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. 1).

![Рис. 1: Тело программы](data:application/octet-stream;base64,)

Рис. 1: Тело программы

1. Вывожу результат (рис. 2).

![Рис. 2: Результат работы](data:application/octet-stream;base64,)

Рис. 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 переводим элементы в биты  
 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.