

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

Шифры простой замены

Студент: Масолова Анна Олеговна, НФИМд-02-21

Содержание

1	Цель работы	5
2	Задание	6
3	Теоретическое введение	7
3.1	Шифр Цезаря	7
3.2	Шифр Атбаш	8
4	Выполнение лабораторной работы	9
4.1	Листинг	9
4.2	Полученные результаты	12
5	Выводы	16
	Список литературы	17

List of Figures

4.1	Взаимодействие с программой	12
4.2	Шифр Цезаря	13
4.3	Шифр Атбаш	15

List of Tables

1 Цель работы

Познакомиться с шифрами простой замены и реализовать шифры Цезаря и Ат-баш.

2 Задание

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

3 Теоретическое введение

Шифры простой замены — это наиболее часто используемые шифры. Они характеризуются тем, что какие-либо отдельные символы исходного текста заменяются другими символами. При этом замена осуществляется так, чтобы при расшифровке шифрограммы можно было однозначно восстановить исходное сообщение.

3.1 Шифр Цезаря

Данный шифр замены позволяет зашифровать сообщение путем сдвига каждого символа сообщения на произвольный ключ j . Таким образом, можно вывести соотношение:

$$T_m = T^j, j = 0, 1, \dots, m - 1,$$

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

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

3.2 Шифр Атбаш

Данный шифр является шифром сдвига на всю длину алфавита:

$$m - n + 1,$$

где m – число букв в алфавите, n – порядковый номер заданного символа.

Более подробно о шифрах см. в [1,2].

4 Выполнение лабораторной работы

В рамках данной лабораторной работы были описаны алгоритмы двух типов шифрования.

Для программной реализации шифров были использованы таблица ASCII и функции работы с ней (`ord` и `chr`).

Сначала были заданы константы: порядковый номер первого и последнего символов в таблице ASCII, количество символов в алфавите и игнорируемые символы. Для реализации шифра Цезаря была создана функция `caesar(message, shift, code)`, которая в качестве аргументов получает сообщение, ключ и действие, которое необходимо выполнить (шифрование или дешифрование). Для реализации шифра Атбаш создана функция `atbash(message, code)`, в качестве аргументов она получает сообщение и действие – шифрование или дешифрование. Также было реализовано консольное меню для улучшения взаимодействия с пользователем.

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

4.1 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_ASCII + shift) % alphabet))
        else:
            new_symbol = chr(FIRST_SYMBOL_ASCII + ((ord(symbol) -
FIRST_SYMBOL_ASCII - shift) % alphabet))
        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

```

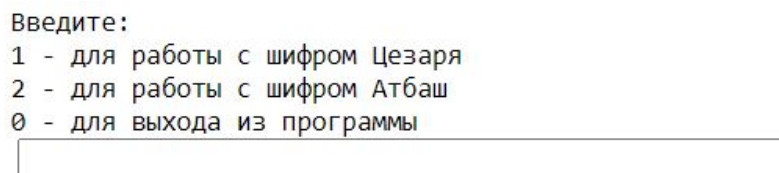
```

while(True):
    code = int(input("\nВведите:\n1 - для работы с шифром Цезаря\n2 -
для работы с шифром Атбаш\n0 - для выхода из программы\n"))
    if (code == 1):
        code1 = int(input("\nВведите:\n1 - для зашифровки сообщения\n2 -
для дешифровки сообщения\n"))
        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 дешифровки сообщения\n"))
        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")

```

4.2 Полученные результаты

В результате выполнения программы пользователю предлагается выбрать действие (рис. 4.1).



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

Figure 4.1: Взаимодействие с программой

Если пользователь хочет использовать шифр Цезаря, то необходимо ввести “1”. Если нужно зашифровать сообщение, то вводится “1”, если дешифровать – “2”. Затем пользователю предлагается ввести сообщение и ключ. Результат выполнения программы представлен на рис 4.2.

Введите:

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

Введите:

- 1 - для зашифровки сообщения
 - 2 - для дешифровки сообщения
- 1

Введите сообщение: banana12

Задайте сдвиг от 1 до 25: 7

Шифр Цезаря

Зашифрованное сообщение:

ihuhuh12

Введите:

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

Введите:

- 1 - для зашифровки сообщения
 - 2 - для дешифровки сообщения
- 2

Введите сообщение: ihuhuh12

Задайте сдвиг от 1 до 25: 7

Шифр Цезаря

Расшифрованное сообщение:

banana12

Figure 4.2: Шифр Цезаря

Для использования шифра Атбаш, нужно ввести “2”. Если нужно зашифровать сообщение, то вводится “1”, если дешифровать – “2”. Затем пользователь вводит сообщение. Результат выполнения программы представлен на рис. 4.3.

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: abcd!

Шифр Атбаш
Зашифрованное сообщение:
zuxw!

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: zuxw!

Шифр Атбаш
Расшифрованное сообщение:
abcd!

Figure 4.3: Шифр Атбаш

Для выхода из программы нужно ввести "0".

5 Выводы

Таким образом, в рамках данной лабораторной работы я познакомилась с шифрами простой замены и реализовала шифры Цезаря и Атбаш.

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>.