

# Лабораторная работа №7

## Элементы криптографии. Однократное гаммирование

Шагабаев Давид, НПИбд-02-18"

### Содержание

Цель работы .....	1
Выполнение лабораторной работы .....	1
Выводы.....	2

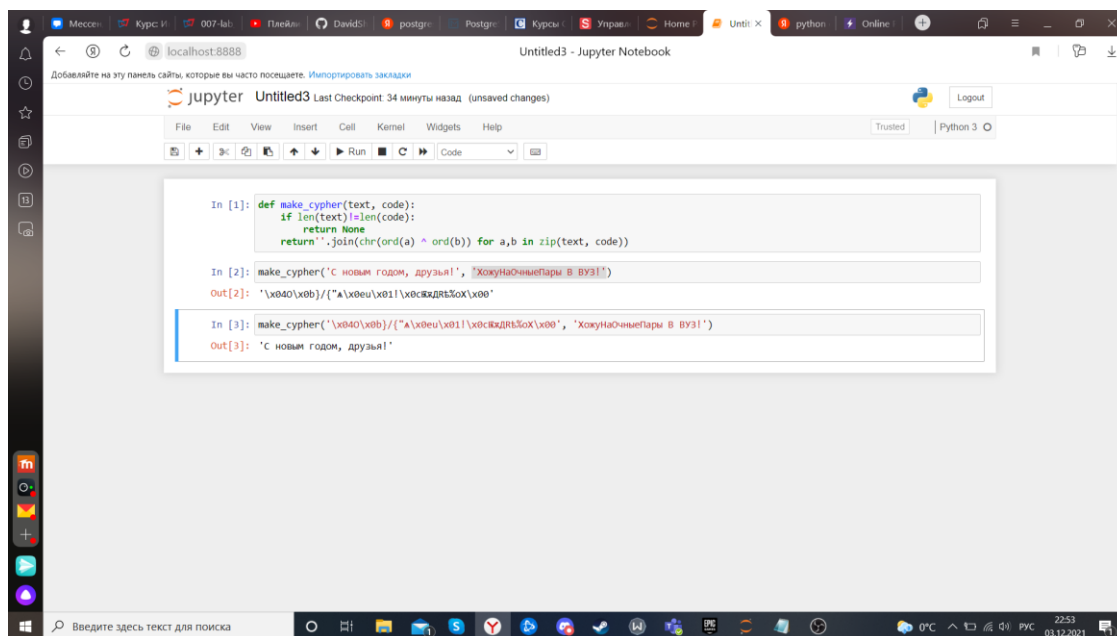
### Цель работы

Освоить на практике применение режима однократного гаммирования.

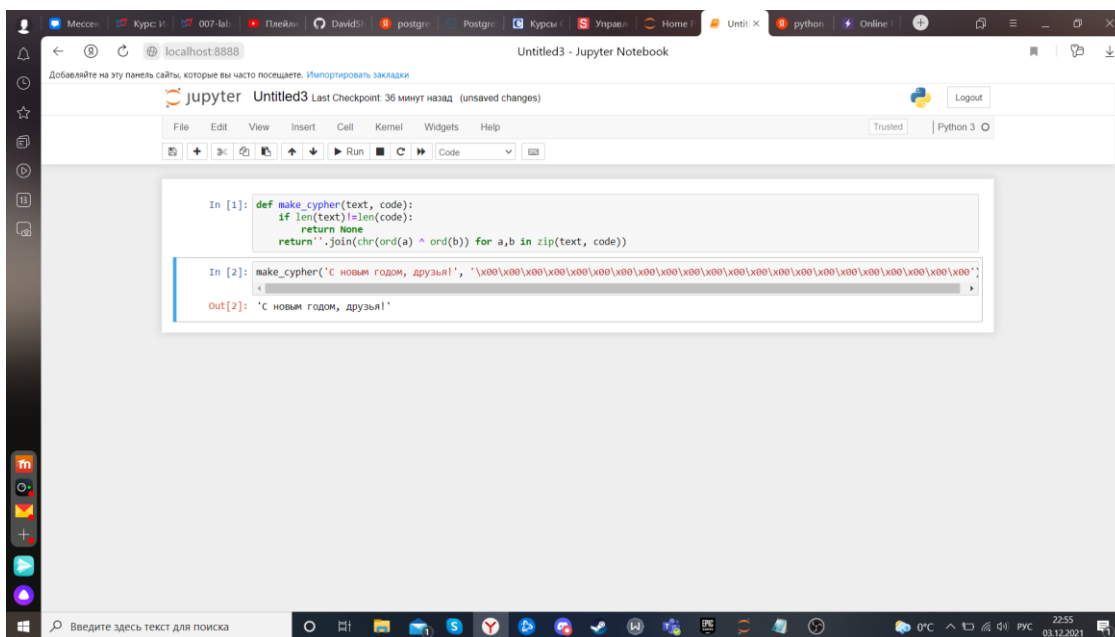
### Выполнение лабораторной работы

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.



The screenshot shows a Jupyter Notebook titled 'Untitled3' running on a local host (localhost:8888). The notebook contains two code cells. The first cell defines a function `make_cipher(text, code)` that implements a Vigenere cipher. The second cell calls this function with the text 'С новым годом, друзья!' and a key consisting of 25 null characters (represented as `'\x00' * 25`). The output of the function is the same text: 'С новым годом, друзья!'.

```
In [1]: def make_cipher(text, code):  
        if len(text) != len(code):  
            return None  
        return ''.join(chr(ord(a) ^ ord(b)) for a,b in zip(text, code))  
  
In [2]: make_cipher('С новым годом, друзья!', '\x00' * 25)  
Out[2]: 'С новым годом, друзья!'
```

## Выводы

Освоил на практике применение режима однократного гаммирования.