



说明：1、客户端生成的公钥和私钥、服务器端公钥和私钥属于非对称加密；
2、客户端生成的会话密钥、服务器生成的会话密钥属于对称加密；
3、非对称加密，加密和解密比较复杂，安全性高，使用公钥加密的数据只能通过私钥进行解密；
4、对称加密，加密和解密使用同一个密钥，比较简单，加解密速度快。