Лабораторная работа №7

Основы информационной безопасности

Набережных Дарина Денисовна, НПМбд-01-19

8 октября 2022 года

Российский университет дружбы народов, Москва, Россия

Элементы криптографии.

Однократное гаммирование

Цель работы

- Освоить на практике применение режима однократного гаммирования.

Задачи лабораторной работы

- Создать программу с шифрованием и расшифрованием данных в режиме однократного гаммирования
- Подобрать ключ, чтобы получить сообщение “С Новым Годом, друзья!”

Ход выполнения лабораторной работы

Создание функции шифрования

Создадим функцию шифрования:

Лабораторная работа №7

Ввод [1]:
```
import re
```

Ввод [2]:
```
alphabeth = ['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', ' ',
              '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', '!',
              '?', '.', ',']
```

Ввод [3]:
```
def encrypt(text, gamma):
    textLen = len(text)
    gammaLen = len(gamma)

    keyText = []
    for i in range(textLen // gammaLen):
        for symb in gamma:
            keyText.append(symb)
    for i in range(textLen % gammaLen):
        keyText.append(gamma[i])

    code = []
    for i in range(textLen):
        code.append(alphabeth[(alphabeth.index(text[i]) + alphabeth.index(keyText[i])) % 71])

    return(print(*code,sep=''))
```

Создадим функцию расшифрования:

Ввод [5]:
```
def decrypt(code, gamma):
    codeLen = len(code)
    gammaLen = len(gamma)

    keyText = []
    for i in range(codeLen // gammaLen):
        for symb in gamma:
            keyText.append(symb)
    for i in range(codeLen % gammaLen):
        keyText.append(gamma[i])

    text = []
    for i in range(codeLen):
        text.append(alphabeth[(alphabeth.index(code[i]) - alphabeth.index(keyText[i]) + 71) % 71])

    return(print(*text,sep=''))
```

Ввод [6]:
```
decrypt('С Долым Годом, друзья!', 'ААъАЙАААААААААААААААА')
```

```
С Новым Годом, друзья!
```

Figure 2: Функция расшифрования

Создание функции для определения ключа

Создадим функцию, которая определяет ключ для преобразования шифротекста в некоторый фрагмент текста

Ввод [7]:
```
def crypt(code, text):
    codeLen = len(code)
    textLen = len(text)

    gamma = []
    for i in range(codeLen):
        text.appen(alphabeth[(alphabeth.index(code[i]) - alphabeth.index(text[i]) + 71) % 71])

    return(print(*code,sep=''))
```

Ввод [8]:
```
decrypt('С Долым Годом, друзья!', 'С Белым Годом, друзья!')
```

```
ААГЙАААААААААААААААА
```

Figure 3: Функция, определяющая ключ

Выводы

- Я освоила на практике применение режима однократного гаммирования