# 非对称加密算法

## 椭圆曲线算法(ECC) 与 RSA算法 的比较

- 椭圆曲线公钥系统是代替RSA的强有力的竞争者。 椭圆曲线加密方法 与 RSA 方法相比，有以下的优点：
  - 安全性能更高 ：如160位ECC与1024位RSA、DSA有相同的安全强度
  - 计算量小，处理速度快： 在私钥的处理速度上（解密和签名），ECC远 比RSA、DSA快得多
  - 存储空间占用小： ECC的密钥尺寸和系统参数与RSA、DSA相比要小得多， 所以占用的存储空间小得多
  - 带宽要求低

## 名词解释

- ECC ：Elliptic Curves Cryptography，椭圆曲线密码编码学
- ECDSA：用于数字签名，是 ECC 与 DSA 的结合，整个签名过程与DSA类似，所不一样的是签名中采取的算法为ECC，最后签名出来的值也是分为r,s。
- ECDH：是基于 ECC （Elliptic Curve Cryptosystems，椭圆曲线密码体制，参看ECC）的 DH （ Diffie-Hellman）密钥交换算法。