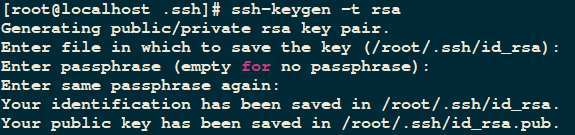
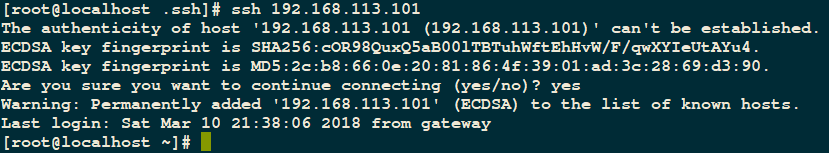
**Ssh公钥认证**

1. **ssh认证过程与原理**
   1. **基本概念**明文 需要传送的消息  
      密文 明文经过加密后的消息  
      加密 明文变为密文的过程  
      解密 从密文恢复出明文的过程  
      对称加密 加密和解密使用同一密钥的加密方法  
      非对称加密 加密和解密使用不同密钥的加密方法
   2. **认证过程**
      1. 版本号协商
      2. 密钥和算法协商  
         服务端和客户端分别发送算法协商报文给对方，报文中包含自己支持的公钥算法列表、加密算法列表、消息验证码算法列表、压缩算法列表等  
         服务端和客户端根据对方和自己支持的算法得出最终使用的算法  
         服务端和客户端利用DH交换算法、主机密钥对等参数，生成会话密钥和会话ID  
         版本号协商完成后，服务端发送公钥到客户端，服务端生成会话id发送给客户端，客户端生成会话密钥，设为key，并使res= id 异或 key,客户端使用服务端公钥加密res，发送给服务端，服务端解密res，用res异或id得到key，会话密钥协商完毕
      3. 认证
         1. 密码  
            客户端发送会话密钥加密过的账户，口令，认证方法，服务端使用相同的会话密钥解密口令账户，认证进行
         2. 密钥  
            客户端发送会话密钥加密后的账户，认证方法，公钥，服务端解密数据得到公钥，比对信任公钥列表，如果未找到认证失败，如果找到，服务端生成随机字符串“质询”，并使用该公钥加密质询，使用会话密钥加密后发送给客户端，客户端解密得到质询，再将其使用会话密钥加密发送给服务端，如果和之前服务端发送的质询相同，则认证通过
2. **开启服务器认证选项**编辑/etc/ssh/sshd\_config文件，开启公钥认证选项  
     
   重启sshd服务  
   
3. **生成客户端公钥**使用ssh-keygen生成密钥对  
   
4. **添加客户端公钥到服务器信任列表**将公钥内容发送至服务器，添加进文件~/.ssh/authorized\_keys中
   1. 拷贝文件  
      
   2. 添加进信任列表  
      
   3. 更改文件权限  
      
5. **免密码登陆服务器**
6. **为登陆方便可以将服务器信息添加进/etc/ssh/ssh\_config**