# 数字摘要

## 数字摘要的定义

一种算法，就是对一个数据源进行一个算法之后得到一个摘要。

著名的摘要算法有RSA公司的MD5算法和SHA-1算法及其大量的变体。

## 数字摘要存在的问题

攻击者可以修改源文件的同时，修改数字摘要文件，，接受者无法根据数字摘要确定数据是否被修改。

## 解决方案

使用**数字签名**来解决。

将数字摘要文件加密，是攻击者无法解密修改数字摘要文件，

# 数字签名

要确保可靠通信，必须要解决两个问题：首先，要确定消息的来源确实是其申明的那个人；其次，要保证信息在传递的过程中不被第三方篡改，即使被篡改了，也可以发觉出来。

数字签名，就是为了解决这两个问题而产生的，它是对前面提到的**非对称加密技术**与**数字摘要**技术的一个具体的应用。

## 数字签名的生成

**前提**：对于消息的发送者来说，先要生成一对公私钥对，将**公钥给消息的接收者**。

消息的发送者有一天想给消息接收者发消息，在发送的信息中，除了要包含原始的消息外，还要加上另外一段消息。这段消息通过如下两步生成：  
1）对要发送的原始消息提取**消息摘要**；  
2）对提取的信息摘要用自己的**私钥加密**。  
通过这两步得出的消息，就是所谓的原始信息的数字签名。  
而对于信息的接收者来说，他所收到的信息，将包含两个部分，一是原始的消息内容，二是附加的那段数字签名。

## 数字签名的验证

1. 对原始消息部分提取消息摘要，注意这里使用的消息摘要算法要和发送方使用的一致；
2. 对附加上的那段数字签名，使用预先得到的公钥解密；
3. 比较前两步所得到的两段消息是否一致。如果一致，则表明消息确实是期望的发送者发的，且内容没有被篡改过；相反，如果不一致，则表明传送的过程中一定出了问题，消息不可信。

## 数字签名存在的问题

但是有一个问题？

数字签名方法，有一个前提，就是消息的接收者必须要事先得到正确的公钥。如果一开始公钥就被别人篡改了，那坏人就会被你当成好人，而真正的消息发送者给你发的消息会被你视作无效的。而且，很多时候根本就不具备事先沟通公钥的信息通道。那么如何保证公钥的安全可信呢？这就要靠**数字证书**来解决了

## 解决方案

数字证书，保证公钥的安全可信，用来解决公钥的安全发放问题。

# 数字证书

数字证书，一般包含以下一些内容：  
（1）证书的发布机构（Issuer）  
（2）证书的有效期（Validity）  
（3）消息发送方的公钥  
（4）证书所有者（Subject）  
（5）数字签名所使用的算法  
（6）数字签名。

数字证书其实也用到了数字签名技术。只不过要签名的内容是消息发送方的公钥。数字证书中签名者不是随随便便一个普通的机构，而是要有一定公信力的机构。一般来说，这些有公信力机构的**根证书已经在设备出厂前预先安装到了你的设备上了**。所以，**数字证书可以保证数字证书里的公钥确实是这个证书的所有者的**，或者证书可以用来确认对方的身份。数字证书主要是用来解决公钥的安全发放问题。

# 总结

数字签名和签名验证的大体流程如下图所示：

