RSA加密算法的学习与实现

RSA是一种非对称密码算法，能够抵抗目前为止大多数已知的密码的攻击，已被ISO推荐为公钥数据加密标准。通过网络我了解了RSA算法的加密原理，在公开密钥密码体制中，加密密钥（即公开密钥）PK是公开信息，而解密密钥（即秘密密钥）SK是需要保密的。加密算法E和解密算法D也都是公开的。虽然秘密密钥SK是由公开密钥PK决定的，但是却不能根据PK计算出SK。基于这种理论，RSA算法顺势而生。通常是先生成一对RSA密钥，其中之一是保密密钥，由用户保存；另一个为公开密钥，可对外公开，甚至可在网络服务器中注册。为提高保密强度，RSA密钥至少为500位长，一般推荐使用1024位。这就使加密的计算量很大。为减少计算量，在传送信息时，常采用传统加密方式与公开密钥加密方式相结合的方式，即信息采用改进的DES或IDEA对话密钥加密，然后使用RSA密钥加密对话密钥和信息摘要。对方接收到信息后，用不同的密钥解密可核对信息摘要。

SuperSocket网络通信基本框架搭建完成