### 前言

先看一下百度百科对数字签名和数字证书的解释：

****数字签名：****

将[报文](http://baike.baidu.com/view/175122.htm" \t "F:/%E5%AF%86%E9%92%A5%E7%AE%A1%E7%90%86%E5%BC%80%E5%8F%91/_blank)按双方约定的HASH[算法](http://baike.baidu.com/view/7420.htm" \t "F:/%E5%AF%86%E9%92%A5%E7%AE%A1%E7%90%86%E5%BC%80%E5%8F%91/_blank)计算得到一个固定位数的[报文摘要](http://baike.baidu.com/view/4971320.htm" \t "F:/%E5%AF%86%E9%92%A5%E7%AE%A1%E7%90%86%E5%BC%80%E5%8F%91/_blank)。在[数学](http://baike.baidu.com/view/1284.htm" \t "F:/%E5%AF%86%E9%92%A5%E7%AE%A1%E7%90%86%E5%BC%80%E5%8F%91/_blank)上保证：只要改动报文中任何一位，重新计算出的[报文摘要](http://baike.baidu.com/view/4971320.htm" \t "F:/%E5%AF%86%E9%92%A5%E7%AE%A1%E7%90%86%E5%BC%80%E5%8F%91/_blank)值就会与原先的值不相符。这样就保证了报文的不可更改性。

将该报文摘要值用发送者的私人[密钥加密](http://baike.baidu.com/view/3871584.htm" \t "F:/%E5%AF%86%E9%92%A5%E7%AE%A1%E7%90%86%E5%BC%80%E5%8F%91/_blank)，然后连同原报文一起发送给接收者，而产生的报文即称[数字签名](http://baike.baidu.com/view/7626.htm" \t "F:/%E5%AF%86%E9%92%A5%E7%AE%A1%E7%90%86%E5%BC%80%E5%8F%91/_blank)

****数字证书：****

数字[证书](http://baike.baidu.com/view/169817.htm" \t "F:/%E5%AF%86%E9%92%A5%E7%AE%A1%E7%90%86%E5%BC%80%E5%8F%91/_blank)就是互联网通讯中标志通讯各方[身份](http://baike.baidu.com/view/1034208.htm" \t "F:/%E5%AF%86%E9%92%A5%E7%AE%A1%E7%90%86%E5%BC%80%E5%8F%91/_blank)信息的一系列数据，提供了一种在Internet上验证您[身份](http://baike.baidu.com/view/1034208.htm" \t "F:/%E5%AF%86%E9%92%A5%E7%AE%A1%E7%90%86%E5%BC%80%E5%8F%91/_blank)的方式，其作用类似于司机的驾驶执照或日常生活中的身份证。它是由一个由权威机构-----CA机构，又称为[证书](http://baike.baidu.com/view/169817.htm" \t "F:/%E5%AF%86%E9%92%A5%E7%AE%A1%E7%90%86%E5%BC%80%E5%8F%91/_blank)授权（Certificate Authority）中心发行的，人们可以在网上用它来识别对方的[身份](http://baike.baidu.com/view/1034208.htm" \t "F:/%E5%AF%86%E9%92%A5%E7%AE%A1%E7%90%86%E5%BC%80%E5%8F%91/_blank)。数字[证书](http://baike.baidu.com/view/169817.htm" \t "F:/%E5%AF%86%E9%92%A5%E7%AE%A1%E7%90%86%E5%BC%80%E5%8F%91/_blank)是一个经证书授权中心[数字签名](http://baike.baidu.com/view/7626.htm" \t "F:/%E5%AF%86%E9%92%A5%E7%AE%A1%E7%90%86%E5%BC%80%E5%8F%91/_blank)的包含[公开密钥](http://baike.baidu.com/view/1145160.htm" \t "F:/%E5%AF%86%E9%92%A5%E7%AE%A1%E7%90%86%E5%BC%80%E5%8F%91/_blank)拥有者信息以及公开密钥的文件。最简单的[证书](http://baike.baidu.com/view/169817.htm" \t "F:/%E5%AF%86%E9%92%A5%E7%AE%A1%E7%90%86%E5%BC%80%E5%8F%91/_blank)包含一个[公开密钥](http://baike.baidu.com/view/1145160.htm" \t "F:/%E5%AF%86%E9%92%A5%E7%AE%A1%E7%90%86%E5%BC%80%E5%8F%91/_blank)、名称以及证书授权中心的[数字签名](http://baike.baidu.com/view/7626.htm" \t "F:/%E5%AF%86%E9%92%A5%E7%AE%A1%E7%90%86%E5%BC%80%E5%8F%91/_blank)。

对数字签名和数字证书的理解一直较模糊。

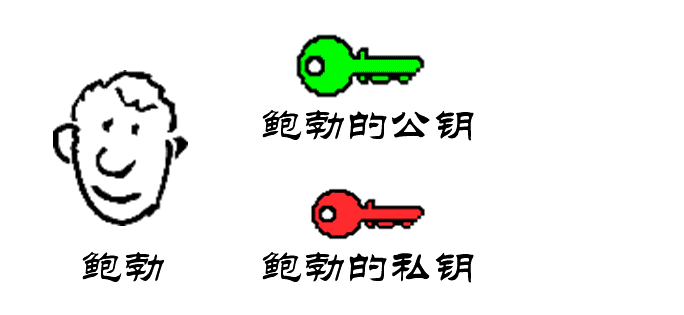
最近看了一篇很形象的关于数字证书的图形化介绍， 豁然就开朗了^^

原文：[What is a Digital Signature?](http://www.youdzone.com/signature.html)

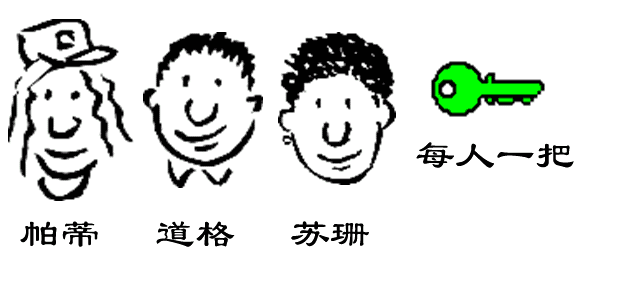
[中文版](http://www.ruanyifeng.com/blog/2011/08/what_is_a_digital_signature.html)

### 正文

1. 鲍勃有两把钥匙，一把是公钥，另一把是私钥。



2.  鲍勃把公钥送给他的朋友们----帕蒂、道格、苏珊----每人一把。



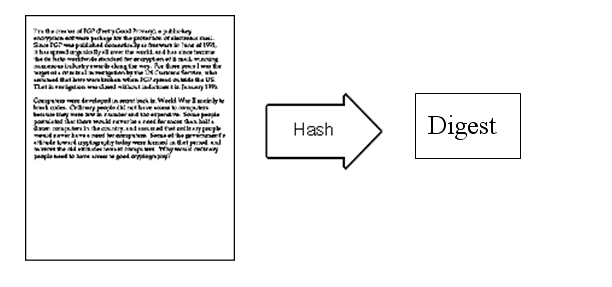
3.  苏珊要给鲍勃写一封保密的信。她写完后用鲍勃的公钥加密，就可以达到保密的效果



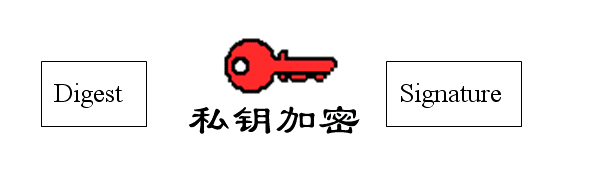
4. 鲍勃收信后，用私钥解密，就看到了信件内容。这里要强调的是，只要鲍勃的私钥不泄露，这封信就是安全的，即使落在别人手里，也无法解密。



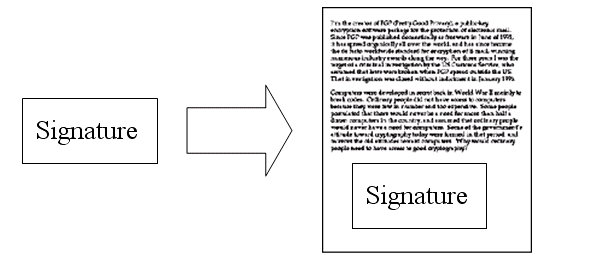
5.  鲍勃给苏珊回信，决定采用****"数字签名"****。他写完后先用Hash函数，生成信件的摘要（digest）



6. 然后，鲍勃使用私钥，对这个摘要加密，生成"数字签名"（signature）。



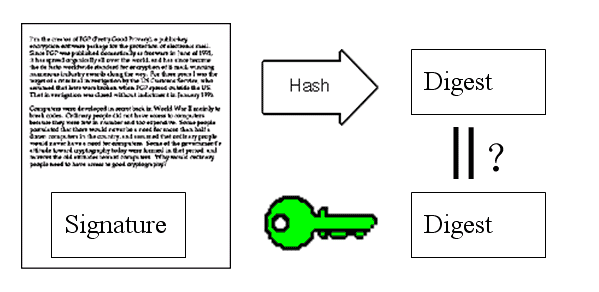
7. 鲍勃将这个签名，附在信件下面，一起发给苏珊。



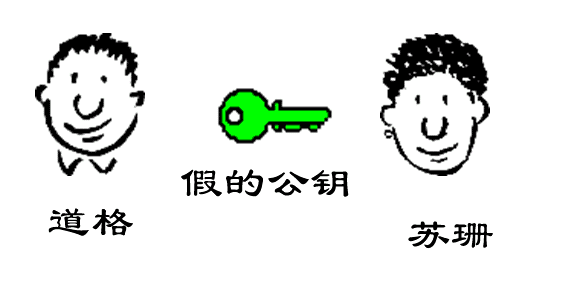
8. 苏珊收信后，取下数字签名，用鲍勃的公钥解密，得到信件的摘要。由此证明，这封信确实是鲍勃发出的。



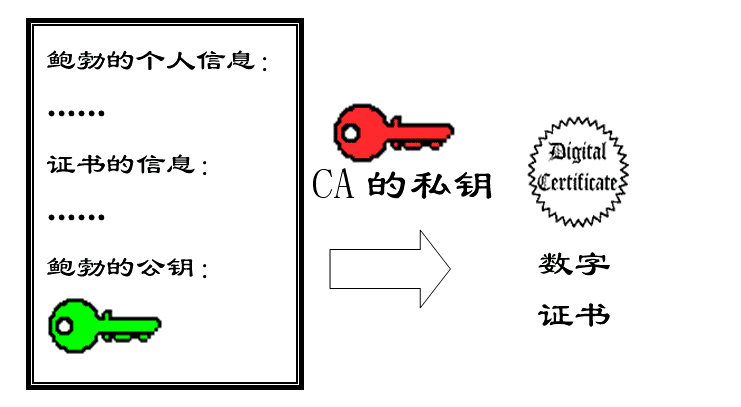
9. 苏珊再对信件本身使用Hash函数，将得到的结果，与上一步得到的摘要进行对比。如果两者一致，就证明这封信未被修改过。



10.  复杂的情况出现了。道格想欺骗苏珊，他偷偷使用了苏珊的电脑，用自己的公钥换走了鲍勃的公钥。此时，苏珊实际拥有的是道格的公钥，但是还以为这是鲍勃的公钥。因此，道格就可以冒充鲍勃，用自己的私钥做成"数字签名"，写信给苏珊，让苏珊用假的鲍勃公钥进行解密。



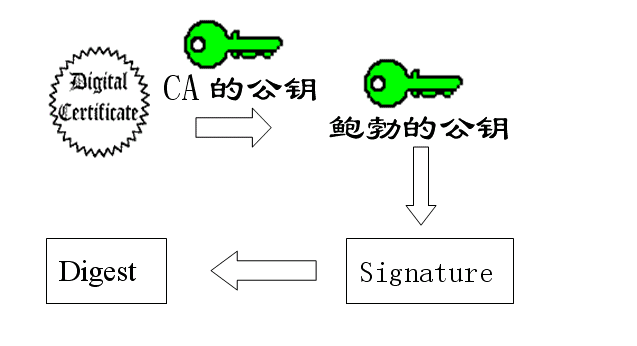
11.  后来，苏珊感觉不对劲，发现自己无法确定公钥是否真的属于鲍勃。她想到了一个办法，要求鲍勃去找"证书中心"（certificate authority，简称CA），为公钥做认证。证书中心用自己的私钥，对鲍勃的公钥和一些相关信息一起加密，生成"数字证书"（Digital Certificate）。



12. 鲍勃拿到数字证书以后，就可以放心了。以后再给苏珊写信，只要在签名的同时，再附上数字证书就行了。



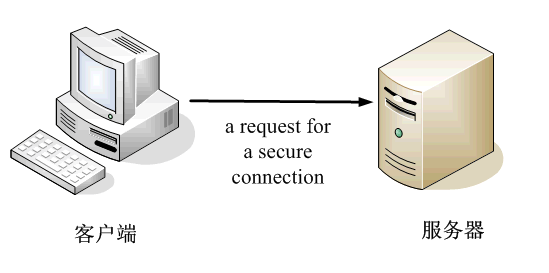
13. 苏珊收信后，用CA的公钥解开数字证书，就可以拿到鲍勃真实的公钥了，然后就能证明"数字签名"是否真的是鲍勃签的。



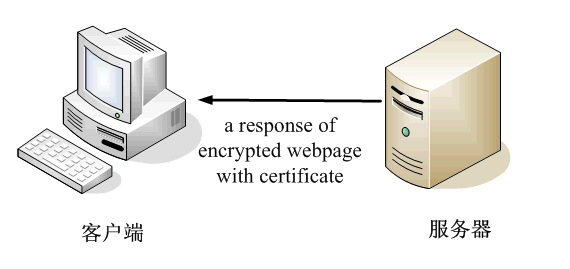
14. 下面，我们看一个应用"数字证书"的实例：https协议。这个协议主要用于网页加密。



15. 首先，客户端向服务器发出加密请求。



16. 服务器用自己的私钥加密网页以后，连同本身的数字证书，一起发送给客户端。



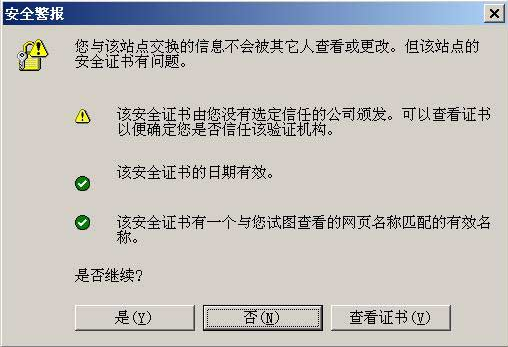
17. 客户端（浏览器）的"证书管理器"，有"受信任的根证书颁发机构"列表。客户端会根据这张列表，查看解开数字证书的公钥是否在列表之内。



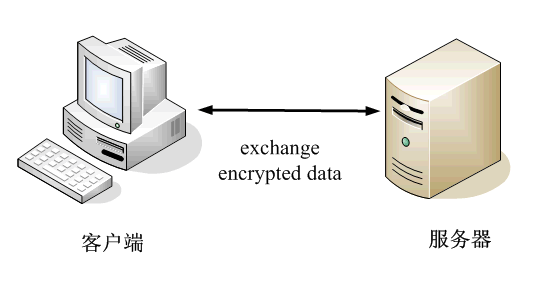
18. 如果数字证书记载的网址，与你正在浏览的网址不一致，就说明这张证书可能被冒用，浏览器会发出警告。



19 .如果这张数字证书不是由受信任的机构颁发的，浏览器会发出另一种警告



20.如果数字证书是可靠的，客户端就可以使用证书中的服务器公钥，对信息进行加密，然后与服务器交换加密信息。



### 总结

数字签名 就是使用个人私密和加密算法加密的摘要和报文，是私人性的。而数字证书是由CA中心派发的.