Информационная безопасность лабораторная работа №7

Элементы криптографии. Однократное гаммирование

Ким Илья Владиславович НФИбд-01-21

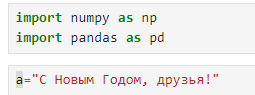
Содержание

# Цель работы

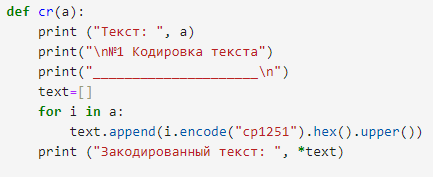
Освоить на практике применение режима однократного гаммирования

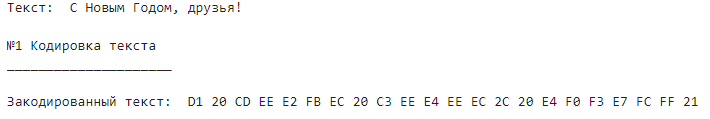
# Выполнение лабораторной работы

1. Подключил библиотеки и ввел сообщение “С Новым Годом, друзья!” (рис. [-@fig:001])

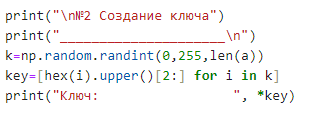


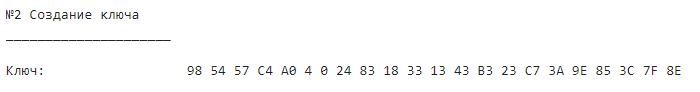
1. Перевод сообщения в шестнадцатеричную систему счисления (рис. [-@fig:002])(рис. [-@fig:003])



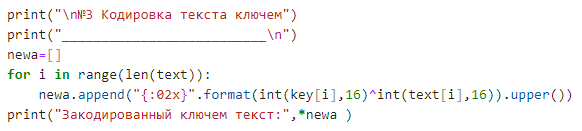


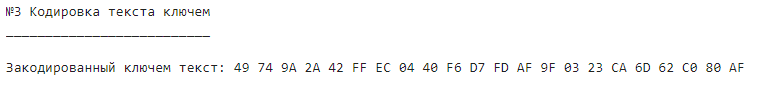
1. Создание ключа (рис. [-@fig:004])(рис. [-@fig:005])



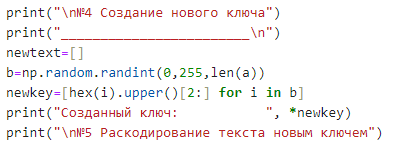


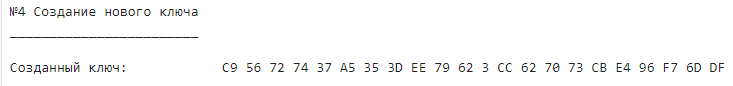
1. Кодировка текста ключем (рис. [-@fig:006])(рис. [-@fig:007])



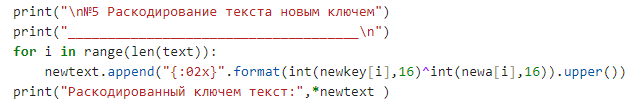


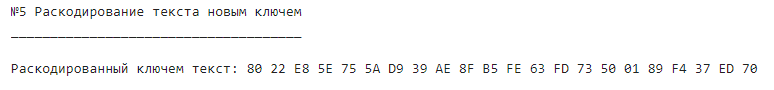
1. Создание нового ключа (рис. [-@fig:008])(рис. [-@fig:009])



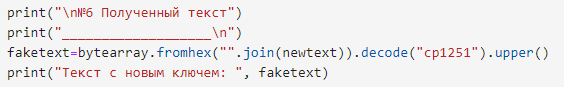


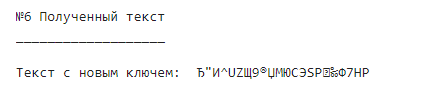
1. Раскодировка текста новым ключем (рис. [-@fig:010])(рис. [-@fig:011])



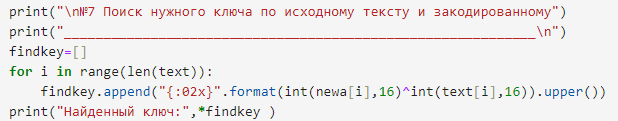


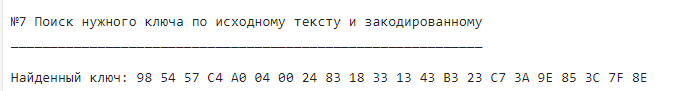
1. Полученный текст (рис. [-@fig:012]) (рис. [-@fig:013])



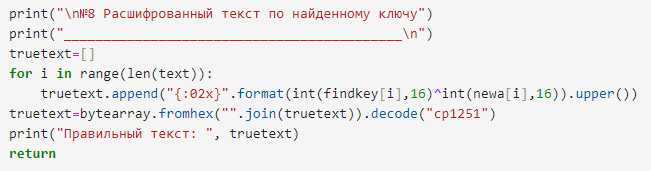


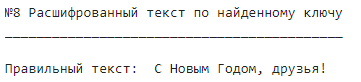
1. Поиск нужного ключа по исходному и закодированному тексту (рис. [-@fig:014])(рис. [-@fig:015])





1. Расшифровка текста по найденному ключу (рис. [-@fig:016])(рис. [-@fig:017])





# Листинг

import numpy as np

import pandas as pd

a=“С Новым Годом, друзья!”

def cr(a): print (“Текст:”, a)

print("\n№1 Кодировка текста")  
  
print("\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\n")  
text=[]  
for i in a:  
 text.append(i.encode("cp1251").hex().upper())  
print ("Закодированный текст: ", \*text)  
  
print("\n№2 Создание ключа")  
print("\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\n")  
k=np.random.randint(0,255,len(a))  
key=[hex(i).upper()[2:] for i in k]  
print("Ключ: ", \*key)  
  
print("\n№3 Кодировка текста ключем")  
print("\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\n")  
newa=[]  
for i in range(len(text)):  
 newa.append("{:02x}".format(int(key[i],16)^int(text[i],16)).upper())  
print("Закодированный ключем текст:",\*newa )  
  
print("\n№4 Создание нового ключа")  
print("\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\n")  
newtext=[]  
b=np.random.randint(0,255,len(a))  
newkey=[hex(i).upper()[2:] for i in b]  
print("Созданный ключ: ", \*newkey)  
  
print("\n№5 Раскодирование текста новым ключем")  
print("\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\n")  
for i in range(len(text)):  
 newtext.append("{:02x}".format(int(newkey[i],16)^int(newa[i],16)).upper())  
print("Раскодированный ключем текст:",\*newtext )  
  
print("\n№6 Полученный текст")  
print("\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\n")  
faketext=bytearray.fromhex("".join(newtext)).decode("cp1251").upper()  
print("Текст с новым ключем: ", faketext)  
  
print("\n№7 Поиск нужного ключа по исходному тексту и закодированному")  
print("\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\n")  
findkey=[]  
for i in range(len(text)):  
 findkey.append("{:02x}".format(int(newa[i],16)^int(text[i],16)).upper())  
print("Найденный ключ:",\*findkey )  
  
print("\n№8 Расшифрованный текст по найденному ключу")  
print("\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\n")  
truetext=[]  
for i in range(len(text)):  
 truetext.append("{:02x}".format(int(findkey[i],16)^int(newa[i],16)).upper())  
truetext=bytearray.fromhex("".join(truetext)).decode("cp1251")  
print("Правильный текст: ", truetext)  
return

# Выводы

Освоил на практике применение однократного гаммирования