**网络传输协议**

1. TCP和UDP：http://blog.csdn.net/li\_ning\_/article/details/52117463
2. HTTP和HTTPS
3. HTTPS工作原理 http://www.cnblogs.com/zery/p/5164795.html
4. Client（浏览器）将自己支持的加密算法套件发送给Server（服务器）；
5. Server接收到Client的加密算法套件后，从中选择一种Server支持的非对称算法和Hash算法（若不存在Server支持的非对称算法则断开连接），通过非对称算法生成一组公钥、私钥。私钥Server自身保存，非对称算法、Hash算法和公钥通过证书的形式返回给Client。（证书的内容会通过Hash算法加密生成证书编号）
6. Client接收到Server的数字证书后，验证证书的合法性（有效期、网站、完整性）。如果通过Hash算法加密证书内容的结果与证书编号相同，则能保证证书未被篡改。如果证书不受信则弹窗提示证书不受信。若证书受信或用户接受了不受信证书，则Client会生成一个随机数会话密钥。Client将经过公钥加密的随机数会话密钥和经过随机数会话密钥加密的握手消息（握手消息和握手消息的Hash值）发送给Server；
7. Server用私钥解密出随机数会话密钥，并用随机数会话密钥解密出握手消息。通过Hash算法加密握手消息并与Client传过来的握手消息Hash值对比，以保证握手消息未被篡改。Server将经过随机数会话密钥加密后的握手消息（握手消息和握手消息的Hash值）发送给Client。
8. Client用随机数会话密钥解密Server传过来的握手消息，通过Hash算法加密握手消息并与Client传过来的握手消息Hash值对比，以保证握手消息未被篡改。握手过程结束。 注：非对称加密算法：RSA，DSA/DSS  对称加密算法：AES，RC4，3DES  HASH算法：MD5，SHA1，SHA256