**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：** | **朱本金** |
| **学生学号：** | **201430615165** |
| **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. **实验目的及要求：**

学习数字证书的申请和安装方法，并使用数字证书进行电子邮件的加密与数字签名。

1. **实验性质与背景知识：**

本实验为必做课程实验，分为认知性、验证性和应用性实验。

数字证书提供了一种在 Internet 上身份验证的方式，是用来标志和证明网络通信双方身份的数字信息文件，与司机驾照或日常生活中的身份证相似。数字证书是由一个由权威机构即CA机构，又称为证书授权（Certificate Authority）中心发行的，人们可以在交往中用它来识别对方的身份。在网上进行电子商务活动时，交易双方需要使用数字证书来表明自己的身份，并使用数字证书来进行有关交易操作。数字证书包含一个公开密钥、名称以及证书授权中心的数字签名。一般情况下证书中还包括密钥的有效时间，发证机关（证书授权中心）的名称，该证书的序列号等信息，证书的格式遵循相关国际标准。

本实验包括数字证书的下载、安装，以及使用数字证书发送加密和签名的安全电子邮件。

**三、实验环境**

一台运行windows的计算机，带有并已经正确安装网卡；局域网络环境，并能上Internet。

**四、实验要求：**

1.掌握数字证书的用途和申请过程。

2. 掌握查看数字证书的方法。

3.掌握数字证书发送加密和签名的E-mail的操作步骤。

**五、实验步骤：**

1． 获得及安装免费数字证书

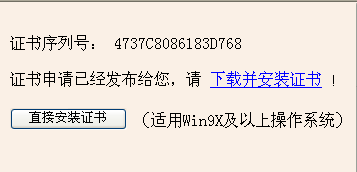
申请地址为https://testca.netca.net/。登陆后，点击“证书申请”，选择“试用型个人数字证书申请”。注意只有安装了根证书（证书链）的计算机，才能完成后面的申请步骤和正常使用读者在CA中心申请的数字证书。

按照提示，通过地址<https://testca.netca.net/download/GetRootCertificateIndi.asp>选择“安装试用CA证书链”。安装成功出现提示框后，可以看到一个表单，如图1所示。

按照表单上的提示，输入完整的个人资料。其中，加密服务提供程序（Cryptographic Service Provider，CSP）一栏中，CSP 负责创建密钥、吊销密钥，以及使用密钥执行各种加、解密操作。这里CSP 都提供了不同的实现方式。某些提供了更强大的加密算法，而另一些则包含硬件组件，例如智能 IC 卡或 USB电子令牌。 当使用特别的数字证书存储介质（如：智能 IC 卡或 USB 电子令牌）存储数字证书及其相应的私有密钥时，可以在“加密服务提供程序（CSP）”下拉框中选择该存储介质生产厂商提供的CSP。我们可以选择“Microsoft Base Cryptagraphic Provider V1.0”。单击“提交”按钮。弹出“潜在的脚本突出”对话框，提示“此网站正在代表您请求一个新的证书。您应该只允许信任的网站为您请求证书。您想现在请求证书吗？”单击“是”按钮，弹出“正在创建新的RSA交换密钥”对话框。如图2所示。



单击“确定”按钮，在接下来的页面中选择“下载并安装证书”，或“直接安装证书”按钮如图3所示。在弹出的“证书”对话框中单击“安装证书”按钮，进入证书导入向导。证书存储位置可以选择系统默认的“根据证书类型，自动选择证书存储区”，最后单击“完成”按钮。系统提示“证书导入成功”表明读者的证书已经成功安装。



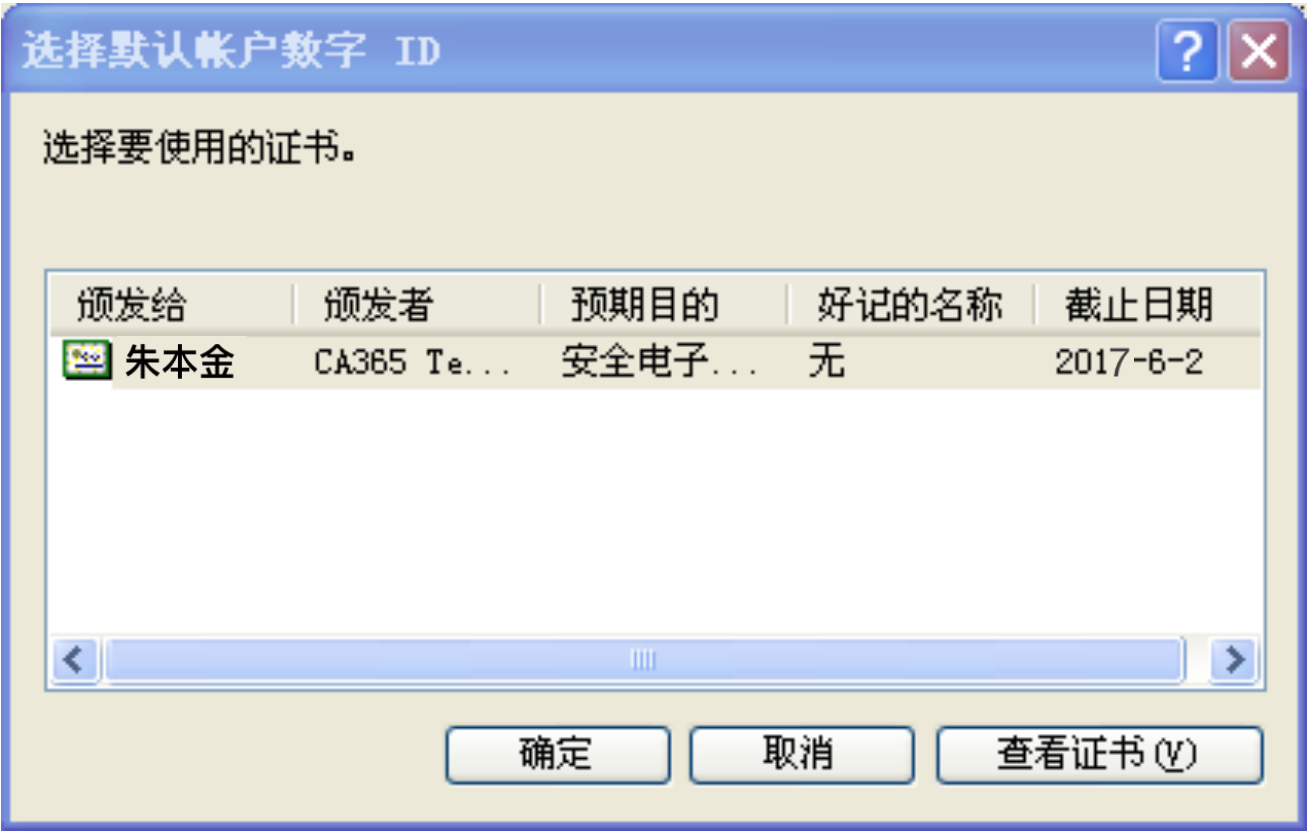
2. 在IE中查看数字证书

首先在打开Internet Explorer，在Internet Explorer的菜单上，单击 “工具”菜单中的 “Internet选项”。选取“内容”选项卡，点击“证书”按钮来查看读者信任的当前证书的列表。

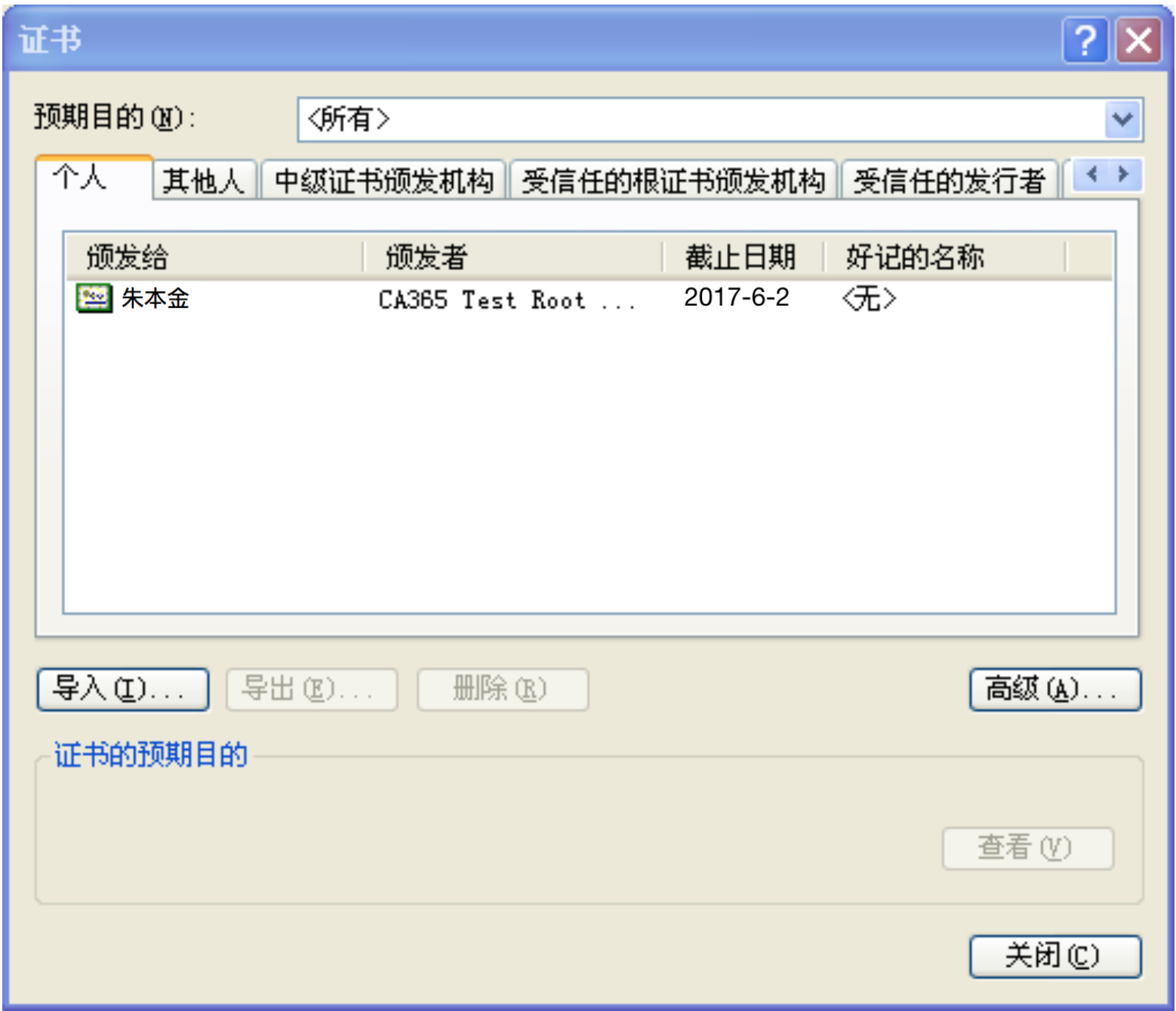
点击“个人”选项卡可以查看读者已经申请的个人数字证书；选定读者要查看的个人数字证书，然后单击 “查看” 按钮，可以查看证书的详细信息。

3.发送加密的E-mail

在Outlook Express6.0单击菜单中的“工具”，选择“账号”，选取“邮件” 选项卡中的用于发送安全电子邮件的邮件账号，即刚才建立的账号“彭文波”，然后单击“属性”。



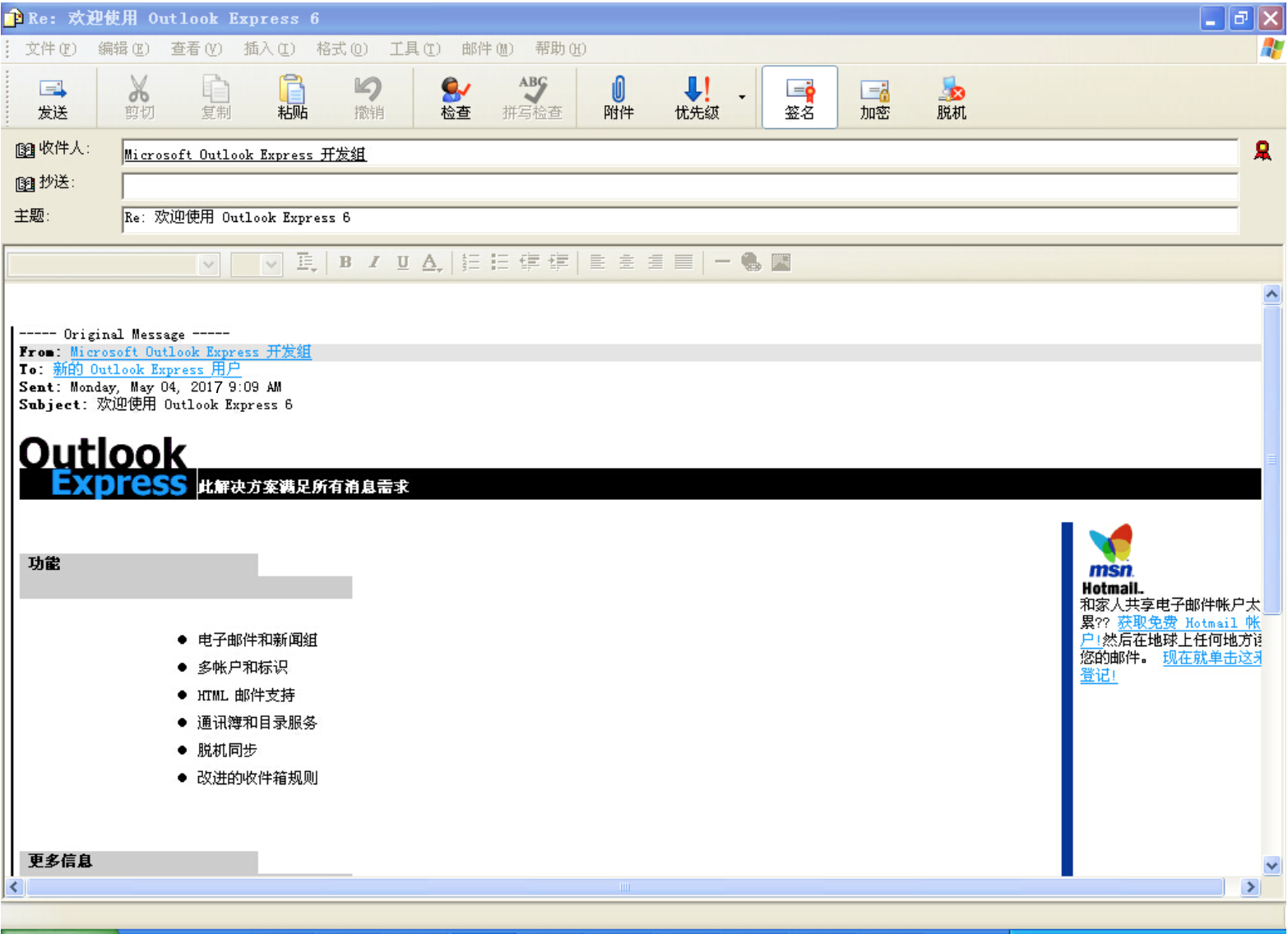
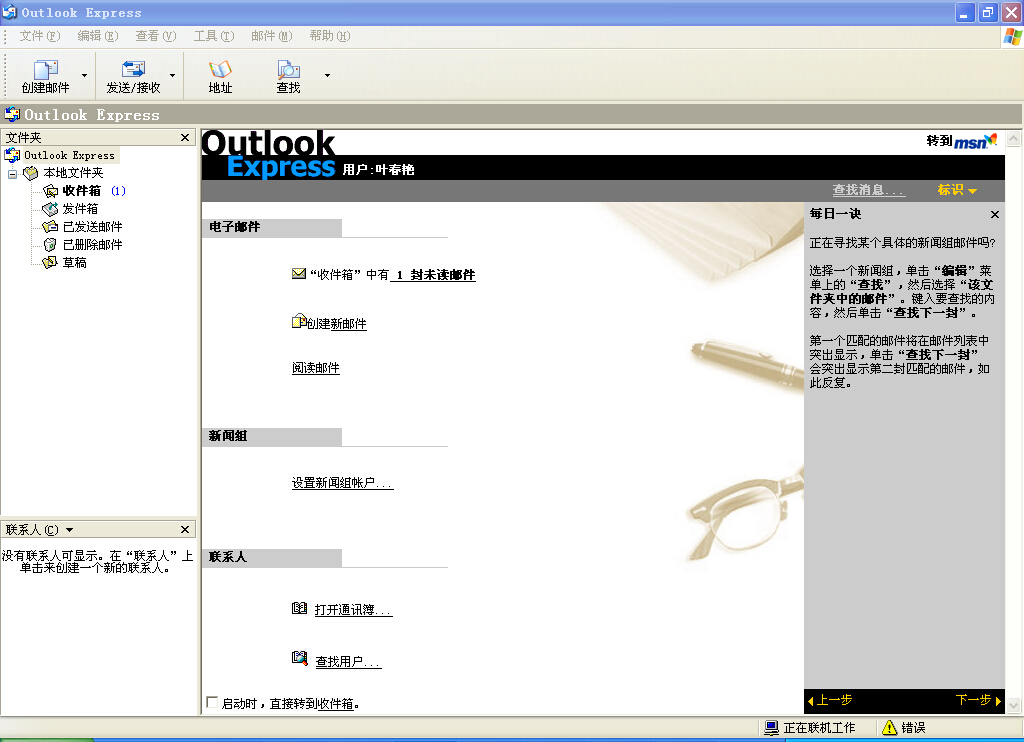


选择上面的“安全”标签，可以看到 “签署证书”和“加密首选项”两栏。通过相关设置，我们可以进行邮件的签署和加密。继续上图的设置，我们在“签名证书”项后，点击“选择”按钮。可以看到我们在https://testca.netca.net/上面申请的证书。选择读者的数字证书，点击“确定”完成邮箱与证书的绑定，读者也可以点击“查看证书”，了解自己证书的详细信息。

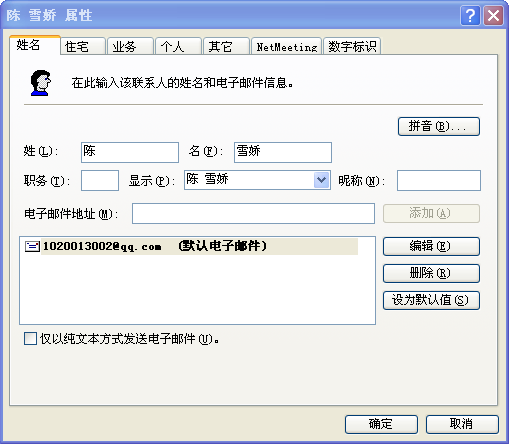
注意：如果点击“选择”按钮，没有相关的证书弹出来，请确认读者的证书已经正确安装且没有过期。

同时要确认读者在Outlook Express中所设置的邮箱与读者在申请数字证书时所提供的邮箱一致。查看读者在申请数字证书时所提供的邮箱方法：在Internet Explorer中，依次点击“工具”中的“Internet选项”，选择“内容”选项卡中的“证书”，选中读者的数字证书，点击“查看”，找到“详细信息”中的“主题”，读者就可以看到邮箱。

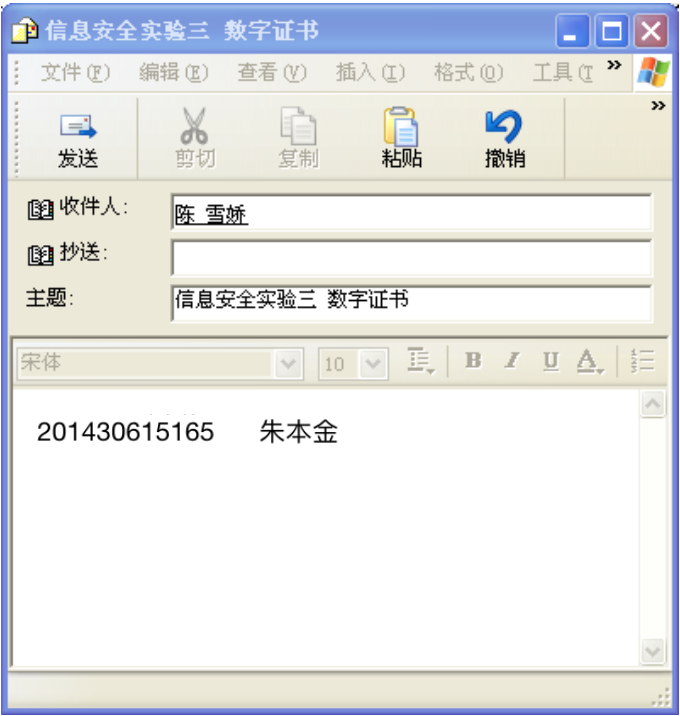
按照同样的方法，读者也可以在“加密首选项”中把读者自己的证书选中。点击确定。就可以准备发送加密电子邮件了

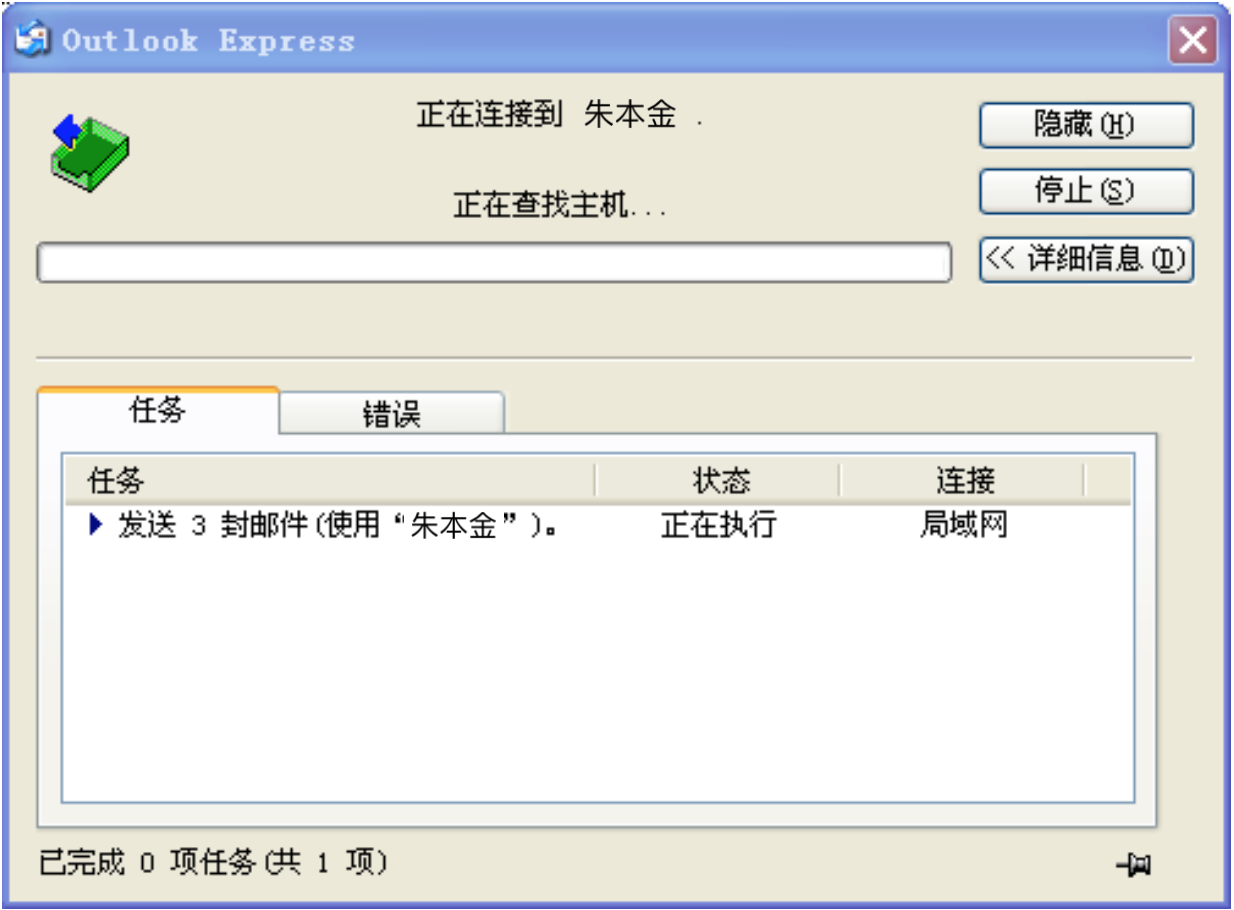


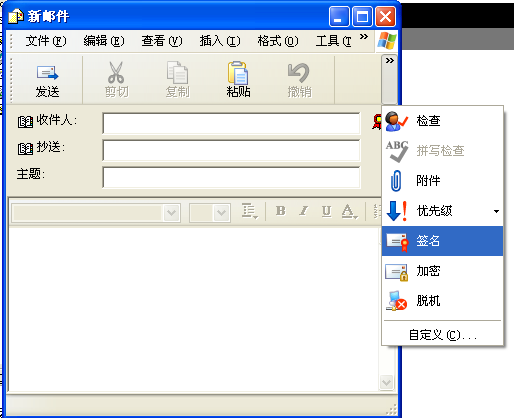
4. 发送数字签名的E-mail

发送加密邮件前必须先获得接收方的数字标识，读者可以首先让接收方给读者发一份签名邮件来获取对方的数字标识或者直接到电子商务安全认证中心的的网站如http://www.cnca.net的站点上面去查询下载来获取对方的数字标识。

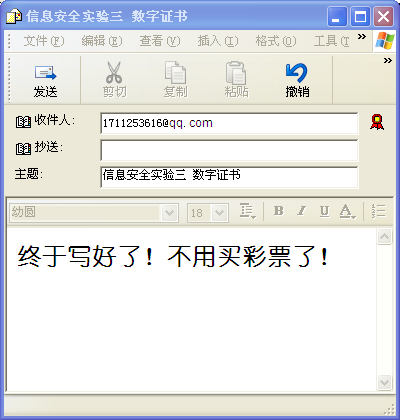




启动Outlook Express6.0，点击“新邮件”，撰写新邮件。同时我们选中右上方的“签名”或者“加密”选



Ø         发送签名电子邮件

点击“发送”，签名邮件发送成功。当收件人收到并打开有数字签名的邮件时，将看到 数字签名邮件的提示信息，按“继续”按钮后，才可阅读到该邮件的内容。



Ø         接收签名电子邮件

若邮件在传输过程中被他人篡改或发信人的数字证书有问题，将出现“安全警告”提示。收到邮件后，我们可以看到，邮件的右边中间有一个小图标，点击它，可以看到相关的数字证书信息，包括把查看他的相关信息、把发信人的数字证书添加到自己的通讯簿。

# **实验结论与思考题**

1. 加密邮件与签名邮件有什么区别？

签名邮件：对电子邮件进行数字签名，能够确保电子邮件中发送的文档不是伪造的，即收件人能够确信该邮件来自于其声称的发件人，同时邮件从发件人的机器传达到接收人的机器没有经过任何改动。

加密邮件：对电子邮件进行加密（使用接收人的数字证书中的公钥进行加密）可以保证所发送的邮件不被除收件人以外的其他人截取和偷阅。

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？

[中华人民共和国电子签名法](https://www.baidu.com/s?wd=%E4%B8%AD%E5%8D%8E%E4%BA%BA%E6%B0%91%E5%85%B1%E5%92%8C%E5%9B)是为了规范电子签名行为，确立电子签名的法律效力，维护有关各方的合法权益而制定的法律。

2. 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？

当发件人对邮件进行加密时，使用接收人的数字证书中的公钥对邮件进行加密。

首先发送方甲生成会话密钥K，利用 密钥K对邮件明文使用加密算法E1进行加密，得到密文E1K（M），并使用接收方的公钥PB加密会话密钥K得到E2PB（K），同时对明文用MD5算法产生报文摘要R作为数字签名，再使用甲的私钥TA加密报文摘要，得到ETB（R）。接着向接收方传输被加密的会话密钥EPB（K）、密文E1K（M）和被加密的摘要ETB（R）。接收方乙收到传输的文件之后，首先利用自己的私钥解密EPB（K）得到会话密钥K，再用K解密密文，得到邮件明文M，为了验证邮件的发出者的真实性，接收方使用发出者的公钥解密报文摘要，再用同样的算法对邮件明文M产生报文摘要，对比两个摘要，如果相等就可确认邮件发送方的身份。

3. 能用他人的证书发送签名邮件吗？为什么？

不行，因为收到的他人的证书中只有公钥，没有私钥，无法使用没有私钥的证书发送签名邮件。