Отчет по лабораторной работе №7

Элементы криптографии. Однократное гаммирование

Исаханян Эдуард Тигранович

2022 Sep 21th

Содержание

# Цель работы

Освоить на практике применение режима однократного гаммирования.

# Задание

1. Написать программу, которая должна определить вид шифротекста при известном ключе и известном открытом тексте;
2. Также эта программа должна определить ключ, с помощью которого шифротекст может быть преобразован в некоторый фрагмент текста, представляющий собой один из возможных вариантов прочтения открытого текста.

# Выполнение лабораторной работы

Напишем функцию шифрования, которая определяет вид шифротекста при известном ключе и известном открытом тексте “С Новы Годом, друзья!”. (рис. 1)

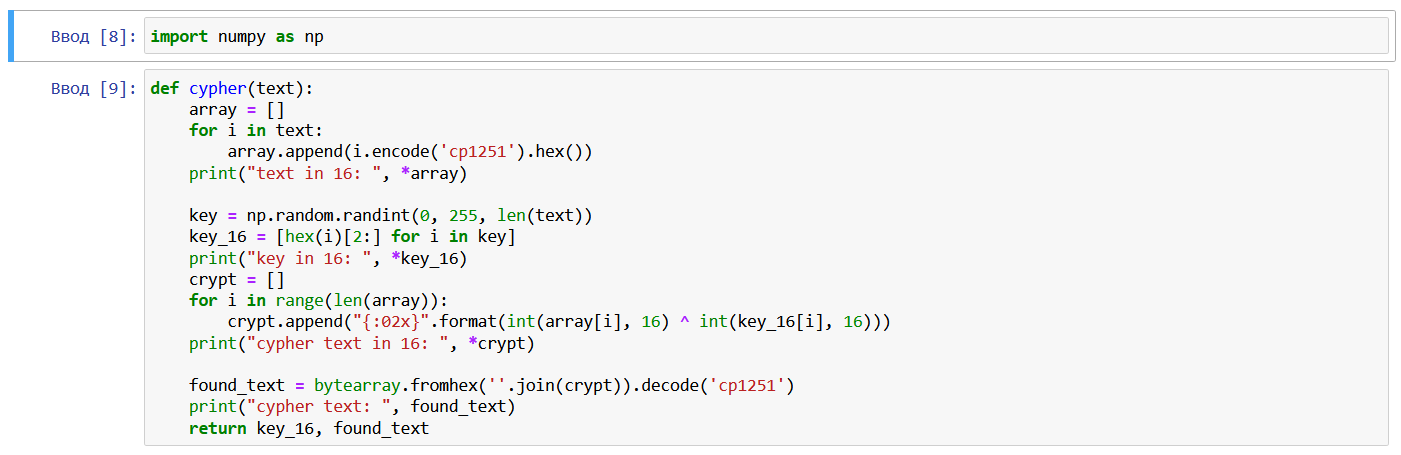


Figure 1: Функция, шифрующая данные

А также посмотрим на работу данной функции. (рис. 2)

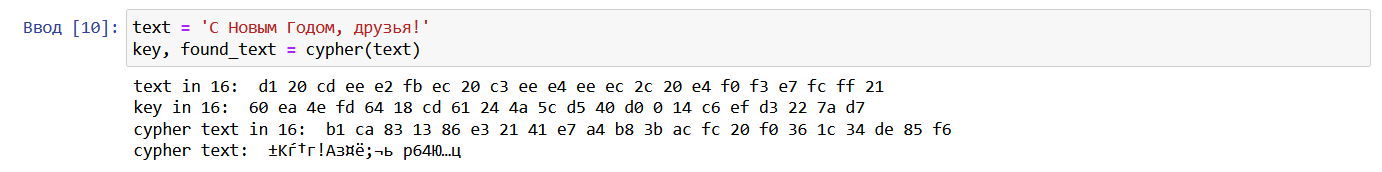


Figure 2: Результат работы функции, шифрующей данные

Напишем функцию дешифровки, которая определяет ключ, с помощью которого шифротекст может быть преобразован в некоторый фрагмент текста, представляющий собой о дин из возможных вариантов прочтения открытого текста. (рис. 3)

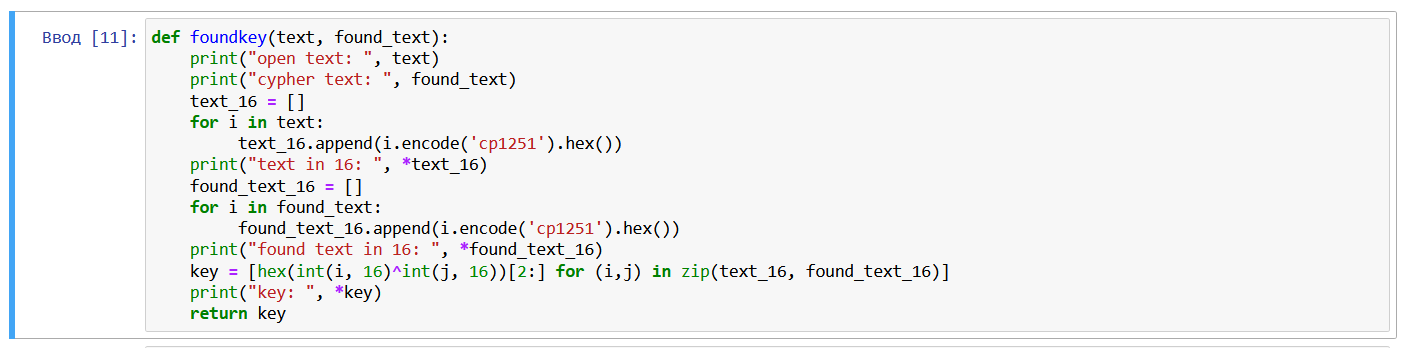


Figure 3: Функция, дешифрующая данные

А также посмторим на результаты работы программы. (рис. 4)

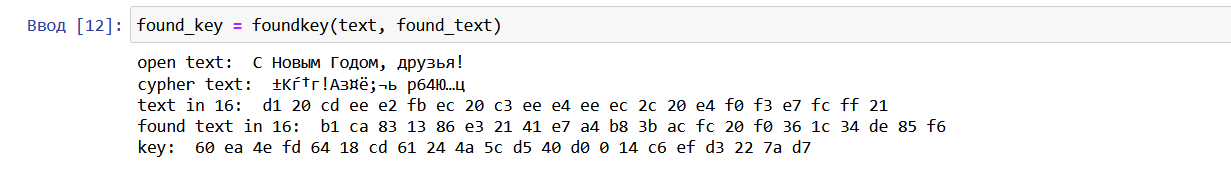


Figure 4: Результат работы функции, шифрующей данные

Сравнение ключей, полученных с помощью первой и второй функций. (рис. 5)

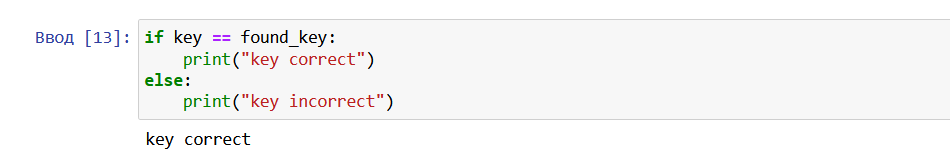


Figure 5: Сравнение ключей

## Контрольные вопросы

1. Поясните смысл однократного гаммирования.  
   Одократное 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.  
   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.  
   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?  
   Длина открытого текста должна совпадать с длиной ключа, т.к. если ключ короче текста, то операция XOR будет применена не ко всем элементам и конец сообщения будет не закодирован, а если ключ будет длиннее, то появится неоднозначность декодирования.
5. Какая операция используется в режиме однократного гаммирования, назовите её особенности?  
   Операция XOR используется в режиме однократного гаммирования. 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?  
   Получение шифротекста по открытому тексту и ключу:
7. Как по открытому тексту и шифротексту получить ключ?  
   Получение ключа по окрытому тексту и шифротексту:
8. В чем заключаются необходимые и достаточные условия абсолютной стойкости шифра?  
   Необходимы и достаточные условия абсолютной стойкости шифра: полная случайность ключа; равенство длин ключа и открытого текста; однократное использование ключа.

# Выводы

Освоили на практике применение режима однократного гаммирования.

# Список литературы

1. Методические материалы к лабораторной работе, представленные на сайте “ТУИС РУДН” https://esystem.rudn.ru/  
   ::: {#refs} :::