《电子支付与商务安全》课程实验指导书

（2012年4月修订）

课程编号：　1100405

实用专业：　电子商务

学时数：　36

学分：　1

编写者：　曾子明

实验一：数字证书的申请与使用（12 学时）

一、实验目的

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。

二、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。可安排在第5学期，学时数为6学时。

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

实验环境如下：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。

按照表单上的提示，输入完整的个人资料。选择加密服务提供程序（Cryptographic Service Provider，CSP），其中，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。每个 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”。

下载证书。进行上述步骤后，系统将发一封申请成功的信件到读者申请时使用的邮箱内，其中包括业务受理号和密码， 数字证书下载的地址。点击数字证书下载地址，填写业务受理号和密码。

然后点击下方的“安装证书”按钮，当系统提示“证书成功下载”和“证书已成功装入应用程序中”后，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”选项。

- 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。

- 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。

五、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。

实验 2：使用 PGP 对文件加密及数字签名（12 学时）

一、实验目的

学习PGP软件的安装、使用以及对文件的加密和数字签名。

二、实验性质和背景知识

本实验为必做综合性实验，可安排在第5学期，学时数为6学时。

PGP（Pretty Good Privacy）软件是一个基于RSA公钥加密体系的文件加密软件，提出

了公共钥匙或不对称文件的加密技术。PGP软件将RSA公钥体系和传统加密体系结合起来，并且在数字签名和密钥认证管理机制上有巧妙的设计，因此PGP已成为广泛采用的文件加密方式之一。

本实验采用PGP 8.0.3版本为例，介绍PGP软件的使用，包括PGP软件的安装与初始设置，使用PGP软件加密文件，以及用PGP软件对文件进行数字签名。

三、实验环境

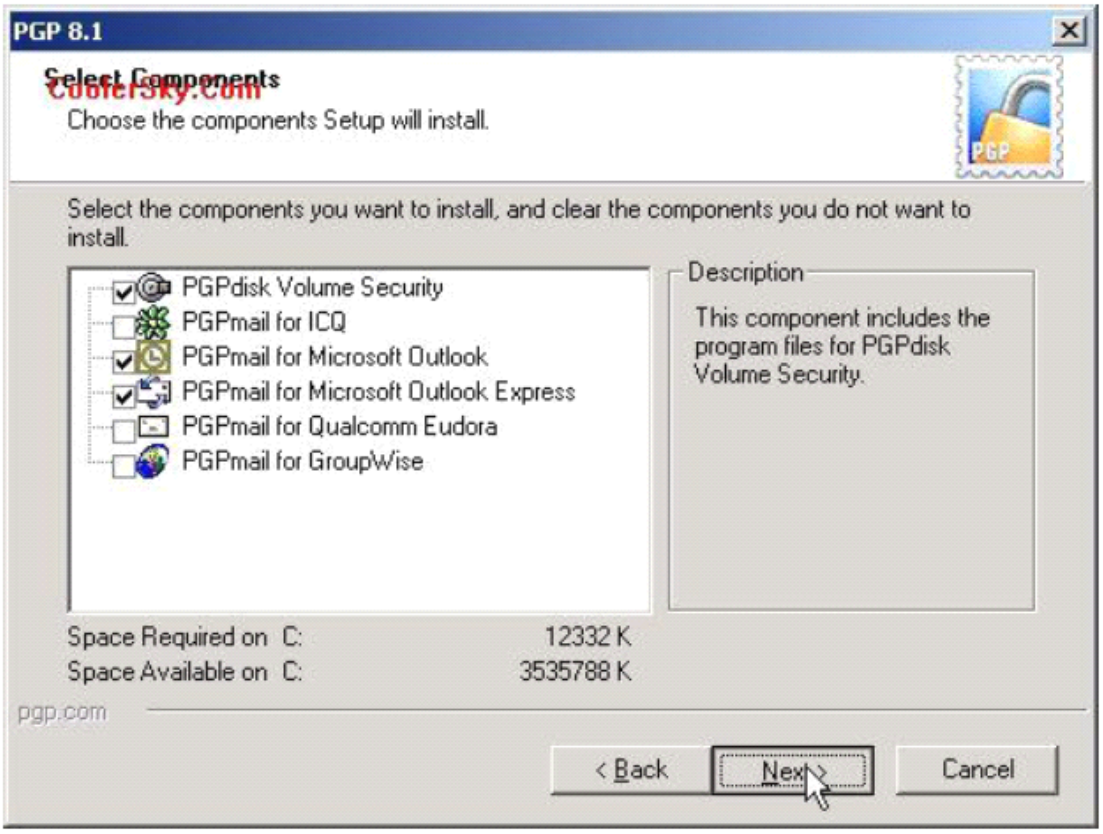
实验环境如下：使用Windows操作系统的计算机；局域网络环境；具备Internet连接。

四、实验步骤

(1) PGP的安装与初始设置

下载软件后，运行pgp8.exe文件开始安装，安装的过程很简单，依次按“next”按钮就可以了。

接下来选择要安装的组件，其中，第一个选项是关于磁盘加密的功能；第二个选项是ICQ的邮件加密功能；第三四个选项是关于OUTLOOK或者OTLOOK EXPRESS邮件加密的功能；最后一个选项适用于群发邮件的加密。用户可以根据自己的需要进行组件选择，一般情况下，默认安装就可以了。如图所示。



（2） 生成密钥对

使用PGP之前，首先需要生成一对密钥，这一对密钥其实是同时生成的，其中的一个称为公钥，意思是公共的密钥，你可以把它分发给你的好友，让他们用这个密钥来加密文件，另一个称为私钥，这个密钥由你保存，你是用这个密钥来解开加密文件的。打开“开始”中

“PGP”的“PGP KEYS”，可看到以下的画面。 点击图标 或者用菜单key>new key开始生成密钥。PGP有一个很好的密钥生成向导，只要跟着它一步一步做下去就可以生成密钥。

① PGP会提示这个向导的目的是生成一对密钥，你可以用它来加密文件或对数字文件进行签名。 ② PGP会要求你输入全名和邮件地址。 ③ 选择一种加密类型。④ 指定密钥的长度。通常来说位数越大被解密的可能性越小就越安全，但是在执行解密和加密时会需要更多的时间，一般1024位就可以了。 ⑤ PGP会问你密钥的过期日期，可以选择从不过期或者指定一个日期作为过期的界限。⑥请重复输入你的密码。建议你的密码大于8位，并且最好包括大小写、空格、数字、标点符号等。 ⑦ 接下来PGP会花一点点时间来生成你的密钥，然后会问你是否想把你的公共密钥发送到服务器上去，一般直接选择 “下一步”就可以完

成了。

（3）文件加密与解密

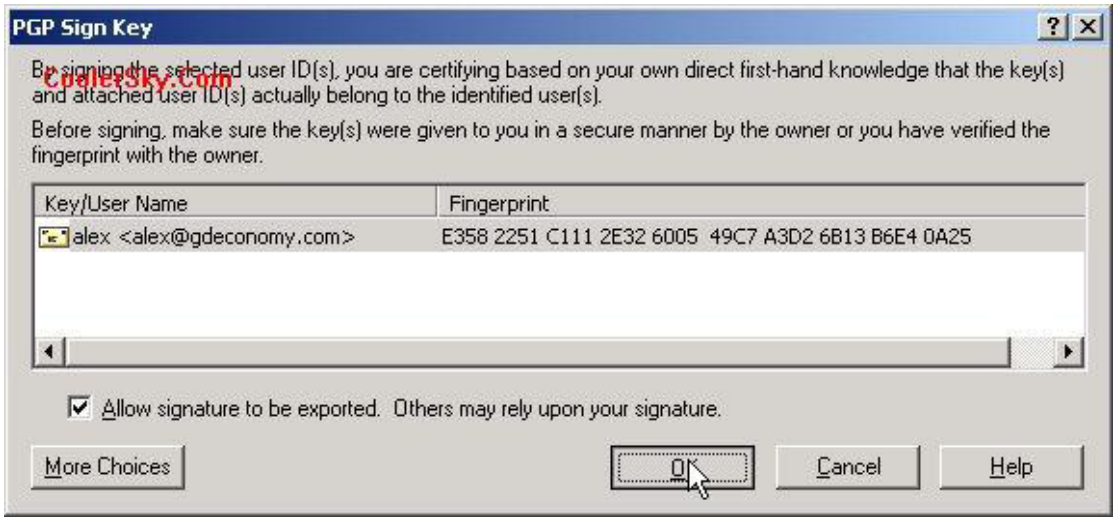
有了对方的公钥之后就可以用对方公钥对文件进行加密，然后再传送给对方。具体操作如下：选中要加密的文件，右键，然后选择“PGP”-“Encrypt”，如图所示。

然后在密钥选择对话框中，选择要接受文件的接收者。注意，用户所持有的密钥全部列出在对话框的上部分，选择要接收文件人的公钥，将其公钥拖到对话框的下部分，点击“OK”，并且为加密文件设置保存路径和文件名。此时，你就可以把该加密文件传送给对方。对方接收到该加密文件后，选中该文件，右键，选择“Decrypt&verify”。 此时，要求输入私钥的密码，输入完后，按“OK”即可。

接下来，要为已经解密的明文文件设置保存路径文件名。保存后，明文就可以被直接查看了。

（4）文件的数字签名 由于公钥是发放给其他人使用的，那么在公钥发放的过程中，存在公钥被人替换的可能。此时，若有一个人对此公钥是否真正属于某个用户的公钥做出证明，那么该公钥的可信任度就比较高。如果A很熟悉B，并且能断定某公钥是B的，并没有人把该公钥替换或者篡改的话，那么可以对B的公钥进行数字签名，以自己的名义保证B的公钥的真实性。具体操作为：运行“始”-“PGP”-“PGP Keys”，选中要进行签名的公钥，然后右键，选择

“Sign”进行签名。 此时，选择该用户的公钥，并且选中“Allow signature to be exported. Others may rely upon your signature ”，点击“OK”，如图所示。



输入私钥的密码，点击“OK”。这样，对公钥的签字就完成了。值得提醒的是，公钥和私钥都可以实现加密的功能，但是当要进行数字签名的时候，就只能使用私钥而不能用公钥。因为私钥只为用户一个人掌握，所以，该私钥能表明他的身份，确定该信息只有他一个人才能发出。 我们也可以对文件进行签名和加密。操作如下：选择要进行签名的文件，点击右键，选择“sign”。要注意的是，对文件签名只能证明是你发出该文件，但是文件的内容并没有被加密，同时，进行数字签名时，在意的是表明该文件是从自己这里发出，因此对于文件的内容并不在意被别人看到，经过数字签名的文件要同原明文文件一同发送给对方，对方才能验

证数字签名是否有效。如果同时要表明文件从自己这里发出，同时又要对文件的信息保密，那么就选择“签名与加密”选项Encrypt&sign。 同样的，在选择密钥的对话框中，从对话框上部的密钥列表中，选择接收文件的用户拖到对话框的下部，点击“OK”。 确定接收人后，输入私钥的密码，进行数字签名或数字签名和加密。

五、实验要求

1. 掌握PGP软件的功能和主要加密原理。
2. 掌握使用PGP软件对文件加密和解密的方法和操作步骤。
3. 掌握使用PGP软件对文件进行数字签名的方法和操作步骤。

实验 3：网上银行系统与安全解决方案 (12 学时)

一、实验目的

熟悉网上银行服务的特点、主要功能和网上银行的申请步骤、服务流程；熟悉网上银行系统的安全解决方案。

二、实验性质和背景知识

网上银行系统与安全解决方案实验为验证性、应用性和综合性实验，通过实验演示和案例调研形式完成，可安排在第5学期完成，学时数为6学时。

网上银行是利用Internet和Intranet技术，为客户提供综合、统一、安全、实时的银行服务，包括提供各种零售和批发的全方位银行业务，还可以为客户提供跨国支付等其他贸易、非贸易的银行业务。网上银行在金融专用网内运行，公网和金融专业网之间的连接要通过支付网关接口，支付信息必须经支付网关才能进入银行的金融系统，进而完成支付工作。

网上银行的功能一般包括银行业务项目、商务服务和信息发布。目前，网络银行的功能主要是信用卡、个人银行和对公业务等客户与银行间关系较密切的部分。

① 银行业务项目：主要包括个人银行、企业银行、信用卡业务、多种付款方式、国际业务、信贷及特色服务等功能。

② 商务服务：包括投资理财、资本市场及政府服务等功能。

③ 信息发布：包括国际市场外汇行情、对公利率、储蓄利率、汇率、国际金融信息、证券行情和银行信息等功能。

通过本实验，熟悉网上银行服务特点和功能，并熟悉网上银行系统的安全解决方案。

三、实验环境

实验环境如下：局域网环境，并能上Internet。

四、实验步骤

(1) 登录招商银行网站，在IE 地址栏中输入http://www.cmbchina.com ，进入招商银行一网通网站。

(2) 登录个人银行专业版，阅读个人银行专业版申请指南。

(3) 下载并安装个人银行专业版客户端软件。

a) 点击安装文件PBSetup36.exe，进入安装向导。

b) 阅读个人银行专业版说明及责任条款，若同意，选择“我接受“单选项，点击“下一步”按钮。

c) 选定安装目录后，进入专业版使用向导。

d) 选择“证书启用”，点击“下一步”按钮。

e) 输入登录信息，系统连接到网络后，根据提示输入用户确认信息和银行卡信息。信息输入无误后，即可完成数字证书的启用工作，但还需等待一段时间，以便银行的计算机系统完成后续处理工作。

(4) 安装完毕后，用户可以从PC机登录个人银行专业版，并使用其中各项功能，包括基于信用卡的网上支付和网上转帐等。

(5) 以招商银行为例，对网上银行系统的安全解决方案进行案例调研，包括信息传递的安全解决方案、业务系统的安全解决方案以及整体的安全解决方案，其中重点对业务系统的安全解决方案进行调研和分析。

五、实验要求

1. 熟悉网上银行服务的特点和申请流程。

2. 熟悉网上安全支付和转账的操作过程。

3. 了解网上银行系统的安全解决方案。