Лабораторная работа №1

Шифры простой замены

Хохлачева Яна Дмитриевна, НПМмд-02-22

Содержание

Список иллюстраций

Список таблиц

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:

$$T_m = T^j, j = 0, 1, ..., m - 1,$$

$$T^j(a) = (a + j)\, mod\, m,$$

где $(a + j)\, mod\, m$ — операция нахождения остатка от целочисленного деления $a + j$ на m; T_m — циклическая подгруппа. Пронумеруем буквы латинского алфавита от 0 до 25: $a = 0, b = 1, c = 3, ..., z = 25$. В латинском алфавите 26 букв и поэтому примем $m = 26$. Тогда операцию шифрования запишем в виде: буква с номером i заменяется на букву с номером $(i + 3)\, mod\, 26$. Возможно и обобщение шифра Цезаря на случай произвольного ключа k: символ с номером i заменится на символ с номером $(i + k)\, mod\, 26$.

Таким образом открытый текст $a_0, a_1, ..., a_N - 1$ преобразуется в криптограмму $T^j(a_o), T^j(a_1), ..., T^j(a_N - 1)$. При использовании для шифрования подстановки T^j символ a открытого текста заменяется символом $a + j$ шифрованного текста. Цезарь обычно для шифрования использовал подстановку T^3.

3.2 Шифр Атбаш

Атбаш — простой шифр подстановки для алфавитного письма. Правило шифрования состоит в замене i-й буквы алфавита буквой с номером $n - i + 1$, где n — 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

```
FIRST_SYMBOL_ASCII = 97
LAST_SYMBOL_ASCII = 122
alphabet = 26
IGNORE_SYMBOLS = " 1234567890.,?!-=:;*+[]{}<>^"

def caesar(message, shift, code):
    new_message = ""
    for symbol in message:
        if symbol in IGNORE_SYMBOLS:
            new_message += symbol
            continue
        if (code == 1):
            new_symbol = chr(FIRST_SYMBOL_ASCII + ((ord(symbol) - FIRST_SYMBOL_AS
        else:
            new_symbol = chr(FIRST_SYMBOL_ASCII + ((ord(symbol) - FIRST_SYMBOL_AS
        new_message += new_symbol
    return new_message
```

```
def atbash(message, code):
    new_message = ""
    for symbol in message:
        if symbol in IGNORE_SYMBOLS:
            new_message += symbol
            continue
        if (code == 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

while(True):
    code = int(input("\nВведите:\n1 - для работы с шифром Цезаря\n2 - для работы
    if (code == 1):
        code1 = int(input("\nВведите:\n1 - для зашифровки сообщения\n2 - для деши
        message = input("Введите сообщение: ")
        shift = int(input("Задайте сдвиг от 1 до 25: "))
        if (code1 == 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 (code == 2):
        code1 = int(input("\nВведите:\n1 - для зашифровки сообщения\n2 - для деши
        message = input("Введите сообщение: ")
        if (code1 == 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 (code == 0):
        break
    else:
        print("Ошибка ввода")
```

4.3 Полученные результаты

Шифрование и расшифровка сообщения шифром Цезаря представлена на рисунке 4.1.

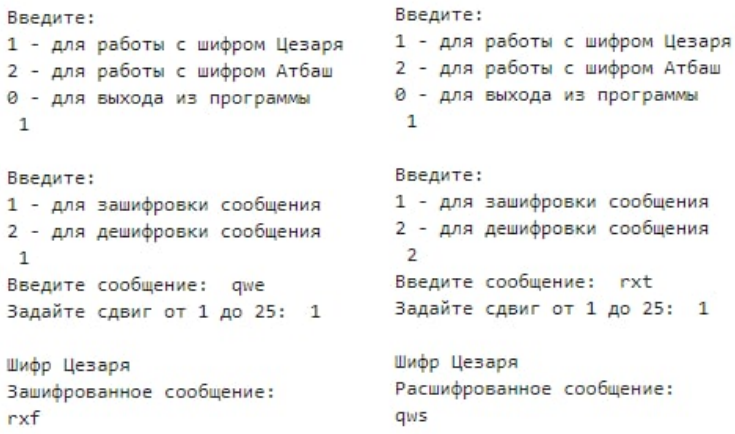

Рис. 4.1: Шифр Цезаря

В результате шифрования шифром Атбаш получено сообщение `zyx`. Шифрование и расшифровка сообщения шифром Атбаш представлена на рисунке 4.2.

```
Введите:
1 - для работы с шифром Цезаря
2 - для работы с шифром Атбаш
0 - для выхода из программы
 2

Введите:
1 - для зашифровки сообщения
2 - для дешифровки сообщения
 1
Введите сообщение:  qwe

Шифр Атбаш
Зашифрованное сообщение:
jdv
```

```
Введите:
1 - для работы с шифром Цезаря
2 - для работы с шифром Атбаш
0 - для выхода из программы
 2

Введите:
1 - для зашифровки сообщения
2 - для дешифровки сообщения
 2
Введите сообщение:  jdv

Шифр Атбаш
Расшифрованное сообщение:
qwe
```

Рис. 4.2: Шифр Атбаш

5 Выводы

Таким образом в процессе лабораторной работы я была изучила теоретические основы шифров простой замены, а также программно реализовала 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.