ПОСТРОЕНИЕ ДЕЦЕНТРАЛИЗОВАННОЙ P2P СЕТИ ОБМЕНА СООБЩЕНИЯМИ С КРИПТОГРАФИЧЕСКОЙ ЗАЩИТОЙ ПЕРЕДАВАЕМЫХ ДАННЫХ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Бессарабов А. С. и Лапотко А. А.

Стройникова Е. Д. - ассистент кафедры информатики

Для решения проблемы незащищенности локальных и глобальных сетей от перехвата передаваемых данных, а также для устранения возможных перебоев в работе внешних серверов, мы предлагаем построить P2P сеть с использованием различных методов шифрования передаваемых данных.

Децентрализованная P2P сеть – это компьютерная сеть, основанная на равноправии участников. В такой сети каждый участник является одновременно и клиентом и сервером, а значит, такая сеть будет сохранять работоспособность при любом количестве/сочетании узлов (участников). Авторами была рассмотрена P2P сеть без участия внешних серверов.

Ниже приведен пошаговый алгоритм создания соединения между двумя пользователями внутри P2P сети для криптографически защищенного обмена сообщениями.

1 этап - установка соединения и проверка подлинности участников.

Шаг 1. Генерация секретного и открытого (публичного) ключей на основе уникальной комбинации логина и пароля.

Шаг 2. Поиск пользователя в сети по его открытому ключу для соединения.

Шаг 3. Проверка подлинности пользователя (подтверждение открытого ключа через цифровую подпись) (рис. 1).

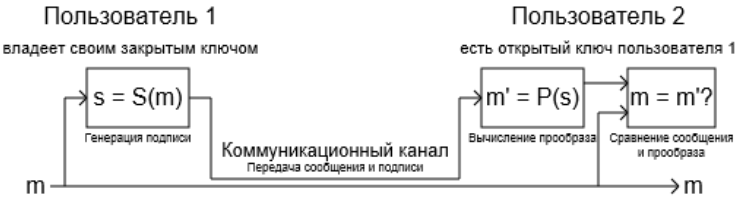

Рис. 1 Схема алгоритма цифровой подписи

2 этап - генерация ключа для симметричного шифрования (через протокол Диффи - Хеллмана) (рис. 2).

3 этап - шифрование, передача и расшифровка сообщений (с помощью ключа симметричного шифрования) (рис. 3).

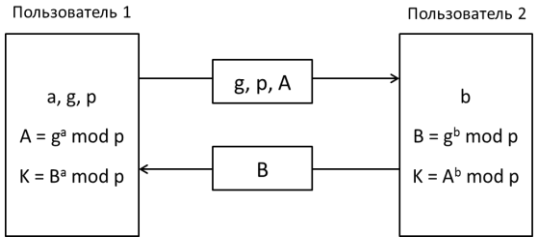

Рис. 2 Схема протокола Диффи – Хеллмана

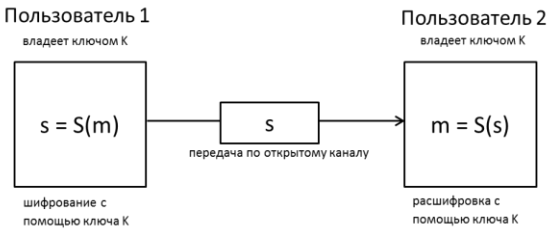

Рис. 3 Схема алгоритма симметричного шифрования

Таким образом, была разработана децентрализованная P2P сеть, обеспеченная криптографической защитой данных и защитой их от попадания в ненужные руки.

В процессе создания приложения использованы: среда программирования Delphi 2010, протокол UDP для передачи данных, интерфейс программирования приложений CryptoAPI, криптографический алгоритм RSA.

Список использованных источников:

1. Свободная интернет-энциклопедия – http://ru.wikipedia.org/