公钥、私钥互为一对，可以用来相互加解密，公钥是公开的，允许存在多个副本、多人拥有，私钥只能一人拥有，不能泄露。

公钥:用来加密和验证，由客户端拥有，

私钥：解密和签名，由服务端拥有。

### 公钥加密、私钥解密过程：

由公钥加密的信息文档只能私钥解密，这个过程能够保证信息传输的安全性，即使信息在传输途中被截获，没有秘钥也解不开。

### 私钥签名（加密）、公钥验证（解密）过程：

私钥加密（签名）信息可由对应公钥解密，由于公钥是公开的，任何持有公钥的都能够解密，所以不能保证信息的安全性。但是由于私钥唯一性，如果公钥能够解开信息，就可以确认信息的来源（发送方），这是私钥加密的签名特性。

### 加密和认证

加密是对信息内容的加密，使得非法用户即使取得加密过的资料，也无法获取正确的资料内容，所以数据加密可以保护数据，防止监听攻击。其重点在于数据的安全 性。身份认证是用来判断某个身份的真实性，确认身份后，系统才可以依不同的身份给予不同的权限。其重点在于用户的真实性。两者的侧重点是不同的。

**数字签名**：

签名使用的是私钥，发送方将传输信息使用hash函数生成摘要（digest），摘要就是一串字符串，并且hash过程是不可逆的，摘要经过私钥加密生成"数字签名"（signature）。

**身份验证**：

接收方收到（正文+数字签名）信息后，取出签名信息使用公钥解密，得到摘要1，将正文信息hash后，得到摘要2，比较两者信息，一致代表信息没有被篡改，且信息来源正常。

**数字证书：**

根证书

根证书是CA认证中心给自己颁发的证书,是信任链的起始点。安装根证书意味着对这个CA认证中心的信任。

数字证书则是由证书认证机构（CA）对证书申请者真实身份验证之后，用CA的根证书对申请人的一些基本信息以及申请人的公钥进行签名（相当于加盖发证书机 构的公章）后形成的一个数字文件。CA完成签发证书后，会将证书发布在CA的证书库（目录服务器）中，任何人都可以查询和下载，因此数字证书和公钥一样是 公开的。可以这样说，数字证书就是经过CA认证过的公钥，而私钥一般情况都是由证书持有者在自己本地生成的，由证书持有者自己负责保管。具体使用时，签名操作是发 送方用私钥进行签名，接受方用发送方证书来验证签名；加密操作则是用接受方的证书进行加密，接受方用自己的私钥进行解密。

Client给server发送信息

前提：client 拥有server的公钥

信息通过公钥加密，传给服务器

参考：

<https://www.jianshu.com/p/34bf240b85a9>

<https://www.jianshu.com/p/3c5212b47bec>

<https://blog.csdn.net/GV7lZB0y87u7C/article/details/80878920>