НОВЫЕ ПРИНЦИПЫ ПОСТРОЕНИЯ СОВРЕМЕННЫХ КРИПТОСИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

Прокопенков В.Ф., Кожин Ю.Н.
Национальный технический университет «Харьковский политехнический институт», г. Харьков

Криптосистема обеспечивает канал обмена информацией и в её задачи входит обеспечение конфиденциальности, аутентификации и целостности передачи информации (текста) от отправителя к получателю. Развитие криптографии выработало основные требования к криптосистемам: знание алгоритма шифрования не должно снижать криптостойкость; зашифрованное сообщение не должно читаться без знания ключа; шифр должен быть устойчив к взлому независимо от наличия большого количества исходных и зашифрованных данных; сложность взлома шифра должна многократно превышать возможности современных компьютеров; незначительное изменение ключа должно существенно изменять зашифрованную информацию; структурные элементы алгоритма шифрования не должны меняться; длина исходного и зашифрованного текста должны совпадать; вводимые в зашифрованный текст дополнительные биты должны быть надёжно скрыты; не должно быть простых зависимостей между ключами, используемыми в процессе шифрования; все возможные ключи должны обеспечивать равную криптостойкость. Современные криптосистемы не являются идеальными или абсолютно криптостойкими. Их надёжность зависит только от быстродействия используемой для взлома вычислительной системы. Говорить о теоретически абсолютной криптостойкости можно, если длина ключа шифрования и исходного текста совпадают, а используемый ключ одноразовый и случайный. Современные криптосистемы делятся на симметричные и системы с открытым ключом. Первые требуют сокрытия ключа шифрования (дешифрования). Во вторых, открытый ключ используется для шифрования, а связанный с ним ключ дешифрования хранится в секрете. Знание отрытого ключа теоретически позволяет выполнить расшифровку, но сложность такого дешифрования многократно превышает сложность шифрования, что и обеспечивает защиту текста.

Для решения проблем предлагаются новые принципы построения криптосистем со свойствами абсолютной криптостойкости. В криптосистеме необходимо выделить два независимых друг от друга блока: блок генерации одноразового ключа, по длине совпадающего с длиной шифруемого текста и блок шифрования, который использует этот ключ. Сгенерированный ключ абсолютно секретен, т.е. недоступен ни его пользователям, ни третьим лицам. Секретным должен быть и метод его генерации, который также должен обладать свойством случайности – алгоритм генерации ключа должен изменяться в зависимости от команды блока генерации ключа (первичного ключа, который также хранится в тайне). Особенно важным для повышения криптостойкости является реализация многоуровневого шифрования.