Отчёт по лабораторной работе №1. Шифры простой замены

Дисциплина: Математические основы защиты информации и информационной безопасности

Студент: Агеева Анастасия Сергеевна, 1032212304
Группа: НФИмд-02-21
Преподаватель: д-р.ф.-м.н., проф. Кулябов Дмитрий Сергеевич

11 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”.
- Данная работа необходима для более глубоко и детального понимания работы алгоритмов шифрования.

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

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

Результаты выполнения данной лабораторной работы

Шифр Цезаря

In [3]:

```python
def caesar(k, word, alphabet):
    m = len(alphabet)
    alphabet = list(alphabet)
    word = list(word)
    new_alphabet = []
    for i in range(m):
        new_alphabet.append(alphabet[(i+k)%m])
    new_word = []
    for i in range(len(word)):
        for j in range(m):
            if word[i] == alphabet[j]:
                new_word.append(new_alphabet[j])
    new_word = ''.join(new_word)
    new_alphabet = ''.join(new_alphabet)
    return new_word, new_alphabet
```

Figure 1: Шифр Цезаря

Шифр Атбаш

In [7]:

```
def atbash(alphabet, word):
    m = len(alphabet)
    alphabet = list(alphabet)
    new_alphabet = []
    for i in range(m):
        new_alphabet.append(alphabet[m-i-1])
    word = list(word)
    new_word = []
    for i in range(len(word)):
        for j in range(m):
            if word[i] == alphabet[j]:
                new_word.append(new_alphabet[j])
    new_word = ''.join(new_word)
    new_alphabet = ''.join(new_alphabet)
    return new_alphabet, new_word
```

Figure 2: Шифр Атбаш

Результаты (1)

- Шифр Цезаря:

```
In [2]:
k = 3 # величина шага
message = "venivedivici"
alphabet = "abcdefghigklmnopqrstuvwxyz"
```

Figure 3: Результат программы Шифр Цезаря

```
In [4]:
new_message, new_alphabet = caesar(k, message, alphabet)

In [5]:
print(k, "- ключ")
print(alphabet, "- алфавит")
print(new_alphabet, "- новый алфавит")
print(message, "- сообщение")
print(new_message, "- зашифрованное собщение")

3 - ключ
abcdefghigklmnopqrstuvwxyz - алфавит
defghigklmnopqrstuvwxyzabc - новый алфавит
venivedivici - сообщение
yhqlyhglylfl - зашифрованное собщение
```

Figure 4: Результат программы Шифр Цезаря

Результаты (2)

- Шифр Атбаш:

```
In [2]:  k = 3 # величина шага
         message = "venivedivici"
         alphabet = "abcdefghigklmnopqrstuvwxyz"
```

Figure 5: Результат программы Шифр Цезаря

```
In [8]:  new_alphabet, new_message = atbash(alphabet, message)

In [9]:  print(alphabet, "- алфавит")
         print(new_alphabet, "- новый алфавит")
         print(message, "- сообщение")
         print(new_message, "- зашифрованное собщение")

         абвгдеёжзийклмнопрстуфхцчшщъыьэюя  - алфавит
          яюэьыъщшчцхфутсрпонмлкйизжёедгвба - новый алфавит
         пришёл увидел победил - сообщение
         рпчзъфамючьыфарсяыьчф - зашифрованное собщение
```

Figure 6: Результат программы Шифр Атбаш

Выводы

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