Лабораторная работа №8.

Элементы криптографии. Шифрование (кодирование) различных исходных текстов одним ключом

Силкина Мария Александровна

Содержание

# Цель работы

Освоить на практике применение режима однократного гаммирования на примере кодирования нескольких различных текстов одним ключом.

# Задачи

1. Написать программу, которая должна определять вид шифротекстов при известных открытых текстах и при известном ключе. Также эта программа должна определить вид одного из текстов, зная вид другого открытого текста и зашифрованный вид обоих текстов без использования ключа.
2. Ответить на контрольные вопросы

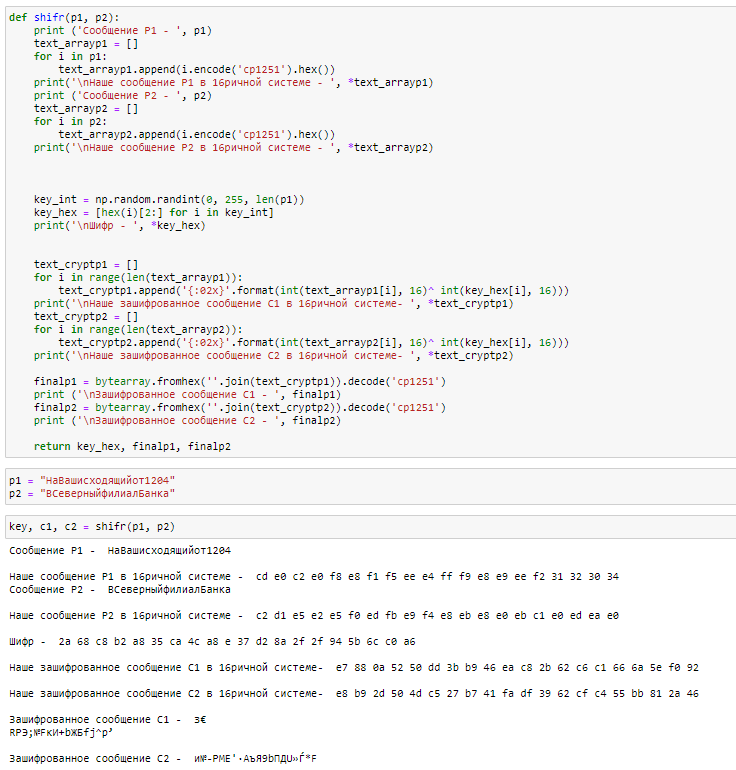
# Выполнение лабораторной работы

##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

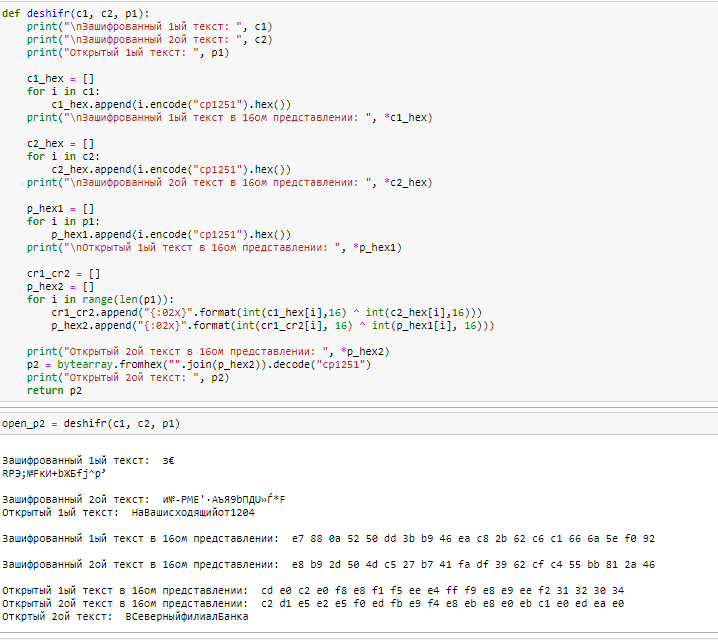
## Выполнение задач

Первым шагом написала функцию шифрования, которая определяет вид шифротекстов при известном ключе и известном открытом тексте. В выводе я получила наши изначальные тексты, их представление в шестнадцатеричной системе, рандомный ключ и зашифрованные тексты. (рис - @fig:001)



Функция, шифрующая данные и ее выполнение

Далее я создала функцию для дешифрования, которая при знании зашифрованных текстов и иодного изначального, может найти второй (неизвестный) текст. (рис - @fig:002)



Функция, дешифрующая данные и ее выполнение

##Контрольные вопросы

1. Зная один из текстов, мы можем определить другой, вопспользовавшись следующей формулой: , где и - шифротексты. Т.е. ключ в данной формуле не используется.
2. При повторном использовании ключа при шифровании текста получим исходное сообщение.
3. Режим шифрования однократного гаммирования одним ключом двух открытых текстов реализуется по следующей формуле:

где - шифротексты, - открытые тексты, - единый ключ шифровки

1. Недостатки шифрования одним ключом двух открытых текстов:

* Имея на руках одно из сообщений в открытом виде и оба шифротекста, злоумышленник способен расшифровать каждое сообщение, не зная ключа.
* Зная шаблон сообщений, злоумышленник получает возможность определить те символы сообщения , которые находятся на позициях известного шаблона сообщения .

1. Преимущество шифрования одним ключом двух текстов заключается в том, что такой подход помогает упростить процесс шифрования и дешифровки. Также, при отправке сообщений между двумя компьютерами, удобнее пользоваться одним общим ключом для передаваемых данных

# 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 № 8. Элементы криптографии. Шифрование (кодирование) различных исходных текстов одним ключом.