目录

[服务器基础入门 1](#_Toc477185558)

[基本名词 1](#_Toc477185559)

# 服务器安全

## SSH

数字签名：<http://www.ruanyifeng.com/blog/2011/08/what_is_a_digital_signature.html>

### 密钥（私钥）

1.用私钥来解密接收到的公钥信息

2.发送信息时，用私钥来加密(hash digiset->signature)

### 公钥

1. 用公钥来加密
2. 收到信息后，用公钥来解密

### 操作命令

#### 生成密钥、公钥

ssh-keygen

#### 远程登录

ssh -p 22 [root@192.168.72.130](mailto:root@192.168.72.130)

其过程会要求yes确认及输入远程账号的密码，如果想不输入密码

则要将公钥追加到远程机器上的authorized\_keys里，如果远程机没有authorized\_keys文件则要先创建

退出用exit