Математические основы защиты информации и информационной безопасности. Отчет по лабораторной работе № 1

Шифры простой замены

Мохамед Либан Абдуллахи

Содержание

Цель работы

Освоить на практике применение Шифры простой замены [1].

Задание

1 реализовать шифр цезаря с произвольным ключом k.

2 реализовать шифр Атбаш.

Выполнение лабораторной работы

Для выполнения работы была написана программа (@fig:1 - @fig:4) с помощью языка программирования Python, которая получает исходных текста от пользователья и произвольным ключом k = 3, затем шифрует исходные тексты методом шифр цезаря.

caesar_cipher.py

caesar cipher > caesar_cipher.py > ...

```python
#реализовать шифр цезаря с произвольным ключом k

def caesar_cipher(text, k):
    incryption = ''

    for char in text:

        shift = ''

        if char.isalpha():

            if char.isupper():
                shift = 65

            else:
                shift = 97

            char_index = ord(char) - shift
            incryption += chr((char_index + k) % 26 + shift)

        else:
            incryption += char

    return incryption

```

```python

def decryption(incryptedText, k):
    text = ''

    for char in incryptedText:

        shift = ''

        if char.isalpha():

            if char.isupper():
                shift = 65

            else:
                shift = 97

            char_index = ord(char) - shift
            text += chr((char_index - k) % 26 + shift)

        else:
            text += char

    return text

```

```
48
49  plainText = input("Enter Text: ")
50  key = 3
51  ciphertext = caesar_cipher(plainText, key)
52
53  print("\nШифрование")
54  print("Plaintext:", plainText)
55  print("Ciphertext:", ciphertext)
56
57  print("")
58  print("Расшифровка")
59  decrypted = decryption(ciphertext, key)
60  print("Ciphertext:", ciphertext)
61  print("Plaintext:", decrypted)
62
```

```
MINGW64:/e/RUDN_Lessons/Semester1/Mathematical foundations of information protection and information security/Laps/Lap1/work/2023-2024/MOZIiIB/laboratory/lab01/caesar cipher

Liban@DESKTOP-DV3O6IP MINGW64 /e/RUDN_Lessons/Semester1/Mathematical foundations of information protection and information security/Laps/Lap1/work/2023-2024/MOZIiIB/laboratory/lab01/caesar cip
her
$ python caesar_cipher.py
Enter Text: Mohamed Liban Abdullahi

Шифрование
Plaintext: Mohamed Liban Abdullahi
Ciphertext: Prkdphg Oledq Degxoodkl

Расшифровка
Ciphertext: Prkdphg Oledq Degxoodkl
Plaintext: Mohamed Liban Abdullahi

Liban@DESKTOP-DV3O6IP MINGW64 /e/RUDN_Lessons/Semester1/Mathematical foundations of information protection and information security/Laps/Lap1/work/2023-2024/MOZIiIB/laboratory/lab01/caesar cip
her
$
```

Выводы

Освоено на практике применение Шифры простой замены.

Список литературы

1. Методические материалы курса