# Лабораторная работа № 8. Элементы криптографии. Шифрование (кодирование) различных исходных текстов одним ключом

Волков Тимофей Евгеньевич НПИбд-01-18

# Цель работы

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

# Функции

Ввод [1]:
```
import string
import random
```

Ввод [2]:
```
def hex_(text):
    return ' '.join(hex(ord(i))[2:] for i in text)
```

Ввод [3]:
```
def gen_key(size):
    return ''.join(random.choice(string.ascii_letters + string.digits) for _ in range(size))
```

Ввод [4]:
```
def encrypt(text, key):
    return ''.join(chr(a^b) for a, b in zip(text, key))
```

Ввод [5]:
```
def decrypt(encrypt, key):
    return ''.join(chr(a^b) for a, b in zip(encrypt, key))
```

**Figure 1:** Функции

# Вывод результата

Ввод [9]:

```
P1 = 'НаВашисходящийот1204'
P2 = 'ВСеверныйфилиалБанка'

key = gen_key(len(P1))
hex_key = hex_(P1)

print("Ключ: ", hex_key)

P1_encrypt = encrypt([ord(i) for i in P1], [ord(i) for i in key])
P1_hex_encrypt = hex_(P1_encrypt)

P2_encrypt = encrypt([ord(i) for i in P2], [ord(i) for i in key])
P2_hex_encrypt = hex_(P2_encrypt)

print("Зашифрованное сообщение C1: ", P1_hex_encrypt)

print("Зашифрованное сообщение C2: ", P2_hex_encrypt)

C = encrypt([ord(i) for i in P1_encrypt], [ord(i) for i in P2_encrypt])

P1_decrypt = decrypt([ord(i) for i in C], [ord(i) for i in P2])

print("Расшифрованное сообщение P1: ", P1_decrypt)

P2_decrypt = decrypt([ord(i) for i in C], [ord(i) for i in P1])

print("Расшифрованное сообщение P2: ", P2_decrypt)
```

```
Ключ:  41d 430 412 430 448 438 441 445 43e 434 44f 449 438 439 43e 442 31 32 30 34
Зашифрованное сообщение C1:  45c 445 46a 440 471 475 430 40b 473 446 427 40a 47d 440 47f 418 43 68 5e 7a
Зашифрованное сообщение C2:  453 454 44d 442 40c 40d 44c 405 474 436 450 478 47d 449 47a 44b 442 467 454 47e
Расшифрованное сообщение P1:  НаВашисходящийот1204
Расшифрованное сообщение P2:  ВСеверныйфилиалБанка
```

**Figure 2:** Вывод результата