加解密

非对称加密算法

非对称加密算法需要两个密钥：[公开密钥](https://baike.baidu.com/item/%E5%85%AC%E5%BC%80%E5%AF%86%E9%92%A5/7453570)（publickey:简称公钥）和私有密钥（privatekey:简称私钥）。**公钥与私钥是一对，如果用公钥对数据进行加密，只有用对应的私钥才能解密**。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。

## 工作原理

[编辑](javascript:;)

1.A要向B发送信息，A和B都要产生一对用于加密和解密的[公钥](https://baike.baidu.com/item/%E5%85%AC%E9%92%A5)和[私钥](https://baike.baidu.com/item/%E7%A7%81%E9%92%A5)。

2.A的私钥保密，A的公钥告诉B；B的私钥保密，B的公钥告诉A。

3.A要给B发送信息时，A用B的公钥加密信息，因为A知道B的公钥。

4.A将这个消息发给B（已经用B的公钥加密消息）。

5.B收到这个消息后，B用自己的私钥解密A的消息。其他所有收到这个报文的人都无法解密，因为只有B才有B的私钥。

**特点**  
算法强度复杂，安全性依赖于算法与密钥。  
**缺点**  
由于其算法复杂，而使得加密解密速度没有对称加密解密的速度快。  
**与对称加密算法的对比**

* 优点：其安全性更好，对称加密的通信双方使用相同的秘钥，如果一方的秘钥遭泄露，那么整个通信就会被破解。而非对称加密使用一对秘钥，一个用来加密，一个用来解密，而且公钥是公开的，秘钥是自己保存的，不需要像对称加密那样在通信之前要先同步秘钥。
* 缺点：非对称加密的缺点是加密和解密花费时间长、速度慢，只适合对少量数据进行加密。

**在非对称加密中使用的主要算法有：RSA、Elgamal、ESA、背包算法、Rabin、D-H、ECC（椭圆曲线加密算法）等。不同算法的实现机制不同，可参考对应算法的详细资料。**

**经典算法-->RSA**

RSA算法基于一个十分简单的数论事实：将两个大质数（素数）相乘十分容易，但是想要对其乘积进行因式分解却极其困难，因此可以将乘积公开作为加密密钥。比如：取两个简单的质数：89、97，得到两者乘积很简单8633；但是要想对8633进行因式分解，其工作量成几何增加。