成都温江区-电子签章-电子印章-电子章办理-

产品名称	成都温江区-电子签章-电子印章-电子章办理-
公司名称	四川中科防伪印章有限公司
价格	.00/件
规格参数	
公司地址	成都高新政务中心对面- 复城国际T2栋9楼(备案刻章)
联系电话	028-85356153 19980888908

产品详情

成都温江区刻章-电子签章-电子印章-电子章办理-CA数字证书

电子合同的技术基础电子印章技术

本节对电子合同所涉及的技术概念进行梳理。

***加密算法

答：首先我们需要了解一下加密相关的知识，加密可以分为对称加密和非对称加密。两者的主要区别就是是否使用同一个秘钥，对称加密需要用同一个秘钥。非对称加密不需要用同一个秘钥，而是需要两个秘钥：公开密钥（publickey）和私有密钥（privatekey），并且加密密钥和解密密钥是成对出现的。

四川电子印章办理电子签章地址：

成都所在地：成都高新区政务中心斜对面复城国际T2栋-9层（四川中科防伪印章公司）

百度地图（高德地图）直接导航：中科印章公司即可。按定位很准确的，到了楼下能看到大楼墙上有个【保利国际影城】几个大字，大字下方就是T2写字楼大厅(旁边有个廖记棒棒鸡)，进大厅右边前台,喊前台帮忙刷一下. -9-楼电梯卡既可，出.
-9-楼电梯就到了。如果找不到请打133的手机.或者地图上面的座机号码。或者加微信联系我都可以哦

四川中科防伪印章公司主要负责：公安备案印章，公章、财务章、合同章、发票章、法人章。等等。

和其他杂件印章制作，正规合法印章单位；一站式备案刻章单位；我处可以现场办理制作电子印章，申请电子公章，刻电子合同章

***对称算法

答：对称加密算法的特点是算法公开、计算量小、加密速度快、加密效率高。对称加密有很多种算法，由于它效率很高，所以被广泛使用在很多加密协议的核心当中。不足之处是，交易双方都使用同样钥匙，安全性得不到保证。常见的对称加密有 DES、AES 等。

***非对称算法

答：非对称加密使用一对“ 私钥-
公钥 ”，用私钥加密的内容只有对应公钥才能解开，反之亦然。非对称加密有以下特性：

· 对于一个公钥，有且只有一个对应的私钥；

· 公钥是公开的，并且不能通过公钥反推出私钥；

· 通过私钥加密的密文只能通过公钥能解密，通过公钥加密的密文也只能通过私钥能解密；

非对称加密不需要共享同一份秘钥，安全性要比对称加密高，但由于算法强度比对称加密复杂，加解密的速度比对称加解密的速度要慢。常见的非对称加密有 RSA、ESA、ECC 等。

***摘要算法

答：除了加密算法，摘要算法在互联网安全体系中也扮演了重要的角色。摘要算法又叫哈希算法，具有以下特性：

· 只要源文本不同，计算得到的结果，必然不同（或者说机会很少）。

· 无法从结果反推出源数据。

基于以上特性，我们一般使用摘要算法来校验原始内容是否被篡改。常见的摘要算法有 MD ***SHA 等。

摘要算法不能算作加密算法，加密算法需要使用秘钥加解密，但摘要算法无法根据结果反推出内容。

***再举传输文件的例子

答：假设甲公司要给乙公司发送一份机密的文件，那么这次传输需要确保以下几点：

文件内容不能被读取————（方案：加密）

只有乙公司能接收—————（方案：数字信封）

***证明发送方是甲公司————（方案：数字签名）

***文件内容不能被篡改————（方案：对比摘要）

***文件不能被掉包—————（方案：数字证书）

***文件加密

答：由于对称加密的高效性，对文件的加密处理，通常采用对称加密方案。对称加密需要用同一份秘钥，这一份秘钥的约定就有被中途截获的可能。

***数字信封

答：因此可以采用非对称加密算法加密对称秘钥的方式来加密内容，也就是“ 用接收方的公钥加密对称秘钥 ”，这就叫“ 给乙的数字信封 ”，并用这个对称秘钥加密文件内容。

假设这份文件被黑客截获，但是黑客没有乙的私钥无法解出对称秘钥，也就无法解密文件内容。但是这里还有个风险，虽然黑客无法解密文件内容，但他可以自己生成一份秘钥并用乙的公钥加密，再用这份秘钥加密一份伪造的文件发给乙，这种情况下乙收到的就是被假冒的文件。

***数字签名

答：上面提到乙有可能收到被假冒的文件，这个问题可以用数字签名的方式解决，数字签名就是用摘要算法提取出源文件的摘要并用发送人的私钥进行加密后的内容。

针对上面的问题，甲在发送文件时再附带上源文件的数字签名。如果被黑客截取到加密后的文件和数字签名，黑客即使使用甲的公钥解出了文件摘要，由于摘要算法的特性黑客也无法还原出原始内容。但乙可以解密出文件内容再用同样的摘要算法提取出摘要来和数字签名里的摘要进行比对，摘要一致则说明文件没有被篡改过。

到目前为止还有一个风险就是乙无法确定自己用的公钥就是甲提供的，如果黑客将乙手里的甲的公钥替换成自己的并用自己的私钥生成数字签名，那么乙还是会收到被篡改的文件。