《电子商务安全与管理》

实　验　指　导　书

赵　波　　编 写

适用专业：　电 子 商 务

广州大学经济管理实验教学中心

内容简介

《电子商务安全与管理》是电子商务专业的一门专业课，是学生从事电子商务专业必须学习的一门重要的专业课程。该课程将全面介绍电子商务行业所涉及的安全方面的基本理论、基本技术、常用的安全协议等。讲授的内容有：对称加密体制、非对称加密体制、数字签名技术、身份识别技术、常用的安全协议、PKI、电子商务安全中的管理问题等。

本实验是《电子商务安全与管理》课程的课内实验课，教学的主要任务是通过实验使学生更进一步的理解课堂教学中所讲授的理论和算法，同时通过课内实验还可使学生对电子商务安全的实现技术有一个基本的了解，使学生初步具备对电子商务系统中的安全问题进行评价、分析及提供解决方案的能力。

实验 1 对称加密体制实验

一、 实验目的

电子商务和电子贸易的迅猛发展，使得因特网以及网络的安全问题越来越受到关注。本次实验将对电子商务常用的软件平台(Java 2)平台下的加密及解密方法进行验证，通过本次实验具体要达到的实验目的如下:

1. 掌握对称密码体制的基本原理;
2. 掌握典型对称加密体制 DES 的基本算法;
3. 掌握 Java 2 平台下的密码体系结构;
4. 掌握 Java 2 平台下的对称加密体制 API 的使用方法;
5. 掌握在 Java 2 平台下编写加密及解密代码的方法.

二、 实验内容

1. 熟悉 Java 2 平台下的对称加密及解密函数的使用方法;
2. 采用 DES 加密算法加密一个文本文件;
3. 采用 DES 算法将前一步中加密的密文解密成明文;
4. 对比解密后的明文与原始明文，验证你所实现的加密和解密代码是正确的。

三、 实验原理

（略）

四、 实验步骤

1. 采用文本编辑器（任意一个）编辑一包含明文的文件（plaintext.txt），该文件中应不小于 200 字(汉字或字符);
2. 编写 Java 代码，采用 DES 算法对上述文件进行加密，加密后的密文的文件名为 cipher.dat(二进制文件);

3. 编写 java 代码 ，采用 DES 算法将 cipher.dat 解密成明文,文件名为 decrypt.txt

4. 编写 java 代码，用于比较 plaintext.txt 和 decrypt.txt

五、 实验报告要求

1. 实验报告中要给出你所使的 Java API;
2. 实验报告中要给出你用于加密测试的明文及加密后的密文（给出其字符方式表示的十六进制数）;
3. 分析 Java2 平台加密系统体系结构的特点;

实验 2 非对称加密体制实验

六、 实验目的

电子商务和电子贸易的迅猛发展，使得因特网以及网络的安全问题越来越受到关注。本次实验将对电子商务常用的软件平台(Java 2)平台下的加密及解密方法进行验证，通过本次实验具体要达到的实验目的如下:

6. 掌握非对称密码体制的基本原理;
7. 掌握典型非对称加密体制 RSA 的基本算法;
8. 掌握 Java 2 平台下的非对称加密体制 API 的使用方法;
9. 掌握在 Java 2 平台下编写加密及解密代码的方法.

七、 实验内容

5. 熟悉 Java 2 平台下的非对称加密及解密函数的使用方法;
6. 生成一对密钥;
7. 采用 RSA 加密算法加密一个文本文件;
8. 采用 RSA 算法将前一步中加密的密文文件解密成明文;
9. 对比解密后的明文与原始明文，验证你所实现的加密和解密代码是正确的。

八、 实验原理

参考教材中的相关内容。

九、 实验步骤

5. 编写 Java 代码生成一对密钥，并将密钥对转换成十六进制字符串形式输出。
6. 选择一串用于加密和解密实验的文字;
7. 采用公钥对一串文字进行加密;

8. 采用私钥将 2 中加密的文字解密;

9. 采用私钥对同样一串文安加密;

10. 采用公钥将其解密。

十、 实验报告要求

4. 实验报告中要给出你所使的 Java API;
5. 实验报告中要给出你用于加密测试的明文及加密后的密文（给出其字符方式表示的十六进制数）;
6. 分析 Java2 平台加密系统体系结构的特点;

实验 3 数字签名实验

十一、 实验目的

电子商务和电子贸易的迅猛发展，使得因特网以及网络的安全问题越来越受到关注。本次实验将对电子商务常用的软件平台(Java 2)平台下的加密及解密方法进行验证，通过本次实验具体要达到的实验目的如下:

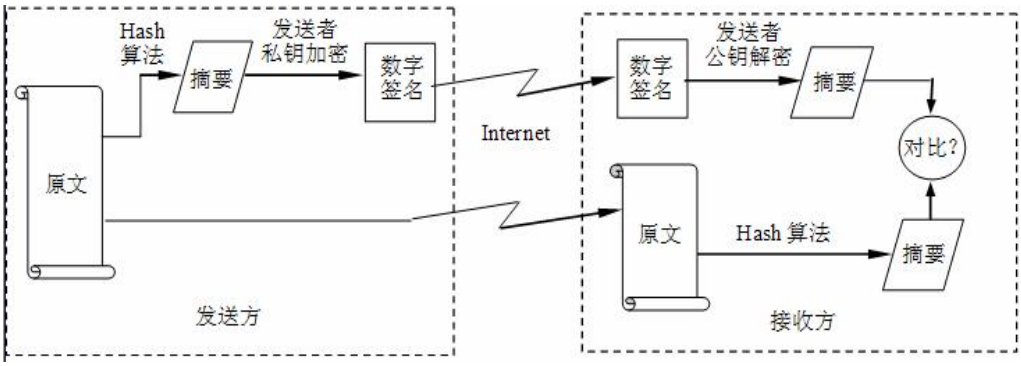
10. 数字签名的基本原理，理解数字签名的作用;
11. 掌握数字摘要算法的基本原理
12. 掌握 Java 2 平台下的数字签名算法的实现;

十二、 实验内容

1. 熟悉 Java SDK 中数字摘要算法 API 的用法;
2. 计算一个文件的摘要;
3. 对计算出的摘要进行数字签名;
4. 对数字签名进行验证

十三、 实验原理

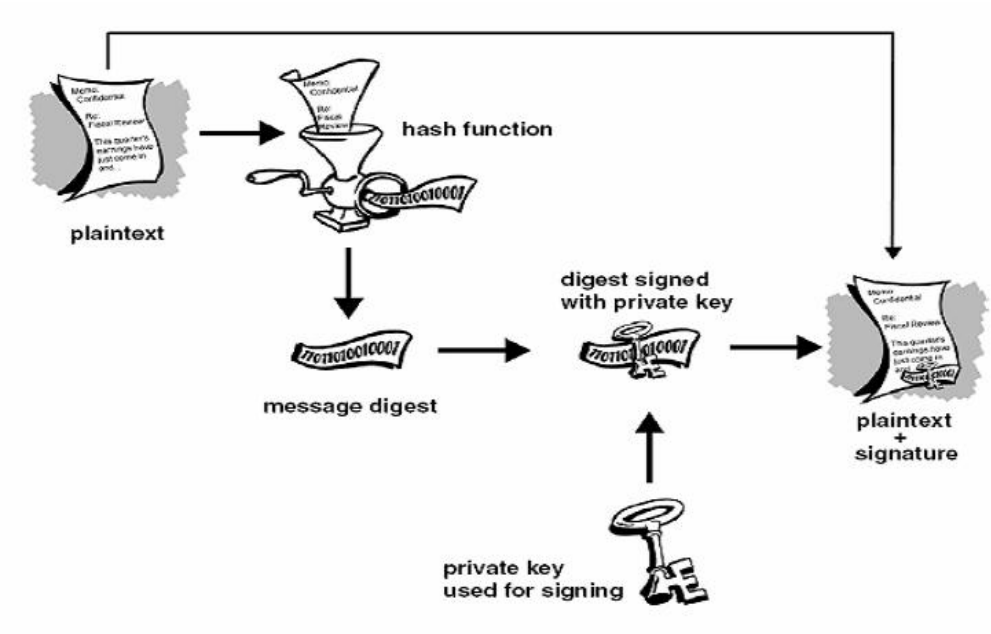
1. 数字签名的原理图



2. 数字签名的处理过程

- ✧ 使用摘要函数对信息进行编码将发送文件加密产生 128bit(或 160bit)的数字摘要;
- ✧ 发送方用自己的专用密钥对摘要再加密，形成数字签名;
- ✧ 将原文和加密的摘要同时传给对方;
- ✧ 接收方用发送方的公共密钥对摘要解密，同时对收到的文件用摘要函数产生同一摘要;
- ✧ 将解密后的摘要和收到的文件在接受方重新计算产生的摘要相互对比，如果两者一致，则说明在传送过程中信息没有破坏和篡改。否则，则说明信息已经失去安全性和保密性。

3. 基于 RSA 的数字签名算法



4. Java 对数字签名算法的支持

- ✧ KeyPairGenerator

由于 RSA 算法是基于大素数分解数学难题的，因此该算法的主要问题是要产生一对大素数。KeyPairGenerator 是一个用于产生 RSA 加密体制中的公钥和私钥对的引擎 .

- PublicKey

  PublicKey 类封装了 RSA 算法中的公钥（一个大素数）。

- PrivateKey

  PrivateKey 类封装了 RSA 算法中的私钥(一个大素数)

- MessageDigest 类

  该类提供了对各种摘要算法的支持

- Cipher 类

  该类实现了对对称加密带来解密算法的支持。

  单步加密时使用 Cipher 类中的 doFinal(…)方法;

  多步加密时则要联合使用 Cipher 中的

  update(…)方法和 doFinal(…)方法。

十四、 实验步骤

1. 准备一个文件,文件名为 source.txt;
2. 采用 Java 中的密钥 API 生一个 RSA 密钥对，并存入文本文件中,文件名为 keypair.txt;
3. 编写程序，完成数字签名:

   - 从 keypair.txt 中读入 RSA 密钥对，生成 PublicKey 和 PrivateKey 对象
   - 读入文件 source.txt,采用 SHA 算法计算该文件的摘要;
   - 采用 RSA 算法计算 source 的数字签名,并写入文件中,文件名为 digitaliginature.dat;

4. 编写程序，完成数字签名的验证

   ✧ 保持 source.txt 不变，对 source 的数字签名进行验证，确定 source 的完整性;

   ✧ 对 source.txt 进行某些修改，再对 source.txt 进行验证，看一下，通过数字签名能否发现文件已被篡改过。

十五、 实验要求：

7. 实验报告中要给出你所使的 Java API;
8. 实验报告中要给出你的实验过程;
9. 实验报告中要写出通过实验，你对数字签名有什么新的认识。

实验 4 身份认证实验

十六、 实验目的

电子商务和电子贸易的迅猛发展，使得因特网以及网络的安全问题越来越受到关注。本次实验将对电子商务常用的软件平台(Java 2)平台下的身份认证方法进行验证，通过本次实验具体要达到的实验目的如下:

13. 理解身份认证的基本原理和应用方法;
14. 初步掌握 JAAS 的基本框架;
15. 初步掌握基于 JAAS 的认证与授权的实现方法;

十七、 实验内容

1. 阅读 Sample.java，熟悉 JAAS 中认证的基本框架
2. 阅读 SampleAction.java，熟悉 JAAS 中授权的基本框架
3. 阅读 Sample_login.config 熟悉 JAAS 认证配配置文件的基本原理
4. 阅读 sampleazn.policy 熟悉 JAAS 策略文件的基本情况
5. 运行程序，验证基于 JAAS 的认证与授权

十八、 实验原理

见 JDK6.0 doc(JAAS)

十九、 实验步骤分

1. 阅读 Sample.java，熟悉 JAAS 中认证的基本框架
2. 阅读 SampleAction.java，熟悉 JAAS 中授权的基本框架
3. 阅读 Sample_login.config 熟悉 JAAS 认证配配置文件的基本原理
4. 阅读 sampleazn.policy 熟悉 JAAS 策略文件的基本情况
5. 执行 SampleAction.java ，观察程序的执行结果
6. 在命令行中加入-Djava.security.manager，观察程序的执行结果
7. 运行 Sample.java 观察程序的执行结果

8. 在命令行中加入-Djava.security.manager，观察程序运行的结果
9. 在上次运行的基础之止，再在命令行中加入
   -Djava.security.policy=sampleazn.policy，观察程序运行的结果。
10. 在上次运行的基础之止，再在命令行中加
    -Djava.security.auth.login.config=Sample_login.config，观察程序的运行结果
11. 修改 Principal com.sun.security.auth.NTUserPrincipal "asus" 中的 asus 为你所使用的计算机的 NTUserPrincipal，重复 10.
12. 分别注释掉以下几行，运程 Sample.java ，观察程序的运行.

    permission java.util.PropertyPermission "java.home", "read";
    permission java.util.PropertyPermission "user.home", "read";
    permission java.io.FilePermission "foo.txt", "read";

二十、 实验**要求**：

10. 实验报告中要给出你所使的 Java API;
11. 实验报告中要给出你的实验过程;
12. 实验报告中要写出通过实验，你对身份认证有什么新的认识。

实验 5 PKI 实验

一、 实验目的

电子商务安全可分成网络安全和商务交易安全。在网络环境下的交易安全最主要的任务就是确定交易双方的真实身份-即身份认证。现阶段解决交易双方身份识别题的技术手段就是 PKI.

本实验的具体目的如下:

- ✧ 掌握对称密钥体制;
- ✧ 掌握非对称加密体制;
- ✧ 掌握认证算法及其应用;
- ✧ 掌握网络安全协议;
- ✧ 掌握 PKI 技术.

二、 实验内容

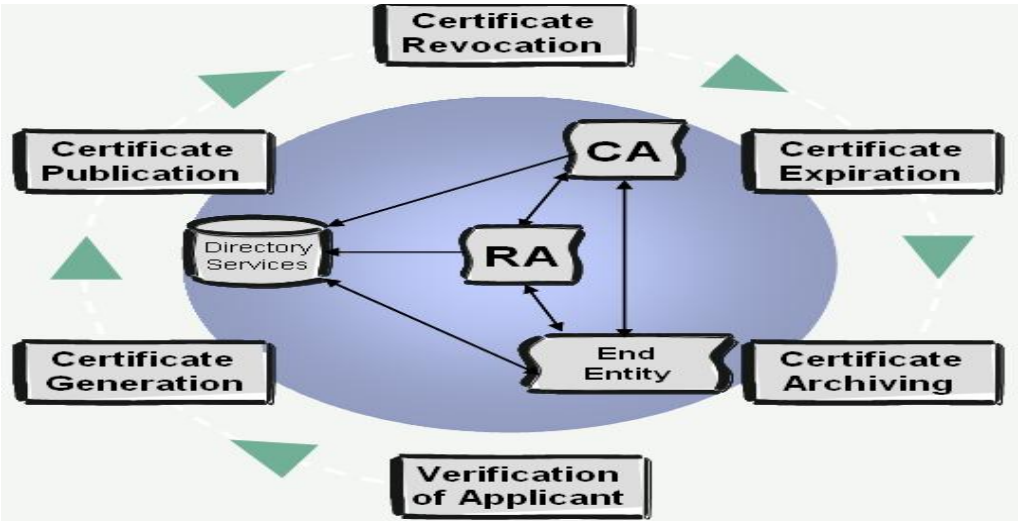
在 B2C 电子商务应用系统中,确定商家和客户的身份是确保电子商务交易安全进行的必要条件，请设计一个基于 PKI 技术的电子商务系统中的身份识别模块。

三、 实验原理

1、 PKI 的基本概念

公钥基础设施 PKI(Public Key Infrastructure)是一种遵循既定标准的密钥管理平台,它能够为电子商务、电子政务、网上银行和网上证券等所有网络应用提供一整套安全基础平台，它是创建、颁发、管理、撤销公钥证书所涉及到的所有软件、硬件的集合体。加密技术和认证技术是 PKI 的基础技术，PKI 的核心机构是认证中心（Certificate Authority, CA)，数字证书是 PKI 最关键的产品和服务。

2、 PKI 的基本组成



- 权威认证机构(CA)
- 数字证书库
- 密钥备份及恢复系统
- 证书作废系统
- 应用接口（API）

3、 基于 PKI 的身份认证基本原理

■ PKI 加密密钥对的使用原理

✧ 发送方欲将加密数据发送给接收方，首先要获取接收方的公开的公钥(**通过 PKI 获取并验证**)，并用此公钥加密要发送的数据，即可发送；

✧ 接收方在收到数据后，只需使用自己的私钥即可将数据解密。此过程中，假如发送的数据被非法截获，由于私钥并未上网传输，非法用户将无法将数据解密，更无法对文件做任何修改，从而确保了文件的机密性和完整性。

- PKI 签名密钥对的使用原理

- ✧ 此过程与加密过程相对应。接收方收到数据后，使用私钥对其签名并通过网络传输给发送方，发送方用公钥(**经 PKI 验证确实是发送者的公钥**)解开签名，由于私钥具有唯一性，可证实此签名信息确实为由接收方发出。
- ✧ 此过程中，任何人都没有私钥，因此无法伪造接收方的签名或对其作任何形式的篡改，从而达到数据真实性和不可抵赖性的要求。

4、 Java 对基于 PKI 的应用的支持

- ✧ 关于数字证书的类

CertificateFactory;

X509Certificate

PublicKey

X509CRL

X509CRLEntry

KeyStore

PrivateKey

四、 实验步骤

本实验要求学生完成如下任务:

- ✧ 对要解决的实际问题进行需求分析;
- ✧ 设计如何利用 PKI 实现商户和客户的身份认别;
- ✧ 给出要解决问题的详细设计（模决);;
- ✧ 设计、调试;

- ✧ 撰写说明(包含在实验报告中);
- ✧ 提交一个完整的实用小程序。

五、 实验要求：

基本要求:

本实验要求学生完成完整的程序:

- ✧ 设计各模块要采用的技术;
- ✧ 设计、调试;
- ✧ 撰写说明书（体现在实验报告中）;

成绩评定:

- ✧ 实验要求独立完成
- ✧ 若发现雷同实验报告或软件，则本次实验计 0 分。

提交成果:

- ✧ 实验报告

实验 6 安全协议实验

六、 实验目的

电子商务安全中所涉及的基础理论和基本算法较多，但在具体应用时，我们一般较少直接应用这些算法去设计实际电子商务应用系统，而是采用现有的各种安全协议。通过指定一种安全协议，让学生去设计一个使用该协议的实验系统，对学生掌握这些协议的使用具有非常重要的意义。

本实验的具体目的如下:

- ✧ 掌握对称加密算法的原理与使用方法;
- ✧ 掌握非对称加密算法的原理与使用方法;
- ✧ 掌握认证算法及其应用;
- ✧ 掌握密钥交换协议的原理与实用方法;
- ✧ 掌握 SSL 协议的原与使用方法

七、 实验内容和步骤

某单位拟通过互联网建立一个与其下属分支单位进行安全数据交换的系统。请根据《面向对象程序设》和《电子商务安全》两门课程中所学的知识，为该单位设计一个能满足其要求的程序。

本实验要求学生完成如下任务:

- ✧ 对要解决的实际问题进行需求分析;
- ✧ 给出要解决问题的详细设计（模决);
- ✧ 设计各模块要采用的技术;
- ✧ 设计、调试;
- ✧ 撰写说明(包含在实验报告中);
- ✧ 提交一个完整的实用小程序。

八、 提示

- ✧ 采用 TCP/IP 协议设计一个 Client/Server 程序;
- ✧ 为使程序简单一些，可考虑采用字符界面(即控制台应用程序)
- ✧ 为了实现安全数据通信，系统中可采用对称加密体制实现对通信数据的实时加密与解密;
- ✧ 在一个还安全的信道中实现安全通信，涉及的问题较多，因此可考虑采用 SSL 协议实现。

九、 实验要求：

基本要求:

本实验要求学生完成完整的程序:

- ✧ 设计各模块要采用的技术;
- ✧ 设计、调试;
- ✧ 撰写说明书（体现在实验报告中）;
- ✧ 提交一个完整的实用小程序。

成绩评定:

- ✧ 实验要求独立完成（实验报告、软件）;
- ✧ 若发现雷同实验报告或软件，则本次实验计 0 分。