实验一：私有CA证书签发的简单实现

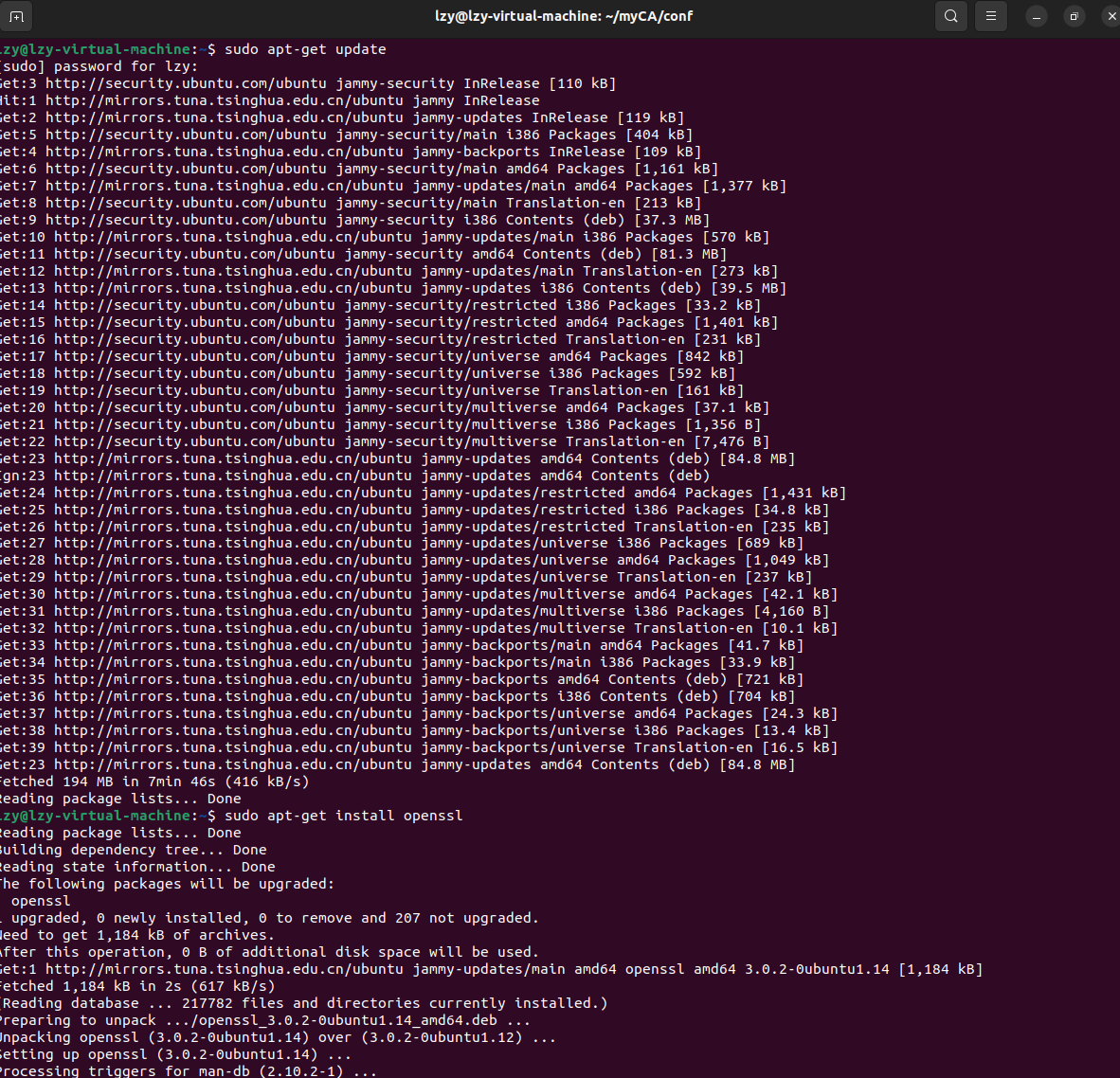
专业：密码科学与技术 姓名：柳致远 学号：2113683

实验过程：

1. 搭建私有CA
2. 安装OpenSSL：

**sudo apt-get update**

**sudo apt-get install openssl**



1. 创建私有CA所需要的文件目录，保存CA的相关信息

相关指令如下：

mkdir myCA //创建CA根文件夹

cd myCA //进入CA根文件夹

mkdir newcerts private conf //创建三个文件夹，用来存放新发放证书、私钥和配置文件

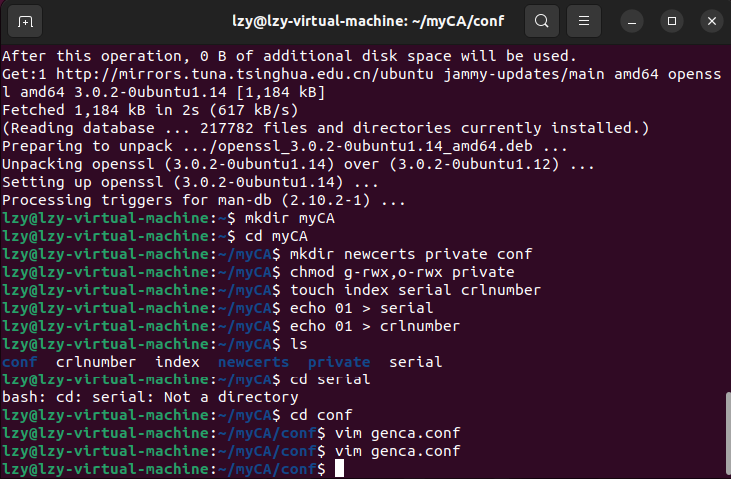
chmod g-rwx,o-rwx private //设置private文件夹的操作权限

touch index serial crlnumber //创建证书信息数据库、证书序号文件、crl序号文件

echo 01 > serial //初始化证书的序号

echo 01 > crlnumber //初始化吊销证书序号

实验过程截图：



1. 创建生成CA自签名证书的配置文件

相关指令如下：

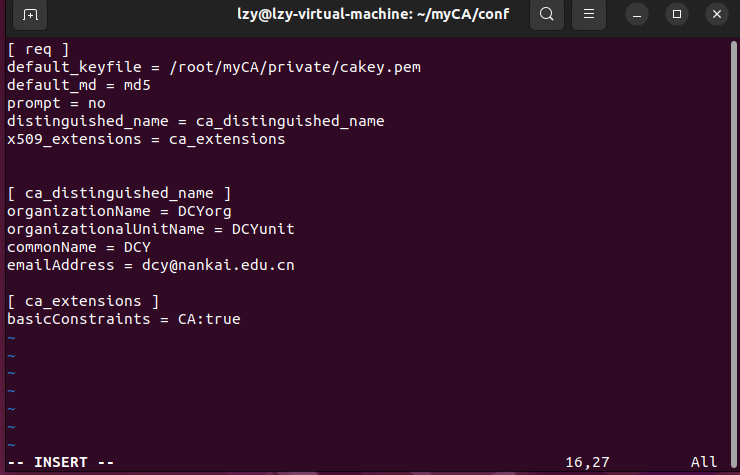
cd conf

//进入配置文件夹

vim genca.conf

//创建用来生成自签名证书的配置文件

配置文件配置如下：



1. 生成私有CA的私钥和自签名证书（根证书）

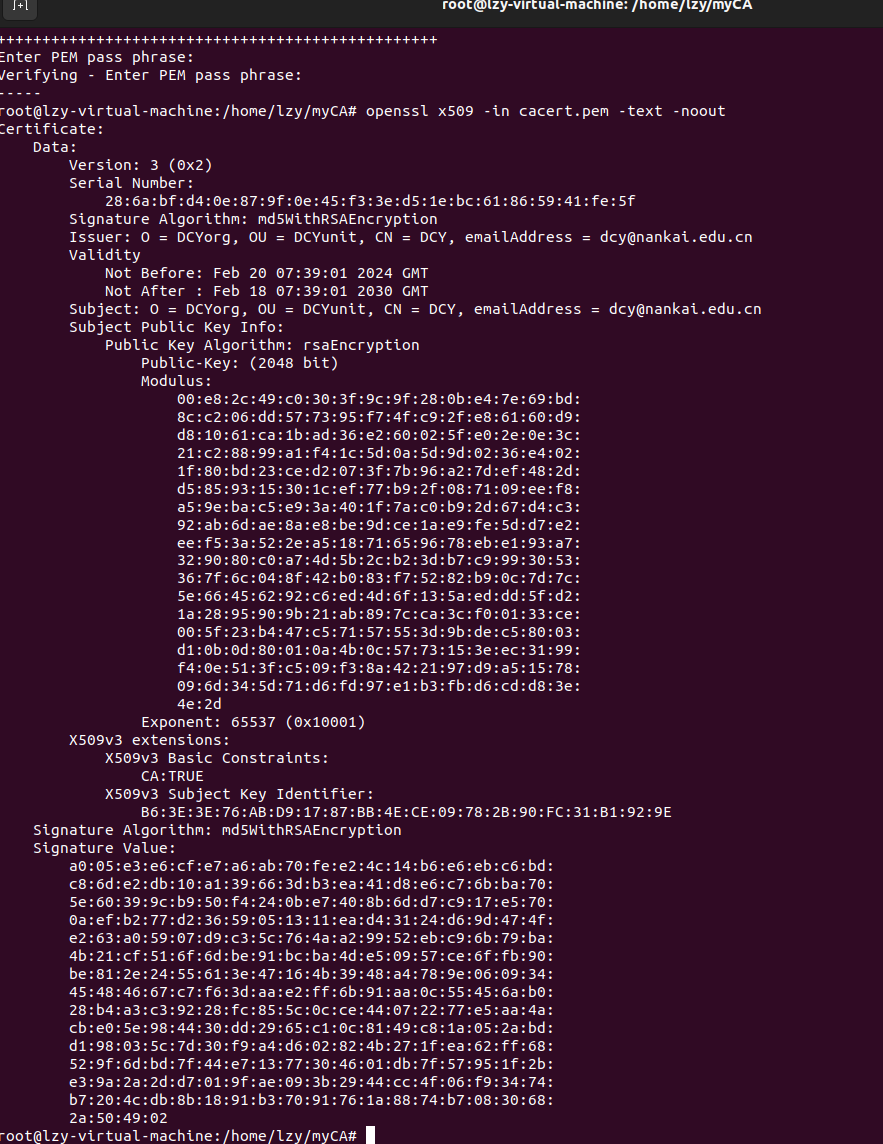
指令如下：

openssl req -x509 -newkey rsa:2048 -out cacert.pem -outform PEM -days 2190 -config /root/myCA/conf/genca.conf

//回到myCA根目录下，生成x509自签名证书，过程中需要输入CA私钥的保护密码，请牢记。

//CA会按照gentestca.conf文件中配置的规则自签名生成证书

CA自签名证书截图如下：



1. 私有CA为服务器签发证书
2. 创建用来为其他请求签发证书的配置文件

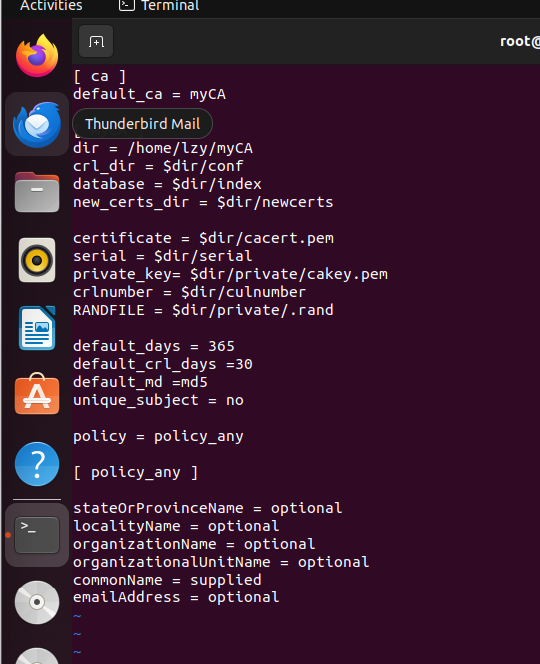
cd conf

//再次进入配置文件夹

vim ca.conf

//创建用来为其他请求签发证书的配置文件

配置文件配置如下：



1. 模拟服务器，生成私钥与证书申请的请求文件

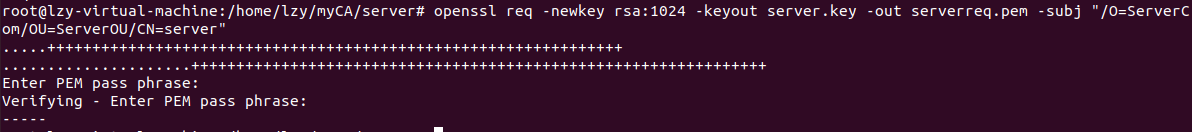
mudar server

//在任意路径下创建服务器文件夹server

openssl req -newkey rsa:1024 -keyout server.key -out serverreq.pem -subj “/O=ServerCom/OU=ServerOU/CN=server”

//生成server的1024位私钥server.key和证书申请的请求文件serverre.pem，此时需要设置服务器的私钥保护密码，请牢记

结果截图如下：



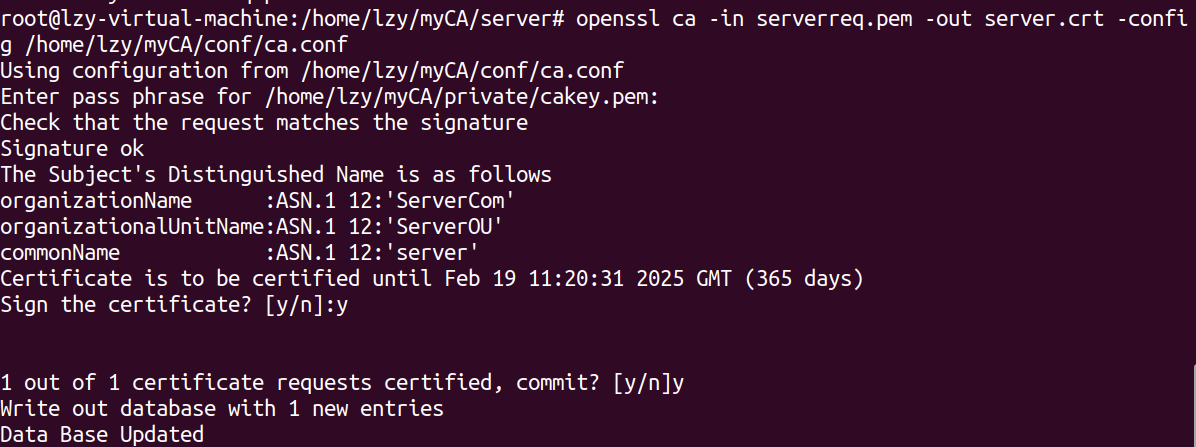
1. CA根据服务器的证书请求文件生成证书并将其返回给服务器

openssl ca -in serverreq.pem -out server.crt -config /root/myCA/conf/ca.conf

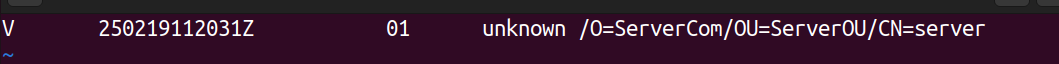
//向私有CA提交证书请求文件serverreq.pem，CA生成并返回证书server.crt

//生成证书的规则是参照之前为CA定义的ca.conf配置文件执行的

实验过程截图如下：



1. 在myCA下的index（证书信息数据库）中可以看到证书信息数据库的更新数据



以及，在newcerts目录下可以看到CA发放给服务器的证书文件备份。



1. 私有CA为客户端签发证书

1、即仿照为服务端签发证书的过程为客户端签发证书即可

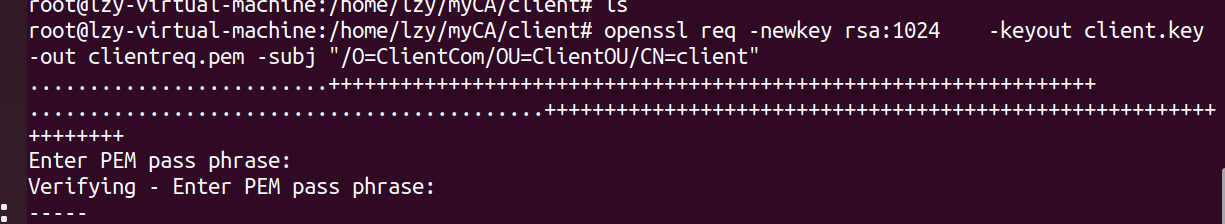
首先在myCA目录下创建文件夹client：

mkdir client

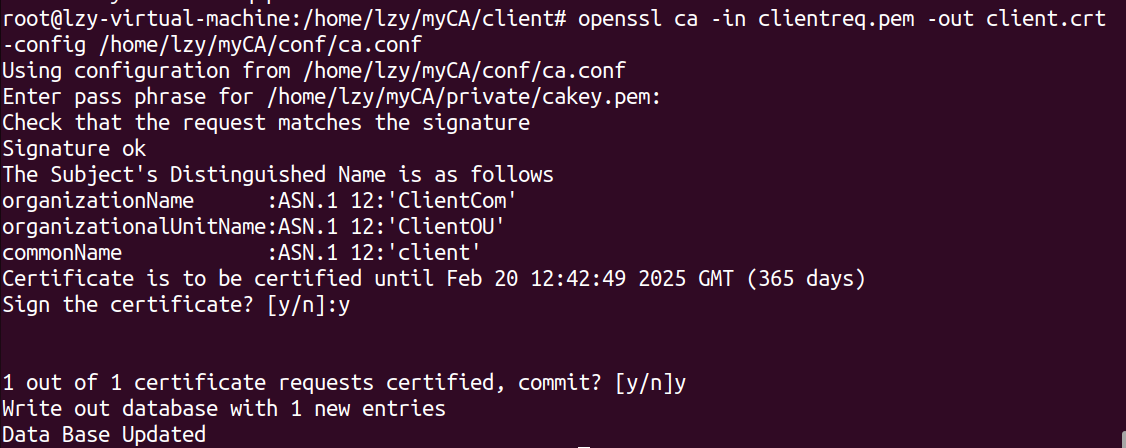
接着生成client的1024位私钥client.key和证书申请的请求文件client.pem，此时需要设置服务器的私钥保护密码，代码修改如下：

openssl req -newkey rsa:1024 -keyout client.key -out clientreq.pem -subj "/O=ClientCom/OU=ClientOU/CN=client"

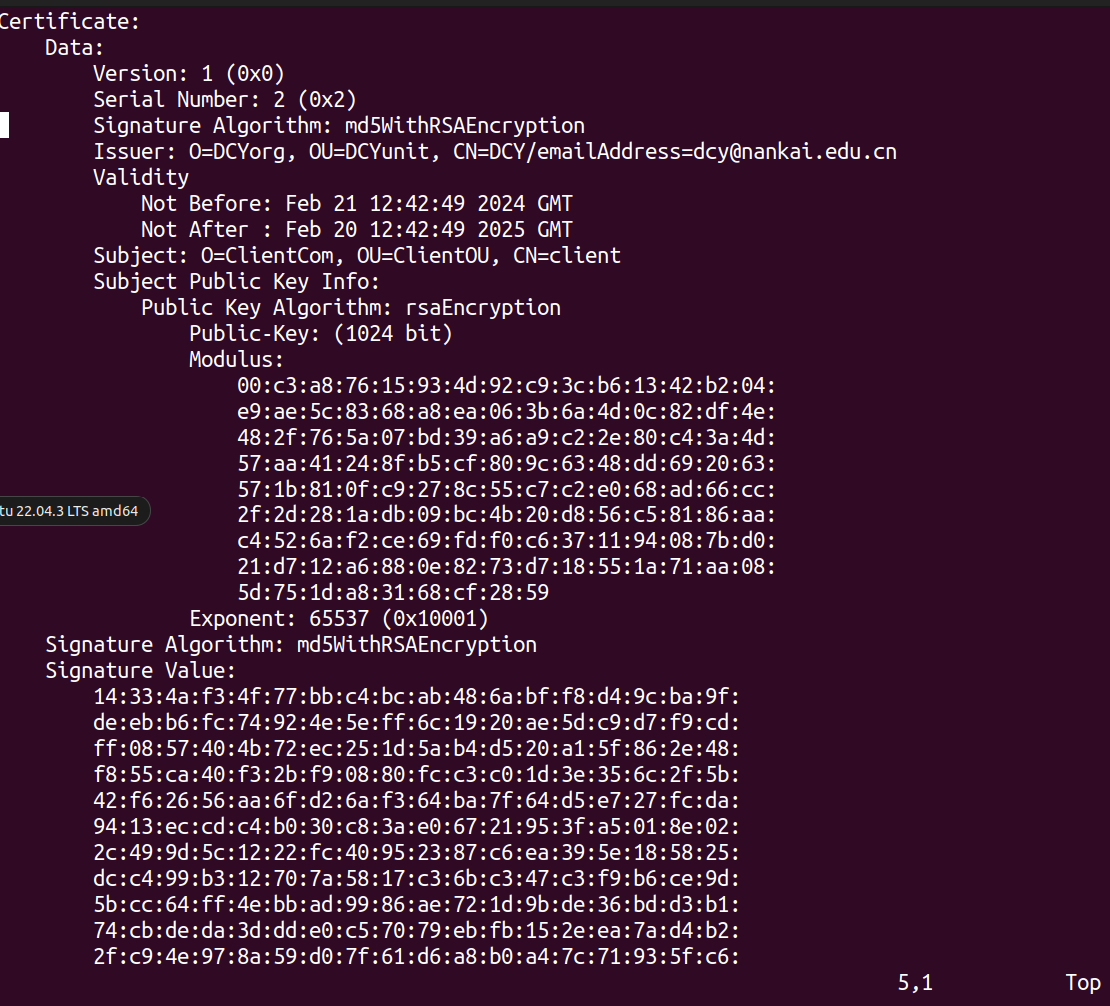
实验过程截图如下：



2、同样使用之前的配置文件ca.conf为客户端生成并返回证书client.crt



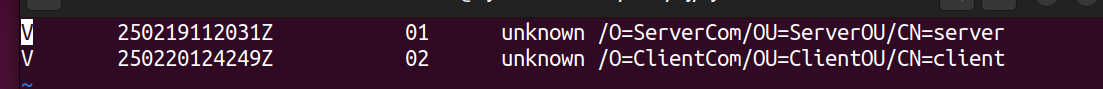
查看证书client.crt



在newcerts文件夹内保存了该证书的备份



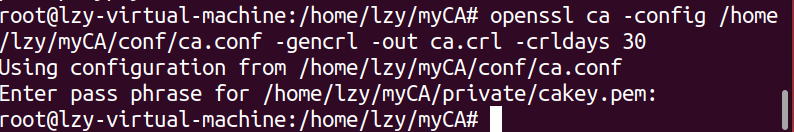
并在myCA下的index（证书信息数据库）中可以看到证书信息数据库的更新数据



1. CA吊销用户证书
2. 在之前的配置文件ca.conf的基础上生成证书吊销列表ca.crl：

openssl ca -config /home/lzy/myCA/conf/ca.conf -gencrl -out ca.crl -crldays 30

实验结果截图如下：

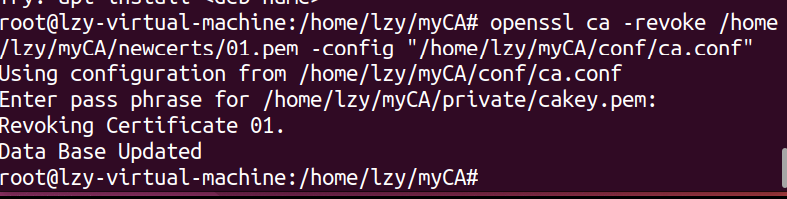


1. 吊销01证书，使用命令

openssl ca -revoke /home/lzy/myCA/newcerts/01.pem

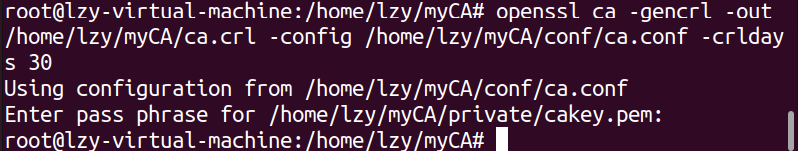
-config "/home/lzy/myCA/conf/ca.conf" 进行吊销

实验结果截图如下：



1. 、使用命令 openssl ca -gencrl -out /home/lzy/myCA/ca.crl -config /home/lzy/myCA/conf/ca.conf -crldays 30 更新证书吊销列表

实验过程截图如下



使用命令 openssl crl -in ca.crl -noout -text 可以查看 crl 文件

