

湖南省高等教育自学考试

课程考试大纲

移动商务安全

(课程代码: 12255)

湖南省教育考试院组编
2016 年 12 月

高等教育自学考试课程考试大纲

课程名称：移动商务安全

课程代码：12255

第一部分 课程性质与目标

一、课程性质与特点

（一）本课程的性质

移动商务安全是高等教育自学考试电子商务（移动商务管理方向）（本科）专业的专业核心课程。课程主要介绍目前电子商务安全所涉及到的主要技术，主要内容包括：电子商务安全的目标和体系结构、密码技术、数字技术、人证技术、密钥管理技术、网络安全技术、常用的安全协议标准和 PKI 技术、移动商务安全技术等内容。

（二）课程特点

本课程是电子商务专业的专业核心课程。移动商务安全技术是计算机软件技术、硬件技术、网络技术、通信技术、数据库技术和信息安全技术等的应用技术。本课程主要讲授移动电子商务安全的基本概念、基本理论、基本方法和实用技术等。通过本课程的学习，掌握移动电子商务安全的关键技术，学习计算机网络、数据库、信息安全理论和技术在电子商务安全中的综合应用方法，掌握移动电子商务安全系统分析设计的基本方法。

二、课程目标与基本要求

（一）课程目标：移动商务安全是一门综合性的课程，通过本课程的学习，考生应能够系统地学习和掌握电子商务安全的关键技术，掌握电子商务安全系统分析设计的基本方法。

通过本课程的学习，考生应对电子商务中将会遭遇的各种安全风险有一个清醒的认识，知道怎样通过制定安全标准、安全政策和安全管理措施来对电子商务的安全问题进行管理；深入理解网络安全与电子商务的基本理论；掌握网络安全与电子商务的基本方法；在电子商务中能熟练运用网络安全技术。通过课程的学习，能够担负电子商务系统的安全管理工作。

（二）基本要求：

要求考生了解加密技术、数字签名技术等基本的信息安全技术；掌握电子商务所采用的各种安全协议，尤其是安全套接层协议 SSL 和安全电子交易协议 SET 的作用及其应用；明确数字证书的格式、制作、以及 CA 认证中心在保障电子商务安全中的地位与作用，同时结合实际掌握 1-2 种数字证书的申请和使用方法。

1. 知识要求

- （1）了解电子商务安全的基本常识；
- （2）掌握电子商务安全的目标和体系结构；

- (3) 掌握电子商务安全涉及的基本技术;
- (4) 了解电子商务安全常用的安全协议标准和 PKI 技术—移动商务安全技术。
- 2. 素质要求
 - (1) 敬业精神: 树立敬业精神;
 - (2) 团队精神: 电子商务安全是一门综合性技术, 必须具有很强的合作团队精神;
 - (3) 保密意识: 良好的保密意识, 是做好电子商务安全的前提;
 - (4) 较强的技术应用能力: 电子商务安全的关键在于网络技术与电子商务技术的完美结合。
- 3. 能力技能要求
 - (1) 网络操作能力;
 - (2) 网络应用能力;
 - (3) 网络技术开发能力;
 - (4) 网络技术创新能力;

三、与本专业其他课程的关系

本课程的先修课程为电子商务概论、计算机网络等。本课程与移动商务技术和移动商务管理有共通之处, 也有其专业特点, 鉴于电子商务安全的操作性比较强, 理论讲解比较枯燥, 建议该课程配合较多的实训课来完成教学。

第二部分 考核内容与考核目标

第一章 概述

一、学习目的与要求

移动电子商务的安全问题已经成为影响移动电子商务发展的重要因素。通过本章的学习, 了解移动电子商务安全的基本需求、移动电子商务安全的主要技术及其安全体系结构, 为进入以后各章具体内容的学习提供必要的引导。重点是了解移动电子商务安全的需求现状及安全技术。

二、考核知识点与考核目标

- (一) 移动电子商务的安全需求 (重点)
 - 识记: 移动电子商务的特点
 - 理解: 移动电子商务的现状
- (二) 移动电子商务的安全体系结构 (一般)
 - 识记: 移动电子商务的安全体系结构
 - 理解: 面临的安全问题
- (三) 移动电子商务技术基础 (一般)
 - 识记: 移动电子商务主要相关技术
- (四) 移动电子商务的安全 (重点)
 - 识记: 有线网络和移动网络的安全比较
 - 理解: 移动商务安全主要相关技术

第二章 移动电子商务的安全协议和标准

一、学习目的与要求

因特网上电子商务的进行需要明确参与交易各方的身份，保证网上传输信息的安全。通过本章的学习，了解移动电子商务对比传统商务的优点，了解移动电子商务对安全性提出的更高要求。重点是了解目前应用广泛的移动电子商务安全协议和标准。

二、考核知识点与考核目标

（一）无线应用协议（次重点）

识记：（1）WAP 的特点；（2）WAP 的安全实现模型

（二）WPKI 体系（次重点）

识记：WPKI 技术及其现状

理解：（1）WPKI 技术的应用；（2）WPKI 技术的发展趋势

（三）蓝牙技术（次重点）

识记：蓝牙技术的优势

理解：（1）蓝牙的应用；（2）蓝牙的安全机制

（四）3G 系统的安全体系（重点）

识记：（1）移动通信系统的主要安全威胁；（2）3G 系统的安全体系

理解：（1）3G 系统的防范策略；（2）3G 系统安全的发展方向

第三章 移动电子商务的基础

一、学习目的与要求

通过本章的学习，了解移动电子商务的安全隐患，移动电子商务的安全要求，从多个层次了解移动电子商务的安全保障。重点了解无线网络安全隐患和无线移动设备存在的安全问题。

二、考核知识点与考核目标

（一）移动电子商务的安全隐患（重点）

理解：多方面造成的安全威胁

（二）移动电子商务的安全原则（次重点）

识记：授权、完整性、保密性、可靠性和可用性等安全要求

（三）移动电子商务的安全保障（次重点）

识记：（1）管理措施；（2）法律措施；（3）技术措施

（四）无线网络安全隐患（一般）

识记：（1）网络本身的威胁；（2）无线应用的威胁；（3）网络漫游的威胁；

（4）物理威胁

（五）无线移动设备的安全问题（重点）

理解：无线移动设备面临的六个主要安全问题

第四章 信誉和信任模型

一、学习目的与要求

网络安全问题日益严重，提出一种基于社会网络的具有抗攻击能力的信誉与信任模型是很有必要的。通过本章的学习，了解信誉和信任模型的应用和安全场景，着重了解基于 PKI 的信任模型的结构模型以及这个模型的应用实例。同时还应了解信息加密和个人隐私在移动电子商务信息加密技术中的应用。

二、考核知识点与考核目标

（一）应用和安全场景（一般）

识记：（1）信誉模型和信任模型的应用背景；（2）信誉和信任模型的安全性

理解：信誉与信任模型的基本概念

（二）信任模型（重点）

理解：（1）创建信任模型的相关问题；（2）典型信任模型

应用：（1）移动电子商务中信息加密技术应用实例；（2）基于 PKI 的信任模型应用实例

（三）信誉模型（次重点）

识记：信誉模型的核心内容

理解：信誉模型与信任模型的关系

应用：常见信誉模型

（四）信息加密和个人隐私（一般）

识记：信息加密和个人隐私产生的背景

理解：信息加密的常用方法

应用：应用实例

第五章 入侵检测和攻击分析

一、学习目的与要求

入侵检测技术作为一种主动的安全技术，成为目前安全网络技术研究的热点。通过本章的学习，了解入侵检测的原理和方法、分布式入侵检测模型、移动防火墙。在此基础上还应了解无线接入控制技术中的特点和手机病毒相关知识与防范方法。

二、考核知识点与考核目标

（一）入侵检测原理和方法（重点）

识记：入侵检测的定义

理解：IDS 的评价标准

应用：入侵检测技术

（二）分布式无线入侵检测模型（一般）

识记：基本概念

理解：系统结构

- 应用：系统部署
- (三) 移动防火墙（次重点）
 - 识记：来电防火墙
 - 理解：短信防火墙
 - 应用：手机网络防火墙
- (四) 网络接入控制（一般）
 - 识记：无线接入控制技术及其特点
 - 理解：无线网络中接入控制技术的研究热点
- (五) 手机病毒（次重点）
 - 识记：（1）手机病毒概述；（2）手机病毒发展趋势
 - 理解：手机漏洞分析
 - 应用：手机病毒的防范

第六章 基于策略的访问控制

一、学习目的与要求

本章从技术实现的角度介绍了基于策略的访问控制模型。通过本章的学习，了解访问控制技术的作用，访问控制系统的组成，现有的访问控制模型。同时，也应了解访问策略的特点和移动中间件相关概念。

二、考核知识点与考核目标

- (一) 访问控制概述（重点）
 - 识记：（1）什么是访问控制；（2）访问控制的分类
 - 理解：（1）访问控制的系统组成；（2）访问控制的基本原则
- (二) 访问控制技术及其安全（一般）
 - 理解：（1）自主访问控制；（2）强制访问控制；（3）基于角色的访问控制
- (三) 访问策略（次重点）
 - 识记：（1）策略的定义；（2）策略的一般特性
 - 理解：（1）共有特性；（2）安全属性；（3）安全规则
- (四) 移动中间件（一般）
 - 识记：（1）远程过程调用；（2）面向消息的中间件；（3）对象请求代理；（4）事物处理监控
 - 理解：面临的一些问题

第七章 基于 XML 的信任沟通模型

一、学习目的与要求

本章主要介绍了基于 XML 的信任沟通模型。通过本章的学习，需要了解信任关系的性质，了解目前存在的几种信任关系模型，了解信任_X 协商的几个阶段。

二、考核知识点与考核目标

(一) 信任沟通模型的基本概念 (重点)

识记: 信任协商

理解: 信任关系的性质

(二) 信任沟通模型 (次重点)

识记: 信任模型概述

理解: 信任模型的研究现状

(三) 信任沟通语言 (一般)

识记: X_TNL 信任沟通语言概述

理解: 信任_X 的协商过程

应用: 信任_X 的合成资源的协商

第八章 基于代理模型的移动电子商务安全问题

一、学习目的与要求

本章主要介绍了基于代理模型的移动电子商务安全问题。通过本章的学习,应该了解移动代理技术的主要内容。了解移动代理的性质、应用领域,包括移动 Agent 系统存在的安全问题及其相应的解决方法。重点了解基于移动代理技术的交易模型设计。

二、考核知识点与考核目标

(一) 移动代理技术概述 (次重点)

识记: 移动代理技术

理解: (1) 移动 Agent 系统的组成; (2) 移动 Agent 技术的优势

(二) 移动代理技术的应用 (重点)

识记: 应用现状

应用: 基于移动代理技术的交易模型设计

(三) 移动代理技术的安全问题 (一般)

识记: 移动 Agent 通信的安全保护

理解: 保护主机

应用: 保护移动 Agent

第九章 安全多播移动电子商务的问题和挑战

一、学习目的与要求

通过本章的学习需要了解基于安全多播移动电子商务安全的相关知识。了解多播的基本概念,多播的必要性,了解多播数据路由和多播路由协议,重点学习基于移动网络的多播路由协议。同时,还需要了解多播的安全风险、多播应用对安全的具体要求和影响多播组安全的因素。

二、考核知识点与考核目标

(一) 多播概述 (次重点)

- 识记：多播的基本概念
- 理解：网络中多播的必要性
- (二) 多播路由（重点）
 - 识记：多播数据路由
 - 理解：多播路由协议
 - 应用：移动网络多播路由协议
- (三) 多播安全问题（次重点）
 - 识记：(1) 多播的安全风险；(2) 多播应用的安全要求；(3) 影响多播组安全的因素

第十章 支付系统和欺诈管理

一、学习目的与要求

移动电子商务的发展离不开完善的支付方式和支付手段。本章首先了解移动支付的概念，在此基础上通过对移动市场进行合理细分，了解基于金融机构发行的卡支付、移动运营商运作的手机支付、第三方提供的卡支付、第三方提供的手机支付四种移动支付方式，并重点了解一种以移动运营商为核心的移动电子商务安全支付方式。

二、考核知识点与考核目标

- (一) 移动支付方案（重点）
 - 识记：移动支付概述
 - 理解：移动支付方式的分类
 - 应用：一种移动电子商务安全支付方案
- (二) 欺诈管理系统（一般）
 - 识记：欺诈概述
 - 理解：防欺诈系统分析
 - 应用：康柏欺诈管理系统案例
- (三) 多方小额支付方法（重点）
 - 识记：(1) 小额支付的现状；(2) 小额支付的特点；(3) 小额支付的应用领域
 - 理解：小额支付模型
 - 应用：小额支付方案
- (四) 多方小额支付系统（次重点）
 - 理解：小额支付系统的实现方式
 - 应用：移动小额支付系统主要的几种实现方式对比

第十一章 移动数字签名

一、学习目的与要求

应用移动数字签名技术，并结合信息加密技术，可满足移动电子商务的安全需求。本章需考察 RSA 公钥密码系统、基于椭圆曲线的签名技术、盲签名技术、代理签名体制等数字签名方案，最后对移动数字签名系统进行实例分析。

二、考核知识点与考核目标

（一）数字签名概述（重点）

识记：（1）数字签名定义；（2）数字签名的分类

理解：（1）数字签名的原理；（2）特殊的数字签名方案

（二）移动数字签名需求（一般）

识记：（1）移动数字签名的应用环境；（2）移动数字签名的应用需求

（三）数字签名技术（次重点）

识记：（1）RSA 签名体制；（2）椭圆曲线数字签名方案

理解：（1）RSA 算法基本原理；（2）椭圆曲线数字签名原理；（3）盲签名技术；（4）多代理签名技术

应用：各个数字签名技术的计算与应用

（四）移动数字签名系统实例分析（一般）

理解：系统结构

应用：数字签名过程设计

第三部分 有关说明与实施要求

一、考核的能力层次表述

本大纲在考核目标中，按照“识记”、“理解”、“应用”三个能力层次规定其应达到的能力层次要求。各能力层次为递进等级关系，后者必须建立在前者的基础上，其含义是：

识记：能知道有关的名词、概念、知识的含义，并能正确认识和表述，是低层次的要求。

理解：在识记的基础上，能全面把握基本概念、基本原理、基本方法，能掌握有关概念、原理、方法的区别与联系，是较高层次的要求。

应用：在理解的基础上，能运用基本概念、基本原理、基本方法联系学过的多个知识点分析和解决有关的理论问题和实际问题，是最高层次的要求。

二、教材

1. 指定教材：

移动商务安全，戴宏，对外经济贸易大学出版社，2012 年版

2. 参考教材

姜楠，王健，移动网络安全技术，电子工业出版社，2014 年版

移动应用安全，Himanshu Dwivedi（美），电子工业出版社，2012 年版

三、自学方法指导

1. 在开始阅读指定教材某一章之前，先翻阅大纲中有关这一章的考核知识点

及对知识点的能力层次要求和考核目标，以便在阅读教材时做到心中有数，有的放矢。

2. 阅读教材时，要逐段细读，逐句推敲，集中精力，吃透每一个知识点，对基本概念必须深刻理解，对基本理论必须彻底弄清，对基本方法必须牢固掌握。

3. 在自学过程中，既要思考问题，也要做好阅读笔记，把教材中的基本概念、原理、方法等加以整理，这可从中加深对问题的认知、理解和记忆，以利于突出重点，并涵盖整个内容，可以不断提高自学能力。

4. 完成书后作业和适当的辅导练习是理解、消化和巩固所学知识，培养分析问题、解决问题及提高能力的重要环节，在做练习之前，应认真阅读教材，按考核目标所要求的不同层次，掌握教材内容，在练习过程中对所学知识进行合理的回顾与发挥，注重理论联系实际和具体问题具体分析，解题时应注意培养逻辑性，针对问题围绕相关知识点进行层次（步骤）分明的论述或推导，明确各层次（步骤）间的逻辑关系。

移动商务安全课程内容涉及面较宽，涉及到网络技术、无线网络技术、密码学、网络安全、电子商务等许多方面。考生在自学时往往会感到有一定困难，但自学能力的培养对获取知识是非常必要的。考生在自学过程中应注意如下几个方面：

（1）根据考核要求中的能力层次，在全面系统学习的基础上掌握重点概念和重点问题，注意各章内容之间的内在联系。

（2）本课程的自学考试大纲是自学本课程的主要依据。在自学本课程前应先通读大纲，了解课程的要求，获得课程完整的概况。在开始自学某一章时，先阅读大纲，了解该章的课程内容，考核知识点和考核要求，在自学过程中有的放矢。

（3）阅读指定教材时，要求吃透每个考核知识点。对基本概念要做到深刻理解，对基本原理要弄清弄懂，对基本方法要熟练掌握。

（4）重视每章末的习题的作用，考生需要多做习题，可以检查学习掌握知识的程度。

（5）本课程是一门实践性较强的课程，考生在自学过程中必须注意理论联系实际，按实验的目的、要求和内容认真做好实验。建议实验与课程自学过程同步进行。

（6）考生在自学时要注意基本能力的培养，即系统分析和综合能力，分析问题和理解知识的能力，抓住重点阐述问题的能力，以及实验能力等。

四、对社会助学的要求

1. 应熟知考试大纲对课程提出的总要求和各章的知识点。

2. 应掌握各知识点要求达到的能力层次，并深刻理解对各知识点的考核目标。

3. 辅导时，应以考试大纲为依据，指定的教材为基础，不要随意增删内容，以免与大纲脱节。

4. 辅导时，应对学习方法进行指导，宜提倡“认真阅读教材，刻苦钻研教材，主动争取帮助，依靠自己学通”的方法。

5. 辅导时，要注意突出重点，对考生提出的问题，不要有问即答，要积极启发引导。
6. 注意对考生能力的培养，特别是自学能力的培养，要引导考生逐步学会独立学习，在自学过程中善于提出问题，分析问题，做出判断，解决问题。
7. 要使考生了解试题的难易与能力层次高低两者不完全是一回事，在各个能力层次中会存在着不同难度的试题。
8. 助学学时：本课程共 5 学分，建议总课时 90 学时，其中助学课时分配如下：

章 次	内 容	学 时
第一章	概述	6
第二章	移动电子商务的安全协议和标准	10
第三章	移动电子商务的安全基础	12
第四章	信誉和信任模型	10
第五章	入侵检测和攻击分析	10
第六章	基于策略的访问控制	8
第七章	基于 XML 的信任沟通模型	8
第八章	基于代理模型的移动电子商务安全问题	8
第九章	安全多播移动电子商务的问题和挑战	6
第十章	支付系统和欺诈管理	6
第十一章	移动数字签名	6
合 计		90

五、关于命题考试的若干规定

1. 本大纲各章所提到的内容和考核目标都是考试内容。试题覆盖到章，适当突出重点。
2. 试卷中对不同能力层次的试题比例大致是：“识记”为 30%、“理解”为 40%、“应用” 30%
3. 试题难易程度应合理：易、较易、较难、难比例为 2：3：3：2。
4. 每份试卷中，各类考核点所占比例约为：重点占 60%，次重点占 30%，一般占 10%。
5. 试题类型一般分为：单项选择题、多项选择题、填空题、名词解释题、简答题、应用题。
6. 考试采用闭卷笔试，考试时间 150 分钟，采用百分制评分，60 分合格。

六、题型示例（样题）

一、单项选择题（本大题共■小题，每小题■分，共■分）

在每小题列出的四个备选项中只有一个是符合题目要求的，请将其选出并将“答题卡”上的相应字母涂黑。错涂、多涂或未涂均无分。

1. 无线局域网使用的技术主要是

- A. Wi-Fi B. WCDMA C. GPRS D. 以上都不对

二、多项选择题（本大题共■小题，每小题■分，共■分）

在每小题列出的五个备选项中至少有两个是符合题目要求的，请将其选出并将“答题卡”上的相应字母涂黑。错涂、多涂、少涂或未涂均无分。

1. 手机病毒的传播方式有

- A. 用短信和电话攻击手机本身 B. 利用蓝牙方式传播
C. 利用 MMS 多媒体信息服务方式传播 D. 利用攻击和控制“网关”进行传播
E. 用电话攻击手机本身

三、填空题（本大题共■小题，每小题■分，共■分）

1. 在人类历史上第一次使现代网络信息技术和现代通讯技术最大范围地走出高深、为大众所掌握的是_____。

四、名词解释题（本大题共■小题，每小题■分，共■分）

1. 移动商务

五、简答题（本大题共■小题，每小题■分，共■分）

1. 移动电子商务应用有哪些类型？

六、应用题（本大题共■小题，每小题■分，共■分）

1. 无论基于何种算法的数字签名机制，数字签名都要经历生成证书、认证、数字签名和数据加解密过程，下图所示为数字签名的流程，其中 A、B、C、D 人别表示什么？（图略）