《信息安全引论》第二次课程实验报告

- 姓名：
- 学号：
- 日期：

实验: 公钥加密与 PKI 实验

实验内容

本实验包含公钥加密，数字签名，公钥认证，认证授权，基于 PKI 授权等内容。实验内容为建立基于 PKI 的安全信道。

实验环境

蓝桥云课/ Ubuntu。本部分需要配置较多环境，建议使用蓝桥云课的在线平台。

具体内容

请详见蓝桥云课课程：https://www.lanqiao.cn/courses/243

本实验涉及上述链接课程的三个部分（3.1-3.3）：

1. 成为数字证书认证机构（CA）
2. 为 PKILabServer.com 生成证书
3. 在网站中使用 PKI

点击左侧步骤后将有具体提示，根据提示在蓝桥云课云端环境中完成实验。具体步骤请在如图所示位置查看（以 第一步-成为数字证书认证机构 为例）：

3.1 成为数字证书认证机构（CA）

> 数字证书认证机构（英语：Certificate Authority，缩写为 CA），也称为电子商务认证中心、电子商务认证授权机构，是负责发放和管理数字证书的权威机构，并作为电子商务交易中受信任的第三方，承担公钥体系中公钥的合法性检验的责任。

> 数字证书的作用是证明证书中列出的用户合法拥有证书中列出的公开密钥。CA 机构的数字签名使得攻击者不能伪造和篡改证书。它负责产生、分配并管理所有参与网上交易的个体所需的数字证书，因此是安全电子交易的核心环节。

想要从商业 CA 获取数字证书需要向其支付一定的金钱，不过我们不用那么破费，可以自己成为 root CA，为自己发布证书。

在本实验中，我们将成为 root CA，并为该 CA 生成证书。不像其他 CA 需要被另外的 CA 认证， root CA 的证书是自己为自己认证的，一般 Root CA 的证书都已事先加载在大多数操作系统，浏览器或者依赖 PKI 的软件之中了。Root CA 的证书是被无条件信任的。

配置文件：openssl.conf

为了使用 openssl 生成证书，我们首先需要进行配置，配置文件扩展名为.cnf。openssl 的 ca， req， x509 命令常常会用到这份配置文件。你可以从 `/usr/lib/ssl/openssl.cnf` 获得一份拷贝。将文件拷贝到工作目录后，创建以下在配置文件中指定的子文件夹（详情查看配置文件[CA default]处）

首先我们新建一个工作目录：

```
$ cd /home/shiyanlou
$ mkdir openssl
$ cd openssl
```

需要的文件夹和文件配置在 `openssl.cnf` 中都能找到：

```
dir = ./demoCA # Where everything is kept
certs = $dir/certs # Where the issued certs are kept
crl_dir = $dir/crl # Where the issued crl are kept
new_certs_dir = $dir/newcerts # default place for new certs.
database = $dir/index.txt # database index file.
serial = $dir/serial # The current serial number
```

`openssl.cnf` 中相关配置截图：

```
39 ####################################################################
40 [ CA_default ]
41
42 dir             = ./demoCA              # Where everything is kept
43 certs           = $dir/certs            # Where the issued certs are kept
44 crl_dir         = $dir/crl              # Where the issued crl are kept
45 database        = $dir/index.txt        # database index file.
46 #unique_subject = no                    # Set to 'no' to allow creation of
47                                          # several ctificates with same subject.
48 new_certs_dir   = $dir/newcerts         # default place for new certs.
49
50 certificate     = $dir/cacert.pem       # The CA certificate
51 serial          = $dir/serial           # The current serial number
52 crlnumber       = $dir/crlnumber        # the current crl number
53                                          # must be commented out to leave a V1 CRL
```

实验要求

- 按照操作指导，完成步骤 1-3 中的操作。
- 在实验报告中简述本实验完整流程，并附上关键步骤的运行结果截图。