Лабораторная работа №1

Шифры простой замены

Баулин Егор Александрович, НФИмд-02-22

Содержание

# 1 Цель работы

Знакомство с шифрами простой замены: Цезаря и Атбаш.

# 2 Задание

1. Релизовать шифр Цезаря с произвольным ключом k.
2. Реализовать шифр Атбаш.

# 3 Теоретическое введение

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.Шифр простой замены, простой подстановочный шифр, моноалфавитный шифр — класс методов шифрования, которые сводятся к созданию по определённому алгоритму таблицы шифрования, в которой для каждой буквы открытого текста существует единственная сопоставленная ей буква шифр-текста. Само шифрование заключается в замене букв согласно таблице. Для расшифровки достаточно иметь ту же таблицу, либо знать алгоритм, по которому она генерируется [1].

## 3.1 Шифр Цезаря

Шифр Цезаря, также известный как шифр сдвига, код Цезаря — один из самых простых и наиболее широко известных методов шифрования.Это вид шифра подстановки, в котором каждый символ в открытом тексте заменяется символом, находящимся на некотором постоянном числе позиций левее или правее него в алфавите. Например, в шифре со сдвигом вправо на 3, А была бы заменена на Г, Б станет Д, и так далее [2].

Математически процедуру шифрования можно описать следующим образом:

где — операция нахождения остатка от целочисленного деления на — циклическая подгруппа. Пронумеруем буквы латинского алфавита от 0 до 25: . В латинском алфавите 26 букв и поэтому примем . Тогда операцию шифрования запишем в виде: буква с номером заменяется на букву с номером . Возможно и обобщение шифра Цезаря на случай произвольного ключа : символ с номером заменится на символ с номером .

Таким образом открытый текст преобразуется в криптограмму . При использовании для шифрования подстановки символ открытого текста заменяется символом шифрованного текста. Цезарь обычно для шифрования использовал подстановку .

## 3.2 Шифр Атбаш

Атбаш — простой шифр подстановки для алфавитного письма. Правило шифрования состоит в замене -й буквы алфавита буквой с номером , где — число букв в алфавите. Данный шифр является шифром сдвига на всю длину алфавита [3].

# 4 Выполнение лабораторной работы

## 4.1 Структура программной реализации

## 4.2 Листинг

Для работы программы необходимо определить алфавит при помощи символов таблицы ASCII [4] и символы для игнорирования. При реализации использовались символы латинского алфавита.

FIRST\_SYMBOL\_ASCII = 97  
LAST\_SYMBOL\_ASCII = 122  
alphabet = 26  
IGNORE = " 1234567890.,?!-=:;+\*{}[]<>^"

Шифр Цезаря с произвольным ключом k реализован в функции caesar(), которая принимает на вход три параметра: сообщение, сдвиг и действие.

def caesar(message, shift, action):  
 new\_message = ""  
 for symbol in message:  
 if symbol in IGNORE:  
 new\_message += symbol  
 continue  
 if (action == 1):  
 new\_symbol = chr(FIRST\_SYMBOL\_ASCII + ((ord(symbol) - FIRST\_SYMBOL\_ASCII + shift) % alphabet))  
 else:  
 new\_symbol = chr(FIRST\_SYMBOL\_ASCII + ((ord(symbol) - FIRST\_SYMBOL\_ASCII - shift) % alphabet))  
 new\_message += new\_symbol  
 return new\_message

Шифр Атбаш реализован в функции atbash(), которая принимает на вход три параметра: сообщение и действие.

def atbash(message, action):  
 new\_message = ""  
 for symbol in message:  
 if symbol in IGNORE:  
 new\_message += symbol  
 continue  
 if (action == 1):  
 new\_symbol = chr(FIRST\_SYMBOL\_ASCII + LAST\_SYMBOL\_ASCII - ord(symbol))  
 else:  
 new\_symbol = chr(FIRST\_SYMBOL\_ASCII - ord(symbol) + LAST\_SYMBOL\_ASCII)  
 new\_message += new\_symbol  
 return new\_message

Взаимодействия с программой реализовано в виде наборов ввода/вывода с численными параментрами.

while(True):  
 action = int(input("\nВведите:\n1 - шифр Цезаря\n2 - шифр Атбаш\n0 - для выхода\n"))  
 if (action == 1):  
 action\_1 = int(input("\nВведите:\n1 - шифрование\n2 - расшифровка\n"))  
 message = input("\nВведите сообщение:")  
 shift = int(input("\nВведите сдвиг"))  
 if (action\_1 == 1):  
 result = caesar(message, shift, 1)  
 print("\nШифр Цезаря\nЗашифрованное сообщение:\n{}".format(result))  
 else:  
 result = caesar(message, shift, 2)  
 print("\nШифр Цезаря\nРасшифрованное сообщение:\n{}".format(result))  
 elif (action ==2):  
 action\_2 = int(input("\nВведите:\n1 - шифрование\n2 - расшифровка\n"))  
 message = input("\nВведите сообщение:")  
 if (action == 1):  
 result = atbash(message, 1)  
 print("\nШифр Атбаш\nЗашифрованное сообщение:\n{}".format(result))   
 else:  
 result = atbash(message, 2)  
 print("\nШифр Атбаш\nРасшифрованное сообщение:\n{}".format(result))   
 elif (action == 0):  
 break  
 else:  
 print("Ошибка")

## 4.3 Полученные результаты

В качестве примера работы программы было зашифровано и расшифровано примитивное сообщение из трех первых букв латинского алфавита abc.

В результате шифрования шифром Цезаря с параметром сдвига равным 1, получено сообщение bcd. Шифрование и расшифровка сообщения шифром Цезаря представлена на рисунке 1.

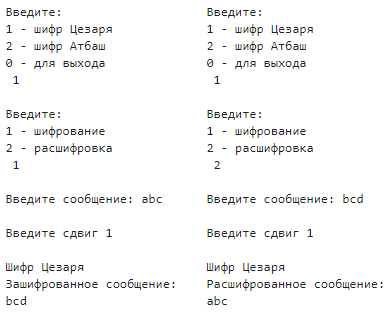


Рис. 1: Шифр Цезаря

В результате шифрования шифром Атбаш получено сообщение zyx. Шифрование и расшифровка сообщения шифром Атбаш представлена на рисунке 2.

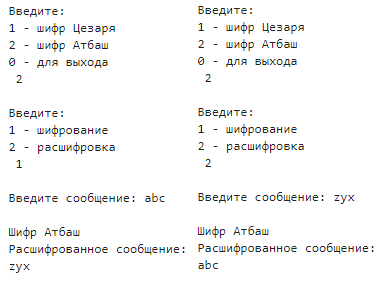


Рис. 2: Шифр Атбаш

# 5 Выводы

Таким образом в процессе лабораторной работы была изучена теоретическая основа шифров простой замены, а также программно реализован шифр Цезаря с с произвольным ключом k и шифр Атбаш.

# Список литературы

1. Шифр Цезаря [Электронный ресурс]. Википедия, 2022. URL: <https://ru.wikipedia.org/wiki/Шифр_простой_замены>.

2. Шифр Цезаря [Электронный ресурс]. Википедия, 2022. URL: <https://ru.wikipedia.org/wiki/Шифр_Цезаря>.

3. Шифр Атбаш [Электронный ресурс]. Википедия, 2022. URL: <https://ru.wikipedia.org/wiki/Атбаш>.

4. Таблица ASCII [Электронный ресурс]. Википедия, 2022. URL: <https://ru.wikipedia.org/wiki/ASCII>.