Отчёт по лабораторной работе №1. Шифры простой замены

Дисциплина: Математические основы защиты информации и информационной безопасности

Студент: Лапшенкова Любовь Олеговна, 1032217633
Группа: НФИмд-02-21
Преподаватель: д-р.ф.-м.н., проф. Кулябов Дмитрий Сергеевич

13 ноября, 2021, Москва

Прагматика

Прагматика данной лабораторной работы

- В рамках дисциплины “Математические основы защиты информации и информационной безопасности” нам необходимо изучить ее разделы. Данная лабораторная работа входит в раздел “Шифрование”.
- Необходимость выполнения данной работы обусловлена успешным прохождением курса.

Цель

Цель выполнения данной лабораторной работы

- Целью данной лабораторной работы является ознакомление с двумя методами шифрования: шифром Цезаря и шифром Атбаш. Также необходимо реализовать оба шифра на одном из известных языков программирования.

Задачи

Задачи выполнения данной лабораторной работы

- Задачи данной лабораторной работы:

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

Результаты выполнения данной лабораторной работы

Шифр Цезаря

```
def tsezar_code():
    alphabet_kir="абвгдежзийклмнопрстуфхцчшщъыьэюя"#задаем алфавит
    alphabet_latin="abcdefghijklmnopqrstuvwxyz"#задаем алфавит
    k=input('Введите k:',)#просим пользователя ввести k
    k=int(k)#делаем k интовым
    phrase=input('Введите фразу для зашифровки:',)#просим пользователя ввести фразу для зашифровки
    new_phrase=""#задали пустую строку для шифра
    for i in phrase:#прогоняем фразу посимвольно
        if (i==" ") or (i==".") or (i==",") or (i=="!") or (i=="?") or (i==":") or (i==";") or (i=="-"):#проверка условия на наличие определеннных символов
            new_phrase=new_phrase+i#прибавление символа без изменения к шифру
            continue #переход к следующему прогону цикла
        if ((phrase[0] in alphabet_latin) or (phrase[1] in alphabet_latin) or (phrase[2] in alphabet_latin)):#проверка на алфавит
            index=alphabet_latin.find(i)#определяем индекс для буквы из фразы в алфавите
            index=int(index)#делаем интовым
            jindex=(index+k)%(len(alphabet_latin))#расчет нового индекса для шифровки
            new_phrase=new_phrase+alphabet_latin[jindex]#создание шифра
        else:#проверка на алфавит
            index=alphabet_kir.find(i)#определяем индекс для буквы из фразы в алфавите
            index=int(index)#делаем интовым
            jindex=(index+k)%(len(alphabet_kir))#расчет нового индекса для шифровки
            new_phrase=new_phrase+alphabet_kir[jindex]#создание шифра
    print('Зашифрованная фраза:',new_phrase)#вывод шифра
tsezar_code()#запуск функции
```

Figure 1: Шифр Цезаря

Шифр Атбаш

```
def atbash_code():
    alphabet_kir_2="абвгдежзийклмнопрстуфхцчшщъыьэюя "#задаем алфавит с пробелом
    alphabet_latin_2="abcdefghijklmnopqrstuvwxyz "#задаем алфавит с пробелом
    rev_alphabet_kir_2=alphabet_kir_2[::-1]#все элементы списка в обратном порядке
    rev_alphabet_latin_2=alphabet_latin_2[::-1]#все элементы списка в обратном порядке
    phrase=input('Введите фразу для зашифровки:',)#просим пользователя ввести фразу для зашифровки
    new_phrase=""#задали пустую строку для шифра
    for i in phrase:#прогоняем фразу посимвольно
        if ((phrase[0] in alphabet_latin_2) or (phrase[1] in alphabet_latin_2) or (phrase[2] in alphabet_latin_2)):#проверка на алфавит
            index=alphabet_latin_2.find(i)#определяем индекс для буквы из фразы в алфавите
            new_phrase=new_phrase+rev_alphabet_latin_2[index]#создание шифра с помощью реверснутого алфавита
        else:
            index=alphabet_kir_2.find(i)#определяем индекс для буквы из фразы в алфавите
            new_phrase=new_phrase+rev_alphabet_kir_2[index]#создание шифра с помощью реверснутого алфавита
    print('Зашифрованная фраза:',new_phrase)#вывод шифра
atbash_code()
```

Figure 2: Шифр Атбаш

Выводы (1)

- Мной были получены следующие результаты выполнения программ:
- Шифр Цезаря:

```
Введите k:3
Введите фразу для зашифровки:veni,vidi,vici!
Зашифрованная фраза: yhql,ylgl,ylfl!
```

- Шифр Атбаш:

```
Введите фразу для зашифровки:abcd
Зашифрованная фраза:  zyx
```

Выводы (2)

- Исходя из теоретических сведений, программы выполнены без ошибок, чему свидетельствуют полученные результаты.
- В ходе выполнения данной работы были выполнены поставленные цели и задачи.