

*Отчёт по лабораторной работе*

**Лабораторная работа №\_07 / Элементы криптографии. Однократное  
гаммирование**

*Габриэль Тьерри*

**Содержание**

<b>Цель работы .....</b>	
<b>Выполнение лабораторной работы .....</b>	
<b>Выводы .....</b>	
<b>Список литературы.....</b>	

# Цель работы

Освоить на практике применение режима однократного гаммирования

## Выполнение лабораторной работы

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.

```
In [4]: import random
import string

#set a seed for reproducibility
random.seed(23)
# the text that i will use
text = "С Новым Годом, друзья!"

# initialize an empty key
key = ""

# Generate a random key with the same length as the text
for i in range(len(text)):
    #choose a random character for the set of ASCII letters and digits
    key += random.choice(string.ascii_letters + string.digits)

# Print the generated key
print(f"ключ: {key}")
```

ключ: 7X8s51fbLtByHwiUmrCa0N

```

In [7]: def F_encrypted_text(text, key):
        # check if the length of the key and the text match
        if len(key) != len(text):
            return "error length"
        # initialize an empty string to store the encrypted text
        encrypted_text = ""
        # iterate through each character of the key and text
        for i in range(len(key)):
            # Perform XOR operation on ASCII values of the text and key characters
            encrypted_text_symbol = ord(text[i])^ord(key[i])
            # Convert the result back to a character and append it to the encrypted text
            encrypted_text += chr(encrypted_text_symbol)
        return encrypted_text

        # Encrypt the text using the F_encrypted_text function
        encrypted_text = F_encrypted_text(text, key)
        print(f"encrypted_text: {encrypted_text}")
        print(f"Original_text: {F_encrypted_text(encrypted_text, key)}")
        print(f"Ключ: {F_encrypted_text(encrypted_text, text)}")

        encrypted_text: жххэЮъВуьѸчѹ[ІwэВѸРо
        Original_text: С Новым Годом, друзья!
        Ключ: 7X8551fbL8yHwIUmrCaON

```

## Выводы

Освоить на практике применение режима одноразового гаммирования

## Список литературы

1. А.А. Аргановский, Р.А.Хади. Практическая криптография: алгоритмы и их программирование. солон пресс, 2009.