Отчёт по лабораторной работе №1. Шифры простой замены

Дисциплина: Математические основы защиты информации и информационной безопасности

Студент: Майорова О.А., 1032212322
Группа: НФИмд-02-21
Преподаватель: д.ф.-м.н., Кулябов Д. С.

Москва, 2021

Цель и задачи

Цель: Ознакомиться с шифрами простой замены на примере шифров Цезаря и Атбаш.

Задачи:

- Рассмотреть и реализовать шифр Цезаря с произвольным ключом k.
- Рассмотреть и реализовать шифр Атбаш.

Теоретическое введение

Шифр простой замены - шифрование, осуществляемое путём создания таблицы шифрования, в которой каждой букве открытого текста сопоставляется по определённому алгоритму единственная буква шифр-текста.

Шифр Цезаря: шифроалфавит представляет собой сдвинутый исходный алфавит на k позиций.

Шифр Атбаш: шифроалфавит представляет собой отражённый исходный алфавит.

Реализация шифра Цезаря

Функция на языке Python:

```
# c - буква для шифрования
# k - ключ


def Caesar(c, k):
    n = [(i + k) % 26 for i in range(26)][ord(c) - ord('a')]
    return chr(ord('a') + n)
```

Проверка реализации шифра Цезаря

- для ключа *k*=3: “Veni vidi vici” -> YHQL YLGL YLFL

```
for c in 'veni vidi vici':
    if c == ' ':
        print(' ', end='')
    else:
        print(Caesar(c, 3), end='')
```

```
yhql ylgl ylfl
```

- для ключа *k*=1: “Festina lente” -> GFTUJOB MFOUF

```
for c in 'festina lente':
    if c == ' ':
        print(' ', end='')
    else:
        print(Caesar(c, 1), end='')
```

```
gftujob mfouf
```

Реализация и проверка реализации шифра Атбаш

Функция на языке Python:

```
# c - буква для шифрования

def Atbash(c):

    return chr(ord('a') + (ord('я') - ord(c)))
```

Проверка 1:

```
1 Atbash('a')
```

```
'я'
```

```
1 Atbash('я')
```

```
'a'
```

Проверка 2:

```
1 for c in 'мозиииб':
2     print(Atbash(c), end='')
```

```
усшччю
```

Заключение

Таким образом, была достигнута цель, поставленная в начале лабораторной работы.

- Было осуществлено знакомство с шифрами простой замены на примере шифров Цезаря и Атбаш.
- Была получена реализация шифра Цезаря с произвольным ключом k для латинского алфавита нижнего регистра.
- Была получена реализация шифра Атбаш для кириллицы нижнего регистра.

Спасибо за внимание