数字签名 （又称公钥数字签名、电子签章） 是一种类似写在纸上的普通的物理签名， 但是使用了公钥加密领域的技术实现， 用于鉴别数字信息的方法。 一套数字签名通常定义两种互补的运算，一个用于签名，另一个用于验证。

数字签名， 就是只有信息的发送者才能产生的别人无法伪造的一段数字串， 这段数字串同时也是对信息的发送者发送信息真实性的一个有效证明。

数字签名是非对称密钥加密技术与数字摘要技术的应用。

原理：

数字签名的文件的完整性是很容易验证的 （不需要骑缝章， 骑缝签名， 也不需要笔迹专家） ，而且数字签名具有不可抵赖性（不需要笔迹专家来验证） 。

简单地说 ,所谓数字签名就是附加在数据单元上的一些数据 ,或是对数据单元所作的密码变换。这种数据或变换允许数据单元的接收者用以确认数据单元的来源和数据单元的完整性并保护数据 ,防止被人 (例如接收者)进行伪造。它是对电子形式的消息进行签名的一种方法 ,一个签名消息能在一个通信网络中传输。 基于公钥密码体制和私钥密码体制都可以获得数字签名,主要是基于公钥密码体制的数字签名。包括普通数字签名和特殊数字签名。普通数字签名算法有 RSA、 ElGamal、 Fiat-Shamir、 Guillou- Quisquarter 、 Schnorr、 Ong-Schnorr-Shamir 数字签名算法、 Des/DSA, 椭圆曲线数字签名算法和有限自动机数字签名算法等。特殊数字签名有盲签名、代理签名、群签名、不可否认签名、公平盲签名、门限签名、具有消息恢复功能的签名等 ,它与具体应用环境密切相关。 显然 ,数字签名的应用涉及到法律问题 ,美国联邦政府基于有限域上的离散对数问题制定了自己的数字签名标准 (DSS)。

主要功能：

保证信息传输的完整性、发送者的身份认证、防止交易中的抵赖发生。

数字签名技术是将摘要信息用发送者的私钥加密， 与原文一起传送给接收者。 接收者只有用发送者的公钥才能解密被加密的摘要信息，然后用 HASH 函数对收到的原文产生一个摘要信息， 与解密的摘要信息对比。 如果相同，则说明收到的信息是完整的，在传输过程中没有被修改，否则说明信息被修改过，因此数字签名能够验证信息的完整性。

数字签名是个加密的过程，数字签名验证是个解密的过程。

签名过程

“ 发送报文时，发送方用一个哈希函数从报文文本中生成报文摘要 ,然后用自己的私人密钥对这个摘要进行加密，这个加密后的摘要将作为报文的数字签名和报文一起发送给接收方，接收方首先用与发送方一样的哈希函数从接收到的原始报文中计算出报文摘要， 接着再用发送方的公用密钥来对报文附加的数字签名进行解密， 如果这两个摘要相同、 那么接收方就能确认该数字签名是发送方的。

数字签名有两种功效： 一是能确定消息确实是由发送方签名并发出来的， 因为别人假冒不了发送方的签名。 二是数字签名能确定消息的完整性。 因为数字签名的特点是它代表了文件的特征，文件如果发生改变， 数字摘要的值也将发生变化。 不同的文件将得到不同的数字摘要。一次数字签名涉及到一个哈希函数、发送者的公钥、发送者的私钥。 ”

数字签名：

发送方用自己的密钥对报文 X 进行 Encrypt(编码)运算，生成不可读取的密文 Dsk，然后将 Dsk 传送给接收方， 接收方为了核实签名， 用发送方的公用密钥进行 Decrypt(解码)运算， 还原报文。

识别病毒

如何区分数字签名攻击呢？有两个方法：

1.查看数字签名的详细信息，我们应该查看该数字签名的详细信息，点击 “ 详细信息 ” 按钮即可。

我们会发现正常 EXE 和感染（或捆绑木马）后的 EXE 数字签名的区别。

正常 EXE 的数字签名详细信息。

被篡改后的 EXE 数字签名信息无效。

2. 使用数字签名验证程序 sigcheck.exe （可以百度一下找这个工具，著名系统工具包 Sysinternals Suite 的组件之一。）

数字签名异常的结果为：

C:\Documents and Settings\litiejun\??\modify.exe:

Verified: Unsigned

File date: 15:46 2008-5-23

Publisher: n/a

Description: n/a

Product: n/a

Version: n/a

File version: n/a

数字签名正常的结果为：

C:\Documents and Settings\litiejun\??\che.exe:

Verified: Signed

Signing date: 16:28 2008-4-29

Publisher: n/a

Description: n/a

Product: n/a

Version: n/a

File version: n/a

原理特点

每个人都有一对“ 钥匙 ” （数字身份），其中一个只有她 /他本人知道（密钥） ，另一个公开的（公钥）。签名的时候用密钥，验证签名的时候用公钥。又因为任何人都可以落款声称她 / 他就是你， 因此公钥必须向接受者信任的人（身份认证机构） 来注册。 注册后身份认证机构给你发一数字证书。 对文件签名后， 你把此数字证书连同文件及签名一起发给接受者， 接受者向身份认证机构求证是否真地是用你的密钥签发的文件。

在通讯中使用数字签名一般基于以下原因：

鉴权

公钥加密系统允许任何人在发送信息时使用公钥进行加密，数字签名能够让信息接收者确认发送者的身份。当然，接收者不可能百分之百确信发送者的真实身份，而只能在密码系统未被破译的情况下才有理由确信。

鉴权的重要性在财务数据上表现得尤为突出。举个例子，假设一家银行将指令由它的分行传输到它的中央管理系统，指令的格式是 (a,b)，其中 a 是账户的账号，而 b 是账户的现有金额。这时一位远程客户可以先存入 100 元，观察传输的结果，然后接二连三的发送格式为 (a,b) 的指令。这种方法被称作重放攻击。

完整性

传输数据的双方都总希望确认消息未在传输的过程中被修改。加密使得第三方想要读取数据十分困难，然而第三方仍然能采取可行的方法在传输的过程中修改数据。一个通俗的例子就是同形攻击：回想一下，还是上面的那家银行从它的分行向它的中央管理系统发送格式为 (a,b) 的指令，其中 a 是账号，而 b 是账户中的金额。一个远程客户可以先存 100 元，然后拦截传输结果，再传输 (a,b3)，这样他就立刻变成百万富翁了。

不可抵赖

在密文背景下，抵赖这个词指的是不承认与消息有关的举动（即声称消息来自第三方）。消息的接收方可以通过数字签名来防止所有后续的抵赖行为，因为接收方可以出示签名给别人看来证明信息的来源。

实现方法

数字签名算法依靠公钥加密技术来实现的。在公钥加密技术里，每一个使用者有一对密钥：一把公钥和一把私钥。公钥可以自由发布，但私钥则秘密保存；还有一个要求就是要让通过公钥推算出私钥的做法不可能实现。

普通的数字签名算法包括三种算法：

1.密码生成算法；

2.标记算法；

3.验证算法。

关于数字签名的创新：

随着科技迅速发展，　网络已经广泛的进入到了人们的生活当中，比如（公司的机密、超市的收银、使用的监控设备和发送数据时所需要用的发送软件等等，　都是我们需要网络所用到的，但也会有负面的如黑客的攻击、　拦截，以此目的来实现非法行为，　这些也是我们防不胜防的，设想一下如果我们创造一个数字签名与　ip 绑定技术，根据　ip 绑定我们不需要再去一遍一遍的去使用已有签名技术。

（1）数字签名与　ip 地址的绑定，根据用户使用的不同时间和防止别人利用自己的　iP 来直接获取所需要的机密，　数字签名绑定　ip 技术则会使用定期或长期的一种数字签名与　ip 绑定，当用户不在时则取消与　ip 的绑定，　如：（qq 在登陆过程中如果客户一直使用，　在不断电不关机电脑的情况下我们都可以使用　qq 与人发送消息，当用户离开时为了防止别人偷看自己的信息就会给　qq 上锁回来时用密码打开或者直接退出　qq）如果数字签名与　ip 绑定技术也使用上锁和退出与登录时有登录密码，这样就会方便许多用户。