# 密码学

## 对称加密

对称加密算法的加密和解密使用的密匙是相同的，也就是说如果通讯两方如果使用对称加密算法来加密通讯数据，那么通讯双方就需要都知道这个密匙，收到通讯数据后用这个密匙来解密数据。

这类算法在加密和解密时使用相同的密钥，或是使用两个可以简单地相互推算的密钥。事实上，这组密钥成为在两个或多个成员间的共同秘密，以便维持专属的通信联系。与非对称加密相比，要求双方获取相同的密钥是对称密钥加密的主要缺点之一。常见的对称加密算法有 DES、3DES、AES、Blowfish、IDEA、RC5、RC6。

**对称加密的速度比公钥加密快很多，在很多场合都需要对称加密**。

## 非对称加密

它需要两个密钥，**一个是公开密钥，另一个是私有密钥；一个用作加密的时候，另一个则用作解密**。使用其中一个密钥把明文加密后所得的密文，只能用相对应的另一个密钥才能解密得到原本的明文；甚至连最初用来加密的密钥也不能用作解密。由于加密和解密需要两个不同的密钥，故被称为非对称加密；

虽然两个密钥在数学上相关，但如果知道了其中一个，并不能凭此计算出另外一个；因此其中一个可以公开，称为 **公钥**，任意向外发布；不公开的密钥为 **私钥** ，必须由用户自行严格秘密保管，绝不透过任何途径向任何人提供，也不会透露给要通信的另一方，即使他被信任。

公钥 & 私钥 均可以作为加密密钥

## 数字签名

数字签名是一种类似写在纸上的签名，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。在网络上，我们可以使用“数字签名”来进行身份确认。数字签名是一个独一无二的数值，若公钥能通过验证，那我们就能确定对应的公钥的正确性，数字签名兼具这两种双重属性："可确认性"及"不可否认性（不需要笔迹专家验证）"。

数字签名就是将公钥密码反过来使用。签名者将讯息用私钥加密（**这是一种反用，因为通常非对称加密中私钥用于解密**），然后公布公钥;验证者使用公钥将加密讯息解密并比对消息（一般签名对象为消息的散列值）。

## 密码散列函数

密码散列函数（英语：Cryptographic hash function），又译为加密散列函数、密码散列函数、加密散列函数，是散列函数的一种。它被认为是一种 **单向函数**，也就是说极其难以由散列函数输出的结果，回推输入的数据是什么。这种散列函数的输入数据，通常被称为消息（ message ），而它的输出结果，经常被称为消息摘要（ message digest ）或摘要（ digest ）。