Отчёт по лабораторной работе 7

Агеева Анастасия Борисовна

11 декабря, 2021

Цель работы

Приобретение практических навыков установки операционной системы на виртуальную машину, настройки минимально необходимых для дальнейшей работы сервисов.

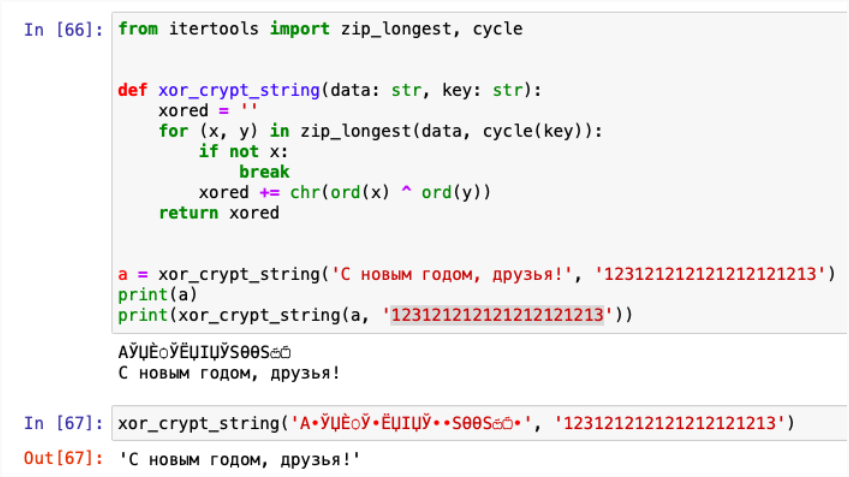
Задание

Лабораторная работа подразумевает установку на виртуальную машину VirtualBox (https://www.virtualbox.org/) операционной системы Linux, дистрибутив Centos.

Выполнение лабораторной работы

Выполнение лабораторной работы

1. Разработаем приложение, позволяющее шифровать и дешифровать данные в режиме однократного гаммирования. (рис.1).



```
In [66]: from itertools import zip_longest, cycle


         def xor_crypt_string(data: str, key: str):
             xored = ''
             for (x, y) in zip_longest(data, cycle(key)):
                 if not x:
                     break
                 xored += chr(ord(x) ^ ord(y))
             return xored


         a = xor_crypt_string('С новым годом, друзья!', '123121212121212121213')
         print(a)
         print(xor_crypt_string(a, '123121212121212121213'))

         АЎЏÈ○ЎЁЏІЏЎS0θS♂♁
         С новым годом, друзья!

In [67]: xor_crypt_string('А•ЎЏÈ○Ў•ЁЏІЏЎ••S0θS♂♁•', '123121212121212121213')
Out[67]: 'С новым годом, друзья!'
```

Figure 1: рис.1. Программа.

2. Подоберём ключ, чтобы получить сообщение «С Новым Годом Вас!». После ключа текст становится неизменным. (рис.2).

Figure 2: рис.2. Определение ключа.

3. Контрольные вопросы

1) Поясните смысл однократного гаммирования. Каждый символ попарно с символом ключа складываются по модулю.
2) Перечислите недостатки однократного гаммирования. Ключ нельзя переиспользовать. Размер ключа должен быть такой же, как и размер текста.
3) Перечислите преимущества однократного гаммирования. Основные преимущества однократного гаммирования – это симметричность и криптостойкость.
4) Почему длина открытого текста должна совпадать с длиной ключа? Потому что каждый символ открытого текста должен складываться символом ключа попарно.
5) Какая операция используется в режиме однократного гаммирования, назовите её особенности? В режиме однократного гаммирования используется сложение по

Выводы

Выводы

Я приобрела практические навыки применения режима однократного гаммирования.

Спасибо за внимание