Математические основы защиты информации и информационной безопасности.Лабораторная работа №1

Шифры простой замены

Студент: Лесков Данила Валерьевич НФИмд-02-21
Преподаватель: Кулябов Дмитрий Сергеевич

Содержание

List of Figures

List of Tables

1 Цель работы

Ознакомиться с шифрами простой замены на примере шифра Цезаря и Атбаш.

2 Задание

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

3 Теоретическое введение

3.1 Шифр Цезаря

Данный шифр замены позволяет зашифровать сообщение путем сдвига каждого символа сообщения на произвольный ключ `j`. Таким образом, можно вывести соотношение для шифра Цезаря [1]:

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

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

где T_m — циклическая подгруппа; $(a+j) mod\, m$ - операция нахождения остатка от целочисленного деления $a + j$ на m.

3.2 Шифр Атбаш

Шифрование Атбаш - шифрование, правило замены которого строится из следующего соотношения:

$$m - n + 1,$$

где переменная m - число букв в алфавите; n - порядковый номер заданного символа. Говоря по простому метод сдвига на порядковый номер буквы в алфавите.

Более подробно о шифрах см. в [1,2].

4 Выполнение лабораторной работы

Для выполнения данной работы были описаны два метода: `caesar(message, shift)` для выполнения алгоритма шифрования Цезаря и `atbash(message)` для шифрования Атбаш. Первый метод принимает исходное сообщение и ключ смещения shift, а второй метод только сообщение. Оба метода возвращают зашифрованное сообщение. В качестве алфавита был выбран английский строчный алфавит, а для взаимодействия с ним была использована таблица ASCII (рис. 4.1).

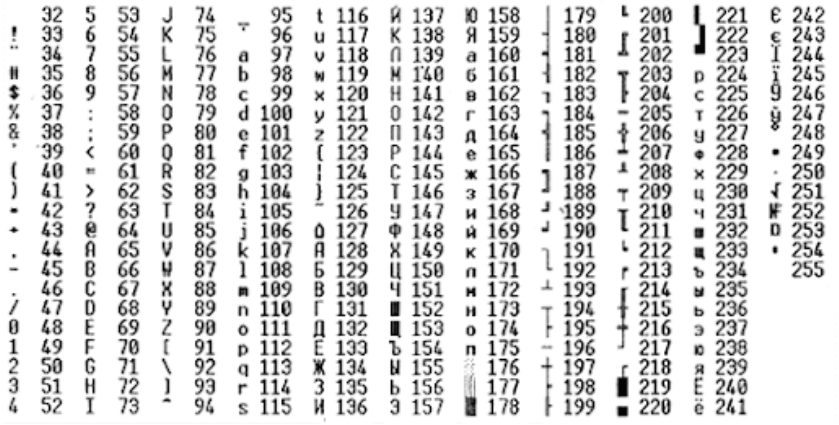

Figure 4.1: Таблица ASCII

На языке python системные методы `ord()` и `chr()` преобразуют строковой символ в порядковый номер ASCII и обратно соответсвенно. Благодаря этим методам в данной лабораторной работе осуществляется работа со смещением символов строковых элементов.

Более подробно о таблице ASCII и методах работы с ней см. в [3,4].

4.1 Листинг кода

Программный код был написан на языке python.

```
FIRST_SYMBOL_ACII = 97
LAST_SYMBOL_ACII = 122
alphabet = {"en": 26}
IGNORE_SYMBOLS = " 1234567890-=./[]';<>*-+|?,!"


def caesar(message, shift):
    new_message = ""
    for symbol in message:
        if symbol in IGNORE_SYMBOLS:
            new_message += symbol
            continue
        new_symbol = chr(FIRST_SYMBOL_ACII +
                         ((ord(symbol) - FIRST_SYMBOL_ACII + shift)
                          % alphabet["en"]))
        new_message += new_symbol
    return new_message


def atbash(message):
    new_message = ""
    for symbol in message:
        if symbol in IGNORE_SYMBOLS:
            new_message += symbol
            continue
        new_symbol = chr(FIRST_SYMBOL_ACII +
```

```
                        LAST_SYMBOL_ACII -
                        ord(symbol))
        new_message += new_symbol
    return new_message


if __name__ == '__main__':
    while (True):
        code = int(input(
            "Нажмите: \n\t"
            "1 - для работы с шифром цезаря;\n\t"
            "2 - для работы с шифром атбаш;\n\t"
            "0 - для выхода из программы.\n"))
        if (code == 1):
            message = input("Введите сообщение: ")
            shift = int(input("Задайте сдвиг (от 1 до 25): "))
            result = caesar(message, shift)
            print("\nЗашифрованное сообщение (Шифр Цезаря):\n{}"
                  .format(result))
        elif (code == 2):
            message = input("Введите сообщение: ")
            result = atbash(message)
            print("\nЗашифрованное сообщение (Шифр Атбаш):\n{}"
                  .format(result))
        elif (code == 0):
            break
        else:
            print("Ошибка ввода!")
```

4.2 Результаты и анализ выполнения

В результате работы программы производится шифрование методом Цезаря и Атбаш. Для взаимодействия пользователя с программой был организован вывод меню в консоль для выбора пользователем алгоритма шифрования. На рис. 4.2 представлен сценарий выполнения программы шифрования Цезаря:

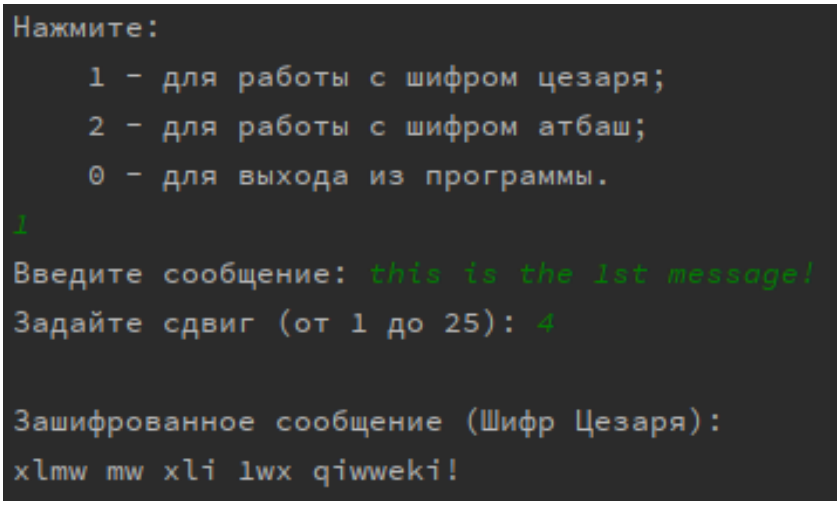

Figure 4.2: Шифр Цезаря

Как видно на рисунке выше, на вход поступает строка, выполняется сдвиг каждой буквы этой строки на 4 символа, а знаки препинания, в свою очередь, остаются без изменений.

На рис. 4.3 представлен сценарий работы программы, если пользователь выбирает шифрование Атбаш:

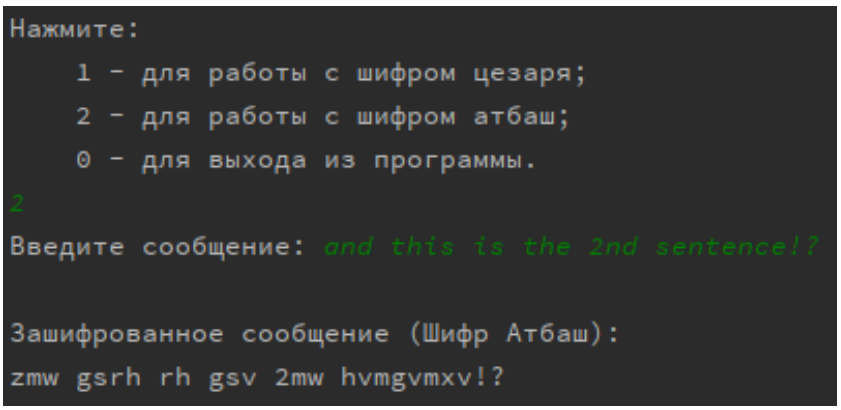

Figure 4.3: Шифр Атбаш

5 Выводы

В ходе выполнения данной лабораторной работы было выполнено ознакомление с шифрами простой замены на примере шиффров Цезаря и Атбаш.
В результате проделанной работы были реализованы методы шифрования Цезаря и Атбаш. Также были получены навыки работы с функциями преобразования строковых символов в таблицу ASCII.
Как итог, поставленные цели и задачи были успешно достигнуты.

Список литературы

1. Шифр Атбаш [Электронный ресурс]. Википедия, 2021. URL: https://ru.wikipedia.org/wiki/Атбаш.
2. Шифр Цезаря [Электронный ресурс]. Википедия, 2021. URL: https://ru.wikipedia.org/wiki/Шифр_Цезаря.
3. Таблица ASCII [Электронный ресурс]. Википедия, 2021. URL: https://ru.wikipedia.org/wiki/ASCII.
4. Функции ord() и chr() в Python [Электронный ресурс]. Pythonim, 2021. URL: https://pythonim.ru/osnovy/ord-chr-python.