

Отчёт по лабораторной работе 7

Кочетов Андрей Владимирович

11 декабря, 2021

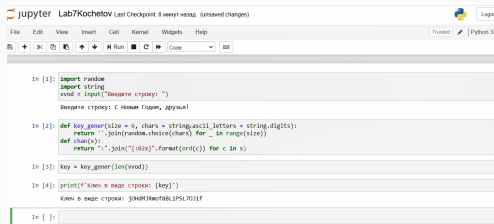
Освоить на практике применение режима однократного гаммирования.

Написание программы.

Выполнение лабораторной работы

Выполнение лабораторной работы

1. Выбрал язык программирования(Python) и начал писать программу(рис.1).



The screenshot shows a Jupyter Lab window titled 'Lab7Kochetov'. The interface includes a top menu bar with options like File, Edit, View, Insert, Cell, Kernel, Widgets, and Help. Below the menu is a toolbar with icons for running and saving code. The main area contains a code editor with the following Python code:

```
In [1]: import random
import string
vword = input("Введите строку: ")
Задайте строку: Ключевой файл

In [2]: def key_gener(size = 6, chars = string.ascii_letters + string.digits):
    return ''.join(random.choice(chars) for _ in range(size))
def chan(s):
    return ''.join("{}{:02x}".format(ord(c)) for c in s)

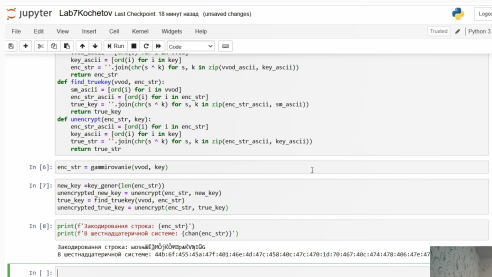
In [3]: key = key_gener(len(vword))

In [4]: print(f'Ключ к шифру: {key}')
Ключ к шифру: j0nR0Xw0f8BLPSL701f

In [ ]:
```

Figure 1: рис.1. Начало

2. Написал основую часть программы и получил закодированную строку, а также еще в шестнадцатеричной системе(рис.2).



```
key_ascii = [ord(i) for i in key]
enc_str = ''.join(chr(s + k) for s, k in zip(vvod_ascii, key_ascii))
return enc_str

def find_truekey(vvod, enc_str):
    sa_ascii = [ord(i) for i in vvod]
    enc_str_ascii = [ord(i) for i in enc_str]
    true_key = ''.join(chr(s - k) for s, k in zip(enc_str_ascii, sa_ascii))
    return true_key

def unencrypt(enc_str, key):
    enc_str_ascii = [ord(i) for i in enc_str]
    key_ascii = [ord(i) for i in key]
    true_str = ''.join(chr(s - k) for s, k in zip(enc_str_ascii, key_ascii))
    return true_str

In [6]: enc_str = gamirovanie(vvod, key)

In [7]: new_key = key_gener(len(enc_str))
unencrypted_new_key = unencrypt(enc_str, new_key)
true_key = find_truekey(vvod, enc_str)
unencrypted_true_key = unencrypt(enc_str, true_key)

In [8]: print(f'Закодированная строка: {enc_str}')
print(f'В шестнадцатеричной системе: {hex(enc_str)}')
```

Закодированная строка: 44b1d6f455145a147f480146e14d147c1458148c147c147011d1701467148c147414781406147e147

В шестнадцатеричной системе: 44b1d6f455145a147f480146e14d147c1458148c147c147011d1701467148c147414781406147e147

Figure 2: рис.2. Строка

3. Вывел ключи и декодированную строку(рис.3).

```
In [6]: enc_str = гаммирование(wod, key)

In [7]: new_key = key_gener(len(enc_str))
unencrypted_new_key = unencrypt(enc_str, new_key)
true_key = find_trunkay(wod, enc_str)
unencrypted_true_key = unencrypt(enc_str, true_key)

In [8]: print('Зашифрованная строка: {enc_str}')
print('С шифростандартичной системы: {chan(enc_str)}')

Зашифрованная строка: ыыыыыыыыыыыыыыыыыыыы
В шифростандартичной системе: ddb:f:455:45a:67f:40d:46e:dd:67c:458:68c:47c:478:1d:70:607:40c:474:478:40b:47e:47

In [9]: print('Подобранный ключ: {new_key}')
print('Строка, расшифрованная ключом: {unencrypted_new_key}')
print('Настоящий ключ: {true_key}')
print('Декодированная строка: {unencrypted_true_key}')

Подобранный ключ: gxxXlNkZpYkKdmsW
Строка, расшифрованная ключом: ыыыыыыыыыыыыыыыыыыыы
Настоящий ключ: JzN8r3XkoG8BLLP5L70JfF
Декодированная строка: С новым Годом, друзья!
```

Figure 3: рис.3. Конец

Выводы

Освоил на практике применение режима однократного гаммирования.

Спасибо за внимание