Отчет по лабораторной работе №8

Информационная безопасность

Евдокимова Юлия Констинтиновна НПИбд-01-18

Содержание

# Цель работы

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

# Выполнение лабораторной работы

1. Необходимо разработать приложение, позволяющее шифровать и дешифровать тексты P1 и P2. Приложение должно определить вид шифротекстов C1 и C2 обоих текстов при известном ключе.

Для разработки используем наработки из лабораторной работы 7. Старый код:

def gamm(t\_text, t\_key):  
 res = ''  
 for i, j in zip(t\_text, t\_key):  
 temp=chr(ord(i) ^ ord(j))  
 res+=temp  
 return res  
  
P1 = 'С Новым годом, друзья!'  
P2 = ''  
Key = 'лабораторная работа н7'  
  
P2 = gamm(P1, Key)  
print(P2)  
  
p\_result = gamm(P2, P1)  
print(p\_result)

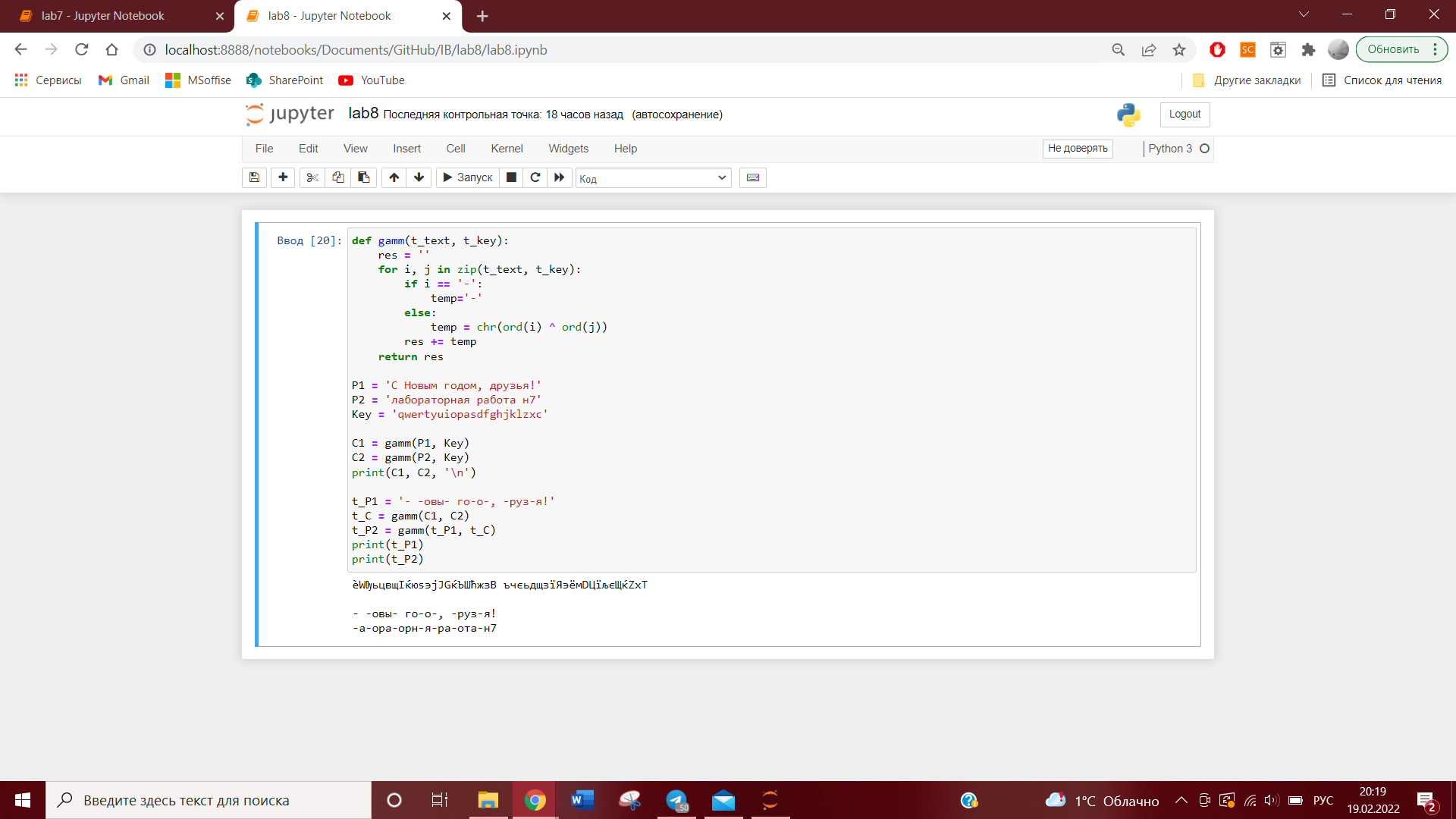
Новый код:

def gamm(t\_text, t\_key):  
 res = ''  
 for i, j in zip(t\_text, t\_key):  
 if i == '-':  
 temp='-'  
 else:  
 temp = chr(ord(i) ^ ord(j))  
 res += temp  
 return res  
  
P1 = 'С Новым годом, друзья!'  
P2 = 'лабораторная работа н7'  
Key = 'qwertyuiopasdfghjklzxc'  
  
C1 = gamm(P1, Key)  
C2 = gamm(P2, Key)  
print(C1, C2, '\n')  
  
t\_P1 = '- -овы- го-о-, -руз-я!'  
t\_C = gamm(C1, C2)  
t\_P2 = gamm(t\_P1, t\_C)  
print(t\_P1)  
print(t\_P2)

1. В функцию gamm добавлена возможность игнорировать отмеченные минусом символы
2. Переменные P - два текста.  
   Key - ключ  
   C - шифротексты.

Злоумышленник знает часть текста - t\_P1, шифротексты C1/C2  
t\_C - результат гаммирования C1 и C2  
t\_P2 - неизвестный текст 2, который в дальнейшем будет выяснен.

1. Задаем переменные
2. Гаммируем P1 и P2 по ключу, получаем C1 и C2
3. Злоумышленник знает C1 и C2, поэтому гаммирует их.
4. Затем злоумышленник гаммирует t\_P1 по получившемуся значению, получает t\_P2.
5. Теперь по имеющимся текстам можно подставить свои предположительные значения и гаммировать их по тому же значению, чтобы пошагово получать всё больше символов из P1 и P2. В данном случае будет достигнуто либо полное открытие всех символов обоих текстов, либо сужение круга возможных решений.
6. Вывод программы:



Вывод

# Контрольные вопросы

1. Как, зная один из текстов ( или ), определить другой, не зная при этом ключа?  
   По формуле
2. Что будет при повторном использовании ключа при шифровании текста?  
   Текст расшифруется.
3. Как реализуется режим шифрования однократного гаммирования одним ключом двух открытых текстов?  
   по формулам режима однократного гаммирования:
4. Перечислите недостатки шифрования одним ключом двух открытых текстов.

* ключ, попав не в те руки, даст возможность злоумышленнику расшифровать оба текста;
* можно расшифровать с помощью открытого текста другие известные шифротексты;
* можно узнать часть текста, используя заранее известный шаблон и формат другого текста.

1. Перечислите преимущества шифрования одним ключом двух открытых текстов.

* скорость шифрования выше;
* простой алгоритм шифрования;
* шифротекст сильно меняется, если изменяется ключ или открытый текст.

# Выводы

На основе проделанной работы освоила на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.