证书生成及应用实验

北京联合大学智慧城市学院《现代密码学课程》
2020-5-14

1、工具

OpenSSL

2、提供的信息

我们事先利用OpenSSL生成了Buu的CA私钥和证书，私钥在实际使用中需要严格保密。

Buu的CA证书buucacert.cer，已发布在QQ群文件夹“证书发布目录”。

Buu的私钥文件buucakey.pem，我们通过微信群发给大家，我们暂且认为这是个“安全信道”。

指导老师的证书lxf.cer，也已发布在QQ群文件夹“证书发布目录”。

3、任务

首先将你作为CA的工作人员，为你生成一个私钥和证书，并且将证书发布在QQ群文件夹“证书发布目录”中，证书文件用自己的名字命名（汉语）。并且生成你自己公私钥信息的PKCS#12文件，在实验中使用。

利用支持公钥签名和加密的email客户端（例如：Thunderbird），给指导老师发布一个签名邮件和加密邮件。指导老师邮箱：xxtxiaofeng@buu.edu.cn，在下面的说明中表示发邮件者自己的中文姓名。

3.1签名邮件格式要求

邮件主题：签名邮件(***)

邮件正文：

```
这是我的第一封签名邮件，真的是我发的。

***
```

3.2加密邮件格式要求

邮件主题：加密邮件(***)

邮件正文：

```
这是我的第一封加密邮件，你看到了吗？

***
```