* [一、 密码概述](http://www.cnblogs.com/mddblog/p/5380556.html#_label0)
* [二、加密与签名区别（RSA）](http://www.cnblogs.com/mddblog/p/5380556.html#_label1)

**一、 密码概述**

发送者对明文进行加密然后生成密文，接受者再对密文解密得到明文的过程。 现在使用的所有加密算法都是公开的！但是密钥肯定不是公开的。

**1 散列(哈希)函数**

* 通常有MD5、SHA1、SHA256、SHA512
* 实质是抽取特征码，这样一般不会重复！是的，不同的文本它的哈希结果是有可能相同的，但概率很小。  
  （举例：比如想要识别一个人，我们可以通过他的指纹来锁定他，指纹出现相同的概率很低吧！在这里，人就相当于数据，而指纹就相当于对人这个数据进行hash后得到的结果）
* 对任意一个二进制数据进行哈希，可以得到定长的字符串结果，例如MD5哈希结果是128位，更多是以32个字符的十六进制格式哈希输出
* 还有就是不可逆的，既然是不可逆的，那么当然**不是用来加密的，而是签名**

**2 对称加密算法**

* 有DES、3DES、AES
* 加密和解密使用同一个秘钥，加密解密的速度快
* 适合给大数据进行加密
* 密钥的安全性非常重要

**3 非对称加密算法：RSA**

1. 使用 公钥 加密，使用 私钥 解密
2. 使用 私钥 加密，使用 公钥 解密（私钥签名，公钥验签）
3. 更安全，当然速度会慢下来，如果随着硬件的突破，使用越来越多，特别是支付

1是对数据加密，2是防止伪造客户端数据，对服务器攻击，更重要是防止模拟了客户端，进行支付相关的操作

**4 对称加密与非对称加密的区别**

就个人理解，最主要的就是密钥的不同，对称加密客户端和服务端使用同一个密钥，非对称加密使用不同的密钥。

客户端的代码是很容易被破解的，IDA、hopper disassembler工具的使用，使得破解更加简单而且破解后容易阅读，再配合Charles抓取网络包，根据关键字很容易就定位到加密代码，然后获取密钥。

由于对称加密密钥一样，所以解密就轻而易举；但是非对称加密就不会出现这种问题，因为服务端和客户端的密钥不一样，公钥加密私钥解密，加密的公钥也是公开的，而私钥一般放在服务端，黑客一般是拿不到的。

另外就是没有密钥情况下强制暴力破解，非对称加密也要比对称加密花的多的多的时间来破解。一条信息就要花你几年的时间，所以很安全。

**二、加密与签名区别（RSA）**

* **最大的区别是，加密是可逆的，而签名是不可逆的。**

比如对于"Hello world!"进行加密后得到结果R，还可以使用密钥通过结果R解密得到"Hello world!";而对"Hello world!"进行签名得到结果R，却不能使用密钥通过R获得"Hello world!"，要不然的话压缩算法要逆天了！比如hash，使用几十个字符就能存储几G几T的数据。。。

* **加密是对数据进行机密性保护，签名主要用于身份验证**

比如A对B发送了信息Message；通过加密后，即便C通过网络包截取获得了Message，它也不知道里面的具体内容，只能看到一堆乱码；通过签名，假设D也用相同的加密算法发送了此Message，但是签名错误，那么B通过签名依然拒绝D的Message。

* **以当前使用的比较多的RSA为例举例：**

假设A、B双方均拥有一对公私钥(PUB\_A、PRI\_A、PUB\_B、PRI\_B)。

A向B发送Message的整个签名和加密的过程如下：

1. A先使用HASH对Message生成一个固定长度的信息摘要Message\_hash\_A
2. A使用A的私钥PRI\_A对Message\_hash\_A进行签名得到Message\_sign（这里为什么不直接对Message进行签名，而要对Message\_hash\_A进行签名呢？因为Message的长度可能很长，而Message\_hash\_A的长度则是固定的，这样性能更高，格式也固定，况且hash的结果一般不会出现重复的可能）
3. A接着使用B的公钥PUB\_B对信息Message和信息Message\_sign进行加密得到Message\_RSA，这时A将Message\_RSA发送给B。

当B接收到A的信息Message\_RSA后，获取Message的步骤如下：

1. B用自己的私钥PRI\_B解密得到明文：Message和Message\_sign；
2. 然后B使用A的公钥PUB\_A解Message\_sign得到Message\_hash\_A；同时，B再对Message使用与A相同的HASH得到Message\_hash\_B；
3. 如果Message\_hash\_A与Message\_hash\_B相同，则说明Message没有被篡改过。

上面的过程中，A知道A的公私钥同时也要知道B的公钥；同理B要知道A的公钥和B的公私钥

关于公私钥再打个比方：公钥就像一把锁一样将数据锁住；私钥就像钥匙一样，能将对应的锁打开。

公钥加密，私钥解密的好处是：公钥可以公开，那么无论谁有公钥都可以给你发送信息，而且也只有你才能解密

我们经常使用的Github就是使用了签名的方法，SSH，在本地电脑生成一对公私钥，将公钥传到github，然后使用私钥进行签名，github通过公钥延签后认为你的身份合法。

另外，加密和编码是不一样的，比如ASCII是属于编码，是将0~255与字符一一对应。