Отчет по лабораторной работе №1

Дисциплина: Математические основы защиты информации и информационной безопасности

Живцова Анна

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

Изучить алгоритмы шифрования с помощью простой замены. Реализовать шифрование и дешифрование шифра Цезаря и шифра Атбаш.

2 Задание

Реализовать шифрование и дешифрование шифра Цезаря и шифра Атбаш.

3 Теоретическое введение

Шифры простой замены (подстановки) реализуются с помощью таблицы, состоящей из двух строк. В первой строке указываются символы исходного алфавита, во второй строке перечисляются символы шифроалфавита (часто являющиеся символами исходного алфавита, перечисленными в ином порядке). Каждому символу исходного алфавита ставится в соответствие символ шифроалфавита. Для шифрования текста все символы исходного сообщения (написанного с помощью исходного алфавита) заменяются на соответствующие символы шифроалфавита. Для дешифрования, наоборот, в все символы в шифростроке (состоящей из символов шифроалфавита) ставятся в соответствие символы исходного алфавита [1,2].

В шифре Цезаря шифроалфавит представляет собой исходный алфавит, циклически смещенный на k символов. В шифре Атабаш исходный алфавит кроме букв содержит еще и символ пробела, а шифроалфавит является исходным алфавитом, записанным в обратном порядке.

4 Выполнение лабораторной работы

Для реализации шифрования и дешифрования шифров Цезаря и Атбаш на языке Python была написанна следующая функция.

`def cript(alphabet, k, string):  return ''.join([alphabet[(alphabet.index(letter.lower()) + k)%len(alphabet)] for letter in string])`

Тут k – параметр смещения алфавита для шифра Цезаря. Для шифрования k > 0. Для дешифрования k < 0. Для шифра Атбаш `k = len(alphabet)`.

Функциональность данной функции была протестирована в среде jupyter notebook (см. рис. 4.1).

```
alphabet = 'а б в г д е ё ж з и й к л м н о п р с т у ф х ц ч ш щ ъ ы ь э ю я'.split(' ')
alphabet_atbash = 'а б в г д е ё ж з и й к л м н о п р с т у ф х ц ч ш щ ъ ы ь э ю я'.split(' ') + [' ']
alphabet_lat = 'a b c d e f g h i j k l m n o p q r s t u v w x y z'.split(' ')
alphabet_atbash_lat = 'a b c d e f g h i j k l m n o p q r s t u v w x y z'.split(' ') + [' ']

def cript(alphabet, k, string):
    return ''.join([alphabet[(alphabet.index(letter.lower()) + k + len(alphabet))%len(alphabet)] for letter in string])

print(cript(alphabet_lat, -3, 'YHQLYLGLYLFL'))
print(cript(alphabet_lat, 3, 'venividivici'))
print(cript(alphabet_atbash_lat, len(alphabet), 'YHQL YLGL YLFL'))
print(cript(alphabet_atbash_lat, len(alphabet), 'veni vidi vici'))
```

```
venividivici
yhqlylglylfl
dnwrfdrmrfdrlr
aktofaojofaoio
```

Рис. 4.1: Тестирование программы

5 Выводы

В данной работе я изучила алгоритмы шифрования с помощью простой замены, а также реализовала шифрование и дешифрование шифра Цезаря и шифра Атбаш.

Список литературы

1. Kulyabov D., Korolkova A., Gevorkyan M. Информационная безопасность компьютерных сетей: лабораторные работы. 2015.
2. Самуйлов К.Е. и др. Сети и телекоммуникации : Учебник и практикум. Издательство Юрайт, 2019. С. 1–363.