Отчёт по лабораторной работе 7

Элементы криптографии. Однократное гаммирование

Максимова Ксения НБИбд-02-18

Содержание

[Цель работы 1](#_Toc90045276)

[Задание 1](#_Toc90045277)

[Теоретическое введение 1](#_Toc90045278)

[Выполнение лабораторной работы 2](#_Toc90045279)

[Выводы 2](#_Toc90045280)

[Список литературы 2](#_Toc90045281)

# Цель работы

Освоить на практике применение режима однократного гаммирования.

# Задание

Разработать приложение, позволяющее шифровать и дешифровать данные в режиме однократного гаммирования.

# Теоретическое введение

Смысл однократного гаммирования заключается в наложении (снятии) 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 [[1]].

Преимущества однократного гаммирования[[1]]: 1. Абсолютная стойкость шифра в случае, когда однократно используемый ключ, длиной, равной длине исходного сообщения, является фрагментом истинно случайной двоичной последовательности с равномерным законом распределения. 2. Криптоалгоритм не даёт никакой информации об открытом тексте: при известном зашифрованном сообщении все различные ключевые последовательности возможны и равновероятны

При всех очевидных приемуществах, есть один весомый недостаток, который сразу бросается в глаза, - это необходимость иметь огромные объемы данных, которые можно было бы использовать в качестве гаммы. Для этих целей обычно пользуются датчиками настоящих случайных чисел[[2]].

Необходимые и достаточные условия абсолютной стойкости шифра[[1]]: - полная случайность ключа; - равенство длин ключа и открытого текста; - однократное использование ключа

# Выполнение лабораторной работы

Программа, позволяющая шифровать и дешифровать данные в режиме однократного гаммирования.

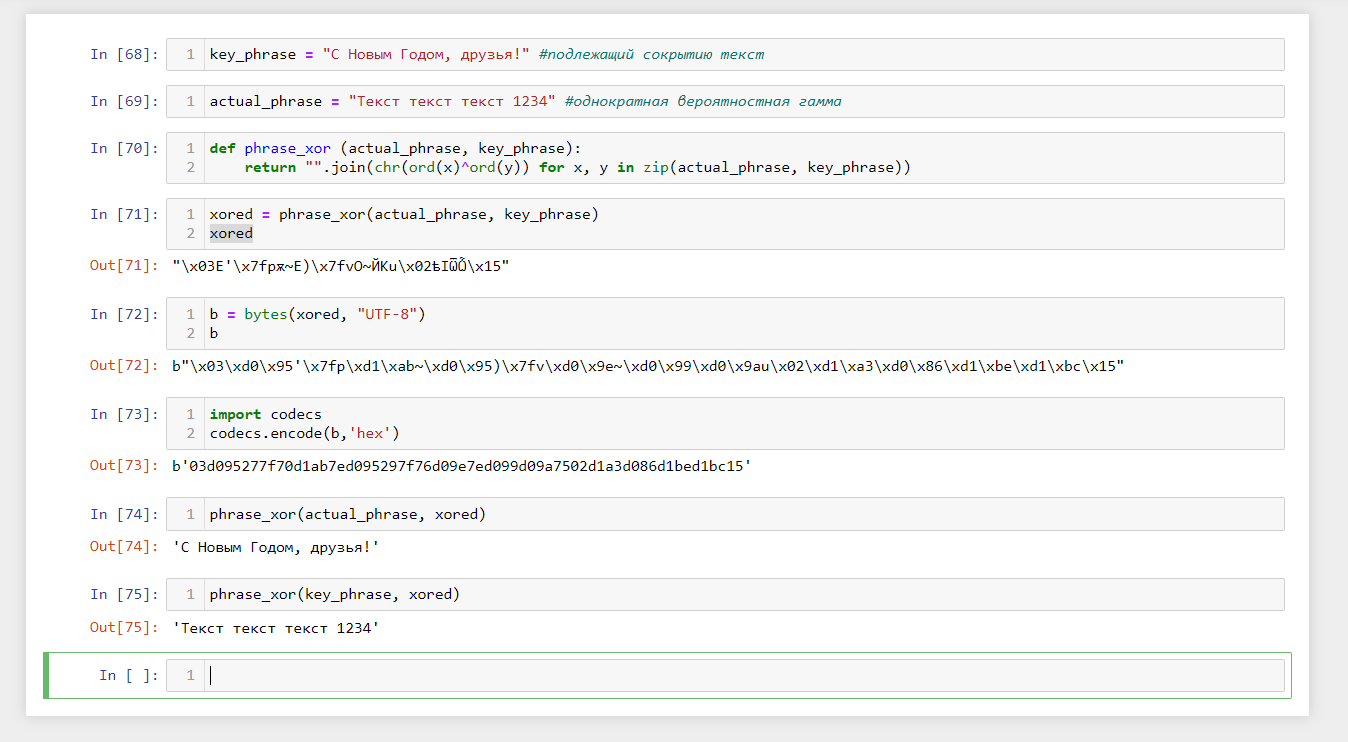


Рис 1.Код программы

[Рисунок 1](image/1.png)

# Выводы

Разработано приложение, позволяющее шифровать и дешифровать данные в режиме однократного гаммирования.

# Список литературы

[1. Элементы криптографии. Однократное гаммирование](https://esystem.rudn.ru/pluginfile.php/1198312/mod_resource/content/2/007-lab_crypto-gamma.pdf)

[2. Прикладные задачи шифрования](https://bugtraq.ru/library/books/crypto/chapter7/)