

Отчёт по лабораторной работе 8

Кочетов Андрей Владимирович

18 декабря, 2021

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

Написание программы по шифрованию.

Выполнение лабораторной работы

Выполнение лабораторной работы

1. Выбрал язык программирования(Python) и написал начало программы, как в предыдущей лабораторной работе(рис.1).

The screenshot shows a Jupyter Notebook window titled "Untitled". The top bar includes logos for Jupyter and Google, along with a login button labeled "Log In". Below the title bar are tabs for File, Edit, View, Insert, Cell, Kernel, Widgets, and Help. On the right side, there's a status indicator saying "Trusted" and a dropdown menu currently set to "Python". A toolbar contains icons for undo, redo, insert code, run, clear output, and save. The main area displays several code cells:

- An initial cell containing `import string`.
- In [11]:

```
def generate_key(length, symbols = string.ascii_letters + string.digits):  
    return ''.join(random.choice(symbols) for i in range(length))  
  
def xoring(text, key):  
    text_conv = [ord(i) for i in text]  
    key_conv = [ord(i) for i in key]  
    return ''.join(chr(a ^ b) for a, b in zip(text_conv, key_conv)))
```
- In [12]:

```
text = 'С Новым годом, друзья!'  
key = generate_key(len(text))  
text_shifr = xoring(text, key)  
print('Имя зашифрованного текста:') , text_shifr  
  
Вид зашифованного текста: p8Kz6HkU9dF7lmeBn0EwR
```
- In [13]:

```
[gaming(gaming(text, key), key)
```

Out[13]: 'С Новым годом, друзья!'
- In [14]:

```
key_2 = generate_key(len(text))  
text_2 = gaming(text_shifr, key_2)  
print('Расшифрованный текст:', text_2)  
  
Расшифрванный текст: С:пЕвмГодомДрузьями!
```

The notebook uses light blue syntax highlighting.

Figure 1: рис.1. Начало

2. Дописал программу и дешифровал текст без использования ключа(рис.2).

```
[13]: gaming(gaming(text, key), key)

[13]: 'С Новым Годом, друзья!'

[14]: key_2 = generate_key(len(text))
      text_2 = gaming(text.shifr, key_2)
      print("Расшифрованный текст:", text_2)

Расшифрованный текст: 8jC8H3z9K0W0t7LwHHeF8

[16]: P1 = 'Нашеискозачиш#0T1204'
      P2 = 'Текстприветствуютеца'
      key = generate_key(len(P1))
      C1 = gaming(P1, key)
      C2 = gaming(P2, key)
      print('C1:', C1)
      print('C2:', C2)

C1: 0лРвФмтхгхгхгхгх{
C2: vylwvutuu stqybzprrh

[19]: summa = gaming(C1, C2)
      P1_uncyfered = gaming(summa, P2)
      print(P1_uncyfered)

Нашеискозачиш#0T1204
```

Figure 2: рис.2. Конец

Выводы

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

Спасибо за внимание