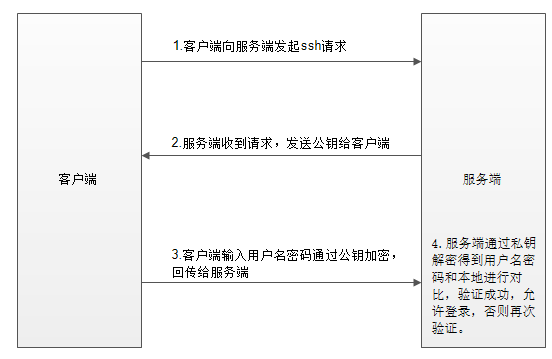
SSH登录方式主要分为两种：

1. 用户名密码验证方式



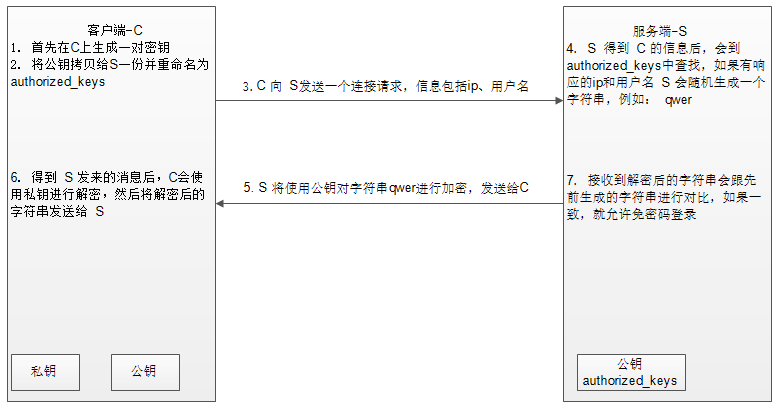
说明：

　　（1） 当客户端发起ssh请求，服务器会把自己的公钥发送给用户；

　　（2） 用户会根据服务器发来的公钥对密码进行加密；

（3） 加密后的信息回传给服务器，服务器用自己的私钥解密，如果密码正确，则用户登录成功。

2. 基于密钥的登录方式



说明：

　　（1） 首先在客户端生成一对密钥（ssh-keygen）；

　　（2） 并将客户端的公钥ssh-copy-id 拷贝到服务端；

　　（3） 当客户端再次发送一个连接请求，包括ip、用户名；

　　（4） 服务端得到客户端的请求后，会到authorized\_keys中查找，如果有响应的IP和用户，就会随机生成一个字符串，例如：qwer；

　　（5） 服务端将使用客户端拷贝过来的公钥进行加密，然后发送给客户端；

　　（6） 得到服务端发来的消息后，客户端会使用私钥进行解密，然后将解密后的字符串发送给服务端；

　　（7） 服务端接受到客户端发来的字符串后，跟之前的字符串进行对比，如果一致，就允许免密码登录。

3.

默认情况下，用户的 SSH 密钥存储在其 ~/.ssh 目录下。 进入该目录并列出其中内容，你便可以快速确认自己是否已拥有密钥：

我们需要寻找一对以 id\_dsa 或 id\_rsa 命名的文件，其中一个带有 .pub 扩展名。 .pub 文件是你的公钥，另一个则是私钥。 如果找不到这样的文件（或者根本没有 .ssh 目录），你可以通过运行 ssh-keygen 程序来创建它们。在 Linux/Mac 系统中，ssh-keygen 随 SSH 软件包提供；

4.

生成私钥的时候提示出入密码，这个密码是私钥的保护密码，用于使用私钥的时候需要提供的密码。作用是防止私钥被盗例如其他人使用了你的电脑，或者是盗取了你的密钥。因为远程连接的时候使用了私钥，所以要提示输入保护密码才可能使用。如果我们私钥保护密码留空，那么远程登录的时候都不需要输入密码。