

# Лабораторная работа №6

Мандатное разграничение прав в Linux атрибутов

---

Victoria M. Shutenko

15 October, 2022, Moscow, Russian Federation

RUDN University, Moscow, Russian Federation

## Цель выполнения лабораторной работы

---

## Цель выполнения лабораторной работы

---

Освоить на практике применение режима однократного гаммирования.

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

a = "С Новым годом, друзья!"
```

## Функция crypt

```
def crypt(a):  
    print("open text: ", a)  
    text = []  
    for i in a:  
        text.append(i.encode("cp1251").hex())  
    print("open text in 16: ", *text)  
    k = np.random.randint(0, 255, len(a))  
    key = [hex(i)[2:] for i in k]  
    newkey = []  
    for i in key:  
        newkey.append(i.encode("cp1251").hex().upper())  
    print("key in 16: ", *key)  
    b=[]  
    for i in range(len(text)):  
        b.append("{:02x}".format(int(key[i],16)^int(text[i],16)))
```

```
def findkey(a, findtext):  
    print("open text: ", a, "\ncypher text: ", fintext)  
    newtext=[]  
    for i in a:  
        newtext.append(i.encode("cp1251").hex())  
    print("open text in 16: ", *newtext)  
    ftext=[]  
    for i in findtext:  
        ftext.append(i.encode("cp1251").hex())  
    print("cypher text in 16: ", *ftext)  
    key = [hex(int(i,16)^int(j,16))[2:] for (i,j) in zip(newtext,ftext)]  
    print("found key in 16: ", *key)  
    return key
```

```
key1=findkey(a,findtext)
```

```
if key==key1:  
    print("correct key")  
else:  
    print("fail, incorrect key")
```

```
In [37]: if key==key1:  
         print("correct key")  
         else:  
             print("fail, incorrect key")  
  
correct key
```

Figure 3: Результат выполнения цикла.

Итоги

---



- изучили шифрование в режиме гаммирования
- написали код из 2-х функций для решения задачи