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。

注：二战以前，加密算法是被保护的不对外公开，缺点是，一但加密算法被破解，整个系统更新加密算法的代价（费用，部署时间等）高昂；二战以后，加密算法成为标准对外公开，密钥是受保护的。

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。

对称加密标准如：AES（256bit密钥）、DES（56bit密钥，容易被暴力破解，算法本身安全）

古代加密法：凯撒加密、福尔摩斯探案集-跳舞的小人

优点：加密速度快，密文长度较明文增加不多。

缺点：密钥传递存在泄密风险，多用户存在多密钥，用户间密钥传递和管理存在困难。

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。

非对称加密标准：MD5、RSA、SHA

优点：密文定长，用户密钥管理和交换方便

缺点：运算时间长，耗费运算资源。

运用场景：

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、非对称加密通讯：

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。

1. 证书（公钥证书）

为了保证用户公钥可靠传输，在PKI（public key infrastructure，相当于法律法规）下，用户寻求第三方CA（证书机构）帮助发布自己的公钥。经CA认证的公钥由Certification（公钥证书）代表。证书的唯一作用就是保证公钥的真实性，不被他人替换。

在安全通信过程中，所用的数字证书符合 International Telecommunication Union (ITU) 的 X.509 标准。该证书用于检查（认证）程序、计算机或组织机构的身份。

X.509 证书主要用于将带有证书主题数据的身份（例如，电子邮件地址或计算机名称）与身份的公钥绑定在一起。身份可以是个人、计算机，也可以是机器设备。

证书由证书颁发机构（Certificate Authority，CA）或证书所有者签发。而 PKI 系统则指定了用户信任证书颁发机构及其所签发证书的规则。证书所有者签发的证书叫自签名证书，不在PKI系统内。

证书认证过程：

1、要获取一份证书，需要向与证书颁发机构相关联的注册机构提交一份证书申请。

2、证书颁发机构将基于既定标准对该申请和申请人进行评估。

3、如果可以清晰识别申请人的身份，则证书颁发机构将签发证书。申请人成为证书持有者。

证书签发：

证书的签发者（CA）使用一个特定的哈希函数（例如，SHA-1，Secure Hash Algorithm），根据证书数据生成一个哈希值。 该 HASH 值是一个长度固定的位串。之后，证书的签发者再使用自己的私钥，生成一个数字签名。通常采用 RSA 签名机制。数字签名将保存在证书中。此时，证书已签名。

验证证书：

证书验证方在获得持有方证书和CA证书后，可读出持有方及CA机构的公钥（CA证书的真实性由上一级CA机构证书保证，上一级CA证书的真实性由上上一级CA证书保证，如此递推可追述到根CA机构的根证书）。 验证时，使用CA同样的哈希算法（例如，SHA-1），根据持有方证书数据生成一个新的哈希值；然后，通过CA的公钥对持有方证书中的CA签名进行解密；解密后的哈希值与上面的新哈希值比较，如果结果一致，则表示证书持有者的身份以及完整性（即，证书内容的可靠性和真实性）均通过验证。

Root 证书及证书链

PKI 证书通常按层级进行组织：层级顶部由根证书构成。这些证书并非由上一级证书颁发机构签名。根证书的证书持有者和证书签发者完全相同（相当于自签名）。根证书享受绝对信任。它们是信任的“锚点”，因此对于验证方，其必须用作绝对（信任）证书。此类证书存储在专门存储受信证书的区域。根证书用于对下级证书颁发机构的证书（即，所谓的中间证书）进行验证。从而实现从 Root 根证书到中间证书信任关系的传递。

1. 现实中的加密通信

现实中的加密通信融合了对称和非对称加密技术。明文通常较长采用对称加密；对称密钥是一个随机数但是文本比较短而采用非对称加密。同时将密文和经非对称加密后的密钥发送给接收方。接受方解密对称密文和非对称密钥后得出明文。