Лабораторная работа №7

Элементы криптографии. Однократное гаммирование

Artem Smirnov"

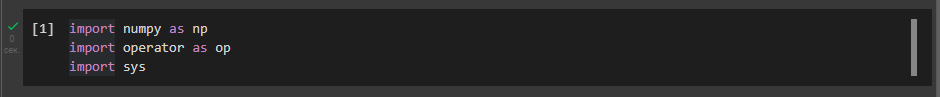
Содержание

# Цель работы

Освоить на практике применение режима однократного гаммирования.

# Выполнение лабораторной работы

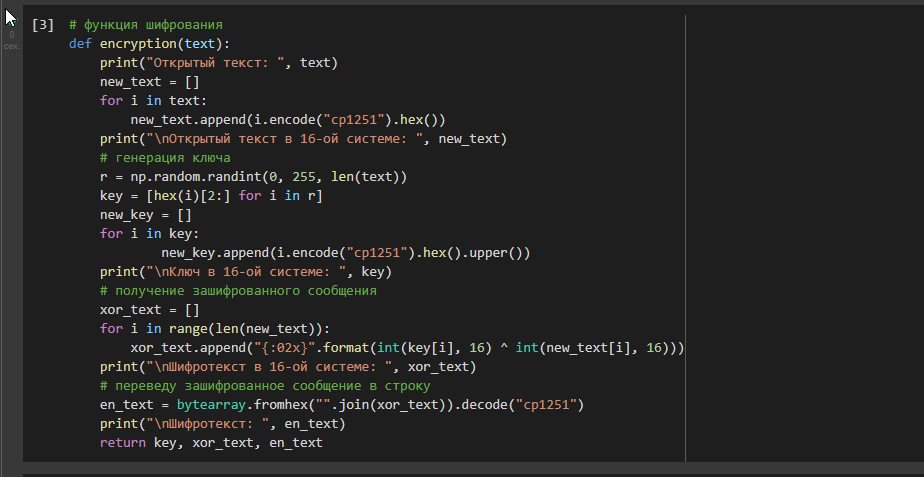
Импортирую библиотеки:



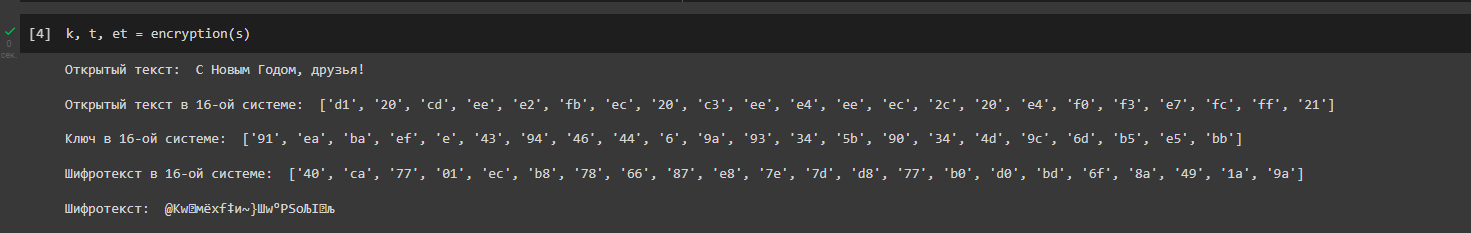
Подаю на вход сообщение:



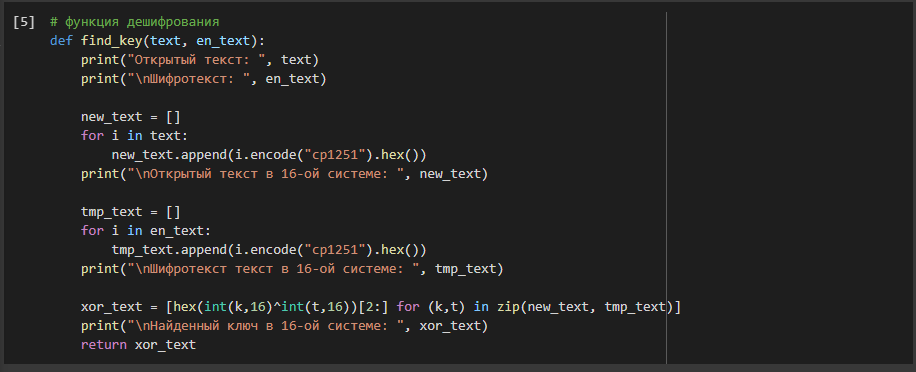
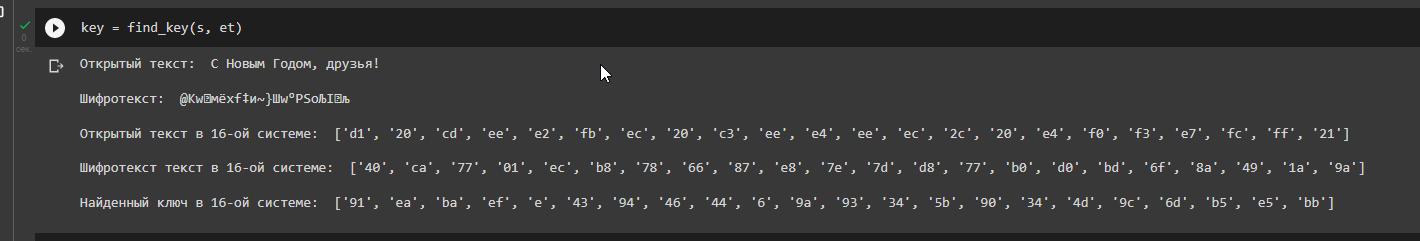
1. Определю вид шифротекста при известном ключе и известном открытом  
   тексте.  
   Функция получает на вход строку, переводит ее в шестнадцатеричную систему  
   счисления. Затем в программе рандомно генерируется ключ. При помощи ключа  
   получаю зашифрованное сообщение в шестнадцатеричной системе счисления. Затем  
   перевожу это сообщение в строковый вид.

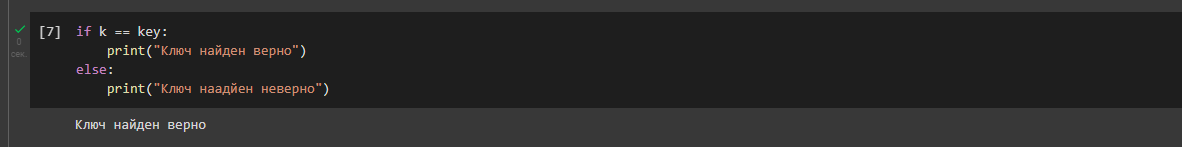


Результат работы функции:



1. Определю ключ, с помощью которого шифротекст может быть преобразован  
   в некоторый фрагмент текста, представляющий собой один из возможных  
   вариантов прочтения открытого текста. Функция нахождения ключа получает на вход две строки: открытый текст и  
   зашифрованный. Затем она преобразует строки в шестнадцатеричный формат и  
   выполняет операцию XOR для нахождения ключа.

* 
* Результат работы функции:
* 
* Проверка:



### Ответы на контрольные вопросы

1. Поясните смысл однократного гаммирования.  
   Гаммирование – выполнение операции XOR между элементами гаммы и  
   элементами подлежащего сокрытию текста. Если в методе шифрования используется  
   однократная вероятностная гамма (однократное гаммирование) той же длины, что и  
   подлежащий сокрытию текст, то текст нельзя раскрыть. Даже при раскрытии части  
   последовательности гаммы нельзя получить информацию о всём скрываемом тексте.
2. Перечислите недостатки однократного гаммирования.  
   Абсолютная стойкость шифра доказана только для случая, когда однократно  
   используемый ключ, длиной, равной длине исходного сообщения, является  
   фрагментом истинно случайной двоичной последовательности с равномерным  
   законом распределения.
3. Перечислите преимущества однократного гаммирования.  
   Во-первых, такой способ симметричен, т.е. двойное прибавление одной и той  
   же величины по модулю 2 восстанавливает исходное значение. Во-вторых,  
   шифрование и расшифрование может быть выполнено одной и той же программой.  
   Наконец, Криптоалгоритм не даёт никакой информации об открытом тексте: при  
   известном зашифрованном сообщении C все различные ключевые  
   последовательности K возможны и равновероятны, а значит, возможны и любые  
   сообщения P.
4. Почему длина открытого текста должна совпадать с длиной ключа?  
   Если ключ короче текста, то операция XOR будет применена не ко всем  
   элементам и конец сообщения будет не закодирован. Если ключ будет длиннее, то  
   появится неоднозначность декодирования.
5. Какая операция используется в режиме однократного гаммирования, назовите  
   её особенности?  
   Наложение гаммы по сути представляет собой выполнение побитовой  
   операции сложения по модулю 2, т.е. мы должны сложить каждый элемент гаммы с  
   соответствующим элементом ключа. Данная операция является симметричной, так  
   как прибавление одной и той же величины по модулю 2 восстанавливает исходное  
   значение
6. Как по открытому тексту и ключу получить шифротекст?  
   В таком случае задача сводится к правилу:  
    Ci = Pi ⊕ Ki, т.е. мы поэлементно получаем символы зашифрованного сообщения,  
    применяя операцию исключающего или к соответствующим элементам ключа и  
    открытого текста.
7. Как по открытому тексту и шифротексту получить ключ?  
   Подобная задача решается путем применения операции исключающего или к  
   последовательностям символов зашифрованного и открытого сообщений:

* Ki = Pi ⊕ Ci.

1. В чем заключаются необходимые и достаточные условия абсолютной  
   стойкости шифра?  
   Необходимые и достаточные условия абсолютной стойкости шифра:

* – полная случайность ключа;  
  – равенство длин ключа и открытого текста;  
  – однократное использование ключа.

### Вывод

В ходе данной лабораторной работы я освоил на практике применение  
режима однократного гаммирования.

# Список литературы

* [Кулябов Д. С., Королькова А. В., Геворкян М. Н Лабораторная работа №7](https://esystem.rudn.ru/pluginfile.php/1651751/mod_resource/content/3/004-lab_discret_extattr.pdf)