Лабораторная работа №8

Основы информационной безопасности

Александрова У.В.

Содержание

1 Цель работы

Цель работы - освоить на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.

2 Задание

Требуется не зная ключа и не стремясь его определить, прочитать оба текста. Необходимо разработать приложение, позволяющее шифровать и дешифровать тексты P1 и P2 в режиме однократного гаммирования.

Приложение должно определить вид шифротекстов C1 и C2 обоих текстов P1 и P2 при известном ключе; Необходимо определить и выразить аналитически способ, при котором злоумышленник может прочитать оба текста, незная ключа и не стремясь его определить.

3 Теоретическое введение

4 Выполнение лабораторной работы

1. Реализую две функции, как и в прошлой лабораторной работе, ввожу необходимые данные (рис. 4.1).

```
In [2]: import random
        import string

        def key_gen(text):
            key = ''
            for i in range(len(text)):
                key += random.choice(string.digits+string.ascii_letters)
            return key

        def shifr(text, key):
            sh_text = ''
            for t,k in zip(text, key):
                xor = ord(t) ^ ord(k) # реализуем умножение по модулю два, при этом переводим элементы в биты
                sh_text += chr(xor)
            return sh_text

In [5]: P1 = 'I like burgers from Lavburger'
        P2 = 'But I dont have any moneyyy'

        key = key_gen(P1)

        sh_text1 = shifr(P1, key)
        sh_text2 = shifr(P2, key)

        new_text1 = shifr(sh_text1, key)
        new_text2 = shifr(sh_text2, key)

        sh_text12 = shifr(sh_text1, sh_text2)
```

Рис. 4.1: Тело программы

2. Вывожу результат (рис. 4.2).

```
In [16]: print('Исходный текст: ', P1, P2)
         print("Ключ: ", key)
         print("Шифр текста 1: ", sh_text1)
         print("Шифр текста 2: ",sh_text2)
         print(new_text1, '\n', new_text2)
         print("Общий шифр: ", shifr_text12)
         print("На основании 1го текста: ", shifr(shifr_text12, P1))
         print("На основании 2го текста: ",shifr(shifr_text12, P2))

Исходный текст:  I like burgers from Lavburger But I dont have any moneyyy
Ключ:  YrXu0dGsmy7UHmXkyx4cH3hxk389L
□□Y□□R□□□A_\>:  □R4□[□g□□□P0:□x
□=)□=K□□M□%\□□□JA□,UyD$□□
I like burgers from Lavburger
 But I dont have any moneyyy
□□EF□□□!□□□□□□I"ED
На основании 1го текста:  But I dont have any moneyyy
На основании 2го текста:  I like burgers from Lavburg
```

Рис. 4.2: Результат работы

5 Листинг

```
import random
import string

def key_gen(text):
    key = ''
    for i in range(len(text)):
        key += random.choice(string.digits+string.ascii_letters)
    return key

def shifr(text, key):
    sh_text = ''
    for t,k in zip(text, key):
        xor = ord(t) ^ ord(k) # реализуем умножение по модулю два, при этом перев
        sh_text += chr(xor)
    return sh_text

P1 = 'I like burgers from Lavburger'
P2 = 'But I dont have any moneyyy'

key = key_gen(P1)

sh_text1 = shifr(P1, key)
```

```
sh_text2 = shifr(P2, key)

new_text1 = shifr(sh_text1, key)
new_text2 = shifr(sh_text2, key)

sh_text12 = shifr(sh_text1, sh_text2)

print('Исходный текст: ', P1, P2)
print("Ключ: ", key)
print("Шифр текста 1: ", sh_text1)
print("Шифр текста 2: ",sh_text2)
print(new_text1, '\n', new_text2)
print("Общий шифр: ", shifr_text12)
print("На основании 1го текста: ", shifr(shifr_text12, P1))
print("На основании 2го текста: ",shifr(shifr_text12, P2))
```

6 Выводы

Я освоила на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.