ПРИМЕНЕНИЕ БИНОМИАЛЬНЫХ СИСТЕМ СЧИСЛЕНИЯ В КАЧЕСТВЕ ЭЛЕМЕНТОВ КРИПТОСИСТЕМ

д-р техн. наук, проф. А. А. Борисенко, ст. Коломиец М. И.

Расширить возможности стандартных симметричных блочных криптосистем (AES, RC5, RC6 и др.) можно за счет использования в качестве внешней управляемой операции зависящей от преобразуемых данных операцию перехода от биномиальной системы счисления к двоичной. При этом аргументом функции перехода F является число единиц k во входной n-битной комбинации. В результате чего образуется шифрограмма, состоящая из m-битной информационной и s-битной ключевой части, т. е. образуется система с неравномерным ключом. Для одного шифруемого блока длина информационной части определяется максимальной мощностью биномиального алфавита (1), а длина ключа максимально возможным количеством единиц во входном блоке (2)

$$m = log_2(C_{n+1}^{\frac{n}{2}+1}) \quad , \tag{1}$$

$$s = log_2 n \quad . \tag{2}$$

При этом функция F – частотно устойчива (n≥32), тогда вероятность расшифровки i-го блока n_i при известной информационной части m_i и неизвестной ключевой составит (3)

$$P(n_i)_{cp} = 1/n \quad . \tag{3}$$

Стойкость системы определяется длиной шифруемого пакета. При неизвестной ключевой информации вероятность расшифровки пакета (n×N) методом простого перебора составит(4)

$$P_{cp} = N^{-1/P(n_i)_{cp}} = N^{-n}, для\ N \geq 2. \tag{4}$$

Следовательно, стойкость криптосистемы повышается на несколько порядков и возрастает с длиной входных пакетов. При этом скорость кодирования возрастает т.к. стандартная система шифрует только «ключевую» информацию, а информационная часть передается напрямую. Недостатком метода является сложность перевода чисел из биномиальных систем в двоичную (проблема эффективно решаема при n≤64), и увеличение объема передаваемой информации (5)

$$n \le m + s, \qquad (5)$$

что для блоков n=16, 32, 64 составит 16%, 10%, 7% при уменьшении объема информации шифруемой при помощи стандартных систем соответственно в 4 , 6.4, 10, 7 раза.

Использование данного метода оправдано при шифровании сообщений, для которых размер «ключевой» информации превышает размер пакетов шифруемых стандартной системой (больше 64 бит) в несколько раз.

При использовании матриц подстановки система аппаратно легко реализуема и фактически работает в режиме реального времени. Эффективность возрастет с увеличением длины блоков n и величины кодируемых пакетов.

Эффективным может быть использование системы самостоятельно с разбросом «ключевой» информации среди «информационного» пакета на основе циклического сдвига управляемого гамма-функцией.

Литература:

1. Моловян А. А. и др. Криптография: скоростные шифры. – СПб.: БХВ – Петербург, 2002. – 496 с.

2. Борисенко А. А. Биномиальные автоматы. Сумы: СумГУ, 2005 – 121с.

3. Коркішко Т. та ін. Алгоритми та процесори симетричного блокового шифрування. – Львів: Бак, 2003. – 168 с.