Отчет по лабораторной работе №7

Информационная безопасность

Евдокимова Юлия Константиновна НПИбд-01-18

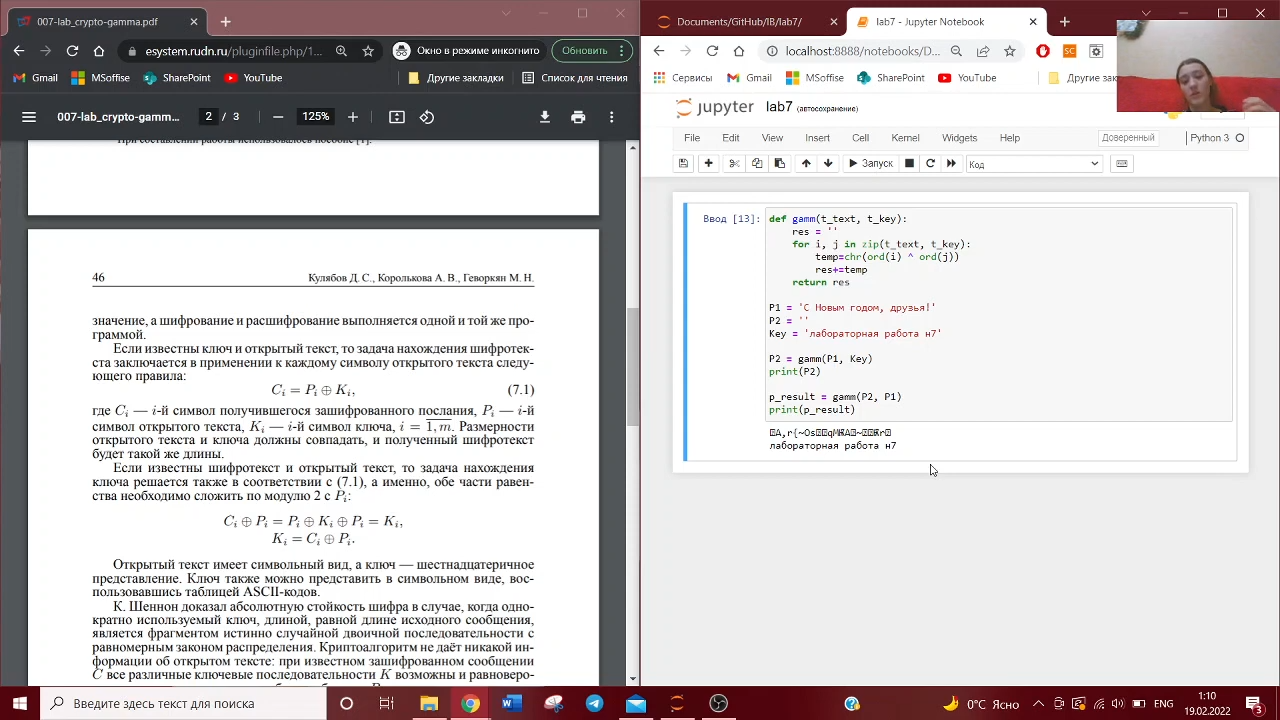
Содержание

# Цель работы

Освоить на практике применение режима однократного гаммирования.

# Выполнение лабораторной работы

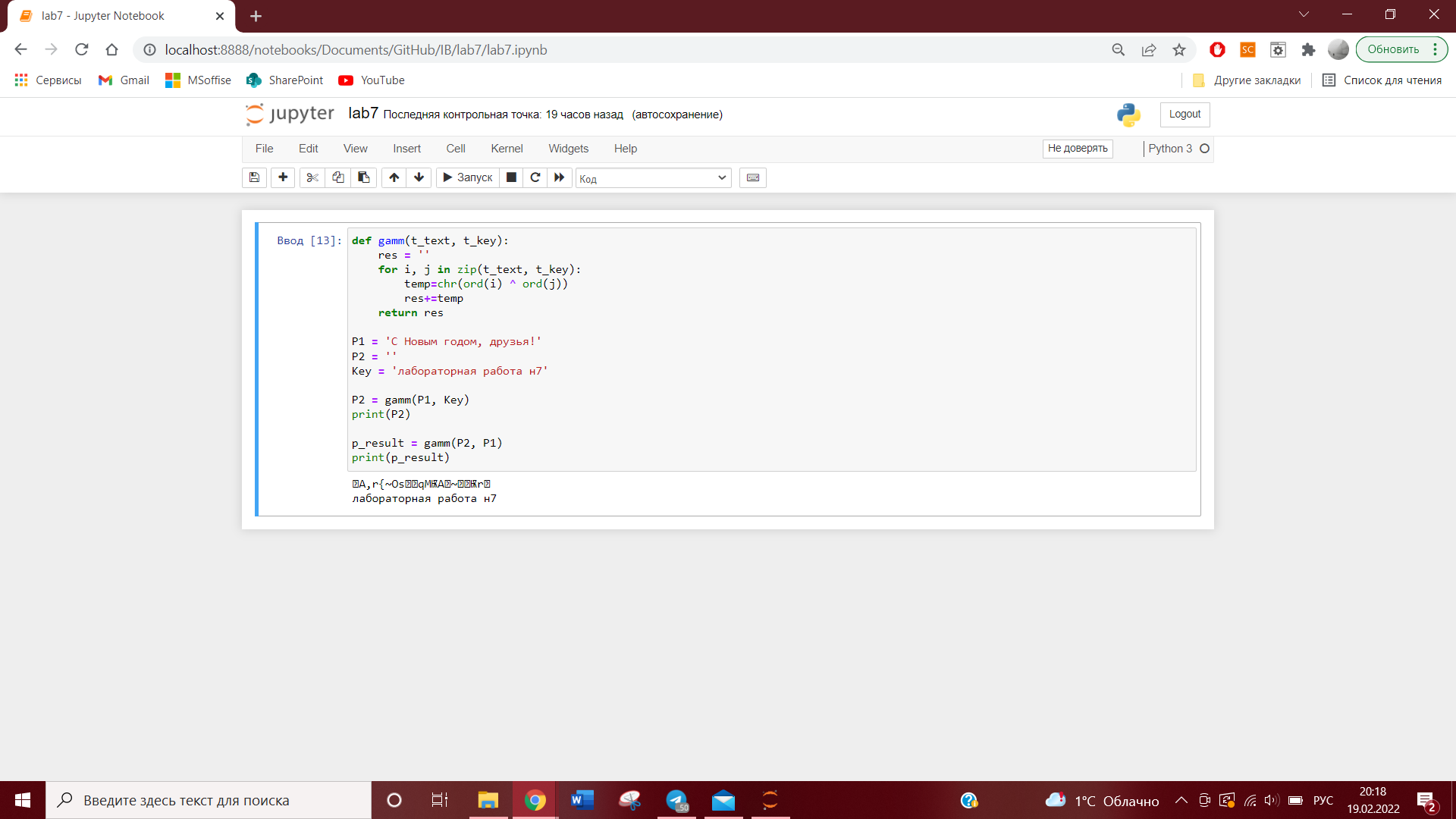
1. Разработаем приложение на языке программирования python для шифрования и расшифрования данных методом однократного гаммирования. Основная функция для гаммирования — gamm
2. После функции объявляем основные переменные. P1 - Сообщение P2 - шифротекст, который нужно получить Key - Ключ для гаммирования из P1 в P2
3. Затем вызовем функцию гаммирования, чтобы найти шифротекст.
4. Повторно вызовем функцию гаммирования, но теперь для нахождения ключа из имеющихся сообщения и шифротекста.



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)

1. Вывод программы:



Вывод

# Контрольные вопросы

1. Поясните смысл однократного гаммирования. Смысл однократного гаммирования состоит в том, что каждый символ попарно с символом ключа побитово складываются по модулю.
2. Перечислите недостатки однократного гаммирования. Недостатками является то, что ключ нельзя использовать повторно, а также размер ключа должен быть равен размеру текста и шифротекста.
3. Перечислите преимущества однократного гаммирования. Основными преимуществами являются симметричность и криптостойкость.
4. Почему длина открытого текста должна совпадать с длиной ключа? Каждый символ открытого текста должен попарно складываться с символом ключа.
5. Какая операция используется в режиме однократного гаммирования, назовите её особенности? В режиме однократного гаммирования используется сложение по модулю 2: при сложении чисел с другим получается исходное. Таблица истинности: 0+0 = 0, 0+1=1, 1+0=1, 1+1=0. Если в методе шифрования используется однократная вероятностная гамма той же длины, что и подлежащий сокрытию текст, то текст нельзя раскрыть.
6. Как по открытому тексту и ключу получить шифротекст? Для этого необходимо сложить попарно символы текста с ключом по модулю 2.
7. Как по открытому тексту и шифротексту получить ключ? Для этого необходимо сложить попарно по модулю 2 символы открытого текста с символами шифротекста.
8. В чём заключаются необходимые и достаточные условия абсолютной стойкости шифра? Необходимые и достаточные условия абсолютной стойкости шифра заключаются в полной случайности ключа; равенстве длин ключа и открытого текста; использовании ключа однократно.

# Выводы

На основе проделанной работы освоила на практике применение режима однократного гаммирования.