УДК 004.056:681.5

Алгоритм защиты информационных потоков в компьютерной сети

Скудняков Ю.А., Хасеневич Б.Б.
Белорусский государственный университет информатики и радиоэлектроники

В настоящее время защита информационных потоков в компьютерной сети остается актуальной темой отрасли. Для того, чтобы защитить данные при передаче через публичные незащищенные сети, существует несколько технических решений. Выбор варианта зависит от множества факторов: 1) от бизнес-модели вещателя — ставит ли он задачу продавать доступ; 2) от того, кто отвечает за сохранность контента; 3) выбор зависит от бюджета.

Для решения задачи защиты контента в работе предложен алгоритм, в основе работы которого положен AES – симметричный итеративный блоковый алгоритм, базирующийся на принципах новой сети подстановок-перестановок. Данный алгоритм имеет новую архитектуру SQUARE (КВАДРАТ), для которой характерно: 1) представление шифруемого блока в виде двумерного байтового массива; 2) шифрование за один раунд всего блока данных (байт-ориентированная структура); 3) выполнение криптографических преобразований как над отдельными байтами массива, так и над его строками и столбцами. Это обеспечивает диффузию данных одновременно в двух направлениях – по строкам и по столбцам. Архитектура SQUARE присуща, кроме шифра AES(RIJNDAEL), шифрам SQUARE, CRYPTON (один из кандидатов на AES). Второе место в конкурсе AES занял другой SP-шифр, SERPENT.По-видимому, SP-сети и, в частности, архитектура SQUARE, в ближайшем будущем станут безраздельно доминировать.

Общие характеристики AES: 1) AES зашифровывает и расшифровывает 128-битовые блоки данных; 2) AES позволяет использовать три различных ключа длиной 128, 192 или 256 бит; 3) от размера ключа зависит число раундов шифрования: длина 128 бит – 10 раундов; длина 192 бита – 12 раундов; длина 256 бит – 14 раундов; 4) все раунды, кроме последнего, идентичны. Основным элементом, которым оперирует алгоритм AES, является байт – последовательность 8 бит, обрабатываемых как единое целое. Для формирования байтов 128 битов блока открытого текста, выходного блока шифротекста и ключа шифра делятся на группы из 8 - ми рядом стоящих бит так, чтобы в целом получился массив байт. Безопасность между серверами и сетевым оборудованием обеспечивается за счет шифрования с использованием протокола IPSec. Реализация процесса контроля за корректностью работы системы защиты контента осуществляется с помощью программного средства, разработанного на языке C++.