Отчёт по лабораторной работе №7

Бабков Дмитрий Николаевич

# Цель работы

Освоить на практике применение режима однократного гаммирования

# Выполнение лабораторной работы

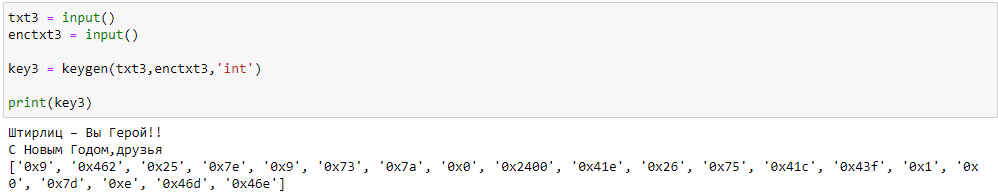
В ходе выполнения лабораторной работы была написана программа, которая может создавать зашифрованный текст, получая на вход исходный текст и ключ шифрования, расшифровывать текст с помощью зашифрованного текста и ключа, а также получать ключ, чтобы превратить заданный зашифрованный текст в расшифрованный текст.

Код программы:

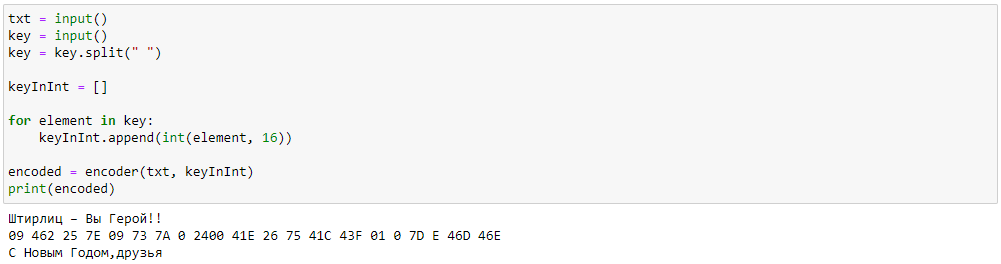
def encoder(text, key):  
   
 encodedText = ''  
   
 if (len(text) == len(key)):  
  
 if(type(key[0]) is int):  
 for i in range(len(text)):  
 encodedText += chr(ord(text[i]) ^ key[i])  
 else:  
 for i in range(len(text)):  
 encodedText += chr(ord(text[i]) ^ ord(key[i]))  
   
 return encodedText  
  
 else:  
 return  
  
def decoder(encodedText, key):  
   
 decodedText = ''  
   
 if (len(encodedText) == len(key)):  
   
 if(type(key[0]) is int):  
   
 for i in range(len(encodedText)):  
   
 decodedText += chr(ord(encodedText[i]) ^ key[i])  
   
 elif(type(encodedText[0]) is int):  
   
 for i in range(len(encodedText)):  
   
 decodedText += chr(encodedText[i] ^ ord(key[i]))  
   
 elif((type(encodedText[0]) is int) & (type(key[0]) is int)):  
   
 for i in range(len(encodedText)):  
   
 decodedText += chr(encodedText[i] ^ key[i])  
   
 else:  
   
 for i in range(len(encodedText)):  
   
 decodedText += chr(ord(encodedText[i]) ^ ord(key[i]))  
   
 return decodedText  
   
 else:  
   
 return  
  
def keygen(text, encodedText, astype):  
   
 if(astype == 'int'):  
   
 key = []  
   
 else:  
   
 key = ''  
   
 if(len(text) == len(encodedText)):  
   
 if (astype == 'int'):  
   
 for i in range(len(encodedText)):  
   
 key.append(hex(ord(text[i]) ^ ord(encodedText[i])))  
   
 else:   
   
 for i in range(len(encodedText)):  
  
 key += chr(ord(text[i]) ^ ord(encodedText[i]))  
   
 return key  
   
 else:  
  
 return  
  
txt = input()  
key = input()  
key = key.split(" ")  
  
keyInInt = []  
  
for element in key:  
 keyInInt.append(int(element, 16))  
  
encoded = encoder(txt, keyInInt)  
print(encoded)  
  
txt2 = input()  
key2 = input()  
key2 = key.split(" ")  
  
keyInInt2 = []  
  
for element in key2:  
 keyInInt2.append(int(element, 16))  
   
print(decoder(txt2, keyInInt2))  
  
txt3 = input()  
enctxt3 = input()  
  
key3 = keygen(txt,enctxt,'int')  
  
print(key3)

Результат выполнения команд (Рис. 1 - 3):

Генерация ключа:



Получение закодированного сообщения из открытого:



Декодирование текста по ключу:

