Лабораторная работа №8

Основы информационной безопасности

Александрова У.В.

25 мая 2024

Российский университет дружбы народов, Москва, Россия

Цель работы

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

Задание

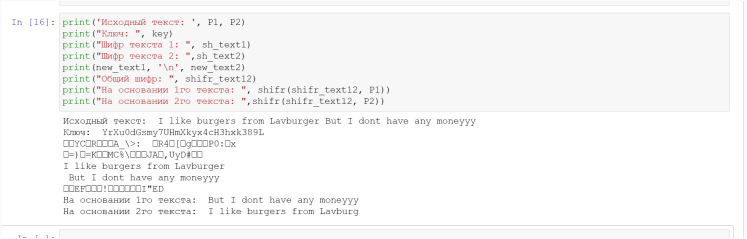
Требуется не зная ключа и не стремясь его определить, прочитать оба текста. Необходимо разработать приложение, позволяющее шифровать и дешифровать тексты P1 и P2 в режиме однократного гаммирования. Приложение должно определить вид шифротекстов C1 и C2 обоих текстов P1 и P2 при известном ключе; Необходимо определить и выразить аналитически способ, при котором злоумышленник может прочитать оба текста, незная ключа и не стремясь его определить.

Выполнение лабораторной работы

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)
```

Figure 1: Тело программы



```
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
□□YC□R□□□A_\>:  □R4□[Cy□□□P0:□x
□=)□=K□□MC%\□□□JA□,UyD#□□
I like burgers from Lavburger
 But I dont have any moneyyy
□□E$□□□!□□□□□□r"ED
На основании 1го текста:  But I dont have any moneyyy
На основании 2го текста:  I like burgers from Lavburg
```

Figure 2: Результат

Выводы

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