# 使用OpenSSL进行加密操作

1. 实验原理

OpenSSL是一个支持SSL认证的服务器．它是一个源码开放的自由软件，支持多种操作系统。OpenSSL软件的目的是实现一个完整的、健壮的、商业级的开放源码工具，通过强大的加密算法来实现建立在传输层之上的安全性。OpenSSL包含一套SSL协议的完整接口，应用程序应用它们可以很方便的建立起安全套接层，进而能够通过网络进行安全的数据传输。

OpenSSL包含一个命令行工具用来完成OpenSSL库中的所有功能，支持强大的密码库。本次实验使用OpenSSL进行加解密操作

1. 实验环境

开启Linux虚拟机，运行 OpenSSL。

1. 实验步骤
2. 打开计算机，开机是选择Windows系统进入
3. 进入系统后，点击VMWare虚拟机，

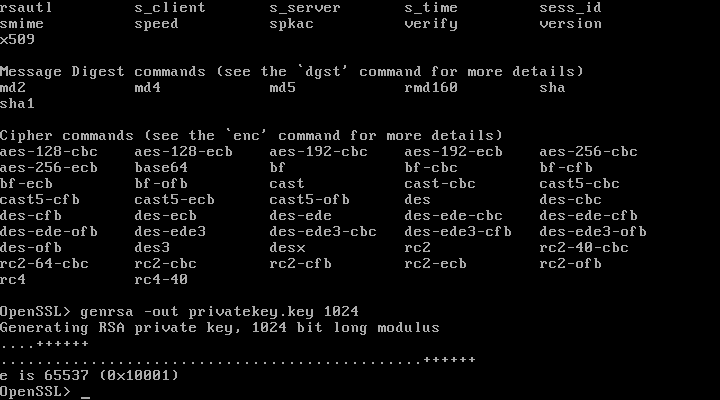


1. 在VMWare里面，选择 “Ubuntu” （或其他Linux版本）启动Linux虚拟机
2. 启动Linux后，即可运行“openssl”命令。如果是图形视窗界面，需要打开一个终端（terminal）操作
3. 可以打开另一个文档“openssl commands”，依次对照文档里面的命令，进行各类加密操作。例如

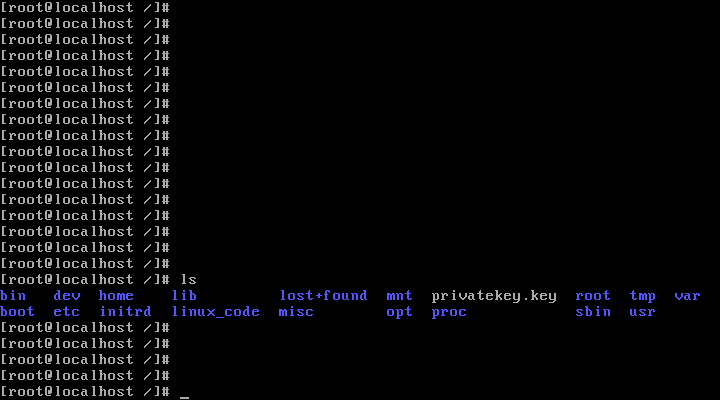
openssl ? \\显示所有命令

openssl genrsa –out privatekey.key 1024

\\生成1024位RSA的私钥，输出到privatekey.key文件

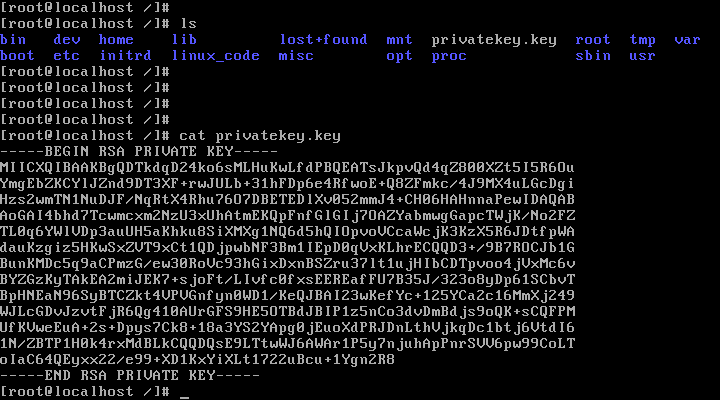


默认输出到主目录下，使用ls可以查看



在linux下使用cat命令查看生成的私钥：cat privatekey.key

cat命令是linux下的一个文本输出命令,通常是用于观看某个文件的内容



1. 实验内容

熟悉操作后，完成下面实验内容并记录到实验报告

1. 使用AES加密算法对文本加密，对不同参数加密后的密文进行截图、比较 （1）使用base64编码和不使用base64编码

（2）使用CBC模式和使用ECB模式

2．自己编辑一个文本（文本需要长一些，可参考文件“lincoln.txt”），使用AES-CBC base64编码加密后得到密文（例如“lincoln.enc”），打开密文文件(例如“lincoln.enc”)分别修改密文最开始1个字符、中间1个字符、最后1个字符，再进行解密。分别看看三次解密会有什么问题，体会CBC和ECB工作模式的区别，截图比较。（如果虚拟机VMWare版本较低，没有按照虚拟机相关工具，则不支持从宿主机复制文件进入虚拟机，可以用linux下的vi编辑器自行录入一段文字，输入尽量多一些，3行以上，每行3个单词以上）

3．生成1024位的RSA私钥和公钥，粘贴到实验报告。思考为什么私钥会比公钥长？

4．以自己的学号建立文本文件（可以使用vi编辑器），内容任意，如“B16040740.txt”,使用刚才生成的私钥对“B16040740.txt”进行签名，再使用公钥验证，如果验证正确，将显示“Verified ok”。将签名信息和验证结果截图保存到实验报告。（截图需要能看清学号信息，可以适当放大，用红框、红线标识，不得使用他人学号文件进行操作，否则按抄袭处理）

5．完成openssl\_commands.doc其他剩余所有操作

注：VMWare的截图快捷键是 Ctrl+Alt+PrtScn

Linux下文本编辑可以用vi编辑器，命令可以参考附件

注意用-out 默认生成的密钥、密文等文件在 \locolhost目录下，可以用cd命令进入

1. 提交的实验报告

完成实验内容，在实验报告里面保存截图记录，并思考相关问题，统一由各班学习委员收齐实验报告（每位同学的实验报告文件名：学号-姓名-实验1.docx）后压缩打包通过QQ发给吴礼发老师。