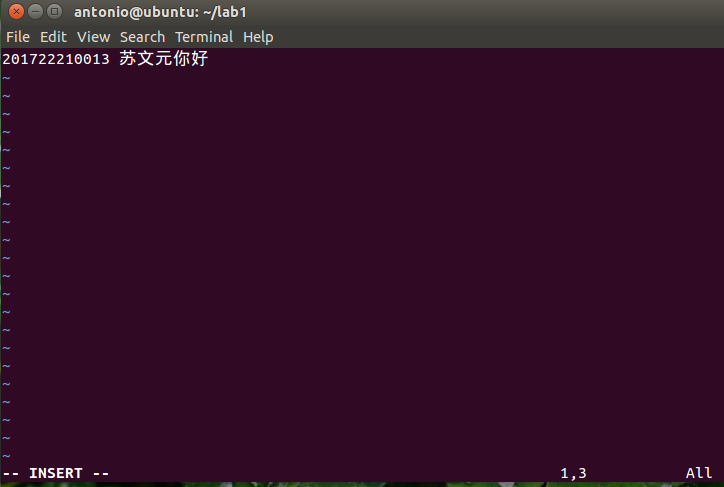
**1. RSA**加密与解密

1) 创建明文*plaintext.txt*，内容为自己的学号+任意一段话。



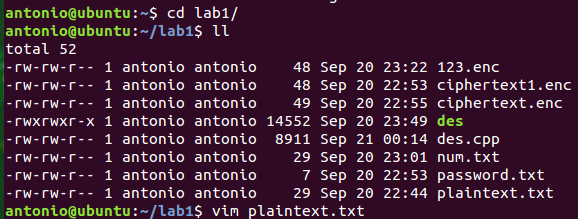
2) 创建密钥。

查阅OpenSSL命令的使用方法，创建1024bit的公钥--私钥对，并从密钥对中提取出公钥和私钥。私钥命名为*private.pem*，公钥命名为*public.pem*。

提示：

1. 创建1024bit的公钥-私钥对：

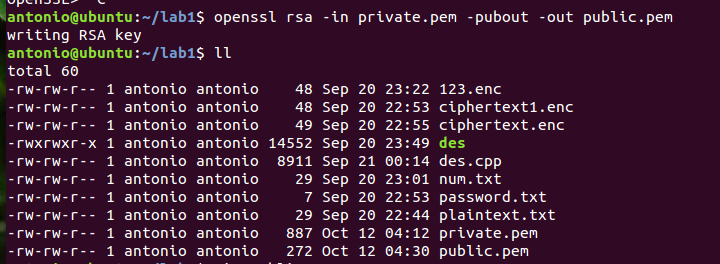
*openssl genrsa -out private.pem 1024*



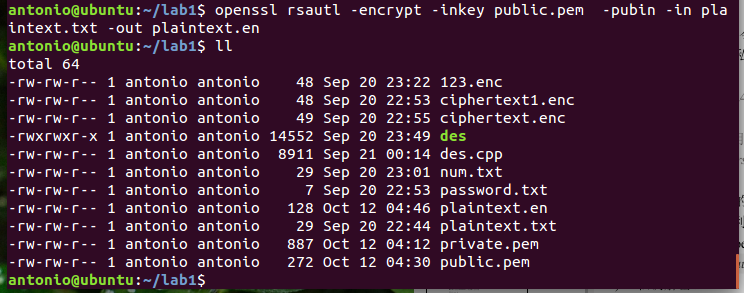


1. 提取密钥对中的公钥：

*openssl rsa -in private.pem -out public.pem* –*pubout*

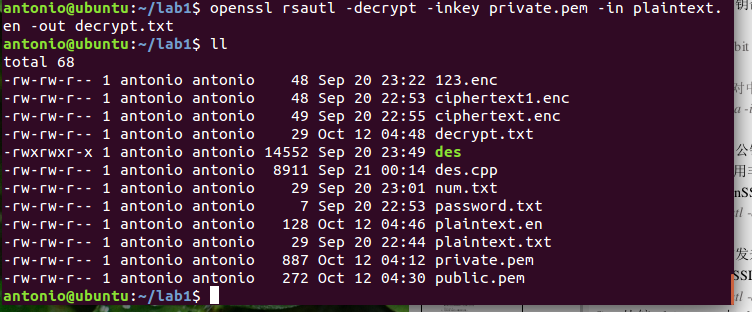


3) 公钥加密。



提示：*openssl rsautl -encrypt –inkey*公钥*-pubin -in* 明文–*out*密文

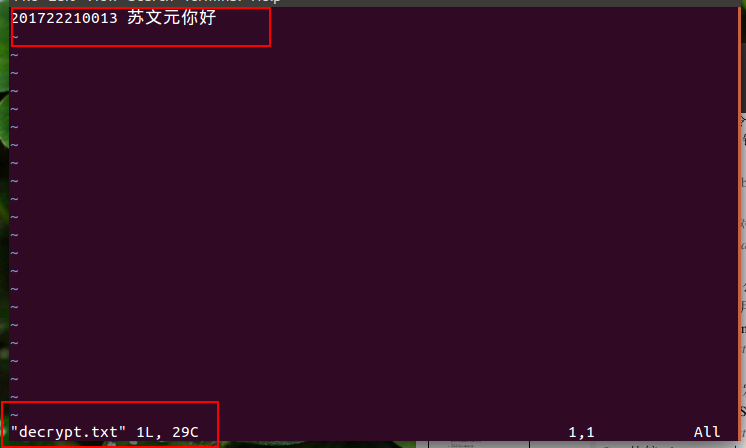
4) 私钥解密。

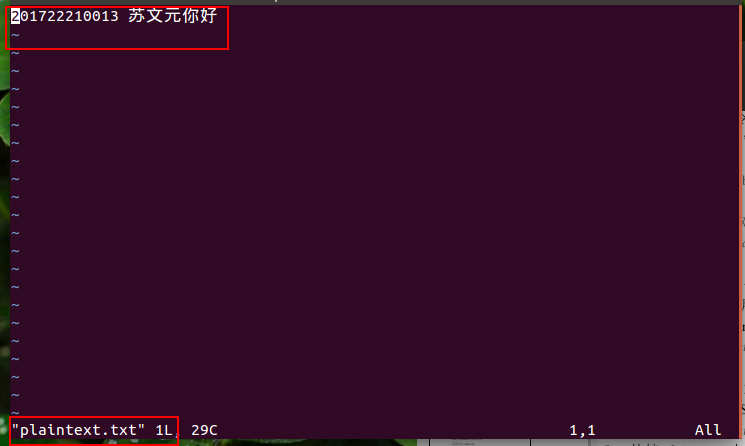


假设你已收到对方发来的加密文件，想利用手中的私钥对文件做解密。现在模拟解密过程。查阅OpenSSL命令的使用方法，对密文做解密，解密后的文件为*decrypt.txt*。

提示：*openssl rsautl -decrypt -inkey* 私钥*-in* 密文*–out*解密后的文件

5) 比较*plaintext.txt*与*decrypt.txt*两个文件之间的差异。

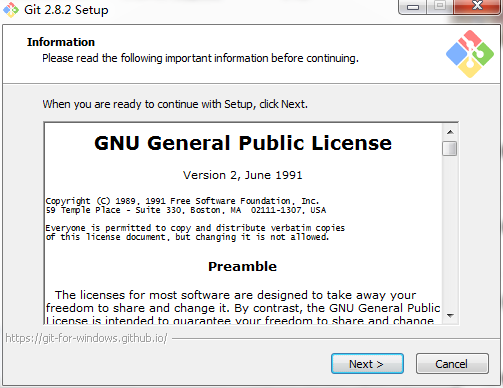


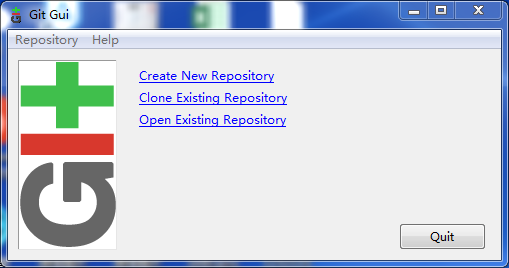


准备工作

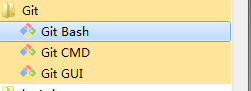
1) 安装Git Bash。

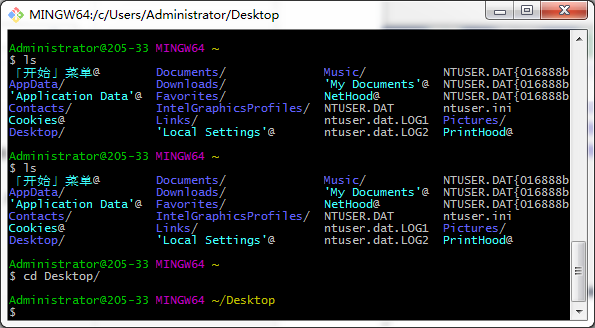
GitBash是Windows下的命令行工具，允许Windows运行一些常用的Linux指令。打开Windows虚拟机的IE浏览器，进入git官方网站，下载与Windows虚拟机位数相对应的git安装包，进行安装。安装时全部选择默认选项即可。





2) 学习使用Git Bash。

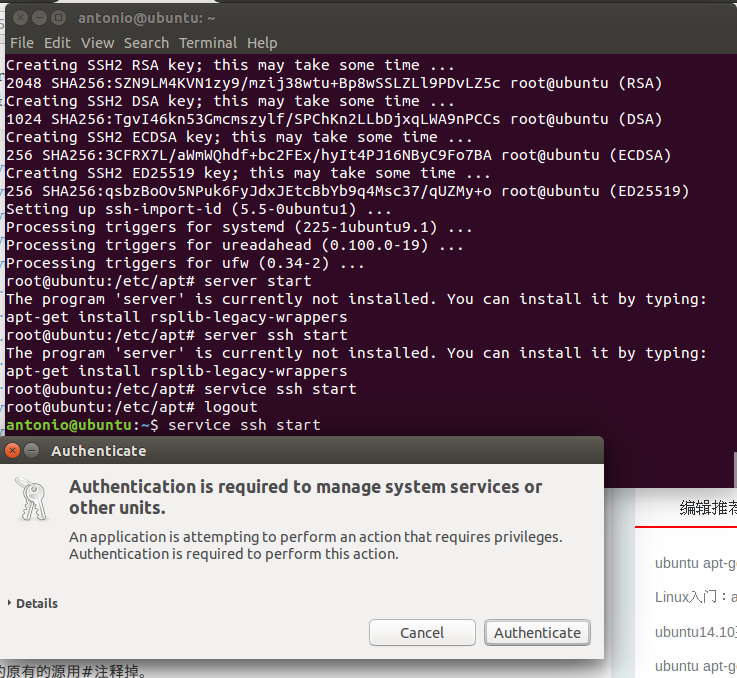




在Windows虚拟机的桌面右键，选择Git Bash Here，打开Git Bash终端。执行一些常用的Linux命令，体会Git Bash的作用。

3) 安装openssh-server。

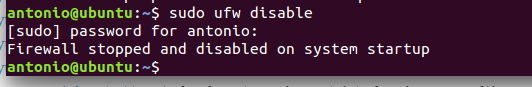
Ubuntu 16.04默认安装了ssh client，但是没有安装ssh server，因此还不能用作SSH服务器。请使用apt-get命令，安装*openssh-server*。安装了SSH服务后，该如何启动/停止/重启ssh服务？如何查询ssh服务的状态？



提示：*service ssh start|stop|restart|status*

4) 关闭防火墙。

Ubuntu16.04默认没有开放22端口，因此客户端发起的SSH连接请求会被防火墙屏蔽。查阅Linux命令手册，关闭防火墙。重启Linux虚拟机。



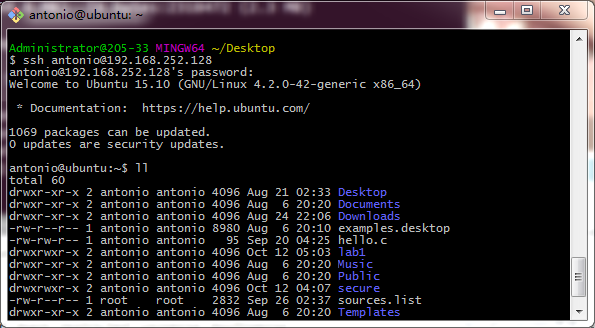
提示：*sudo ufw disable*

**3. SSH**远程登陆

1) 明确客服端、服务器概念。

本实验将Linux虚拟机作为服务器（Server），将Windows虚拟机作为客户端（Client）。假设服务器位于远端，如机房或云端，用户无法对服务器做实际的物理操作。假设客户端为用户的办公电脑。SSH协议允许用户通过客户端，远程登陆到服务器，完成服务器上的各项操作。

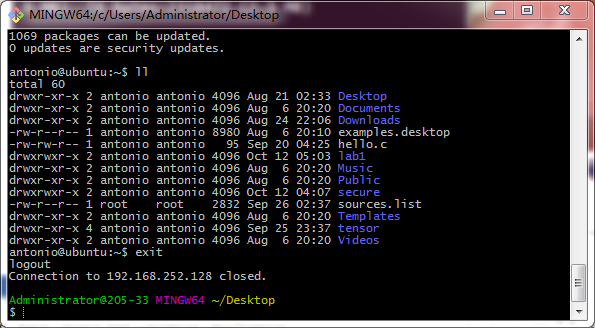
2) SSH远程登陆。



在客户端上完成：客户端（Windows虚拟机）使用ssh命令，远程登陆到服务器（Linux虚拟机）。登录过程是否需要Linux的用户密码？

提示：*ssh LinuxUserName@LinuxIP*

3) 如果客户端已经登陆到了服务器，该如何退出登录？

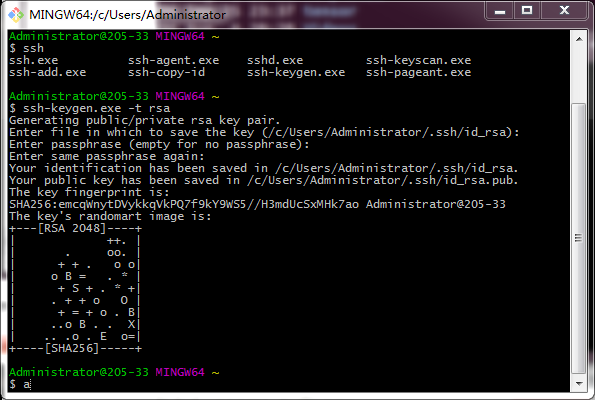


提示：*exit*

**4. RSA**应用：**SSH**认证

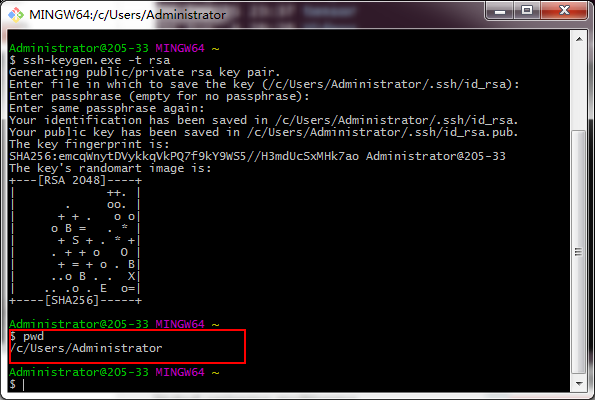
1) 客户端生成RSA密钥。

在客户端上完成：创建2048bit的RSA密钥。



提示：*ssh-keygen.exe* –*t rsa*

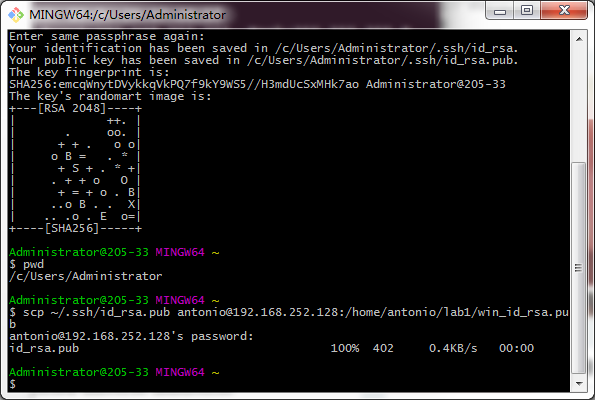
2) 上一步生成的公钥保存于*~/.ssh/id\_rsa.pub*，私钥保存于*~/.ssh/id\_rsa*。这里的~在GitBash中表示Windows下的哪个文件夹？

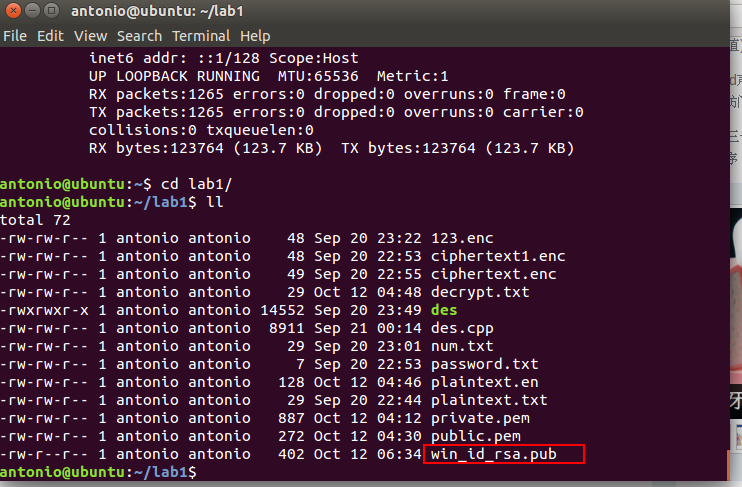


提示：*pwd*

3) 复制客户端的公钥到服务器上。

VMware Workstation自带的VMware Tools，允许用户直接通过拖拽文件的方式，在宿主机操作系统与虚拟机操作系统之间方便地传输文件。尽管可以将Windows虚拟机的公钥文件*id\_rsa.pub*先拖拽到宿主机，再拖拽到Linux虚拟机上，实现文件复制，但并不推荐这么做。更专业的做法是使用scp命令。在客户端上完成：将客户端的公钥*id\_rsa.pub*复制到服务器的用户根目录下，并命名为*win\_id\_rsa.pub*。

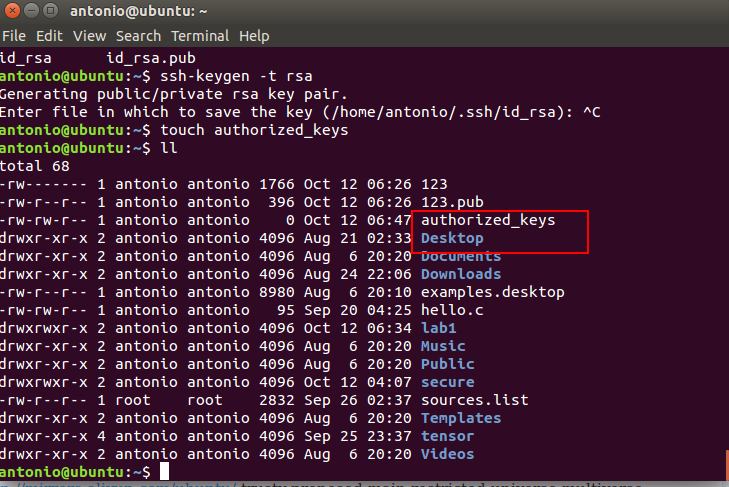


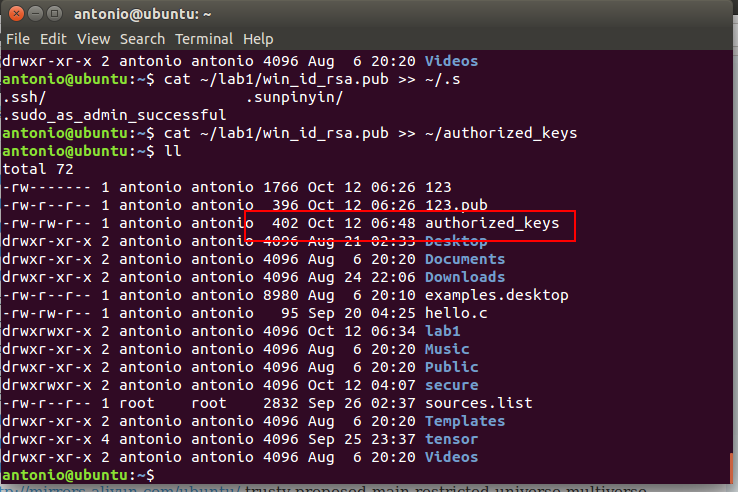


提示：*scp ~/.ssh/id\_rsa.pub LinuxUserName@LinuxIP:/home/LinuxUserName/win\_id\_rsa.pub*

4) 追加客户端的公钥到服务器的配置文件。

在服务器上完成：将客户端公钥*win\_id\_rsa.pub*，追加到服务器的配置文件

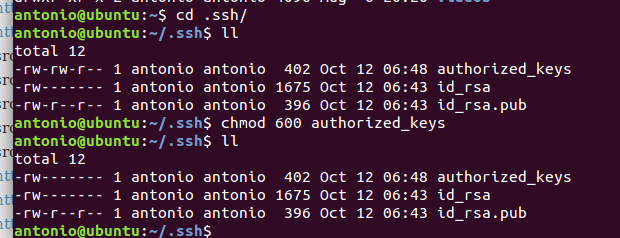




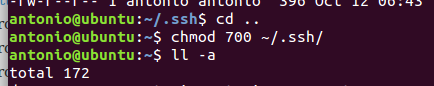
*~/.ssh/authorized\_keys*中。

提示：*cat ~/win\_id\_rsa.pub >> ~/.ssh/authorized\_keys*

5) 修改权限。

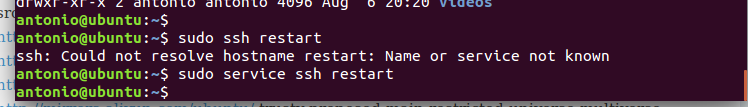


在服务器上完成：将*~/.ssh/authorized\_keys*权限改为600，将*~/.ssh/*权限改为700。Cd



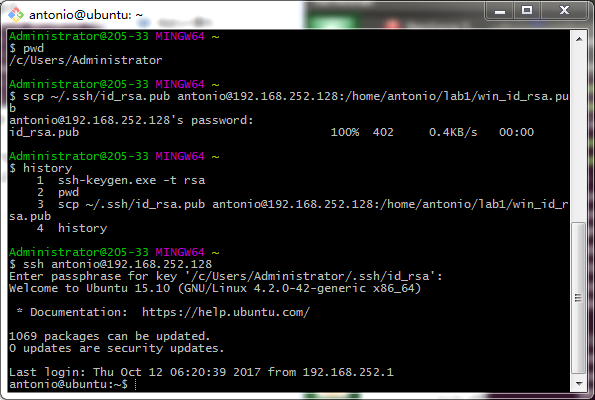
提示：*chmod*

6) 重启服务器的SSH服务。



7) 基于公钥的SSH登录。

在客户端上完成：客户端使用ssh命令，远程登陆到服务器。登录过程是否需要Linux的用户密码？非对称加密在SSH认证中起到了怎样的作用？



不用添加密码