text::String)
    encrypted_text = ""
    for char in text
        if isletter(char)
            base = isuppercase(char) ? 'A' : 'a' # Определяем, прописная или
            строчная буква
            new_char = base + (25 - (char - base)) # Заменяем букву на
            противоположную
            encrypted_text *= Char(new_char)
        else
            encrypted_text *= char # Оставляем символы, не являющиеся буквами
        end
    end
    return encrypted_text
end

# использование:
plaintext = "Hello, World!"
ciphertext = atbash_cipher(plaintext)
println("Зашифрованный текст (Атбаш): ", ciphertext)

```

1.3 Результат выполнения шифр Цезаря произвольным ключом k

```
1  # Функция шифрования Цезаря
2  function caesar_cipher(text::String, k::Int)
3      encrypted_text = ""
4      for char in text
5          if isletter(char)
6              base = isuppercase(char) ? 'A' : 'a' # Определяем, прописная или строчная буква
7              new_char = base + mod((char - base + k), 26) # Вычисляем сдвиг
8              encrypted_text *= Char(new_char)
9          else
10             encrypted_text *= char # Оставляем символы, не являющиеся буквами
11          end
12      end
13      return encrypted_text
14  end
15
16  # Использование:
17  plaintext = "Hello, World!"
18  key = 3 # Произвольный ключ
19  ciphertext = caesar_cipher(plaintext, key)
20  println("Зашифрованный текст: ", ciphertext)
21
```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS

PS C:\Users\KONE> julia "c:\Users\KONE\M1.jl"

C:\Users\KONE>"C:\Users\KONE\AppData\Local\Programs\Julia-1.8.5\bin\julia.exe" c:\Users\KONE\M1.jl

Зашифрованный текст: Khoor, Zruog!

PS C:\Users\KONE>

1.4 Результат выполнения шифр Атбаш

```
C: > Users > KONE > M2.jl > atbash_cipher
1 # Функция шифрования Атбаш
2 function atbash_cipher(text::String)
3     encrypted_text = ""
4     for char in text
5         if isletter(char)
6             base = isuppercase(char) ? 'A' : 'a' # Определяем, прописная или строчная буква
7             new_char = base + (25 - (char - base)) # Заменяем букву на противоположную
8             encrypted_text *= Char(new_char)
9         else
10            encrypted_text *= char # Оставляем символы, не являющиеся буквами
11        end
12    end
13    return encrypted_text
14 end
15
16 # использования:
17 plaintext = "Hello, World!"
18 ciphertext = atbash_cipher(plaintext)
19 println("Зашифрованный текст (Атбаш): ", ciphertext)
20
```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS

```
PS C:\Users\KONE> julia "c:\Users\KONE\M2.jl"

C:\Users\KONE>"C:\Users\KONE\AppData\Local\Programs\Julia-1.8.5\bin\julia.exe" c:\Users\KONE\M2.jl
Зашифрованный текст (Атбаш): Svool, Dliow!
PS C:\Users\KONE>
```

1.11 Вывод

В результате лабораторной работы я повысил навыки использования с шифры простой замены на языке программирования Julia.