Элементы криптографии. Однократное гаммирование

Максимова Ксения НБИбд-02-18[1]

10 декабря, 2021, Москва, Россия

[1]Российский Университет Дружбы Народов

Цель лабораторной работы

Освоить на практике применение режима однократного гаммирования.

Введение

Смысл однократного гаммирования заключается в наложении гаммы, то есть в сложении элементов некоторой строки с элементами открытого (закрытого) текста по некоторому фиксированному модулю, значение которого представляет собой известную часть алгоритма шифрования.

Преимущества однократного гаммирования

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 сообщениивсе различные ключевые последовательности возможны и равновероятны

Недостатки

При проведении процедуру однократного гаммирования необходимо хранить огромные объемы данных, которые можно было бы использовать в качестве гаммы.

Необходимые и достаточные условия абсолютной стойкости шифра

1. полная случайность ключа;
2. равенство длин ключа и открытого текста;
3. однократное использование ключа

Результат лабораторной работы

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