Отчёт по лабораторной работе №1  
Математические основы защиты информации и информационной безопасности

Шифры простой замены

Выполнила: Коняева Марина Александровна,  
НФИмд-01-25, 1032259383

Содержание

# Теоретическое введение

Шифр Цезаря — один из древнейших и наиболее известных алгоритмов шифрования, относящийся к классу моноалфавитных подстановочных шифров. Исторически использовался Юлием Цезарем для защиты военной переписки.

Каждая буква открытого текста заменяется другой буквой, находящейся на фиксированное число позиций (ключ k) дальше в алфавите.

Основным недостатком шифра Цезаря является низкая криптостойкость, так как он уязвим к атаке полным перебором (всего n-1 возможных ключей) и частотному анализу.

Шифр Атбаш — это древний моноалфавитный шифр подстановки, происходящий из еврейской криптографической традиции. Название “Атбаш” образовано от первых и последних букв еврейского алфавита: Алеф (первая), Тав (последняя), Бет (вторая), Шин (предпоследняя).

Алфавит записывается в прямом порядке, а затем под ним записывается в обратном порядке. Каждая буква открытого текста заменяется на соответствующую букву из обратного алфавита.

Для алфавита из n символов: C = (n - 1 - P)

где: - P позиция символа в алфавите открытого текста (от 0 до n-1) - C позиция символа в алфавите шифротекста

Особенностью шифра Атбаш является его самодвойственность: процедуры шифрования и дешифрования идентичны, так как двойное применение преобразования возвращает исходный текст.

# Цель работы

Целью данной работы является изучение алгоритмов шифрования Цезарь и Атбаш, принцип его работы, реализация на Julia.

# Задание

1. Реализовать шифр Цезаря с произвольным ключем k.
2. Реализовать шифр Атбаш.

# Выполнение лабораторной работы

## Шифр Цезаря

Суть шифра Цезаря заключается в том, что происходит смещение всех букв по алфавиту в сообщении на некоторый коеффициент k. Декодирование происходим путем смещения в обратную сторону.

Далее приведена реализация как для русского так и для английского алфавита одновременно

function caesar\_cipher(text::String, k::Int)  
 alphabet = 'а':'я' # русский алфавит без ё  
 len = length(alphabet)  
 result = ""  
   
 for char in lowercase(text)  
 if char in alphabet  
 idx = (findfirst(isequal(char), alphabet) - 1 + k) % len  
 result \*= alphabet[idx + 1]  
 else  
 result \*= char # пробелы и знаки препинания не шифруем  
 end  
 end  
 return result  
end  
  
# Пример использования:  
open\_text = "привет"  
k = 3  
encrypted = caesar\_cipher(open\_text, k)  
decrypted = caesar\_cipher(encrypted, -k)  
  
println("Исходный текст: ", open\_text)  
println("Зашифрованный: ", encrypted)  
println("Расшифрованный: ", decrypted)

В качестве параметров скрипт принимает:

* ‘e’ (encrypt) - зашифровать сообщение
* ‘d’ (decrypt) - расшифровать сообщение
* — (Тип: String) Сообщение, с которым нужно произвести действие. Сообщение может содержать буквы русского алфавита, пробелы и знаки препинания.
* — (Тип: Int) Значение сдвига в шифре Цезаря. Для русского алфавита должен находиться в промежутке [0, 31], для английского алфавита - в промежутке [0, 26]. При значениях за пределами этих диапазонов применяется операция взятия по модулю.

Исходный текст: привет  
Зашифрованный: тулеих  
Расшифрованный: привет

## Шифр Атбаш

Шифр Атбаш, отчасти, похож на шифр Цезаря, но в данном алгоритме разворачивается весь алфавит, а не происходит сдвиг.

function atbash\_cipher(text::String)  
 alphabet = collect('а':'я')  
 reversed\_alphabet = reverse(alphabet)  
 dict = Dict(alphabet .=> reversed\_alphabet)  
   
 result = ""  
 for char in lowercase(text)  
 if char in alphabet  
 result \*= dict[char]  
 else  
 result \*= char  
 end  
 end  
 return result  
end  
  
# Пример использования:  
open\_text = "шифр"  
encrypted = atbash\_cipher(open\_text)  
decrypted = atbash\_cipher(encrypted) # Атбаш самодвойственный  
  
println("Исходный текст: ", open\_text)  
println("Зашифрованный: ", encrypted)  
println("Расшифрованный: ", decrypted)

В качестве параметров скрипт принимает:

- — (Тип: Char) Режим работы: расшифровать или зашифровать сообщение. Возможные значения: ‘d’, ‘e’. Для шифра Атбаш оба режима эквивалентны из-за свойства самодвойственности.

* — (Тип: String) Сообщение, с которым нужно произвести действие.
* — (Тип: String) Алфавит, используемый для шифрования. Позволяет указать, какой алфавит использовать для данного сообщения (например, русский или английский).

# Вывод

В данной лабораторной работе были изучены два алгоритма шифрования: Цезарь и Атбаш, оба алгоритма были реализованы на языке Julia и работают корректно.

# Список литературы. Библиография

[1] Методические материалы курса.

[2] Wikipedia: Caesar cipher (URL: https://en.wikipedia.org/wiki/Caesar\_cipher)

[3] Официальная документация по языку Julia (URL: https://docs.julialang.org/).