# 加密解密技术

利用技术手段把重要的数据变为乱码（加密）传送，到达目的地后再用相同或不同的手段还原（解密）。加密技术包括两个元素：算法和密钥。

密钥加密技术的密码体制分为对称密钥体制和非对称密钥体制。相应的，对数据加密的技术分为两类，即对称加密（私人密钥加密）和非对称加密（公开密钥加密）。对称加密以数据加密标准（DES，Data Encryption Standard）算法为典型代表，非对称加密通常以RSA算法为代表。

对称加密的加密密钥和解密密钥相同；而非对称加密的加密密钥和解密密钥不同，加密密钥可以公开而解密密钥需要保密。

# 什么是对称加密技术?

对称加密采用了对称密码编码技术，它的特点是文件加密和解密使用相同的密钥，即加密密钥也可以用作解密密钥，这种方法在密码学中叫做对称加密算法，对称加密算法使用起来简单快捷，密钥较短，且破译困难，除了数据加密标准（DES），另一个对称密钥加密系统是国际数据加密算法（IDEA），它比DES的加密性好，而且对计算机功能要求也没有那么高。IDEA加密标准由PGP（Pretty Good Privacy）系统使用。

# 什么是非对称加密技术?

1976年，美国学者Dime和Henman为解决信息公开传送和密钥管理问题，提出一种新的密钥交换协议，允许在不安全的媒体上的通讯双方交换信息，安全地达成一致的密钥，这就是“公开密钥系统”。相对于“对称加密算法”这种方法也叫做“非对称加密算法”。与对称加密算法不同，非对称加密算法需要两个密钥：公开密钥（publickey）和私有密 （privatekey）。公开密钥与私有密钥是一对，如果用公开密钥对数据进行加密，只有用对应的私有密钥才能解密；如果用私有密钥对数据进行加密，那么只有用对应的公开密钥才能解密。因为加密和解密使用的是两个不同的密钥，所以这种算法叫作非对称加密算法。

# Des加密

http://blog.csdn.net/qq\_18870023/article/details/52180768