Лабораторная работа №7.

Элементы криптографии. Однократное гаммирование

Силкина Мария Александровна

Содержание

# Цель работы

Освоить на практике применение режима однократного гаммирования.

# Задачи

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.
3. Ответить на контрольные вопросы

# Выполнение лабораторной работы

##Теоретическая справка

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

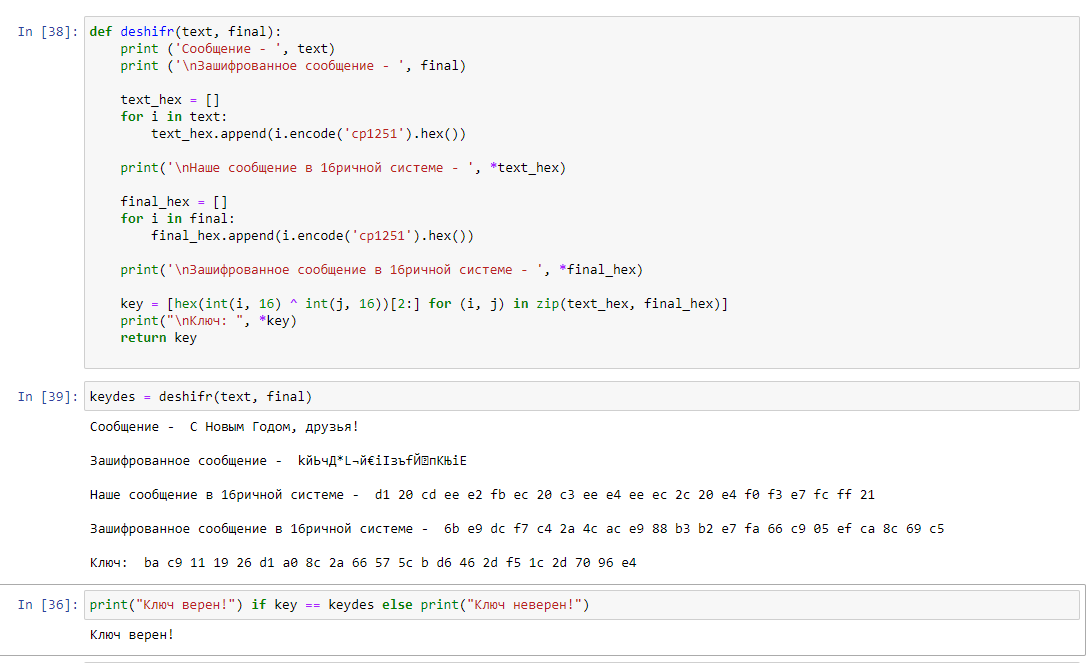
## Выполнение задач

Первым шагом написала функцию шифрования, которая определяет вид шифротекста при известном ключе и известном открытом тексте “С Новым Годом, друзья!”, который был задан по условию. В выводе я получила наш изначальный текст, его вид в шестнадцатеричной системе, рандомный ключ и зашифрованный текст. (рис - @fig:001)



Функция, шифрующая данные и ее выполнение

Далее я создала функцию для дешифрования, которая определяет ключ, с помощью которого шифротекст может быть преобразован в некоторый фрагмент текста, представляющий собой один из возможных вариантов прочтения открытого текста. (рис - @fig:002)



Функция, дешифрующая данные и ее выполнение

##Контрольные вопросы

1. Однократное гаммирование - выполнение операции XOR между элементами гаммы и элементами подлежащего сокрытию текста. Если в методе шифрования используется 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.

Недостаток 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.

1. Преимущества однократного гаммирования:

* Такой способ симметричен, то есть двойное прибавление одной и той же величины по модулю 2 восстанавливает исходное значение.
* Шифрование и расшифрование может быть выполнено одной и той же программой.
* 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.

1. 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.
2. 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.
3. Получение шифротекста по открытому тексту и ключу:
4. Получение ключа по окрытому тексту и шифротексту:
5. Необходимы и достаточные условия абсолютной стойкости шифра: полная случайность ключа; равенство длин ключа и открытого текста; однократное использование ключа.

# Выводы

Освоила использования однократного гаммирования для шифрования и дешифрования данных. # Библиография

1. Кулябов Д. С., Королькова А. В., Геворкян М. Н. Информационная безопасность компьютерных сетей. Лабораторная работа № 5. Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов.