

# Лабораторная работа №7

---

Тимур Алескеров

Декабрь, 2021 Москва

RUDN University, Moscow, Russian Federation

# Прагматика выполнения лабораторной работы

---

Проблемой защиты информации при ее передаче между абонентами люди занимаются на протяжении всей своей истории. Человечеством изобретено множество способов, позволяющих в той или иной мере скрыть смысл передаваемых сообщений от противника. В этой лабораторной работе мы изучили один из методов шифрования - метод однократного гаммирования.

## Цель работы

---

Освоить на практике применение режима однократного гаммирования

## Задачи

---

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.

Результат

---



```
Ввод [42]: text = "С Новым Годом, друзья!"  
          key = "Лабораторная работа N 7."  
  
Ввод [43]: def xor_str(data, key):  
          res = ""  
          for x, y in zip(data, key):  
              res += chr(ord(x)^ord(y))  
          return res  
  
Ввод [44]: c = xor_str(text, key)  
  
Ввод [45]: bytes(c, 'UTF-8').hex()  
Out[45]: '3ad902c00727b7ed09e53030471d09cd1acd090057e0107d1acd08101'  
  
Ввод [46]: text_back = xor_str(c, key)  
          text_back  
Out[46]: 'С Новым Годом, друзья!'  
  
Ввод [47]: key_back = xor_str(c, text)  
          key_back  
Out[47]: 'Лабораторная работа N '
```

Рис. 1: Листинг программы

В ходе данной лабораторной работы я освоил применение режима однократного гаммирования на практике, разработал приложение, позволяющее шифровать и дешифровать данные в режиме однократного гаммирования.

Спасибо за внимание!