Java加密和数字签名5数字证书Java认证考试 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/644/2021_2022_Java_E5_8A_A0_E5_AF_86_c104_644532.htm 数字证书 还有个问题，就是公钥问题，A用私钥加密了，那么B接受到消息后，用A提供的公钥解密；那么现在有个讨厌的C，他把消息拦截了，然后用自己的私钥加密，同时把自己的公钥发给B，并告诉B，那是A的公钥，结果……，这时候就需要一个中间机构出来说话了（相信权威，我是正确的），就出现了 Certificate Authority（也即CA），有名的CA机构有Verisign等，目前数字认证的工业标准是：CCITT的X.509： 数字证书：它将一个身份标识连同公钥一起进行封装，并由称为认证中心或 CA 的第三方进行数字签名。 密钥库：java平台为你提供了密钥库，用作密钥和证书的资源库。从物理上讲，密钥库是缺省名称为 .keystore 的文件（有一个选项使它成为加密文件）。密钥和证书可以拥有名称（称为别名），每个别名都由唯一的密码保护。密钥库本身也受密码保护；您可以选择让每个别名密码与主密钥库密码匹配。 使用工具keytool，我们来做一件自我认证的事情吧（相信我的认证）： 1、创建密钥库keytool -genkey -v -alias feiUserKey -keyalg RSA 默认在自己的home目录下（windows系统是c：documents and settings 