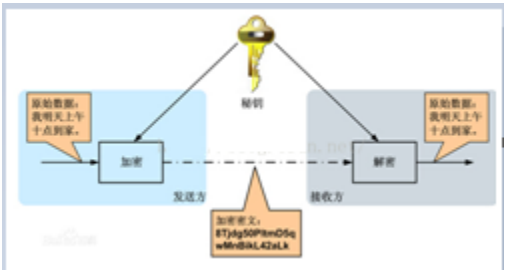
# 数据保密与安全

## 1、对称加密技术

对称加密技术：是指加密系统的加密密钥和解密密钥相同，或者虽然不同，但从其中的任意一个可以很容易的推导出另一个。

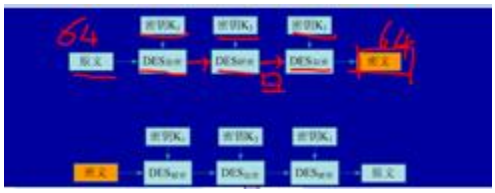



在对称加密算法中，数据发信方将明文（原始数据）和加密密钥一起经过特殊加密算法处理后，使其变成复杂的加密密文发送出去。收信方收到密文后，需要使用同一密钥及相同算法的逆算法解密，使其恢复成明文。在对称加密算法中，使用的密钥只有一个，发收信双方都使用这个密钥进行加密和解密，这就要求解密方事先必须知道加密密钥。

对称加密算法的特点是算法公开、计算量小、加密速度快、加密效率高。不足之处是，交易双方都使用同样钥匙，安全性得不到保证。此外，每对用户每次使用对称加密算法时，都需要使用其他人不知道的惟一钥匙，这会使得发收信双方所拥有的钥匙数量成几何级数增长，密钥管理成为用户的负担。对称加密算法在分布式网络系统上使用较为困难，主要是因为密钥管理困难，使用成本较高。

在计算机专网系统中广泛使用的对称加密算法有 DES、IDEA 和 AES。

**DES（数据加密标准算法）：**主要采用替换和移位的方法加密。它用 56 位（64 位密钥只有 56 位有效密钥）密钥对 64 位二进制数据块进行加密，每次加密可对 64 位的输入数据进行 16 轮编码，经一系列替换和移位后，输入的 64 位原始数据转换成完全不同的 64 位输出数据。



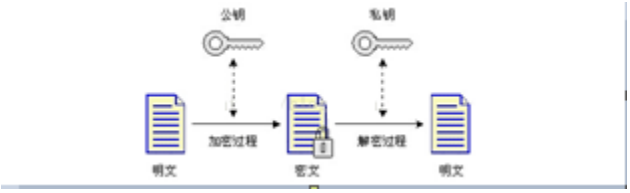
**3DES（三重 DES）：**在 DES 的基础上采用三重 DES，即用两个 56 位的密钥 K1、K2，发送方 K1 加密，K2 解密，再使用 K1 加密。接收方则使用 K1 解密，K2 加密，再使用 K1 解密，其效果相当于将密钥长度加倍。

传统的 DES 由于只有 56 位的密钥，因此已经不适应当今分布式开放网络对数据加密安全性的要求。1997 年 RSA 数据安全公司发起了一项"DES 挑战赛"的活动，志愿者四次分别用四个月、41 天、56 个小时和 22 个小时破解了其用 56 位密钥 DES 算法加密的密文。即 DES 加密算法在计算机速度提升后的今天被认为是不安全的。

**AES：**提供 128 位密钥，因此，128 位 AES 的加密强度是 56 位 DES 加密强度的 1021 倍还多。假设可以制造一部可以在 1 秒内破解 DES 密码的机器，那么使用这台机器破解一个 128 位 AES 密码需要大约 149 亿万年的时间。（宇宙一般被认为存在了还不到 200 亿年）。

## 2、非对称加密技术

对称加密技术是加密、解密使用相同的密钥。而非对称加密技术则是指加密密钥与解密密钥不同，分为公钥和私钥。




不对称加密算法中，是两把不同但又是完全匹配的公钥和私钥。在使用不对称加密算法加密文件时，只有使用匹配的一对公钥和私钥，才能完成对明文的加密和解密过程。加密明文时采用公钥加密，解密密文时使用私钥才能完成，而且发信方（加密者）知道收信方的公钥，只有收信方（解密者）才是唯一知道自己私钥的人。

不对称加密算法的基本原理是，如果发信方想发送只有收信方才能解读的加密信息，发信方必须首先知道收信方的公钥，然后利用收信方的公钥来加密原文；收信方收到加密密文后，使用自己的私钥才能解密密文。显然，采用不对称加密算法，收发信双方在通信之前，收信方必须将自己早已随机生成的公钥送给发信方，而自己保留私钥。

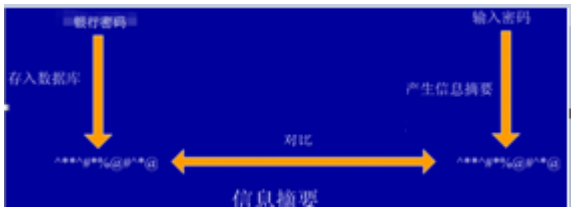
由于不对称算法拥有两个密钥，因而特别适用于分布式系统中的数据加密。广泛应用的不对称加密算法有 RSA 算法和美国国家标准局提出的 DSA。以不对称加密算法为基础的加密技术应用非常广泛。

## 3、信息摘要

信息摘要算法实际上就是一个单向散列函数，数据块经过单向散列函数得到一个固定长度的散列值，攻击者不可能通过散列值而编造数据块，使得编造的数据块的散列值和源数据块的散列值相同。

通过哈希函数从信息中提取摘要，但是摘要本来就是信息的一小部分，而且毫无规律可言，所以就算被人截获也不能反向得出原文。消息摘要算法主要有

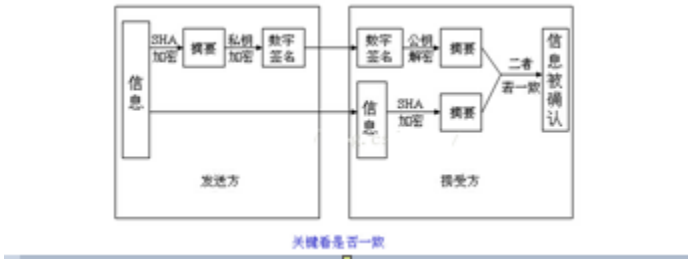
MD5、SHA 等，其算法的散列值分别为 128 位和 160 位，由于 SHA 通常采用密钥比 MD5 长，所以安全性要高于 MD5。




**信息摘要应用：**例如用户的银行卡密码不是直接将密码保存到数据库的，否则管理员都知道每个人的密码监守自盗怎么办。所以都是经过信息摘要算法将结果保存到数据库，然后当用户输入密码时，机器用相同的摘要算法运算，如果和数据库中摘要算法结果相同，证明密码输入正确。

## 4、数字签名

**数字签名的作用：**和日常的签名一样，使得发送者难以否认自己发送过的数据；因为签名不易仿冒，从而使得接收者不能够篡改。即保证信息传输的完整性、发送者的身份认证、防止交易中的抵赖发生。

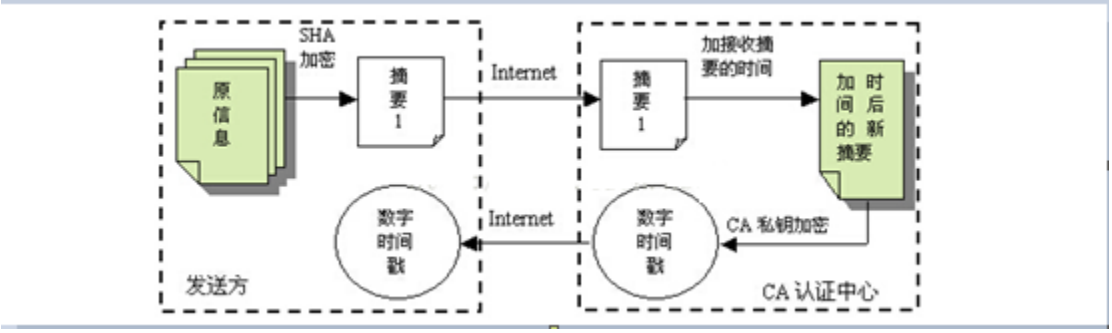



数字签名技术是将摘要信息用发送者的私钥加密，与原文一起传送给接收者。接收者只有用发送者的公钥才能解密被加密的摘要信息，然后用 HASH 函数对收到的原文产生一个摘要信息，与解密的摘要信息对比。如果相同，则说明收到的信息是完整的，在传输过程中没有被修改，否则说明信息被修改过，因此数字签名能够验证信息的完整性。

数字签名是个加密的过程，数字签名验证是个解密的过程。

## 5、数字时间戳

数字时间戳技术就是数字签名技术一种变种的应用。




在电子商务交易文件中，时间是十分重要的信息。数字时间戳服务（Digital Time Stamp Service，DTS）是网上电子商务安全服务项目之一，能提供电子文件的日期和时间信息的安全保护。

一般来说，数字时间戳产生的过程为：用户首先将需要加时间戳的文件用 Hash 算法运算形成摘要，然后将该摘要发送到 DTS。DTS 在加入了收到文件摘要的日期和事件信息后再对该文件加密（数字签名），然后送达用户。

时间戳（time-stamp）是一个经加密后形成的凭证文档，它包括 3 个部分：

- 需加时间戳的文件的摘要（digest）；
- DTS 收到文件的日期和时间；
- DTS 的数字签名。

**与数字签名的区别**:数字签名是没有时间的，而时间戳为数字签名加上时间。