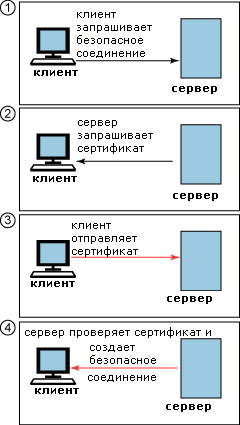
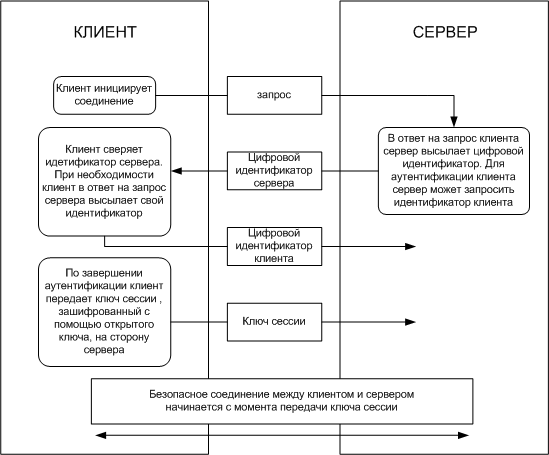
**Рекомендации по выполнению работы**

SSL – это криптографический протокол, предназначенный для безопасной передачи данных по сети. При его использовании создается защищенное соединение между клиентом и сервером. Протокол использует аутентификацию и шифрование для обеспечения защищенного обмена. Протокол SSL обеспечивает целостность и конфиденциальность обмена данными между двумя общающимися приложениями, использующими TCP/IP. Для цифровых подписей и обмена ключами шифрования используется алгоритм с открытым ключом (RSA). В шифровании с открытым ключом используется два ключа, каждый из которых может использоваться для шифрования сообщений. Если один ключ используется для шифрования сообщения, для его расшифровки необходимо использовать другой. Это позволяет получать защищенные сообщения, просто публикуя один (открытый) ключ и храня другой (секретный) ключ в тайне.

В протоколе SSL используются цифровые сертификаты для установления личности владельца, а также для того, чтобы сделать доступным публичный ключ владельца. Протокол SSL использует цифровые сертификаты для обмена ключами, аутентификации серверов и, при необходимости, аутентификации клиентов. Есть три способа получить SSL-сертификат:

1. использовать сертификат от источника сертификатов – это организации, которым доверяет вся отрасль и которые занимаются выдачей Интернет-сертификатов;
2. использовать самоподписанный сертификат – сертификат, созданный самим пользователем;
3. использовать "пустой" сертификат – содержат фиктивную информацию, используемую в качестве временного решения для настройки SSL и проверки его функционирования в конкретной среде.

Процесс аутентификации между клиентом и сервером представлен на рисунке ниже:

SSL-аутентификация сервера позволяет клиенту проверить подлинность сервера. Клиентское ПО, поддерживающее SSL, может с помощью стандартных приемов криптографии с открытым ключом проверить, что сертификат сервера и открытый ключ действительны и были выданы источником, находящимся в списке доверенных источников сертификатов этого клиента. SSL-аутентификация клиента позволяет серверу проверить личность пользователя. Используя те же приемы, что и в случае с аутентификацией сервера, серверное ПО с поддержкой SSL может проверить, что сертификат клиента и открытый ключ действительны и были выданы источником сертификатов, имеющимся в списке доверенных источников сервера.

При генерации сертификата создается пара ключей – открытый и секретный. Cекретный ключ устанавливается на сервере. На основе секретного ключа создается цифровая подпись. Если секретный ключ будет потерян, то сертификат невозможно будет использовать, поэтому рекомендуется создавать резервные копии секретного ключа.

Парный открытый (публичный) ключ устанавливается на сервер и является частью цифрового сертификата. Открытый и секретный ключи связаны математической закономерностью, но не идентичны. Клиент, устанавливающий защищенный сеанс (при помощи SSL протокола) обращается к открытому ключу сертификата и с помощью открытого ключа шифрует посылаемую информацию. Этот процесс происходит мгновенно и незаметно для пользователя. Расшифровать информацию можно только с помощью секретного ключа сервера. Это дает гарантию клиенту, что никакая третья сторона не получит доступ к его информации.

Протокол SSL использует шифрование с открытым ключом для того, чтоб подтвердить клиенту подлинность сервера, и наоборот. Шифрование открытым ключом также используется для определения ключа сессии. Ключ сессии используется симметричными алгоритмами для шифровки большого объема данных. Это объединяет ассиметричное шифрование (для проверки подлинности) и быстрое симметричное шифрование объемных данных (что не требует больших вычислительных ресурсов и больших затрат времени).

Ссылки:

1. Как создать сертификат SSL для MySQL: <http://dev.mysql.com/doc/mysql-security-excerpt/5.5/en/creating-ssl-certs.html>
2. Подключение с использованием SSL: <http://dev.mysql.com/doc/mysql-security-excerpt/5.5/en/using-ssl-connections.html>
3. <https://www.cryptopro.ru/sites/default/files/docs/TLS_description.pdf>
4. <http://www.ibm.com/developerworks/ru/library/ac-iscssl1/>
5. <http://www.inssl.com/about-ssl-protocol.html>
6. <http://www.inssl.com/ssl-fundamentals.html>

**Задание на лабораторную работу**

1. Сгенерировать сертификаты.
2. Настроить mysql для доступа по сети с использованием SSL.
3. Продемонстрировать доступ по сети с правильным / неправильным сертификатом и выполнение команд на изменение данных (клиент и сервер могут быть на разных виртуальных машинах).
4. Разработать прикладное ПО, которое демонстрирует доступ к БД по сети с использованием сертификата и позволяет отображать данные БД в виде таблицы, а также редактировать их.