

# Защита лабораторной работы №8. Элементы криптографии. Шифрование (кодирование) различных исходных текстов одним ключом

---

Асеинова Елизавета

2022 Oct 4th

RUDN University, Moscow, Russian Federation

## Результат выполнения лабораторной работы №8

---

## Цель выполнения лабораторной работы

---

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

# Результат выполнения лабораторной работы

```
[7] import string
    import random

[8] def shest(message):
    return ' '.join(hex(ord(i))[2:] for i in message)

def rand_key(s):
    return ' '.join(random.choice(string.ascii_letters + string.digits) for _ in range(s))

def code(message1, message2):
    mess1 = [ord(i) for i in message1]
    mess2 = [ord(i) for i in message2]
    return ' '.join(chr(a^b) for a,b in zip(mess1, mess2))
```

Figure 1: Функции

# Результат выполнения лабораторной работы

```
[9] P1 = 'НаВашисходящийот1204'
    P2 = 'ВСеве́рныйфилиалБанка'
```

```
[19] key = rand_key(len(P1))
      print('Ключ для шифрования сообщений: ', key)
      hex_key = shest(key)
      print('Ключ в шестнадцатеричной форме: ', hex_key)
```

Ключ для шифрования сообщений: о Е D d 8 Z Н о а М h 5 i ш 7 f 1 Y 3 М  
Ключ в шестнадцатеричной форме: 6f 20 45 20 44 20 64 20 38 20 5a 20 48 20 6f 20 61 20 4d 20 68 20 35 20 69 20 6d 20 37 20 66 20 31 20 59 20 33 20 4d

Figure 2: Создание ключа

```
[26] code_mess1 = code(P1, key)
      code_mess2 = code(P2, key)
      print('Первое зашифрованное сообщение: ', code_mess1)
      print('Второе зашифрованное сообщение: ', code_mess2)
```

Первое зашифрованное сообщение: **Θ Α Ι Α Κ Ι Χ Κ Ι Δ Ε Ψ Ψ Ι Ε Τ Ρ Θ } Θ**  
Второе зашифрованное сообщение: **Ω Ε Ψ Β ψ Ω λ ж Ё К Ъ Л Ψ Α ε β η ν Α**

```
▶ decrypt = code(code_mess1, code_mess1)
print(code(decrypt, P1))
print(code(decrypt, P2))
```

НАВАШИ СКОДЯМИ ОЪ 1909  
В ЁЕВЕ ОНЖЙ КИЛИ АЛБА НК А

Figure 3: Шифрование

В ходе работы мы освоили на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.