首先要了解什么叫对称加密和非对称加密，消息摘要这些知识。

1. 非对称加密

在通信双方，如果使用非对称加密，一般遵从这样的原则：公钥加密，私钥解密。同时，一般一个密钥加密，另一个密钥就可以解密。

因为公钥是公开的，如果用来解密，那么就很容易被不必要的人解密消息。因此，**私钥也可以认为是个人身份的证明。**

如果通信双方需要互发消息，那么应该建立两套非对称加密的机制（即两对公私钥密钥对），发消息的一方使用对方的公钥进行加密，接收消息的一方使用自己的私钥解密。

2.消息摘要

消息摘要可以将消息哈希转换成一个固定长度的值唯一的字符串。值唯一的意思是不同的消息转换的摘要是不同的，并且能够确保唯一。**该过程不可逆**，即不能通过摘要反推明文（似乎SHA1已经可以被破解了，SHA2还没有。一般认为不可破解，或者破解需要耗费太多时间，性价比低）。

利用这一特性，**可以验证消息的完整性。**

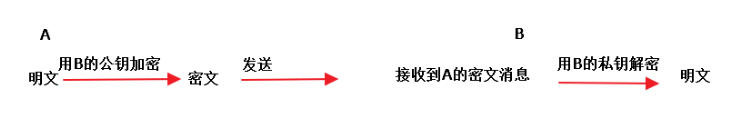
消息摘要通常用在数字签名中，下面介绍用法。

 了解基础知识之后，就可以看一下数字签名和数字证书了。

3.数字签名

假设现在有通信双方A和B，两者之间使用两套非对称加密机制。

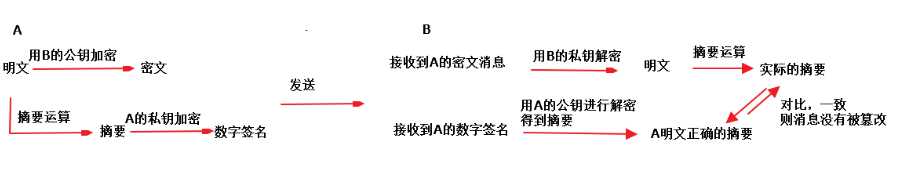
现在A向B发消息。



那么，如果在发送过程中，有人修改了里面密文消息，B拿到的密文，解密之后得到明文，并非A所发送的，信息不正确。

要解决两个问题：1. A的身份认证 2. A发送的消息完整性 那么就要用到上面所讲的基础知识。

数字签名的过程如下图：



简单解释：

A：将明文进行摘要运算后得到摘要（消息完整性），再将摘要用A的私钥加密（身份认证），得到数字签名，将密文和数字签名一块发给B。

B：收到A的消息后，先将密文用自己的私钥解密，得到明文。将数字签名用A的公钥进行解密后，得到正确的摘要（解密成功说明A的身份被认证了）。

对明文进行摘要运算，得到实际收到的摘要，将两份摘要进行对比，如果一致，说明消息没有被篡改（消息完整性）。

疑问：

摘要使用A的私钥加密，如果被拥有A的公钥的第三者截获，不就可以获取到摘要了么？会不会对安全造成威胁。

不会。因为摘要是不可逆推出原文的。

 4.数字证书

理解了数字签名之后，数字证书就好理解了。

由于网络上通信的双方可能都不认识对方，那么就需要第三者来介绍，这就是数字证书。

数字证书由Certificate Authority( CA 认证中心)颁发。

关于数字证书的具体描述，需要百度，目前未完全理解。记一个TODO。

图解如下：

首先A B双方要互相信任对方证书。//TODO

然后就可以进行通信了，与上面的数字签名相似。不同的是，使用了对称加密。这是因为，非对称加密在解密过程中，消耗的时间远远超过对称加密。如果密文很长，那么效率就比较低下了。但密钥一般不会特别长，对对称加密的密钥的加解密可以提高效率。

