

Введение

В криптографии широко используется аддитивный метод (метод гаммирования). Его идея заключается в том, что к открытому тексту на передаче прибавляется псевдослучайная секретная последовательность, а на приеме эта последовательность вычитается. Известны методы криптоанализа (взлома), которые позволяют произвести дешифрацию криптограммы при малом периоде гаммы даже при неизвестном ключе.

В данной лабораторной работе рассматривается возможность повышения криптостойкости аддитивного метода шифрования, которая основывается на том, что при шифровании открытого текста используется не только логическая операция ИСКЛЮЧАЮЩЕЕ ИЛИ, но и другие логические и арифметические операции. Другими операциями могут быть: логические операции равнозначность, инверсия, повторение и арифметическая операция суммирования по модулю два.

В данной работе моделирование криптосистемы осуществляется с помощью программы Multisim.