УДК 004.056.55

ШИФРОВАНИЕ И ПЕРЕСЫЛКА СООБЩЕНИЙ БЕЗ СЕРВЕРА

Р.В. Елисеев, муниципальное бюджетное общеобразовательное учреждение лицей при ТПУ, Томск.
Научный руководитель - аспирант В.Е. Воротов, федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский Томский политехнический университет», г. Томск

Защита данных с помощью криптографического преобразования является эффективным решением проблемы их безопасности. Зашифрованные данные доступны лишь тем, кто знает, как их расшифровать, то есть тем, кто обладает соответствующим ключом шифрования, но в современном мире при пересылке сообщений нельзя быть полностью уверенным в целостности пересылаемой информации и в получении ее конечным пользователем без посредников.

Целью проекта является разработать программу, позволяющую совершать гарантированно безопасный обмен сообщениями.

В этой связи, для шифрования сообщений был выбран ассиметричный алгоритм шифрования. Исходя из теоретической возможности перехвата и подмены пересылаемых сообщений, в общей практике используются центры сертификации для первоначального обмена ключами. Основными факторами затрудняющими реализацию мгновенного обмена зашифрованными сообщениями в сети является сложность вычислений, необходимых для подготовки криптографического ключа и шифрования, и реализация одновременного доступа множества устройств. При использовании единого сервера для связи и вычислений, существует экспоненциальная зависимость от сложности ключа и количества адресатов, сервер всегда должен быть доступен, но это может стать проблемой, ведь необходимо иметь достаточно широкий интернет канал, большие вычислительные мощности и защиту от разного рода атак, поэтому в работе реализовано соединение компьютер-компьютер, но в связи с тем, что такое соединение не всегда возможно установить напрямую, и не каждый провайдер предоставляет такую возможность, те из них, что не могут быть соединены друг с другом, будут соединены через сервер.

Основной идеей данной работы является реализация соединения компьютер-компьютер и шифрование сообщений асимметричным алгоритмом, открытые ключи которого не будут подвержены модификации во время установленной сессии.

С точки зрения практической реализации существуют обоснованные факты, свидетельствующие о нарушении взаимодействия между сертификационным центром и пользователем, так как эти двусторонние отношения строятся на доверии. А значит, существует потенциальная возможность получить доступ или модифицировать передаваемые ключи, при определённых параметрах и вычислительных ресурсах. Для устранения данной проблемы предполагается использование модификации алгоритма гомоморфного шифрования, который на данный момент является достаточно криптостойким. Несмотря на существенное увеличение времени шифрования/дешифрования по сравнению с современными реализациями алгоритмов симметричного и асимметричного шифрования, гомоморфный алгоритм шифрования позволяет исключить проблему «man in the middle».

За счет сочетания алгоритмов хеширования, асимметричного и гомоморфного шифрования гарантируется конфиденциальность передаваемых сообщений. В зависимости от внешних факторов, например присутствия «man in the middle», которые мы можем установить, с помощью реализованных алгоритмов, происходит выбор механизма шифрования. Выбор осуществляется между алгоритмом позволяющим быстро шифровать сообщение, но не позволяющим решить проблему «man in the middle» и алгоритмом,

обеспечивающим решение проблемы «man in the middle», но время выполнения которого существенно увеличивается.

Предложенный комплекс мер позволяет осуществить надежный обмен сообщениями с гарантированной недоступностью их содержимого третьим лицам.