Информационная безопасность.

Лабораторная работа №7.

Филиппова Веорника Сергеевна.

Содержание

[Цель работы 1](#_Toc90119163)

[Задание 1](#_Toc90119164)

[Выполнение лабораторной работы 1](#_Toc90119165)

[Выводы 4](#_Toc90119166)

# Цель работы

Освоить на практике применение режима однократного гаммирования

# Задание

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.

# Выполнение лабораторной работы

Написала функцию шифрования, которая определяет вид шифротекста при известном ключе и известном открытом тексте “С Новы Годом, друзья!” ‘crypto’.



Рисцунок 1

Написала 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.



Рисунок 2

Проверка работы функции шифрования на примере из лабораторной работы

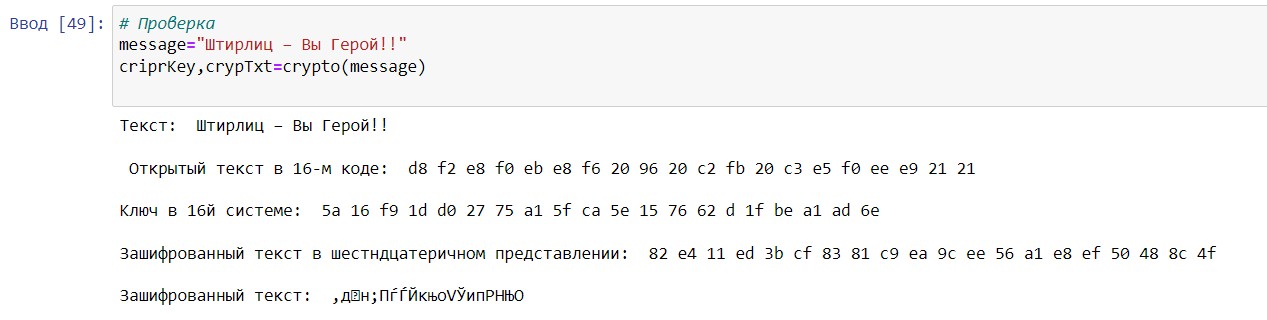


Рисунок 3

Результат функции шифрования.

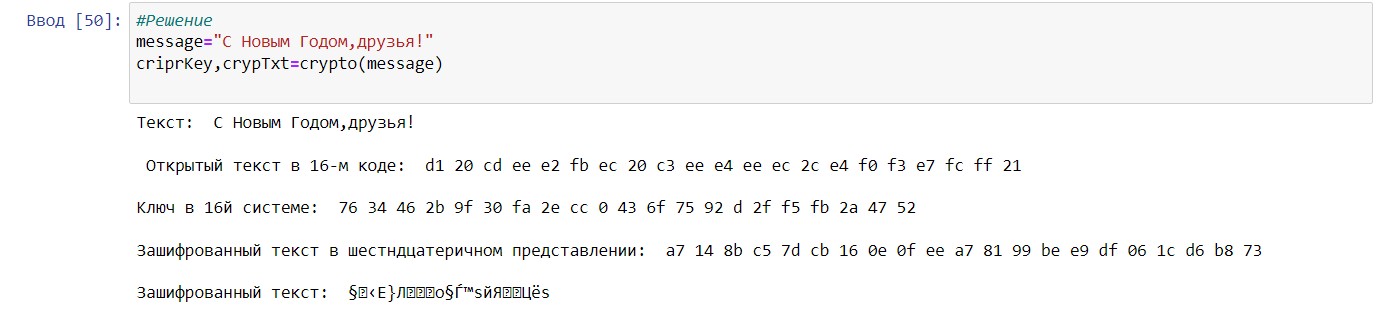


Рисунок 4

Результат функции дешифрования.

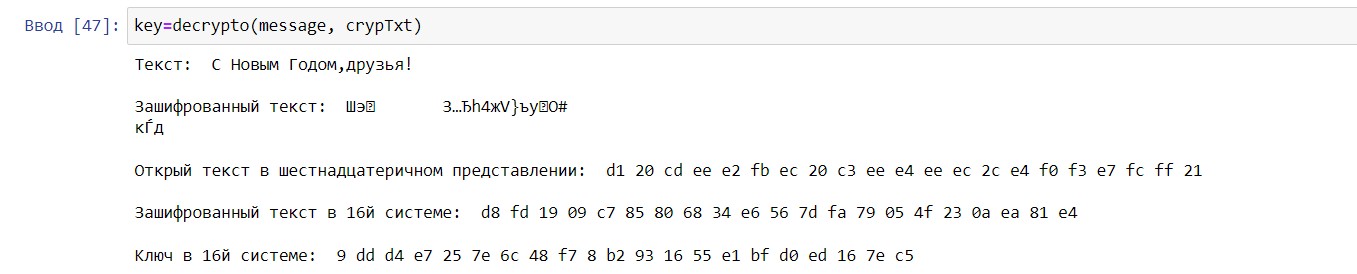


Рисунок 5

#Ответы на вопросы

1. Одократное гаммирование - выполнение операции XOR между элементами гаммы и элементами подлежащего сокрытию текста.  
   Даже при раскрытии части последовательности гаммы нельзя получить информацию о всём скрываемом тексте.
2. 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. 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. 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. 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. Получение шифротекста по открытому тексту и ключу:
7. Получение ключа по окрытому тексту и шифротексту:
8. Необходимы и достаточные условия абсолютной стойкости шифра:
   * полная случайность ключа;
   * равенство длин ключа и открытого текста; однократное использование ключа.

# Выводы

Освоила на практике применение режима однократного гаммирования.