安徽财经大学高等教育自学考试课程

14351《网络支付与安全》（实践） 考试大纲

使用教材：网络支付与安全，徐利敏主编，清华大学出版社 2020 年第 1 版

Ⅰ.课程性质与设置目的

一、课程性质

本课程是电子商务、信息管理与信息系统等本科专业的核心专业课，聚焦网络支付领域的核心理论与安全技术。课程以互联网经济为背景，系统阐述网络支付的体系架构、安全威胁、加密技术、身份认证机制及安全协议等内容，兼具理论深度与实践指导性，是衔接电子商务业务流程与金融安全技术的关键课程。

二、课程目标

- **知识目标：**使学生掌握网络支付的基础理论（如支付系统构成、分类及流程），理解信息加密、完整性校验、身份认证等核心安全技术的原理，熟悉主流安全协议（TLS、SET）的运作逻辑，构建完整的网络支付安全知识体系。
- **能力目标：**培养学生运用安全技术分析实际问题的能力，例如针对网络支付中的信息泄露、交易抵赖等威胁设计解决方案；能够结合行业场景（如 B2C 电商、跨境支付）选择合适的安全协议与技术工具，提升实践应用与创新能力。
- **素养目标：**强化学生对网络支付安全的风险意识，理解支付安全在电子商务生态中的战略地位，培养合规意识与职业道德，使其能够在未来职业中保障支付系统的安全性、可靠性与用户隐私保护，推动行业规范化发展。课程内容与考核要求

Ⅱ.课程内容与考核目标

第一章 电子商务与支付安全

一、学习目的与要求

理解互联网发展对电子商务的支撑作用。

掌握电子商务的分类及支付安全的核心要素。

分析支付安全在电子商务中的重要性。

二、课程内容

（一）互联网发展与电子商务

互联网应用模式（B/S、C/S 等）与发展历程。电子商务的定义、分类（B2B/B2C/C2C 等）与运作模式。

（二） 电子商务与网络支付的关联

支付对电子商务的核心作用，传统支付与网络支付的差异。

（三） 电子商务安全与支付安全

安全威胁类型（窃取、篡改、抵赖等）；安全要素（机密性、完整性、不可否认性）。

三、考核知识点

（一）互联网应用模式的演变；

（二）电子商务分类标准；

（三）支付安全的核心要素及威胁类型。

四、考核要求

识记：互联网发展阶段、电子商务分类。

领会：支付安全对电子商务的影响；安全威胁的具体表现。

应用：分析典型电商场景中的支付安全需求。

第二章 网络支付基础知识

一、学习目的与要求

掌握网络支付的定义、构成及支撑平台。理解网络支付的分类方法及国内外发展现状。

二、课程内容

（一）网络支付的基本理论

定义、产生背景、基本构成（客户、商家、银行、支付网关等）。

（二） 支撑平台

专用网络（EDI）与大众化网络（Internet）的差异与应用场景。

（三） 流程与模式

支付基本流程（订单提交、支付授权、清算结算）；分类（B2C 型、

B2B 型）。

（四） 国内外发展情况

国外信用卡支付体系；国内第三方支付（支付宝、微信支付）的发展特点。

三、考核知识点

（一）网络支付的核心构成要素；

（二）EDI 与 Internet 平台的区别；

（三）国内外网络支付的典型模式(如信用卡支付、第三方支付)。

四、考核要求

识记：网络支付的支撑平台类型；国内外主要支付工具。

领会：B2C 与 B2B 支付模式的差异；第三方支付的优势。

应用：分析某电商平台的支付流程（如京东商城的支付环节）。

第三章 网络支付的安全威胁、需求与解决策略

一、学习目的与要求

识别网络支付的主要安全威胁。理解安全需求（机密性、完整性等）及策略制定原则。

二、课程内容

（一）安全威胁

技术威胁（黑客攻击、病毒感染）；非技术威胁（抵赖、伪造）。

（二） 安全需求

机密性、完整性、身份认证、不可否认性的具体要求。

（三） 解决策略

安全策略制定原则（适用性、动态性）；技术措施（加密、认证）与管理措施。

三、考核知识点

（一）安全威胁的分类与典型案例（如钓鱼网站、数据泄露）。

（二）安全需求与策略的对应关系。

四、考核要求

识记：常见安全威胁类型；安全需求的核心要素。

领会：安全策略制定的逻辑框架；技术措施与管理措施的协同作用。

应用：针对某威胁（如账户被盗）设计解决方案。

第四章 网络支付系统安全与网络安全

一、学习目的与要求

掌握防火墙、入侵检测、病毒防范的原理与应用。

理解网络安全技术在支付系统中的具体实施。

二、课程内容

（一）防火墙技术

原理、类型（包过滤、应用网关）；配置方式（防火墙内 / 外部署）。

（二） 入侵检测技术（IDS）

基于主机 / 网络的检测原理；误判类型（正误判、负误判）。

（三） 计算机病毒防范

病毒特点、分类；网络病毒的防范措施（如加密传输、定期杀毒）。

三、考核知识点

（一）防火墙的核心功能与局限性；

（二）IDS 的工作流程；

（三）病毒传播途径与防范策略。

四、考核要求

识记：防火墙类型；病毒的主要特征。

领会：防火墙与 IDS 的协同防御机制；病毒防范的技术手段。

应用：设计企业网络支付系统的防火墙配置方案。

第五章 信息加密技术

一、学习目的与要求

理解对称加密与非对称加密的原理及应用场景。

掌握数字信封技术的综合应用。

二、课程内容

（一） 对称密钥密码技术（如 DES、AES）

原理（加密 / 解密同一密钥）、优缺点（效率高但密钥管理复杂）。

（二） 非对称密钥密码技术（如 RSA）

公钥 / 私钥对的生成与应用；数字签名的实现流程。

（三） 数字信封技术

结合对称与非对称加密，确保密钥安全传输。

三、考核知识点

（一）DES 与 RSA 算法的核心差异；

（二）数字信封的加密流程；

（三）加密技术在支付信息传输中的应用。

四、考核要求

识记：对称 / 非对称加密的代表算法；数字信封的组成。

领会：公钥加密在身份认证中的作用；数字信封的安全性优势。

应用：描述信用卡信息加密传输的技术流程。

第六章 数据的完整性技术

一、学习目的与要求

掌握数字摘要、数字签名的原理与实现。

理解双重签名在多方交易中的应用。

二、课程内容

（一）数字摘要技术（如 MD5、SHA）

单向哈希算法原理；摘要值的验证流程。

（二）数字签名技术

结合 RSA 算法实现签名与验证；不可否认性的技术实现。

（三） 双重签名与数字时间戳

双重签名在 SET 协议中的应用；时间戳在防抵赖中的作用。

三、考核知识点

（一）哈希算法的核心作用；数字签名与摘要的关系。

（二）双重签名的适用场景（如客户 - 商家 - 银行三方交易）。

四、考核要求

识记：MD5/SHA 的摘要长度；数字签名的构成要素。

领会：双重签名如何保护用户隐私；时间戳的技术实现。

应用：设计订单信息与支付信息的双重签名流程。

第七章 身份认证技术

一、学习目的与要求

掌握基于知识、硬件、生物特征的认证方法。

理解数字证书与 PKI 体系的运作机制。

二、课程内容

（一） 认证方法分类

What you know（密码）、What you have（智能卡）、What you are（指纹 / 虹膜）。

（二） 数字证书与认证机构（CA）

证书内容（公钥、有效期、CA 签名）；CA 的核心功能（签发、吊销证书）。

（三） 公钥基础设施（PKI）

组成（CA、RA、证书库）；PKI 在支付系统中的信任链构建。

三、考核知识点

（一）生物识别技术的类型与安全性；

（二）CA 在证书体系中的作用；

（三）PKI 的核心组件与信任传递机制。

四、考核要求

识记：身份认证的三类方法；数字证书的基本字段。

领会：CA 如何确保证书的可信度；PKI 与支付安全的关系。

应用：描述用户申请数字证书的流程及安全要点。

第八章 网络支付安全协议

一、学习目的与要求

掌握 TLS 与 SET 协议的流程与适用场景。

比较两者的安全性差异。

二、课程内容

（一）传输层安全协议（TLS）

握手流程（客户端 / 服务器认证、密钥协商）；应用场景（HTTPS 加密）。

（二） 安全电子交易协议（SET）

参与方（持卡人、商家、支付网关）；交易流程（订单请求、支付授权）。

（三） TLS 与 SET 的对比

安全性（SET 支持多方认证 vs. TLS 侧重传输加密）；应用范围（SET 适用于信用卡支付）。

三、考核知识点

（一）TLS 握手协议的关键步骤；

（二）SET 协议中的双重签名应用；

（三）两种协议在电子商务中的典型场景（如普通网站支付 vs. 信用卡大额交易）。

四、考核要求

识记：TLS/SET 的核心功能；SET 协议的参与方角色。

领会：SET 协议如何解决支付中的隐私保护问题；TLS 的性能优势。

应用：分析某银行网上支付系统采用的协议及原因。

III.有关说明与实施要求

一、有关考核目标的说明

本课程考核目标分为三个层次：识记、领会、应用，各层次含义如下：

识记：要求考生能识别并记忆课程中的基本概念、原理、技术名称及分类等基础知识（如网络支付的支撑平台类型、加密算法名称）。

领会：要求考生理解知识的内涵与逻辑关系，能解释安全技术的原理、协议流程及安全威胁的成因（如 TLS 握手协议的步骤、对称加密与非对称加密的差异）。

应用：要求考生运用所学知识分析或解决实际问题，能结合案例设计安全方案或评估风险（如针对电商平台设计支付信息加密流程、分析 SET 协议在跨境支付中的适用性）。

二、关于自学教材

（一）指定教材

《网络支付与安全》（徐利敏主编，9787302561101），教材内容覆盖前 8 章核心知识点，包括：

1．网络支付与电子商务的关联、安全威胁与需求；

2．信息加密技术（对称 / 非对称加密、数字信封）；

3．身份认证技术（数字证书、PKI 体系）；

4．安全协议（TLS、SET）的原理与应用。

（二）教材使用建议

1．结合教材中的引导案例（如支付宝安全事件、SWIFT 系统风险）理解理论知识；

2．重点关注教材中技术流程图（如 TLS 记录协议流程、双重签名流程），辅助理解复杂逻辑；

3．通过教材中的思考题（如各章课后习题）检验知识掌握程度，强化应用能力。

三、自学方法指导

（一）分层学习法

先掌握基础概念（如网络支付的定义、安全要素），再深入技术原理（如 RSA 算法、PKI 架构），最后结合案例综合应用。

（二）对比分析法

对比不同技术或协议的特点（如 TLS 与 SET 的安全性差异、对称加密与非对称加密的适用场景），加深理解。

（三）实践驱动法

通过模拟实验（如使用 OpenSSL 工具实现简单加密解密）或行

业案例分析（如分析某银行支付系统的认证流程），将理论转化为实践能力。

（四）框架梳理法

按 “安全威胁→安全需求→技术方案→协议实现” 的逻辑梳理知识框架，构建系统性认知。

四、对社会助学的要求

（一）教学内容与重点

聚焦大纲要求的核心知识点，如信息加密技术、身份认证机制、安全协议流程；

结合行业动态补充案例（如新型支付安全漏洞、区块链在支付中的应用），增强实用性。

（二）教学方法建议

采用案例教学法（如分析 “刷脸支付安全争议”）引导学生理解技术应用；

通过小组讨论（如对比国内外支付安全标准）培养思辨能力；

利用可视化工具（如流程图、动画）演示复杂技术原理（如 PKI 信任链构建）。

（三）学习支持

提供配套习题解析、模拟试题，帮助学生掌握考核重点；

指导学生利用官方网站（如中国金融认证中心 CFCA）获取行业标准与技术文档。

五、关于命题的若干要求

（一）命题原则

以大纲规定的知识范围为依据，覆盖前 8 章核心内容，突出重点（如加密技术、安全协议）。

试题难度分布合理，兼顾识记（20%）、领会（30%）、应用（50%）三个层次。

（二）题型与分值

客观题（70%）：单项选择题、多项选择题、判断题、填空题等；

主观题（30%）：案例分析题、综合设计题等。

（三）命题要求

避免偏题、怪题，注重考查学生对知识的综合运用能力；

试题应结合教材案例或行业实际，体现实用性与时代性（如涉及移动支付安全、跨境支付协议等内容）。

以上内容紧扣教材与大纲要求，旨在明确考核方向、指导自学方法并规范命题标准，确保考试内容科学、合理、全面。