2006数字证书应用全攻略认识数字证书三 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/64/2021_2022_2006_E6_95_B0_E5_AD_97_c40_64686.htm 三、数字认证原理 利用数字证书技术进行网上安全传输数据的基本原理是：首先传输双方互相交换证书，验证彼此的身份；然后，发送方利用证书中的公钥和自己的私钥，对要传输的数据进行加密和签名，这样即可保证只有合法的用户才能解密数据，同时也保证了传输数据的真实性和不可否认性。 1、数据加密 数字证书技术利用一对互相匹配的密钥进行加密、解密。当你申请证书的时候，会得到一把私钥和一个数字证书(公钥)。其中公钥可以发给他人使用，而私钥你应该保管好、不能泄露给其他人，否则别人将能用它以你的名义签名。 当你向朋友发送一份保密文件时，需要使用对方的公钥对数据加密，朋友收到文件后，则使用自己的私钥解密，如果你没有私钥，就不能解密文件，从而保证数据的安全保密性。这种加密是不可逆的，即使你已知明文、密文和公钥，也无法推导出私钥。 2、数字签名 另外，你也可以对文件进行数字签名，即用你的私钥对数据进行加密处理。由于私钥仅为你一个人拥有、别人是无法仿造的，因此经过你签名的文件一定是你自己签名发送的，而且它还未曾篡改过。你可以右击某个文件，查看文件属性，假如没有有效的数字签名，那么你将无法得知该文件的来源，或者无法确保它在发行之后未被篡改过(可能由病毒篡改)。 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com