

# Лабораторная работа № 7

---

Казакова Виктория Алексеевна

2023, Москва

Освоить на практике применение режима однократного гаммирования.

Нужно подобрать ключ, чтобы получить сообщение «С Новым Годом, друзья!». Требуется разработать приложение, позволяющее шифровать и дешифровать данные в режиме однократного гаммирования. Приложение должно:

1. Определить вид шифротекста при известном ключе и известном открытом тексте.
2. Определить ключ, с помощью которого шифротекст может быть преобразован в некоторый фрагмент текста, представляющий собой один из возможных вариантов прочтения открытого текста.

Импортировала необходимые модули Создала функцию для преобразования данных в шестнадцатеричный формат; функцию, генерирующую ключ; функцию для кодирования и декодирования данных.

```
import string
import random

def text(t):
    return "".join(hex(ord(i))[2:] for i in t)

def get_key(size):
    return "".join(random.choice(string.ascii_letters + string.digits) for _ in range(size))

def coder(t, key):
    return "".join(chr(a ^ b) for a, b in zip(t, key))
```

Рис. 1: Кодирование и декодирование строки

## Зашифровала и расшифровала заданный текст

```
message = "С новым годом, друзья!"  
key1 = get_key(len(message))  
key2 = text(key1)  
print("Ключ: ", key2)  
text1 = coder([ord(i) for i in message], [ord(i) for i in key1])  
text2 = text(text1)  
print("Зашифрованное сообщение: ", text2)  
text3 = coder([ord(i) for i in text1], [ord(i) for i in key1])  
print("Расшифрованное сообщение: ", text3)
```

Рис. 2: Остальные команды

```
Ключ: 4d6b654e55506c66724e736230766d63534b52746137  
Зашифрованное сообщение: 46c4b45847046741b4504644147044745c40c5a4d45741340846543842e16  
Расшифрованное сообщение: С новым годом, друзья!
```

**Рис. 3:** Результат

В ходе лабораторной работы было освоено на практике применение режима однократного гаммирования.