

# **Элементы криптографии. Шифрование (кодирование) различных исходных текстов одним ключом**

---

Каримов Зуфар Исматович НПИ-01-18

Информационная безопасность, 18 декабря, 2021, Москва, Россия

RUDN University

# Цель лабораторной работы

---

## Цель лабораторной работы

Освоить на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом. ## Процесс выполнения лабораторной работы

1. Блок функции для расчетов
2. Написал блок обработки данных
3. Итоговый результат

## Результат

```
In [20]: import string
import random

In [21]: def hexx(text):
return ''.join(hex(ord(i))[2:] for i in text)
def gen_key(size):
return ''.join(random.choice(string.ascii_letters + string.digits) for _ in range(size))
def encrypted(FirstText,secondText):
first_text=[ord(i) for i in firstText]
second_text=[ord(i) for i in secondText]
return ''.join(chr( a^b) for a,b in zip(first_text,second_text))
```

Figure 1: Блок функции для расчетов

## Результат

```
In [22]: P1 = "НаВашисходящий1204"
P2 = "ВСеве́рныйФилиалБанка"

key=gen_key(len(P1))
print(key)
hex_key=hexx(key)
print("Ключ в шестнадцатичном виде: ",hex_key)

C1= encrypted(P1,key)
C2= encrypted(P2,key)

print("Шифрованный текст: ",C1)
print("Шифрованный текст: ",C2)

decrypt=encrypted(C1,C2)
print("Расшифрованный текст: ",encrypted(decrypt,P2) )
print("Расшифрованный текст: ",encrypted(decrypt,P1) )

D8NYSqBnFZbx84KV2ndp
Ключ в шестнадцатичном виде: 44 52 4d 59 53 71 42 6d 46 5a 62 78 42 34 4b 59 32 6d 64 78
Шифрованный текст: 1bЦяЛаГw3zIQNvTE_TD
Шифрованный текст: 1o9yA6BЦD0xу0EYah5р
Расшифрованный текст: НаВашисходящий1204
Расшифрованный текст: ВСеве́рныйФилиалБанка
```

Figure 2: Чтение текста

## **Выводы**

---

Освоил на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.