Отчет по лабораторной работе №7

Элементы криптографии. Однократное гаммирование

Смородова Дарья Владимировна

2022 Oct 21st

Содержание

# Цель работы

Освоить на практике применение режима однократного гаммирования.

# Задание лаборатоной работы

Нужно подобрать ключ, чтобы получить сообщение «С Новым Годом, друзья!». Требуется разработать приложение, позволяющее шифровать и дешифровать данные в режиме однократного гаммирования. Приложение должно:

1. Определить вид шифротекста при известном ключе и известном открытом тексте.
2. Определить ключ, с помощью которого шифротекст может быть преобразован в некоторый фрагмент текста, представляющий собой один из возможных вариантов прочтения открытого текста.

# Теоретическое введение[[1]](#footnote-22)

Гаммирование представляет собой наложение (снятие) на открытые (зашифрованные) данные последовательности элементов других данных, полученной с помощью некоторого криптографического алгоритма, для получения зашифрованных (открытых) данных. Иными словами, наложение гаммы — это сложение её элементов с элементами открытого (закрытого)текста по некоторому фиксированному модулю, значение которого представляет собой известную часть алгоритма шифрования.

В соответствии с теорией криптоанализа, 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.

Наложение гаммы по сути представляет собой выполнение операции сложения по модулю 2 (XOR) (обозначаемая знаком ) между элементами гаммы и элементами подлежащего сокрытию текста. Напомним, как работает операция XOR над битами: .

Такой метод шифрования является симметричным, так как двойное прибавление одной и той же величины по модулю 2 восстанавливает исходное значение, а шифрование и расшифрование выполняется одной и той же программой. Если известны ключ и открытый текст, то задача нахождения шифротекста заключается в применении к каждому символу открытого текста следующего правила:

где — -й символ получившегося зашифрованного послания, — -й символ открытого текста, — -й символ ключа. Размерности открытого текста и ключа должны совпадать, и полученный шифротекст будет такой же длины.

Если известны шифротекст и открытый текст, то задача нахождения ключа решается также, а именно, обе части равенства необходимо сложить по модулю 2 с :

Открытый текст имеет символьный вид, а ключ — шестнадцатеричное представление. Ключ также можно представить в символьном виде, воспользовавшись таблицей ASCII-кодов.

К. Шеннон доказал абсолютную стойкость шифра в случае, когда однократно используемый ключ, длиной, равной длине исходного сообщения, является фрагментом истинно случайной двоичной последовательности с равномерным законом распределения. Криптоалгоритм не даёт никакой информации об открытом тексте: при известном зашифрованном сообщении все различные ключевые последовательности возможны и равновероятны, а значит, возможны и любые сообщения .

Необходимые и достаточные условия абсолютной стойкости шифра:

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

# Выполнение лабораторной работы

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

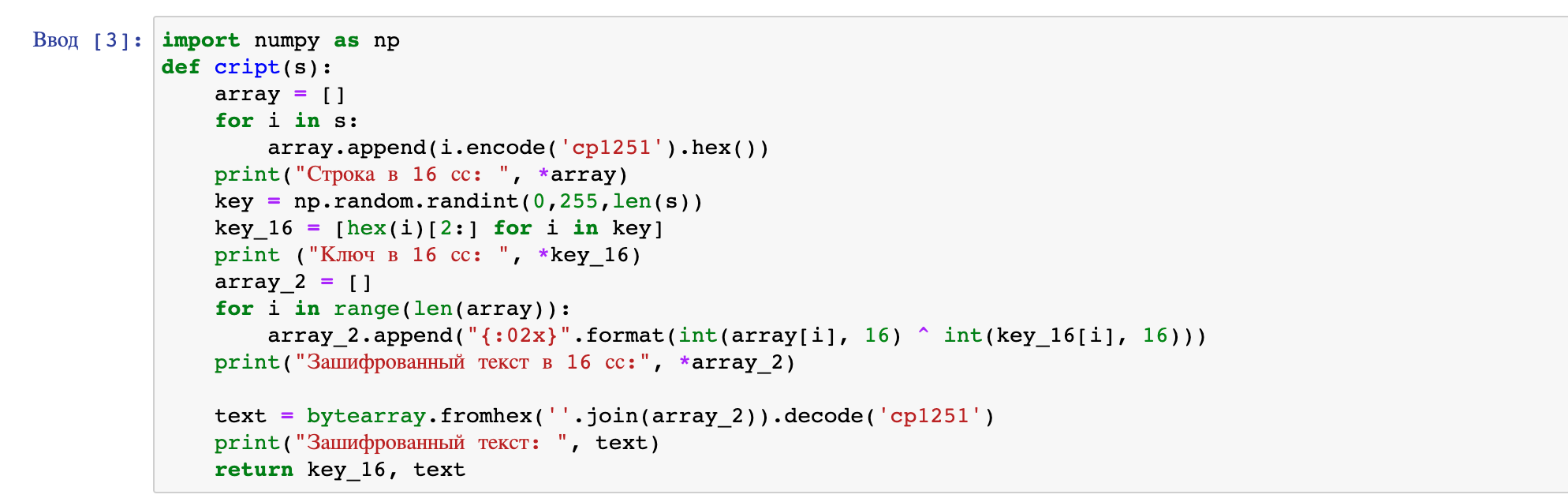


Figure 1: Функция шифрования данных

1. Посмотрим работу данной функции (рис. 2):

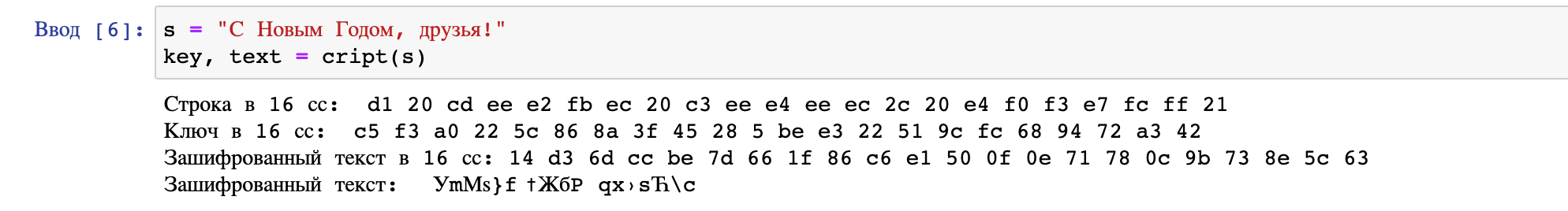


Figure 2: Результат работы функции, шифрующей данные

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



Figure 3: Функция, дешифрующая данные

1. Посмторим на результаты функции дешифрования(рис. 4):

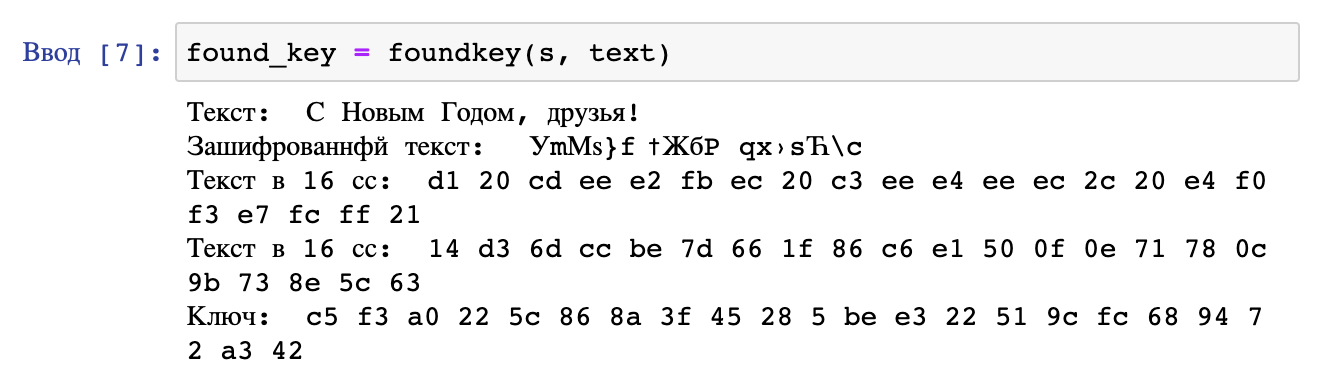


Figure 4: Результат работы функции, дешифрующей данные

5.Сравним ключей, полученные с помощью первой и второй функций (рис. 5):



Figure 5: Сравнение ключей

Ключи совпали, программа работает верно.

# Контрольные вопросы

1. Поясните смысл однократного гаммирования.  
   Одократное гаммирование представляет собой наложение (снятие) на открытые (зашифрованные) данные последовательности элементов других данных, полученной с помощью некоторого криптографического алгоритма, для получения зашифрованных (открытых) данных. Иными словами, наложение гаммы — это сложение её элементов с элементами открытого (закрытого)текста по некоторому фиксированному модулю, значение которого представляет собой известную часть алгоритма шифрования.
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

В ходе выполнения данной лабораторной работы, мы освоили на практике применение режима однократного гаммирования.

# Список литературы

1. [Методические материалы к лабораторной работе, представленные на сайте “ТУИС РУДН”](https://esystem.rudn.ru/)

1. Методические материалы к лабораторной работе [↑](#footnote-ref-22)