Отчёт по лабораторной работе №8

Режим однократного гаммирования

Вакутайпа Милдред

Содержание

Список иллюстраций

Список таблиц

# 1 Цель работы

Освоить на практике применение режим однократного гаммирования на примере кодирования различных исходных текстов одним ключом.

# 2 Выполнение лабораторной работы

В данной работе два текста кодируются одним ключом. Требуется почитать оба текста не зная ключа. Используя код с лабораторной работе №7, генерирую ключ и шифрирую два разных текста одним и тем же ключом. Расшифровываю оба текста с одного ключа, потом предполагаю что ключ неизвестен но известен один текст и расшифровываю второй, зная первый текст и шифротексты.

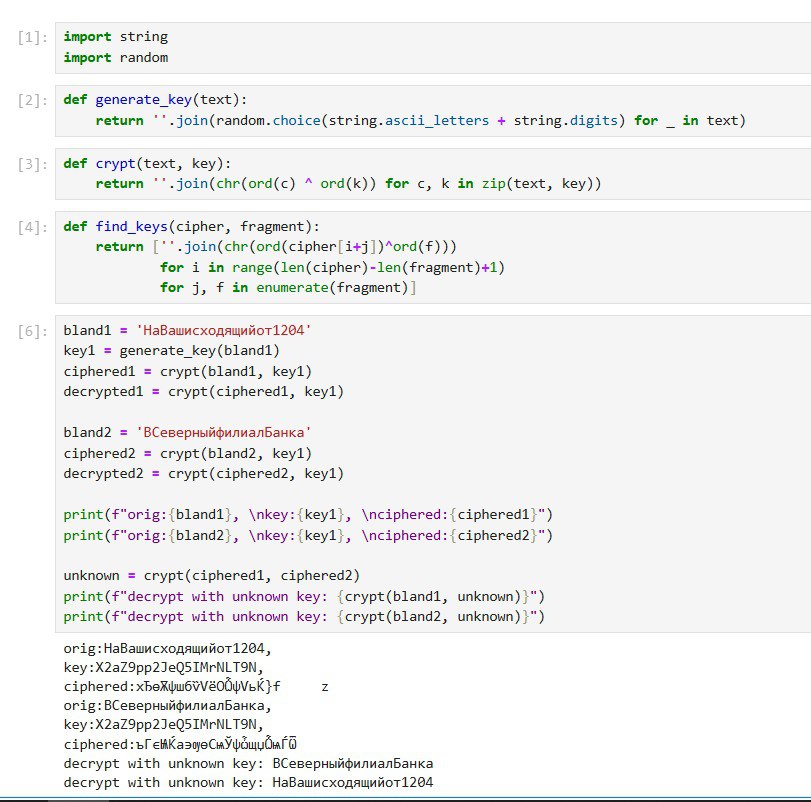


Рис. 1: Расшифрированные тексты

Листинг программы 1

import string  
import random  
  
def generate\_key(text):  
 return ''.join(random.choice(string.ascii\_letters + string.digits) for \_ in text)  
   
def crypt(text, key):  
 return ''.join(chr(ord(c) ^ ord(k)) for c, k in zip(text, key))  
   
def find\_keys(cipher, fragment):  
 return [''.join(chr(ord(cipher[i+j])^ord(f)))  
 for i in range(len(cipher)-len(fragment)+1)  
 for j, f in enumerate(fragment)]  
   
   
bland1 = 'НаВашисходящийот1204'  
key1 = generate\_key(bland1)  
ciphered1 = crypt(bland1, key1)  
decrypted1 = crypt(ciphered1, key1)  
  
bland2 = 'ВСеверныйфилиалБанка'  
ciphered2 = crypt(bland2, key1)  
decrypted2 = crypt(ciphered2, key1)  
  
print(f"orig:{bland1}, \nkey:{key1}, \nciphered:{ciphered1}")  
print(f"orig:{bland2}, \nkey:{key1}, \nciphered:{ciphered2}")  
  
unknown = crypt(ciphered1, ciphered2)  
print(f"decrypt with unknown key: {crypt(bland1, unknown)}")  
print(f"decrypt with unknown key: {crypt(bland2, unknown)}")

# 3 Выводы

При выполнение данной работыб я освоила на практике применение режим однократного гаммирования на примере кодирования различных исходных текстов одним ключом.

# Список литературы