非对称加密是现代通讯安全的基础。简单的说，就是通过算法产生一对密钥，秘钥A和秘钥B。秘钥A加密的内容，只有秘钥B才能解密，秘钥B加密的内容，只有秘钥A才能解密。如果两个人分别持有秘钥A和秘钥B，他们两个人就可以通过加密解和密通话内容进行秘密的通话。

技术上，秘钥就是密码算法的输入参数。

那什么是公钥？什么是私钥？

如果其中一把密钥被公开，它就被称为公钥，另一把没有被公开的密钥就被称为私钥。

所以，公钥加密的内容只有私钥才能解密，私钥加密的内容，只有公钥可以解密。

推论：只要用公钥成功的解密了一份消息，那么就可以断定，这份消息就一定是由配对的那把私钥加密的，而不是别的什么私钥加密的。我们假设私钥的拥有者是期望的信息发送者，他会妥善保管私钥，不会弄丢私钥，那么，我们上面的推论就可以改为：如果用公钥成功的解密了一份消息，那么这份消息就一定是期望的发送者发过来的。这叫做**对发送者的身份识别**。

比如你拥有一把公钥，你的朋友张三拥有一把配对的私钥。张三给你发了一份用私钥加密的消息，你用公钥成功的解密了这份消息。此时你就可以确认，这份消息的确是你的朋友张三发来的，而不是骗子发来的。

用同样的方式，你可以确认一份消息是不是从某个银行发来的，你可以确认消息是不是从某个公司发来的，总之，你可以确认该消息是不是由某个你期望的个人或组织发来的。

如此这般，通过私钥加密公钥解密的方式，你可以确认发来消息的人是谁，也就是确认了发送者的身份。这就是非对称加密的第一个用途：**识别发送者身份**。

识别发送者身份是安全通讯中非常重要的一步。Https通讯时，客户端要识别服务器的身份，就要对服务器的证书进行验证，而验证的过程就包括对证书上的数字签名进行校验，数字签名的校验过程包含着“私钥加密，公钥解密”的过程。

什么是数字签名？

简单的说，签名=哈希值的私钥加密。

从技术上讲，数字签名就是对消息体先做哈希（Hash）计算再用私钥加密后得到的一段信息。什么是哈希？哈希函数或者说哈希计算就是将一串数据按照一定的算法进行计算，结果得到一段固定长度（比如128位）的值，谓之哈希值。不同的数据，其哈希值很难是一样的（如果碰巧一样，这称为hash碰撞，几率很低）。我们就认定：一个消息数据对应着一个哈希值，消息数据如果改变，它的hash值一定也会改变。反过来说，如果它的哈希值改变了，意味着原始数据也改变了。

同时，Hash是不可逆的，你不可能通过Hash值来反过来计算出Hash算出之前的原始数据。

通常，哈希计算用于将一个很大的数据映射成一个很短的数据，将一段长文本映射成一段很短的字符串，总之，就是将一个大的取值空间映射到一个小的取值空间。

所以，哈希也常被称为摘要。

数字签名，是对哈希值的加密，为什么对哈希值加密而不是对原文加密？

因为对哈希值这个很短很小的数据加密比对很长的原始信息加密要快的多。

哈希算法有三类MD(md2,md4,md5) SHA(sha1,sha2,sha3) MAC

签名验证的过程是怎么样的？

比如我们收到了一份数据（这个数据可能是一段文本，一个可执行程序，一个数字证书等，我们姑且叫它A）后，附着在这份数据上的签名会被先拿下来，因为签名是私钥加密的值，所以系统会用你手里对应的公钥解密签名，如果成功，说明是期望的人发过来的，不是骗子发来的。解密签名后的值是B，接着我们对消息体再做一遍哈希计算，得到C，然后比较B和C，如果B=C，则说明消息没有被篡改过。

上述数字签名验证做了两件事：1，识别签署人身份。2，保证信息完整性。

如果A是数字证书，上述过程就是对数字证书的验证过程，验证成功，就说明这个证书是在正经的地方签发的，并且是没有被篡改和替换的，你是可以相信的。

如果A是一段文本，上述过程就是对这段文本的验证过程，验证成功，就说明这段文本是正经的人签署的，并且文本是没有被篡改和替换的，你是可以相信的。

如果A是一个可执行程序，道理也是一样。

数字签名对原文的保密性没有要求，数字签名的主要的作用是认证签署人身份，换句话说就是证明这个签名是我签的，这段附着我的签名的文档或邮件是我写的，不是别人写的，同时我也无法抵赖说这不是我写的。同时证明了文档或邮件没有被替换，没有被篡改。

数字签名不负责对消息保密。

什么是数字证书？

首先，数字证书就是一个文件，扩展名常见的有filename.cer, filename.der, filename.pkcs，这代表了它们的编码格式不同。前两种格式的文件在window下可以直接打开，出现一个证书窗口，显示出证书里的各种信息。你也可以用文本编辑器打开证书文件，会发现，其内容就是一段Base64编码的文本，Base64编码格式就是它的存储格时使用的格式。你把这段文本copy下来保存为.cer文件 (微博里不允许粘贴这个文件的文本)，就可以在window下双击打开，就能查看这个证书的信息。

-----BEGIN CERTIFICATE-----

MIIDujCCAqKgAwIBAgILBAAAAAABD4Ym5g0wDQYJKoZIhvcNAQEFBQAwTDEgMB4G

A1UECxMXR2xvYmFsU2lnbiBSb290IENBIC0gUjIxEzARBgNVBAoTCkdsb2JhbFNp

Z24xEzARBgNVBAMTCkdsb2JhbFNpZ24wHhcNMDYxMjE1MDgwMDAwWhcNMjExMjE1

MDgwMDAwWjBMMSAwHgYDVQQLExdHbG9iYWxTaWduIFJvb3QgQ0EgLSBSMjETMBEG

A1UEChMKR2xvYmFsU2lnbjETMBEGA1UEAxMKR2xvYmFsU2lnbjCCASIwDQYJKoZI

hvcNAQEBBQADggEPADCCAQoCggEBAKbPJA6+Lm8omUVCxKs+IVSbC9N/hHD6ErPL

v4dfxn+G07IwXNb9rfF73OX4YJYJkhD10FPe+3t+c4isUoh7SqbKSaZeqKeMWhG8

eoLrvozps6yWJQeXSpkqBy+0Hne/ig+1AnwblrjFuTosvNYSuetZfeLQBoZfXklq

tTleiDTsvHgMCJiEbKjNS7SgfQx5TfC4LcshytVsW33hoCmEofnTlEnLJGKRILzd

C9XZzPnqJworc5HGnRusyMvo4KD0L5CLTfuwNhv2GXqF4G3yYROIXJ/gkwpRl4pa

zq+r1feqCapgvdzZX99yqWATXgAByUr6P6TqBwMhAo6CygPCm48CAwEAAaOBnDCB

mTAOBgNVHQ8BAf8EBAMCAQYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUm+IH

V2ccHsBqBt5ZtJot39wZhi4wNgYDVR0fBC8wLTAroCmgJ4YlaHR0cDovL2NybC5n

bG9iYWxzaWduLm5ldC9yb290LXIyLmNybDAfBgNVHSMEGDAWgBSb4gdXZxwewGoG

3lm0mi3f3BmGLjANBgkqhkiG9w0BAQUFAAOCAQEAmYFThxxol4aR7OBKuEQLq4Gs

J0/WwbgcQ3izDJr86iw8bmEbTUsp9Z8FHSbBuOmDAGJFtqkIk7mpM0sYmsL4h4hO

291xNBrBVNpGP+DTKqttVCL1OmLNIG+6KYnX3ZHu01yiPqFbQfXf5WRDLenVOavS

ot+3i9DAgBkcRcAtjOj4LaR0VknFBbVPFd5uRHg5h6h+u/N5GJG79G+dwfCMNYxd

AfvDbbnvRG15RjF+Cv6pgsH/76tuIMRQyV+dTZsXjAzlAcmgQWpzU/qlULRuJQ/7

TBj0/VLZjmmx6BEP3ojY+x1J96relc8geMJgEtslQIxq/H5COEBkEveegeGTLg==

-----END CERTIFICATE-----

其次，数字证书是对公钥的封装，而公钥是需要公开出去的，所以数字证书也是公开的。比如，我们访问需要安全认证的网站时，网站会要求我们安装它们的证书，每个访问网站的人都会获取其证书，网站是公开的，其证书也是公开的，这样，接下来就可以拿着证书里的公钥和网站服务器的私钥通过加密解密的方式进行安全通信了。

最后，除了公钥，数字证书里围绕这公钥又增加了一些其它信息，比如证书的有效期，证书发布机构，证书的所有者等。数字证书由权威机构签发，实际上，签发过程就是对申请数字证书的公钥做数字签名，这样你就知道这个证书是不是权威机构签发的；验证过程就是对数字证书的签名做验证。

做签名验证的前提是你已经安装了权威机构的根证书。

现在我们的脑子里有两个证书，一个是数字证书，一个是根证书。数字证书里有公钥，根证书里也有公钥。那么这两种公钥的作用有什么区别？

根证书的里公钥用来验证数字证书的签名，保证数字证书安全（所以，前面有个例子里的公钥X，是指根证书的公钥。）

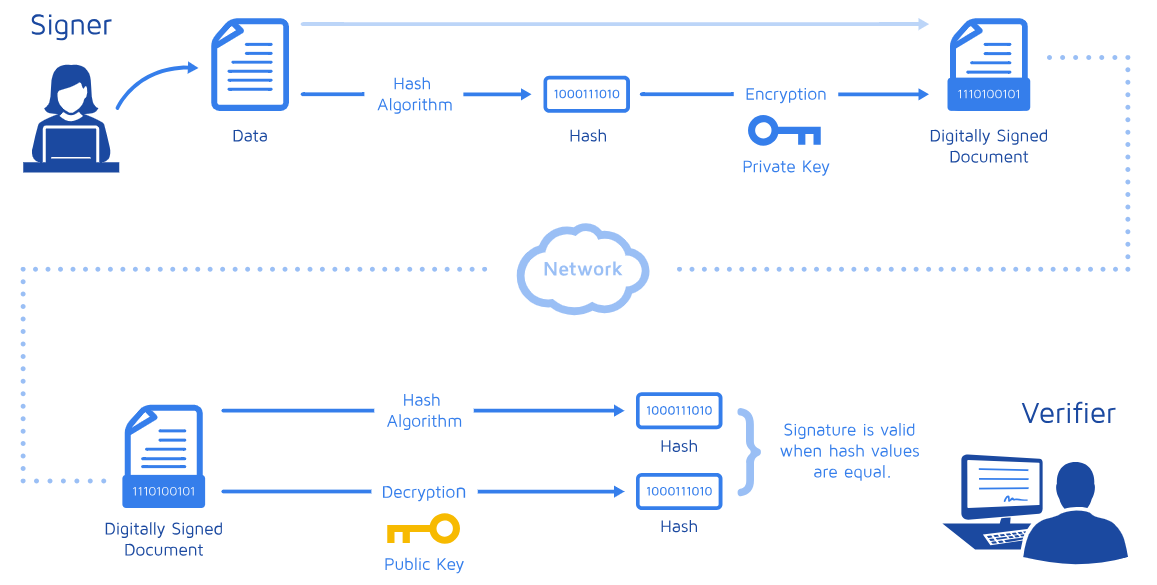
数字证书里的公钥用来保证通讯安全。

也就是说，根证书用来校验证书的合法性，证书用来校验数据的合法性。比如你访问Google，Google会发给你证书，机器的根证书会被用来验证Google发来的证书是不是合法的，验证通过后，再用Google的证书验证Google发来的数据是不是合法的。

接下来我们认识一下根证书的作用与工作流程。

比如，你安装了权威认证中心A公司的根证书，也就意味着你有了A公司的公钥。某宝网的证书也是在A公司签发的，也就意味着某宝网的证书用A公司的私钥做了哈希后加密。你访问某宝网，某宝网会发给你它的证书，你的系统会验证这个证书。验证的过程是用你根证书里的公钥去解密签名，再做哈希对比，发现这个证书没有被篡改过，就算是对该证书验证成功。你可以相信某宝网的证书了。

下图就是证书验证过程，图中的Signer就是权威认证中心A 公司，Verifier就是安装了A公司的根证书的客户端。



证书+数字签名+根证书，基本就堵住了各种安全漏洞。

* 通信数据是安全的，因为用证书里的公钥和服务器的私钥对通讯内容做了加密 （具体加密细节会多一些协商**对称秘钥**的环节，此时不必理会，让我们先从整体上理解它）。黑客没有服务器私钥，所以无法解密对称秘钥，也就无法解密通讯内容。
* 证书是安全可靠的，因为证书有数字签名，数字签名的用途之一就是识别签署人身份，签署人身份安全可靠，证书就安全可靠。证书安全可靠，证书里的公钥就安全可靠，就可以排除公钥伪造。也就是说，黑客无法篡改数字证书的内容，如果篡改了，数字证书的签名验证就会失败。
* 根证书是安全可靠的，因为根证书是从权威认证中心拿来的，windows操作系统还内置了一些根证书。

根证书是信任链条的起点，一定要保证根证书是有效的、合法的。所以，正规的应用一般都是到权威认证中心下载根证书。如果你电脑染上了病毒，病毒可以替换你的根证书，你的计算机就没有任何安全性可言了。

所有上面的这一切，都是因为“非对称加密”这项技术而演化出的一套游戏规则。

作者: Dapple Hou