全国高等教育自学考试　电子商务专业（独立本科段）

电子商务安全导论自学辅导·同步练习

[2005年版]

组编／全国高等教育自学考试指导委员会

主编／蒋汉生

辽宁教育出版社

全国高等教育自学考试

电子商务专业(独立本科段)

电子商务安全导论自学辅导·同步练习

(2005年版)

全国高等教育自学考试指导委员会　组编

主　编　蒋汉生

辽宁教育出版社

沈　阳

目　录

第一部分　怎样认识和学好《电子商务安全导论》

一、学科特点

1. 电子商务安全是一门重要学科

21 世纪将是电子商务大力发展的时代，发达国家已经将电子商务充分运用到现代商务活动的各个环节。我国电子商务发展也极其迅猛，新的电子商务网站和新的电子商务项目迅速增加，发展地域迅速从沿海向内地、从大城市向中小城市蔓延。中国政府明显加强了对电子商务的支持与协调力度，众多企业自觉制定和推出了内部电子商务规则或守则，税务系统、金融系统、证券业、药材业、建筑业等行业开始尝试网上业务的开展。

但是，由于种种原因，电子商务的发展呈现的趋势并不像某些人预计的那样快。其中一个重要原因就是人们对电子商务的安全心存疑虑。到目前为止，虽然人们在 Internet 上的安全方面做了大量的研究和开发，一些电子商务安全协议相继出台，已经能够基本满足电子商务的安全需求。但人们对电子商务安全的担心并没有完全消除，因此，制约了电子商务的进一步发展。

造成电子商务安全问题的原因很多。研究电子商务安全的需求、原因、方法和原理迫在眉睫。《电子商务安全导论》系统地介绍电子商务安全的需求、原因、原理和方法，对电子商务的应用具有指导作用。

2. 电子商务安全是一门新学科

目前许多有识之士已经认识到电子商务中存在的安全问题，逐渐开展这方面的研究，并在实践中不断摸索总结，形成了许多电子商务安全方面的原则、方法和协议。但这种探索还没有达到成熟，对电子商务安全的认识还局限于表面的状态。作为一门高等教育的学科，电子商务安全是一门新学科，有待在实践中不断发展和完善。

《电子商务安全导论》总结了对电子商务安全的认识，反映了在实践中摸索总结所形成的电子商务安全的原则、方法和协议等成果。但由于电子商务安全这门学科属于刚刚起步的新学科，《电子商务安全导论》也会在实践中不断发展和完善。

3. 目的在于加强防范意识和防范能力

《电子商务安全导论》目的在于加强防范意识和防范能力。《电子商务安全导论》不希望“培养”出更多的“黑客”来扰乱网络世界，但希望更多的从事电子商务活动的人了解电子商务安全知识，提高防范意识和防范能力，为有一个安全的电子商务环境作一点贡献。

二、内容、体系结构的特点

电子商务是新开设的专业，而“电子商务安全导论”则是第一次出现的新课程。相

应地，这门课的教材也是在我国电子商务各类高等教育中首次编写。“电子商务安全导论”自学考试指定教材从培养学生实际能力出发，内容系统全面、体系结构清晰合理、理论联系实际性较强。

1. 内容系统全面

《电子商务安全导论》教材所包括的内容系统全面，涉及到与电子商务安全相关的各个方面。电子商务安全包括以下四方面的内容。

（1）电子商务安全需求。这部分内容主要包括的内容有：电子商务安全基础等。

（2）密码理论及其应用。这部分内容主要包括加密理论、密码学以及密码理论的应用等。

（3）电子商务网络安全技术。这部分内容主要包括网络设备的物理安全、防火墙、VPN 技术、接入控制和数据加密等。

（4）公钥证书、证书机构、PKI、电子商务安全协议及其应用等。

本教材将以上内容进行系统的组织，深入浅出，逐步展开讨论。在介绍电子商务安全技术之前，先介绍一些基础知识使读者对电子商务安全相关技术有一个系统的了解和掌握；之后围绕电子商务安全三方面的内容逐步展开，讨论电子商务安全技术的方法、原则及原理，这是本教材的重点内容。最后，给出几个电子商务数字认证中心的案例，使考生对电子商务安全有较全面的认识。

2. 体系结构清晰合理

《电子商务安全导论》教材共分十一章，包括四大部分内容。

第一部分包括第一章电子商务安全基础的内容，涉及电子商务和电子商务安全相关的基本概念、分类、发展等内容。读者通过第一章的学习，对电子商务安全的概貌有一个全面的了解。

第二部分包括第二章和第三章的内容。这部分内容是电子商务安全技术的基础知识。第二章介绍电子商务中的信息安全需求和密码理论；在第三章原理性地介绍密码理论的实际使用方法。通过对有关电子商务安全的基础知识的介绍，使读者对电子商务安全相关技术有一个系统的了解和掌握，从而便于理解和掌握以后各章节关于电子商务安全方面的内容。

第三部分包括第四章至第六章的内容，涉及到网络安全需求及相关技术的内容。其中，第四章介绍有关电子商务网络系统物理安全所涉及的相关内容；第五章介绍防火墙、VPN 技术；第六章介绍接入控制和数据加密的有关内容。

第四部分包括第七章至第十一章的内容。第七章介绍电子商务环境下身份确认的必要性以及认证的相关概念；第八章介绍公钥证书和证书机构的有关内容；第九章介绍 PKI 的基本概念及其在电子商务中作用；第十章介绍电子商务中比较成熟的安全协议 SSL 和 SET；第十一章介绍国内几个典型的数字认证中心，以及相关的政策和规则。

三、自学的要求和方法

1. 自学本课程的目的和要求

自学《电子商务安全导论》的目的和要求可以从以下六个方面来概括：

（1）了解电子商务安全的需求、原因和现状等；

（2）理解密码理论相关内容；

（3）掌握密码理论应用的相关技术；

（4）掌握电子商务系统安全的要求与方法；

（5）掌握数字证书及其使用方法；

（6）了解公钥基础设施的基本构成及其作用；

通过本课程考试，取得规定的学分和单科结业证书。

2. 自学本课程的方法

自学不同于课堂学习，主要依靠学员利用教材及辅导用书发挥主观能动性，循序渐进地认真学习和领会。自学的方法主要有：

（1）通读《电子商务安全导论》教材

在阅读《电子商务安全导论》教材之前，先要大体了解教材的体系、结构、内容等方面的概况和特点。阅读过程中，应根据考试大纲中每章“学习目的和要求”以及“考试目标与具体要求”逐章逐节进行。

（2）划出重点

凡是考试大纲中要求识记的知识点，需领会和应用的重点、难点问题，都应在教材的相应章节中划出。识记的知识点，基本上属于教材中定义性的概念。领会和应用的重点和难点问题，基本上属于教材中有关理论、方法等内容。在划出重点的空白处分别标上“识记”、“领会”等字样。

（3）逐一理解

对根据考试大纲划出的需要识记、领会的内容，逐一阅读、思考。许多内容是前后关联的，因此涉及到有关的概念、方法等问题要前后对照起来看，不能只见树木，不见森林。不懂的问题请教有关的辅导老师或参考有关书籍。

（4）强化记忆

在理解教材内容的基础上，熟记基本概念；熟记需领会及应用问题的要点。凡需熟记的内容，要反复回顾，不能一背了之。在考试前，要争取集中一段时间，再突击强化记忆。

（5）认真阅读辅导书，做习题

辅导书对教材的每章要点均作了提示，同时配以练习题。考生在阅读辅导书的同时，还要认真做好每一道习题。通过做习题，可以自测自己掌握的程度，加深对教材内容的记忆和理解。

第二部分　要点提示与练习

第一章　电子商务安全基础

一、要点提示

本章主要包含三大部分内容：电子商务概述，电子商务安全基础，计算机安全等级。第一部分内容有三个要点：第一，理解商务的概念，第二，了解电子商务的方式，第三，熟悉电子商务的技术要素。第二部分内容有三个要点：第一，理解电子商务的安全隐患，第二，了解信息安全的六性，第三，熟悉各种电子商务安全威胁的原因。第三部分内容有二个要点：第一，了解计算机安全等级的划分，第二，理解计算机安全等级划分的原则。

本章共分三节。

第一节电子商务概述。本节详细阐述了电子商务的概念，首先从商务的含义出发，介绍了商务的演变历史，电子商务的模式及其依赖的技术基础；最后介绍了基于 EDI 的初级阶段到基于因特网的电子商务的发展高潮。

第二节电子商务安全基础。本节从信息安全的实例出发，介绍了基于因特网的电子商务的安全问题。首先介绍了计算机系统的安全隐患，分析了电子商务安全问题，攻击手段和安全保护内容。此外，还介绍了我国电子商务安全的特殊性和紧迫性以及相应对策。

第三节计算机安全等级。本节讲述了美国国家计算机安全中心 NCSC（The National Computers Security Center）制定的“可信任的计算机安全评估标准”，详述了计算机安全等级的分类标准。

本章的基本概念有：（1）电子商务；（2）EDI；（3）系统穿透；（4）植入；（5）机密性；（6）完整性；（7）认证性；（8）不可否认性；（9）不可拒绝性；（10）访问控制性；（11）伪造；（12）篡改；（13）截断信息和介入；（14）嗅探。

本章的基本理论有：（1）商务；（2）电子商务安全；（3）入侵方法；（4）电子商务安全措施；（5）计算机安全等级。

本章的基本知识有：（1）基于因特网的电子商务特点；（2）电子商务安全的中心内容；（3）Internet 的攻击类型；（4）TCP/IP 协议的安全隐患；（5）嗅探入侵；（6）拒绝服务；（7）劫持入侵；（8）保密业务；（9）认证业务；（10）接入控制；（11）数据完整性业务和不可否认性业务。

本章的重点问题有：电子商务及其特点，电子商务的安全性，攻击手段，安全性的六性，安全措施，计算机安全分级。

本章的考核点是：（1）商务；（2）电子商务安全；（3）入侵方法；（4）电子商务安全措施；（5）计算机安全等级。

二、练习题

（一）单项选择题

1. 对 Internet 的攻击的四种类型不包括（　）。

A. 截断信息　　B. 伪造　　C. 篡改　　D. 病毒

2. 电子邮件的安全问题主要有（　）。

A. 网上传送时随时可能被人窃取到　　B. 传输到错误地址

C. 传输错误　　D. 传输丢失

3. 美国的橘黄皮书中为计算机安全的不同级别制定了（　）级标准，它们从高到低依次是（　）级。

A. 4，DCBA　　B. 4，ABCD　　C. 3，CBA　　D. 3，ABC

4. 保护数据不被未授权者修改、建立、嵌入、删除、重复传送或由于其他原因使原始数据被更改是（　）。

A. 数据的机密性　　B. 访问的控制性

C. 数据的认证性　　D. 数据的完整性

5. HTTPS 是使用（　）的 HTTP。

A. SSL　　B. SSH　　C. Security　　D. TCP

（二）多项选择题

1. 组成电子商务的技术要素主要有（　）。

A. 网络　　B. 应用软件　　C. 硬件

D. 商品　　E. 仓库

2. 几种常见的电子商务模式（　）。

A. 大字报/告示牌模式　　B. 在线黄页簿模式

C. 电脑空间上的小册子模式　　D. 虚拟百货店模式

E. 广告推销模式

3. 保证商务数据机密性的手段主要是（　）。

A. 数据加密　　B. 身份认证　　C. 数字签名

D. 信息隐匿　　E. 数字水印

4. 电子商务系统可能遭受的攻击有（　）。

A. 系统穿透　　B. 违反授权原则　　C. 植入

D. 通信监视　　E. 病毒

（三）名词解释

1. 电子商务；　　2. EDI；

3. BtoB；　　4. BtoC；

5. NCSC；　　6. Intranet；

7. Extranet；　　8. 商务数据的机密性；

9. 邮件炸弹；　　10. TCP 劫持入侵；

11. 主动攻击；　　12. 被动攻击；

13. HTTP 协议的“无记忆状态”。

（四）简答题

1. 什么是保持数据完整性？

2. 网页攻击的步骤是什么？

3. 什么是 Intranet？

4. 为什么交易的安全性是电子商务独有的？

5. 攻击 Web 站点有哪几种方式？

6. Web 客户机和 Web 服务器的任务分别是什么？

7. IP 地址顺序号预测攻击的步骤是什么？

8. 普通电子邮件的两个方面的安全问题是什么？由什么原因造成的？

9. 电子商务安全的六项中心内容是什么？

三、练习题参考答案

（一）单项选择题

1. D　　2. A　　3. B　　4. D　　5. A

（二）多项选择题

1. A，B，C　　2. A，B，C，D，E　　3. A，D　　4. A，B，C，D

（三）名词解释

1. 电子商务：顾名思义，是建立在电子技术基础上的商业运作，是利用电子技术加强、加快、扩展、增强、改变了其有关过程的商务。

2. EDI：电子数据交换（EDI，Electronic Data Interchange）是第一代电子商务技术，实现 BtoB 方式交易。

3. BtoB：企业机构间的电子商务活动。

4. BtoC：企业机构和消费者之间的电子商务活动。

5. NCSC：美国国家计算机安全中心（The National Computers Security Center）是美国国家安全局 NSA（National Security Agency）的一个分支机构，NCSC 为政府购买的计算机设立了安全等级。

6. Intranet：是指基于 TCP/IP 协议的企业内部网络，它通过防火墙或其他安全机制与 Internet 建立连接。Intranet 上提供的服务主要面向的是企业内部。

7. Extranet：是指基于 TCP/IP 协议的企业外域网，它是一种合作性网络。

8. 商务数据的机密性：商务数据的机密性（Confidentiality）或称保密性是指信息在网络上传送或存储的过程中不被他人窃取、不被泄露或披露给未经授权的人或组织，或者经过加密伪装后，使未经授权者无法了解其内容。

9. 邮件炸弹：是攻击者向同一个邮件信箱发送大量的（成千上万个）垃圾邮件，以堵塞该邮箱。

10. TCP 劫持入侵：是对服务器的最大威胁之一，其基本思想是控制一台连接于入侵目标网的计算机，然后从网上断开，让网络服务器误以为黑客就是实际的客户端。

11. 主动攻击：是攻击者直接介入 Internet 中的信息流动，攻击后，被攻击的通信双

方可以发现攻击的存在。

12. 被动攻击：是攻击者不直接介入 Internet 中的信息流动，只是窃听其中的信息。被动攻击后，被攻击的通信双方往往无法发现攻击的存在。

13. HTTP 协议的“无记忆状态”：即服务器在发送给客户机的应答后便遗忘了此次交互。Telnet 等协议是“有记忆状态”的，它们需记住许多关于协议双方的信息、请求与应答。

（四）简答题

1. 什么是保持数据完整性？

商务数据的完整性（Integrity）或称正确性是保护数据不被未授权者修改、建立、嵌入、删除、重复传送或由于其他原因使原始数据被更改。在存储时，要防止非法篡改，防止网站上的信息被破坏。在传输过程中，如果接收端收到的信息与发送的信息完全一样则说明在传输过程中信息没有遭到破坏，具有完整性。加密的信息在传输过程，虽能保证其机密性，但并不能保证不被修改。

2. 网页攻击的步骤是什么？

第一步，创建一个网页，看似可信其实是假的拷贝，但这个拷贝和真的“一样”：假网页有与真网页一样的页面和链接。

第二步，攻击者完全控制假网页。所以浏览器和网络间的所有信息交流都经过攻击者。

第三步，攻击者利用网页做假的后果：攻击者记录受害者访问的内容，当受害者填写表单发送数据时，攻击者可以记录下所有数据。此外，攻击者可以记录下服务器响应回来的数据。这样，攻击者可以偷看到许多在线商务使用的表单信息，包括账号、密码和秘密信息。

如果需要，攻击者甚至可以修改数据。不论是否使用 SSL 或 S－HTTP，攻击者都可以对链接做假。换句话说，就算受害者的浏览器显示出安全运行链接图标，受害者仍可能链接在一个不安全链接上。

3. 什么是 Intranet？

Intranet 是指基于 TCP/IP 协议的内连网络。它通过防火墙或其他安全机制与 Internet 建立连接。Intranet 上可以提供所有 Internet 的应用服务，如 WWW，E-mail 等，只不过服务面向的是企业内部。和 Internet 一样，Intranet 具有很高的灵活性，企业可以根据自己的需求，利用各种 Internet 互联技术建立不同规模和功能的网络。

4. 为什么交易的安全性是电子商务独有的？

这也是电子商务系统所独有的。在我们的日常生活中，进行一次交易必须办理一定的手续，由双方签发各种收据凭证，并签名盖章以作为法律凭据。但在电子商务中，交易在网上进行，双方甚至不会见面，那么一旦一方反悔，另一方怎样能够向法院证明合同呢？这就需要一个网上认证机构对每一笔业务进行认证，以确保交易的安全，避免恶意欺诈。

5. 攻击 Web 站点有哪几种方式？

安全信息被破译：Web 服务器的安全信息，如口令、密钥等被破译，导致攻击者进入 Web 服务器。浏览器的强大功能，可以以不同形式访问 Web 站点的数据，这不仅为用

户，同时也为攻击者打开了许多方便之门。攻击者试图在内部网上获取信息或利用计算机资源。因此，必须保护 Web 站点，防止闯入者的袭击。最常见，也是最有效的保护是使用防火墙。

非法访问：未授权者非法访问了 Web 上的文件，损害了电子商务中的隐私性、机密性和完整性。

交易信息被截获：当用户向服务器传输交易信息（如商贸数据或信用卡信息）时被截获。

软件漏洞被攻击者利用：系统中的软件错误，使得攻击者可以对 Web 服务器发出指令，致使系统被修改和损坏，甚至引起整个系统的崩溃。

当用 CGI 脚本编写的程序或其他涉及到远程用户从浏览器中输入表格并进行像检索之类在主机上直接操作命令时，会给 Web 主机系统造成危险。

6. Web 客户机和 Web 服务器的任务分别是什么？

Web 客户机的任务是：

（1）为客户提出一个服务请求——超链时启动；

（2）将客户的请求发送给服务器；

（3）解释服务器传送的 HTML 等格式文档，通过浏览器显示给客户。

Web 服务器的任务是：

（1）接收客户机来的请求；

（2）检查请求的合法性；

（3）针对请求，获取并制作数据，包括使用 CGI 脚本等程序、为文件设置适当的 MIME 类型来对数据进行前期处理和后期处理；

（4）把信息发送给提出请求的客户机。

7. IP 地址顺序号预测攻击的步骤是什么？

黑客进行 TCP/IP 顺序号预测攻击分两步：

首先，得到服务器的 IP 地址。黑客一般通过网上报文嗅探，顺序测试号码，由 Web 浏览器连接到结点上并在状态栏中寻找结点的 IP 地址。因为黑客知道其他计算机有一个与服务器 IP 地址部分公用的 IP 地址，他便致力模拟一个能通过路由器，作为网络用户访问系统的 IP 号码。例如，如果系统的 IP 地址为 200. 0. 0. 20，黑客便知这是一个 C 级网，最多有 255 台计算机可以连入一个 C 级网，并猜出所有最后位在序列中出现过的地址号码：200. 0. 0. 1 至 200. 0. 0. 254。

然后，攻击者在试过这些 IP 地址后，可以开始监视网上传送包的序列号，推测服务器能产生的下一个序列号，再将自己有效地插入到服务器和用户之间。因为有了服务器的 IP 地址，就能产生有正确 IP 地址和顺序码的包裹以截获用户信息的传递，攻击者开始模仿 IP 地址及包裹序列号以愚弄服务器，使之成为受到信任的合法网络用户。接着，便可访问系统传给服务器的密钥文件、日志名、机密数据等信息。

8. 普通电子邮件的两个方面的安全问题是什么？由什么原因造成的？

电子邮件的安全问题主要有两个方面：一是电子邮件在网上传送时随时可能被人窃取到，而邮件是用 ASCII 字符写的，所以谁都可以读懂内容；二是可以冒用别人的身份发信，因为邮件的发送地址等信息通常由用户自己填写，并且整个信头都是可以伪造的。

使用一个“探测程序”就可以阅读电子邮件信息。

9. 电子商务安全的六项中心内容是什么?

(1) 商务数据的机密性 (Confidentiality) 或称保密性是指信息在网络上传送或存储的过程中不被他人窃取、不被泄露或披露给未经授权的人或组织，或者经过加密伪装后，使未经授权者无法了解其内容。

(2) 商务数据的完整性 (Integrity) 或称正确性是保护数据不被未授权者修改、建立、嵌入、删除、重复传送或由于其他原因使原始数据被更改。

(3) 商务对象的认证性 (Authentication) 是指网络两端的使用者在沟通之前相互确认对方的身份。

(4) 商务服务的不可否认性 (Non-repudiation) 是指信息的发送方不能否认已发送的信息，接收方不能否认已收到的信息，这是一种法律有效性要求。

(5) 商务服务的不可拒绝性 (Denial of service) 或称可用性是保证授权用户在正常访问信息和资源时不被拒绝，即保证为用户提供稳定的服务。

(6) 访问的控制性 (Access control) 是指在网络上限制和控制通信链路对主机系统和应用的访问：用于保护计算机系统的资源 (信息、计算和通信资源) 不被未经授权人或以未授权方式接入、使用、修改、破坏、发出指令或植入程序等。

第二章　电子商务安全需求与密码技术

一、要点提示

本章主要包含四大部分内容：电子商务的安全需求，密码技术，密钥管理，密码系统的理论安全性与实用安全性。第一部分内容阐述电子商务过程中七方面的安全因素，要理解真实性、完整性、有效性、不可抵赖性在电子商务中的含义，了解其必要性。第二部分内容有三个要点：一是理解数据加密的基本概念，了解加密对保证数据机密性的作用；二是了解替换加密、转换加密原理，掌握单密钥加密和双钥加密的方法和特点；三是熟悉几种加密算法，如 DES，RSA 等。第三部分内容有四个要点：一是了解密钥的分类，多层次密钥系统的意义；二是理解集中式密钥分配方案和分布式密钥分配方案及其特点；三是掌握 Diffie-Hellman 密钥分配协议。四是了解 Shamir 密钥分存的基本思想。第四部分要了解理论安全性和计算安全性的实际意义。

本章共分四节。

第一节　电子商务的安全需求。电子商务安全是一个复杂的系统问题，在使用电子商务的过程中会涉及到可靠性、真实性、机密性、完整性、有效性、不可抵赖性和内连网的严密性等几个有关安全方面的因素。可靠性是指电子商务系统的可靠性，电子商务系统也就是计算机系统，其可靠性是指为防止由于计算机失效、程序错误、传输错误、硬件故障、系统软件错误、计算机病毒和自然灾害等所产生的潜在威胁，并加以控制和预防，确保系统的安全可靠性。真实性是指商务活动中交易者身份的真实性，亦即是交易双方确实是存在的，不是假冒的。机密性是指交易过程中必须保证信息不会泄露给非授权的人或实体。完整性是指数据在输入和传输过程中，要求能保证数据的一致性，防止数据被非授权建立、修改和破坏。在电子商务中，必须保证贸易数据在确定价格、期限、数量以及确定时间、地点时是有效的。在传统的纸面贸易中，贸易双方通过在交易合同、契约或贸易交易所的书面文件上的手写签名或印章来鉴别贸易伙伴，确定合同、契约、交易所的可靠性，并预防抵赖行为的发生。在电子商务方式下，通过手写签名和印章进行双方的鉴别已是不可能的了。因此，要求在交易信息的传输过程中为参与交易的个人、企业或国家提供可靠的标识，使原发送方在发送数据后不能抵赖；接收方在接收数据后也不能抵赖。

对于内连网，一方面网内有着大量需要保密的信息，另一方面传递着企业内部的大量指令，控制着企业的业务流程。内连网一旦被恶意侵入，可能给企业带来极大的混乱与损失。因此，保证内连网不被侵入，也是开展电子商务的企业应着重考虑的一个安全问题。

第二节　密码理论。本节介绍了早期的简单加密和现代加解密方法。首先介绍了密码理论的几个基本概念，替换加密和转换加密的基本思路和方法，详细阐述了单密钥加

密和公钥密码体制。在单密钥密码体制中，介绍了 DES，IDEA，RC-5 和 AES。公钥密码体制中介绍了 RSA，ELGamal，椭圆曲线密码体制（ECES）。

第三节　密钥管理。本节讲述了密钥的设置、分配、分存和托管技术。从密钥的概念和种类，到分配和托管都作了详细的阐述。重点讲述了 Diffie-Hellman 密钥交换协议。

第四节　密码系统的理论安全性与实用安全性。

本章的基本概念有：（1）明文；（2）密文；（3）加密；（4）解密；（5）加密算法；（6）解密算法；（7）替换加密；（8）转换加密；（9）单钥密码体制；（10）双钥密码体制；（11）密钥；（12）主密钥；（13）密钥管理中心；（14）无条件安全；（15）计算上安全。

本章的基本理论有：（1）电子商务安全因素；（2）替换加密；（3）转换加密；（4）单钥密码体制；（5）双钥密码体制；（6）密钥分配；（7）密钥分存。

本章的基本知识有：（1）替换加密，转换加密；（2）单钥密码体制；（3）DES 加密算法；（4）双钥密码体制；（5）RSA 算法；（6）Diffie-Hellman 密码交换协议；（7）多层次密钥系统；（8）密钥的分存；（9）密钥托管；（10）密码系统的安全性。

本章的重点问题有：替换加密和转换加密；单钥密码体制及 DES 加密算法；双钥密码体制及 RSA 算法；密钥分配及 Diffie-Hellman 协议。

本章的考核点是：电子商务安全因素；替换加密和转换加密；单钥密码体制的特点，掌握 DES 加密算法，了解其它算法；双钥密码体制特点，RSA 算法；密钥分配及 Diffie-Hellman 协议的思想，密钥分存，密码系统的安全性。

二、练习题

（一）单项选择题

1. IDEA 加密算法首先将明文分为（　）位的数据块，然后进行（　）轮迭代和一个输出变换。

A. 64，8　　B. 64，16

C. 128，8　　D. 128，16

2. IDEA 的输入和输出都是（　）位，密钥长度为（　）位。

A. 128，128　　B. 64，64

C. 128，64　　D. 64，128

3. DES 的加密运算法则是：每次取明文中的连续 64 位（二进制位，以下同）数据，利用（　）位密钥，经过 16 次循环（每一次循环包括一次替换和一次转换）加密运算，将其变为（　）位的密文数据。

A. 56，64　　B. 64，64

C. 128，128　　D. 16，32

4. 收发双方持有不同密钥的是（　）体制。

A. 对称密钥　　B. 数字签名

C. 公钥　　D. 完整性

5. 现在常用的密钥托管算法是（　）算法。

A. EES　　B. Skipjack

C. Diffie-Hellman　　D. RSA

（二）多项选择题

1. 双钥密码体制算法的特点是（　）。

A. 算法速度慢　　B. 只适合加密小数量的信息

C. 适合密钥的分配　　D. 适合密钥的管理

E. 算法速度快

2. 一种加密体制采用不同的加密密钥和解密密钥，两密钥间存在一种函数关系，这种加密体制是（　）。

A. 双密钥加密　　B. 单密钥加密

C. 替换加密　　D. 转换加密

E. 未加密

3. 按密码学的观点，一个密码系统的安全性取决于（　）。

A. 密匙的保密　　B. 算法的保密　　C. 公匙的保密

D. 加密协议　　E. 密钥长度

4. 某加解密算法使用两个密钥，该算法可能是（　）。

A. 双密钥加密　　B. 双重 DES

C. 单密钥加密　　D. 三重 DES

（三）名词解释

1. 明文；　　2. 密文；

3. 加密；　　4. 解密；

5. 加密算法；　　6. 解密算法；

7. 密钥；　　8. 主密钥；

9. 无条件安全；　　10. 计算上安全；

11. 多字母加密；　　12. 单钥密码体制；

13. 双钥密码体制。

（四）简答题

1. 电子商务的可靠性的含义指什么？

2. 电子商务的真实性的含义指什么？

3. 单钥密码体制的特点是什么？

4. 简述替换加密和转换加密的区别。

5. 什么是双钥密码体制？

6. 什么是集中式密钥分配？

7. 什么是分布式密钥分配？

8. Shamir 密钥分存思想是什么？

9. 双钥密码体制最大的特点是什么？

10. 试述双钥密码体制的加密和解密过程。

11. 替换加密和转换加密的主要区别是什么？

12. 列举单钥密码体制的几种算法。

13. 简述 DES 的加密运算法则。

14. 什么是双重 DES 加密方法？简述其算法步骤。

15. 什么是三重 DES 加密方法？简述其算法步骤。

16. 简述 IDEA 加密算法的基本运算、设计思想及加密过程。

17. 简述两类典型的自动密钥分配途径。

（五）论述题

1. 试用 Ceasar 算法加密 newspaper，假设密钥 Key = 4，写出加密过程和密文 C。

2. 取两个素数为 7 和 17，根据 RSA 密码体制公式，构成一组公钥和私钥。如果明文为 15，e 取 5，则密文是什么值？

3. RSA 加密算法中密钥的计算方法。

4. 简述密码系统的理论安全性与实用安全性？

5. 试述双钥密码体制的加密和解密过程及其特点？

6. 试述椭圆曲线密码体制（ECC）加密解密过程。

7. Shamir 针对什么问题提出了解决方案。试述 Shamir 密钥的分存思想？

三、练习题参考答案

（一）单项选择题

1. A　　2. D　　3. B　　4. C　　5. A

（二）多项选择题

1. A，B，C，D　　2. B　　3. A　　4. A，B，C

（三）名词解释

1. 明文：原始的、未被伪装的消息称做明文，也称信源。通常用 M 表示。

2. 密文：通过一个密钥和加密算法将明文变换成的一种伪装信息，称为密文。通常用 C 表示。

3. 加密：就是用基于数学算法的程序和加密的密钥对信息进行编码，生成别人难以理解的符号，即把明文变成密文的过程。通常用 E 表示。

4. 解密：由密文恢复成明文的过程，称为解密。通常用 D 表示。

5. 加密算法：对明文进行加密所采用的一组规则，即加密程序的逻辑称做加密算法。

6. 解密算法：消息传送给接收者后，要对密文进行解密时所采用的一组规则称做解密算法。

7. 密钥：加密和解密算法的操作通常都是在一组密钥的控制下进行的，分别称作加密密钥和解密密钥。通常用 K 表示。

8. 主密钥：多层次密钥系统中，最高层的密钥也叫作主密钥。

9. 无条件安全：若它对于拥有无限计算资源的破译者来说是安全的，则称这样的密码体制是无条件安全的。

10. 计算上安全：如若一个密码体制对于拥有有限计算资源的破译者来说是安全的，则称这样的密码体制是计算上安全的，计算上安全的密码表明破译的难度很大。

11. 多字母加密：是使用密钥进行加密。密钥是一组信息（一串字符）。同一个明文经过不同的密钥加密后，其密文也会不同。