ИСПОЛЬЗОВАНИЕ БИНОМИАЛЬНЫХ КОДОВ ДЛЯ РЕШЕНИЯ НЕКОТОРЫХ ЗАДАЧ КРИПТОГРАФИИ

д.т.н., проф. Борисенко А. А., Коломиец М. И.

Предлагаемый алгоритм основан на методе защиты информации при помощи сжатия [1,2]. Блок входных данных представляется в виде комбинации равномерного биномиального кода с параметрами n – разрядность блока и k – количество единиц в блоке. Шифрование заключается в получении двоичного номера для этого блока. Алгоритм шифрования с позиции криптографии представляет собой управляемую операцию, зависящую от преобразуемых данных [3]. Математически алгоритм представляет собой функцию с секретом. Секретом является количество единиц во входном блоке k.

В ходе шифрования формируется криптограмма, состоящая из информационной части и ключа, то есть образуется криптосистема с неравномерным ключом. Длина информационной части и ключа зависит от максимального диапазона чисел представляемых при помощи биномиальных кодов с параметрами n и k, количества единиц во входном блоке и рассчитывается по формулам (1)

$$m = \left\lfloor \log_2 (C_{n+1}^{n/2}) \right\rfloor, \qquad s = \lceil \log_2 n \rceil, \tag{1}$$

где m – длина информационной части, s – длина ключа.

Стойкость зависит от длины блока n . При известной информационной части и неизвестном ключе, стойкость отдельно взятого блока определяется выражением (2)

$$P = p(n)^{-1} \cdot n = \frac{n^2 \cdot C_{n+1}^{n/2}}{2} \left(\sum_{k=1}^{n/2} \frac{C_{n+1}^{k} - C_{n+1}^{k-1}}{n - 2k + 2} \right)^{-1}, \tag{2}$$

где $p(n)$ – вероятность выбора алгоритма преобразования методом простого перебора значений k

Стойкость системы в целом определяется длиной шифруемого пакета. Для случая шифрования пакета состоящего из N статистически независимых блоков разрядности n, стойкость системы при неизвестных ключах для метода простого перебора будет иметь вид (3)

$$P(N) = P^N. \qquad (3)$$

Практическая стойкость системы определятся стойкостью алгоритма шифрования или передачи ключевой информации.

Можно выделить несколько методов использования описанного алгоритма в задачах криптографии.

Первый метод служит для повышения эффективности существующих криптосистем. При этом биномиальная криптосистема на первом этапе в процессе сжатия данных производит первичное шифрование, а на втором этапе шифруются только ключи. Эффективность системы повышается за счет уменьшения количества информации шифруемой на втором этапе.

Второй метод основан маскировании ключей среди информационной части криптограммы. Например, при помощи гаммирования.

Основными достоинствами предложенного криптографического метода является: возможность сквозного контроля аутентичности информации и простота как программной, так и аппаратной реализации.

Литература:

1. Хаффман Л.Дж. Современные методы защиты информации. /Пер. с англ. – М.: Советское радио, 1980. – 262 с.

2. Борисенко А. А. Защита информации на основе сжатия //Вісник СумДУ. – 2006. - № 4. – С. 53-55.

3. Борисенко А. А. Введение в теорию биномиального счета: Монография. – Сумы: Университетская книга, 2004. – 88 с.