

**实 验 报 告**

**实验3-数字证书及其应用**

**（安全协议）**

|  |  |
| --- | --- |
| **课程名称：** | **信息系统安全** |
| **学生姓名：** | **唐子齐** |
| **学生学号：** | **201430620169** |
| **学生专业：** | **软件工程** |
| **开课学期：** | **2016-2017 第二学期** |

**XXXX单位**

**2016年5月**

**实验3-数字证书及其应用**

**（安全协议）**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **地 点：** | B7 楼 | 133 房； | **实验台号：** |  |
| **实验日期与时间：** | 2017年3月21号 | | **评 分：** |  |
| **预习检查纪录：** | 良好 | | **实验教师：** | 陈春华 |

# 实验过程与结果

1. **实验目的**

1）学习了解数字证书、公钥基础设施（Public Key Infrastructure、PKI）技术和基于数字证书的认证技术原理。

2）学习数字证书的一些典型应用，如安全电子邮件，掌握其原理和分析其安全性。

1. **实验原理**
2. **PKI技术与原理**

PKI是由公钥密码技术、数字证书、证书认证中心和关于公开密钥的安全策略等基本成分共同组成，管理密钥和证书的系统或平台。一个完整的PKI系统必须具备CA、数字证书库、密钥备份及恢复系统、证书作废系统和API等基本组成部分。

（以下详细信息来自wiki）

a. 权威认证机构：权威认证机构简称CA，是PKI的核心组成部分，也称作认证中心。它是数字证书的签发机构。CA是PKI的核心，是PKI应用中权威的、可信任的、公正的第三方机构。

b.数字证书库：在使用公钥体制的网络环境中，必须向公钥的使用者证明公钥的真实合法性。因此，在公钥体制环境中，必须有一个可信的机构来对任何一个主体的公钥进行公证，证明主体的身份以及它与公钥的匹配关系。目前较好的解决方案是引进证书(Certificate)机制。（1）证书。证书是公开密钥体制的一种密钥管理媒介。它是一种权威性的电子文档，形同网络环境中的一种身份证，用于证明某一主体的身份以及其公开密钥的合法性。（2）证书库。证书库是证书的集中存放地，是网上的一种公共信息库，供广大公众进行开放式查询。到证书库访问查询，可以得到想与之通信实体的公钥。证书库是扩展PKI系统的一个组成部分，CA的数字签名保证了证书的合法性和权威性。

c.密钥备份及恢复系统：如果用户丢失了密钥，会造成已经加密的文件无法解密，引起数据丢失，为了避免这种情况，PKI提供密钥备份及恢复机制。

d.证书作废系统：有时因为用户身份变更或者密钥遗失，需要将证书停止使用，所以提供证书作废机制。

e.PKI应用接口系统： PKI应用接口系统是为各种各样的应用提供安全、一致、可信任的方式与PKI交互，确保所建立起来的网络环境安全可信，并降低管理成本。没有PKI应用接口系统，PKI就无法有效地提供服务。

**b) 电子邮件的数字签名和加密**

电子邮件的信息安全主要可以通过两种手段，加密手段以及数字签名手段，两者具体的工作原理如下：

数字签名：数字签名则是发送方使用私钥对邮件进行数字签名，收件方使用对应的公钥对签名进行核实，签证数字签名的有效性（时效性，CA是否可信任等等）。

加密：分为对称加密以及非对称加密两种，对称和非对称的区别在于加密解密使用的密钥是否一样。首先是对称加密，发件方使用密钥对邮件进行加密，收件方使用相同的密钥对秘文进行解密。而非对称加密则是发送方使用对方的公钥对会话进行加密，而解密方使用自己的私钥对会话进行解密。公钥和私钥是对应的但是不一样，所以被陈伟是非对称。

1. **实验环境**

处理器：Intel(R) Core(TM) i7-7500 CPU @ 2.70GHz

内存：8GB

系统类型：windows 10

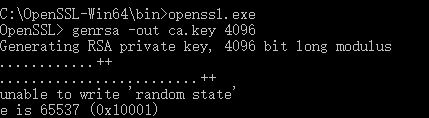
网络：scut校园网

1. **实验步骤以及截图**

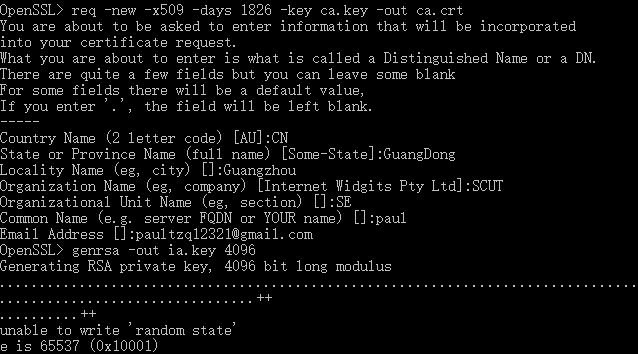
1） 使用Openssl文件生成自己的PKI系统，包含CA以及数字证书

首先下载openssl，配置环境变量，截图省略。

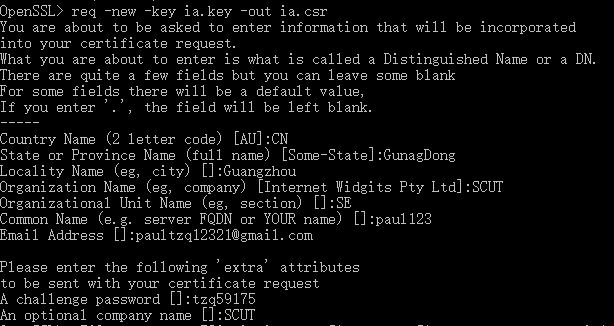
首先为根CA生成一个RSA key:



然后，创建自签发的根CA，需要提供以下信息：



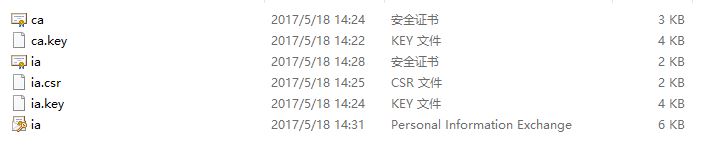
然后创建一个子证书：



使用根CA对子证书进行签名：

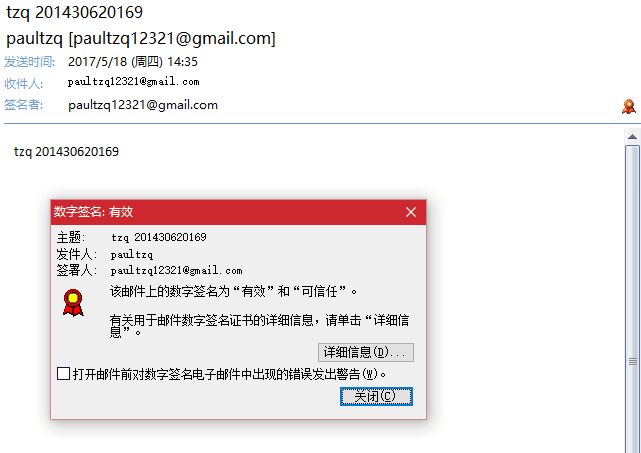
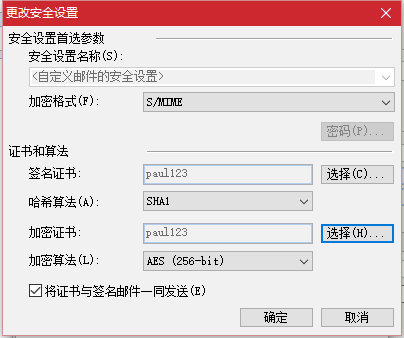
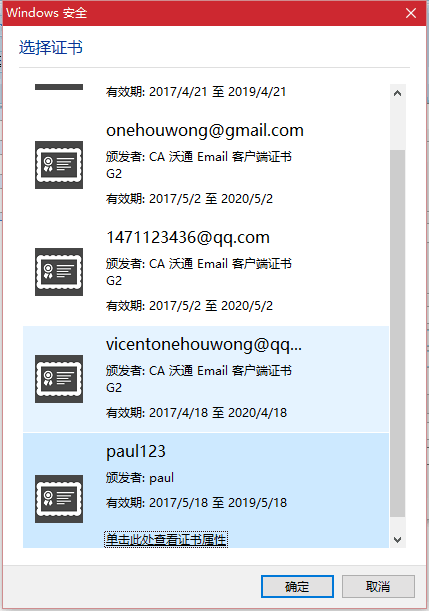


生成的CA，密钥，证书如下图：



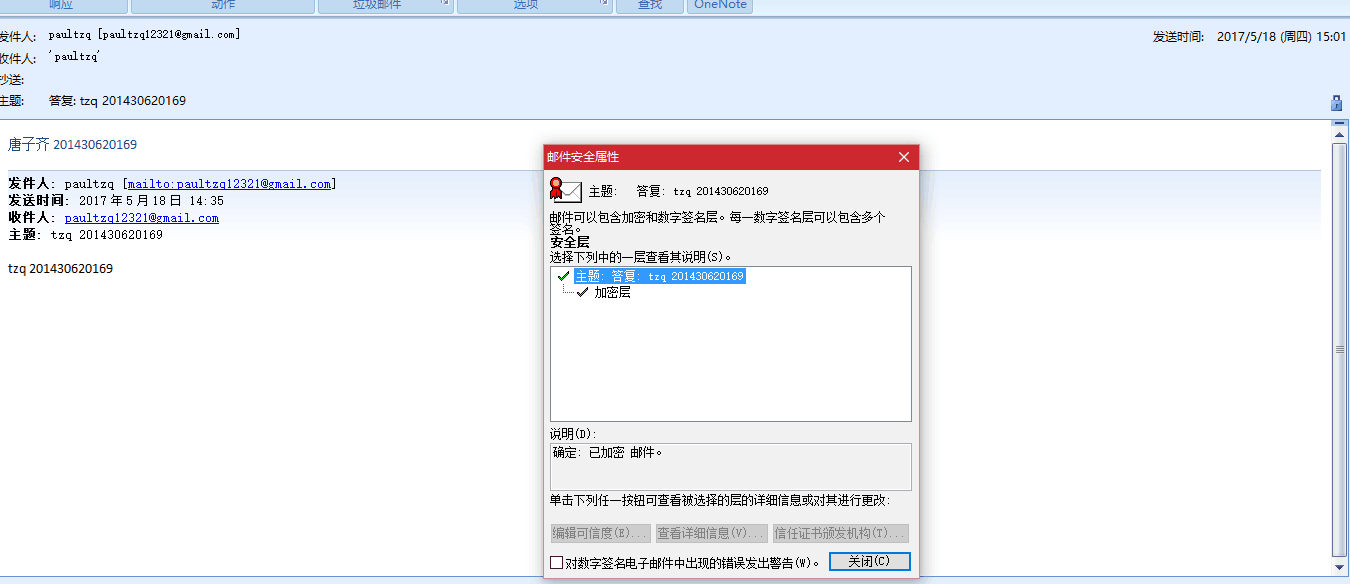
2） 使用Microsoft Outlook 2007发送加密邮件以及数字签名

使用刚生成的证书对邮件进行数字证书的签署：



然后再使用公钥进行加密并发送，收到的结果如下：

点进去才能阅读内容，右上角的加锁标志表示加密邮件：



# 实验结论与思考题

1. **加密邮件与签名邮件有什么区别？**
2. 加密邮件：对电子邮件进行加密是邮件的发送人使用邮件接收人的数字证书的公钥进行加密，可以保证所发送的邮件不被除收件人以外的其他人截取然后进行修改等恶性操作。然后，收件人接受到邮件之后，使用自己的对应私钥对邮件进行解密，可以使得邮件的内容从密文变成明文。由于只有对应的私钥才能解密公钥加密的文件，而只有邮件的接受方才有机密公钥对应的私钥，从而保证了该邮件不能被恶意人员解密、篡改等等。
3. 签名邮件：当发件人在即将被发送的邮件中添加数字签名时，与加密邮件不同，发件人是在该邮件中加入了数字签名和自己（而非收件人）的[数字证书](https://www.baidu.com/s?wd=%E6%95%B0%E5%AD%97%E8%AF%81%E4%B9%A6&tn=44039180_cpr&fenlei=mv6quAkxTZn0IZRqIHckPjm4nH00T1YkPWD3mW6zPjcYmyDknvFh0ZwV5Hcvrjm3rH6sPfKWUMw85HfYnjn4nH6sgvPsT6KdThsqpZwYTjCEQLGCpyw9Uz4Bmy-bIi4WUvYETgN-TLwGUv3EPHmkrHDdn1mk)。邮件的接收方接收到该邮件后，首先判断发件人的证书是否有效（该证书是否是可信任的CA签发的，该证书是否在有效期内，该证书是否已经被撤销），如果证书有效，从发件人的证书中提取公钥信息，来验证邮件的数字签名是否有效。
4. **随着中华人民共和国电子签名法的颁布实施，你认为签名电子邮件具有法律效力吗？**

签名电子邮件是具有法律效力的，当不发分子试图破解密钥并对原邮件进行篡改的行为应该属于违法行为。

1. **为什么发送加密邮件需要对方的数字证书？其加密原理是什么？真的是使用接收方的公钥直接对邮件的内容进行加密吗？**

因为邮件收件人接受到邮件之后，使用自己的对应私钥对邮件进行解密，只有对应公钥的私钥才能将加密的邮件解密，所以发送加密邮件的时候需要对方的数字证书，可以使得邮件的内容从密文变成明文。由于只有对应的私钥才能解密公钥加密的文件，而只有邮件的接受方才有机密公钥对应的私钥，从而保证了该邮件不能被恶意人员解密、篡改等等。

1. **能用他人的证书发送签名邮件吗？为什么？**

可以，数字证书的作用就是加密和签名，使用他人的证书给自己发送邮件加密，就能只让有盖证书私钥的对方解密密文邮件，从而实现了邮件的加密。