加密：

明文通过某运算得出密文。某运算是加密运算。加密运算中的一个由用户提供的特征参数是（加）密钥，不能对外泄漏。

解密：

密文通过某逆运算得出（原）明文。某逆运算是解密运算。解密运算中的一个由用户提供的特征参数是（解）密钥，不能对外泄漏。

对称加密：

（加）密钥与（解）密钥相同，或者互为函数关系，则称加密方式为对称加密。

非对称加密：

（加）密钥与（解）密钥不相同且没有函数关系，则称加密方式为非对称加密。

非对称加密的密钥通常以密钥对的形成出现，分别是私钥和公钥。私钥由用户保存，不能泄露；公钥对外公开发布。

使用方式：

A用户有密钥对：私钥Pri\_a和公钥Pub\_a。A还有B的公钥Pub\_b。

B用户有密钥对：私钥Pri\_b和公钥Pub\_b。B还有A的公钥Pub\_a。

1、加密通讯：

A用户向B用户发送加密信息：A将明文用Pub\_b加密后发送，B收到密文后用Pri\_b解密，B收到A的信息原文。

B用户向A用户发送加密信息：B将明文用Pub\_a加密后发送，A收到密文后用Pri\_a解密，A收到B的信息原文。

1. 数字签名

A用户将原文用Pri\_a加密后对外发布，其他用户仅能用Pub\_a解密后才能获得原文。由仅能用Pub\_a（其它Pub密钥不能）解密后才能获得原文得知，原文出自用户A且A不能否认；由A持有唯一的Pri\_a，其它用户无法获取该Pri\_a得知，其他用户无法篡改原文，如果篡改，由于没有A的Pri\_a，将无法得到正确的密文。