СРАВНИТЕЛЬНАЯ ОЦЕНКА СИММЕТРИЧНОГО И АСИММЕТРИЧНОГО ШИФРОВАНИЯ

А.А. Иванов

Современные методы шифрования представляют собой математические преобразования (алгоритмы), в которых сообщения рассматриваются как числа или алгебраические элементы в некотором пространстве. В криптографии определены некоторые методы, которые можно разделить в зависимости от количества ключей, которые используются в соответствующих алгоритмах: одноключевые, двухключевые и бесключевые. Алгоритмы шифрования делятся на два больши класса: симметричные и асимметричные. Симметричные алгоритмы шифрования используют один и тот же ключ для зашифровывания информации и для ее расшифровывания, а асимметричные алгоритмы используют два ключа – один для зашифровывания, другой для расшифровывания. Такая разница хоть и кажется простой, но она представляет большие функциональные различия между двумя формами шифрования и способами их использования. Основными различиями являются: длина ключей (128 бит в симметричном шифровании и 2048 бит – в асимметричном) и распределение ключей (в симметричном шифровании ключ передается всем, кому потребуется доступ, что создает определенные риски, а в асимметричном – открытый ключ, который могут знать все участники, используется для шифрования, а приватный, который знает только получатель, – для дешифрования).

В результате подробного изучения различных методов шифрования, а также проведенного сравнительного анализа было установлено, что симметричные методы шифрования отличаются высокой скоростью обработки данных и незначительным временем для генерации ключей, но при этом для несанкционированного дешифрования данных, зашифрованных симметричным методом шифрования, например, AES, требуется около 2^{256} операций. В то время как для данных, зашифрованных асимметричным методом шифрования, например, RSA, требуется 2^{1024} операций, что объясняет его использование для защиты программного обеспечения, цифровой подписи, аутентификации пользователей, в протоколах SSL, IPsec и др. [1–3].

Литература

1. Мао В. Современная криптография. Теория и практика. М.: Вильямс, 2005. 763 с.

2. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии. М.: Гелиос АРВ, 2001. 479 с.

3. Бауэр Ф. Расшифрованные секреты. Методы и принципы криптологии. М.: Мир, 2007. 550 с.