

Презентация к лабораторной работе №7

Элементы криптографии. Однократное гаммирование

Ким И. В. НФИбд-01-21

Российский университет дружбы народов, Москва, Россия

Цели и задачи

Освоить на практике применение режима однократного гаммирования

Выполнение лабораторной работы

Подключил библиотеки и ввел сообщение “С Новым Годом, друзья!”

```
import numpy as np  
import pandas as pd
```

```
a="С Новым Годом, друзья!"
```

Перевод сообщения в шестнадцатеричную систему счисления

```
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)
```

Текст: С Новым Годом, друзья!

№1 Кодировка текста

Закодированный текст: D1 20 CD EE E2 FB EC 20 C3 EE E4 EE EC 2C 20 E4 F0 F3 E7 FC FF 21

```
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)
```

№2 Создание ключа

Ключ: 98 54 57 C4 A0 4 0 24 83 18 33 13 43 B3 23 C7 3A 9E 85 3C 7F 8E

Кодировка текста ключем

```
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 )
```

№3 Кодировка текста ключем

Закодированный ключем текст: 49 74 9A 2A 42 FF EC 04 40 F6 D7 FD AF 9F 03 23 CA 6D 62 C0 80 AF


```
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")
```

№4 Создание нового ключа

Созданный ключ:

C9 56 72 74 37 A5 35 3D EE 79 62 3 CC 62 70 73 CB E4 96 F7 6D DF

Раскодировка текста новым ключем

```
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 )
```

№5 Раскодирование текста новым ключем

Раскодированный ключем текст: 80 22 E8 5E 75 5A D9 39 AE 8F B5 FE 63 FD 73 50 01 89 F4 37 ED 70

```
print("\n№6 Полученный текст")
print("_____ \n")
faketext=bytearray.fromhex("".join(newtext)).decode("cp1251").upper()
print("Текст с новым ключем: ", faketext)
```

№6 Полученный текст

Текст с новым ключем: Ъ"И^UZЩ9®ЦМЮСЭSP®%Ф7HP

Поиск нужного ключа по исходному и закодированному тексту

```
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 )
```

№7 Поиск нужного ключа по исходному тексту и закодированному

Найденный ключ: 98 54 57 C4 A0 04 00 24 83 18 33 13 43 B3 23 C7 3A 9E 85 3C 7F 8E

Расшифровка текста по найденному ключу

```
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
```

№8 Расшифрованный текст по найденному ключу

Правильный текст: С Новым Годом, друзья!

Выводы

Освоил на практике применение однократного гаммирования