

Лабораторная работа №8

Основы информационной безопасности

Серёгина Ирина Андреевна

25 мая 2024

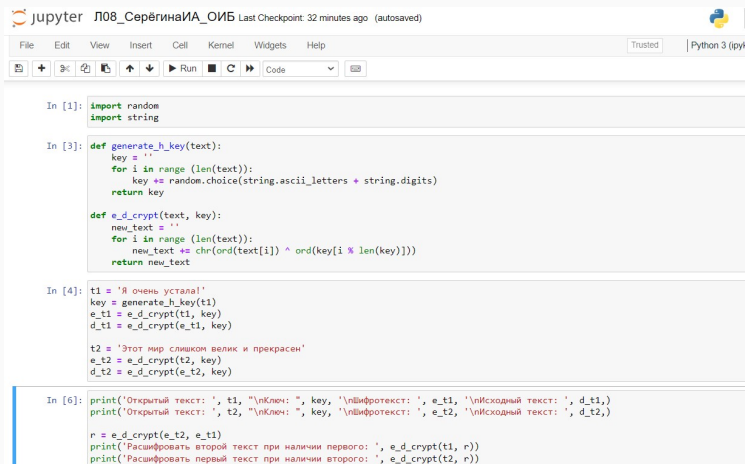
Российский университет дружбы народов, Москва, Россия

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

Требуется не зная ключа и не стремясь его определить, прочитать оба текста. Необходимо разработать приложение, позволяющее шифровать и дешифровать тексты P1 и P2 в режиме однократного гаммирования. Приложение должно определить вид шифротекстов C1 и C2 обоих текстов P1 и P2 при известном ключе; Необходимо определить и выразить аналитически способ, при котором злоумышленник может прочесть оба текста, не зная ключа и не стремясь его определить.

1.

Реализую две функции, как и в прошлой лабораторной работе, ввожу необходимые данные (рис. 1).



The screenshot shows a Jupyter Notebook window titled "jupyter л08_СерёгинаИА_ОИБ" with a last checkpoint of 32 minutes ago. The interface includes a menu bar (File, Edit, View, Insert, Cell, Kernel, Widgets, Help) and a toolbar with icons for file operations, running cells, and code execution. The notebook contains six input cells with the following code:

```
In [1]: import random
import string

In [3]: def generate_h_key(text):
    key = ''
    for i in range (len(text)):
        key += random.choice(string.ascii_letters + string.digits)
    return key

    def e_d_crypt(text, key):
        new_text = ''
        for i in range (len(text)):
            new_text += chr(ord(text[i]) ^ ord(key[i % len(key)]))
        return new_text

In [4]: t1 = 'Я очень устала!'
key = generate_h_key(t1)
e_t1 = e_d_crypt(t1, key)
d_t1 = e_d_crypt(e_t1, key)

t2 = 'Этот мир слишком велик и прекрасен'
e_t2 = e_d_crypt(t2, key)
d_t2 = e_d_crypt(e_t2, key)

In [6]: print('Открытый текст: ', t1, "\nКлюч: ", key, '\nШифротекст: ', e_t1, '\nИсходный текст: ', d_t1,)
print('Открытый текст: ', t2, "\nКлюч: ", key, '\nШифротекст: ', e_t2, '\nИсходный текст: ', d_t2,)

r = e_d_crypt(e_t2, e_t1)
print('Расшифровать второй текст при наличии первого: ', e_d_crypt(t1, r))
print('Расшифровать первый текст при наличии второго: ', e_d_crypt(t2, r))
```

Получаю необходимый результат (рис. 2).

```
r = e_d_crypt(e_t2, e_t1)
print('Расшифровать второй текст при наличии первого: ', e_d_crypt(t1, r))
print('Расшифровать первый текст при наличии второго: ', e_d_crypt(t2, r))
```

Открытый текст: Я очень устала!
 Ключ: yNMIAuZZEe4szUJ
 Шифротекст: ineŸVwXzIФŸusk
 Исходный текст: Я очень устала!
 Открытый текст: Этот мир слишком велик и прекрасен
 Ключ: yNMIAuZZEe4szUJ
 Шифротекст: eКeŃaщbКeФЦьвzVxnpŵQ0zŵEђгящЦUŸV
 Исходный текст: Этот мир слишком велик и прекрасен
 Расшифровать второй текст при наличии первого: Этот мир слишком
 Расшифровать первый текст при наличии второго: Я очень устала!Я очень устала!Я оч

Figure 2: результат работы программы

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

Спасибо за внимание!