高纲 4211

江苏省高等教育自学考试大纲

14350　网络支付与安全

南京财经大学编（2024 年）

Ⅰ　课程的性质及其设置的目的和要求

《网络支付与安全》是电子商务专业（专升本）中一门重要的专业必修课程。电子商务基本流程主要包括了信息流、物流、商流和支付流，其中支付流是电子商务开展的重要保障，该课程就是介绍支付流是如何运作以及保障安全的。通过该课程的学习，使考生理解网络支付运作的底层逻辑，熟知支付安全的主要问题，掌握安全问题解决的机密性技术、完整性技术、身份认证技术以及相关的安全协议，同时了解国内外中大额网络支付的各类系统以及小额支付的各类工具的发展情况和未来趋势。学习和掌握课程的内容，培养提高考生分析问题解决问题的能力，增强信息安全意识和支付风险防御能力。

本课程与相关课程的联系（先修、后继课程）

先修课程：《电子商务安全导论》

后继课程：《电子商务系统分析与设计》

Ⅱ　考核目标

本大纲在考核目标中，按照识记、领会、应用三个层次规定其应达到的能力层次要求。三个能力层次是递升的关系，后者必须建立在前者的基础上。各能力层次的含义是：

识记：要求考生能够识别和记忆本课程中有关网络支付与安全的主要内容（如定义、公式、原理、重要结论、方法及特征、特点等），并能够根据考核的不同要求，做正确的表述、选择和判断。

领会：要求考生能够领悟和理解本课程中有关网络支付与安全的内涵及外延，理解概念的确切含义，能够鉴别关于概念的似是而非的说法；理解相关知识的区别和联系，并能根据考核的不同要求对相关概念问题进行合理推理和论证，做出正确的判断、解释和文字或作图说明。

应用：要求考生能够根据已知的知识和事实、条件，对课程内容相关的具体问题进行分析，得出正确的结论或做出正确的判断，并能把分析过程正确地表达出来。

Ⅲ　课程内容与考核要求

第一章　电子商务和网络支付安全

一、考核知识点

（一）互联网发展与电子商务

（二）电子商务的发展与网络支付

（三）电子商务安全与网络支付安全

二、考核要求

识记：①互联网特点；②互联网应用模式；③电子商务定义、分类等概念；④电子商务安全要素。

领会：①支付与电子商务的关联；②支付与结算方法的发展历程及原因；③网络支付安全的主要问题。

第二章　网络支付基础知识

一、考核知识点

（一）网络支付的产生与定义

（二）网络支付的基本构成

（三）网络支付的基本功能

（四）网络支付的特征

（五）专用成熟的 EDI 支付平台

（六）大众化网络平台 Internet

（七）网络支付的基本过程

（八）网络支付的基本系统模式

（九）按开展电子商务的实体的性质分类

（十）按支付数据流的内容性质分类

（十一）按网络支付金额的规模分类

（十二）国外网络支付发展情况

（十三）我国网络支付发展情况

二、 考核要求

识记：①网络支付的定义、基本构成、基本功能和特征；②网络支付的分类；③支付网关的定义和作用。

领会：①网络支付的支撑平台；②大众化网络平台 Internet 的构成；③网络支付的过程；④网络支付模式的分类：类支票和类现金系统的构成和理解。

第三章　网络支付的安全威胁、需求与解决策略

一、 考核知识点

（一）网络支付安全威胁的内容

（二）网络支付安全需求的内容

（三）网络支付安全策略制定的目的

（四）网络支付安全策略制定的原则

（五）安全策略的内容

（六）保证网络支付安全的解决方法

二、考核要求

识记：①网络支付的安全威胁；②网络支付的安全问题；③网络支付的安全需求；④网络支付安全策略制定的目的和原则。

领会：①安全策略的内容；②保证网络支付安全的解决方法。

第四章　网络支付系统安全与网络安全

一、考核知识点

（一）防火墙的基本原理

（二）防火墙的功能

（三）防火墙的类型

（四）电子商务中防火墙与 Web 服务器的配置方式

（五）防火墙的优缺点

（六）常见的防火墙软件介绍

（七）入侵检测

（八）入侵检测系统的分类

（九）入侵检测系统的优缺点

（十）计算机病毒概述

（十一）计算机病毒的特点

（十二）计算机病毒的分类

（十三）网络病毒的防范方法

二、考核要求

识记：①防火墙的定义；②防火墙的功能；③防火墙的类型；④防火墙的优缺点；⑤入侵检测的相关定义；⑥入侵检测的分类；⑦计算机病毒的概念、特征。

领会：①防火墙的基本原理；②计算机病毒的分类。

应用：①电子商务中防火墙与 Web 服务器的配置方式。

第五章 信息加密技术

一、考核知识点

（一）密码技术的发展

（二）密码技术的基本知识

（三）对称(私有)密钥密码技术的基本原理

（四）对称(私有)密钥密码技术的分类

（五）对称(私有)密钥密码技术的优缺点

（六）非对称(公开)密钥密码技术的基本原理

（七）非对称(公开)密钥密码技术的常用算法

（八）非对称(公开)密钥密码技术的优缺点

（九）对称密钥密码技术和非对称密钥密码技术的比较

（十）数字信封的基本原理

（十一）数字信封的优点

二、考核要求

识记：①密码技术发展的历程；②密码技术的基本概念；③非对称(公开)密钥密码技术的常用算法；④数字信封的定义。

领会：①对称(私有)密钥密码技术的基本原理（包括原理图）；②对称(私有)密钥密码技术的分类；③对称(私有)密钥密码技术的优缺点；④非对称(公开)密钥密码技术的基本原理（包括原理图）；⑤非对称(公开)密钥密码技术的优缺点；⑥数字信封的基本原理（包括原理图）。

应用：①对称密钥密码技术和非对称密钥密码技术的比较；②数字信封的优

点。

第六章 数据的完整性技术

一、考核知识点

（一）数字摘要技术的基本原理

（二）数字摘要的常用算法和示例

（三）数字摘要的优缺点

（四）数字签名的基本原理

（五）数字签名的作用

（六）数字时间戳的概念

（七）获得数字时间戳的过程

（八）数字时间戳的性质

（九）双重数字签名技术的原理

（十）双重数字签名技术的应用

二、考核要求

识记：①数字摘要的常用算法和实例；②数字时间戳的概念；③数字时间戳的性质。

领会：①数字摘要技术的基本原理（包括原理图）；②数字摘要的优缺点；③数字签名的基本原理（包括原理图）；④数字签名的作用；⑤获得数字时间戳的过程；⑥双重数字签名技术的原理（包括原理图）。

应用：①双重数字签名技术的应用。

第七章 身份认证技术

一、考核知识点

（一）基于 what you know 的认证方法

（二）基于 what you have 的认证方法

（三）基于 what you are 的认证方法

（四）数字证书

（五）数字证书认证机构 CA

（六）PKI 的组成

（七）PKI 的核心技术

（八）PKI 的功能

（九）PKI 的优势

二、考核要求

识记：①基于 what you know 的认证方法；②基于 what you have 的认证方法；③基于 what you are 的认证方法；④数字证书的定义、类型和内容；⑤数字证书认证机构 CA 的定义。

领会：①三种认证方法的判别；②PKI 的组成；③PKI 的核心技术；④PKI 的功能；⑤PKI 的优势；⑥数字证书的有效性；⑦CA 的信任模型和主要功能。

应用：①数字证书的申请和使用。

第八章　网络支付安全协议

一、考核知识点

（一）安全协议的概念

（二）安全协议的目的

（三）TLS 协议概述

（四）TLS 协议的构成

（五）TLS 记录协议

（六）TLS 握手协议

（七）修改密文规范协议

（八）警告协议

（九）SET 协议的目标

（十）SET 交易参与方及应用系统框架

（十一）SET 交易过程

（十二）SET 的证书管理

（十三）SET 的交易特点

（十四）SET 与 TLS 的比较

（十五）安全 HTTP(S-HTTP)协议

（十六）安全电子邮件协议

（十七）虚拟专用网

二、考核要求

识记：①安全协议的概念；②安全协议的目的；③TLS 协议概述；④SET 协议的定义和目标；⑤安全 HTTP(S-HTTP)协议；⑥安全电子邮件协议；⑦虚拟专用网。

领会：①TLS 协议的构成；②TLS 记录协议；③TLS 握手协议；④修改密文规范协议；⑤警告协议；⑥SET 交易参与方及应用系统框架；⑦SET 交易过程、证书管理和交易特点。

应用：①SET 与 TLS 的比较。

第九章　企业级电子支付系统

一、考核知识点

（一）电子汇兑系统简介

（二）电子汇兑系统的特点和类型

（三）电子支票系统简介

（四）电子支票的安全解决手段

（五）电子支票的网络支付模式

（六）SWIFT 系统

（七）CHIPS 系统

（八）中国国家金融通信网 CNFN

（九）中国国家现代化支付系统 CNAPS

（十）EDI 概述

（十一）EDI 的特点

（十二）EDI 的应用

（十三）EDI 的作用

（十四）EDI 的工作步骤

（十五）EDI 标准体系

（十六）网上银行概述

（十七）企业网上银行的定义和功能

二、考核要求

识记：①电子汇兑系统定义、特点和类型；②电子支票定义、属性和优缺点；

③SWIFT 的定义；④CHIPS 的定义、系统成员组成、优势与特点；⑤SWIFT 在中国的应用情况；⑥中国国家金融通信网 CNFN 的定义；⑦中国国家现代化支付系统 CNAPS 的定义、参与者、作用；⑧EDI 的定义、特点、应用领域、作用、标准体系；⑨网上银行的定义、分类和特点；⑩企业网上银行的定义和功能。

领会：①电子支票的安全解决手段；②电子支票网络支付模式；③SWIFT 的目标、任务和服务；④SWIFT 报文传送和标准；⑤中国国家金融通信网 CNFN 的网络结构；⑥中国国家现代化支付系统 CNAPS 的支付业务系统；⑦EDI 的工作过程。

应用：①CHIPS 系统的运作构架。

第十章　消费者级的网络支付方式

一、考核知识点

（一）银行卡的分类

（二）银行卡支付参与各方

（三）银行卡网上支付模式

（四）电子现金的定义与起源

（五）电子现金的属性与特点

（六）电子现金的工作原理

（七）电子现金的发展——加密货币

（八）央行数字货币

（九）电子钱包的含义

（十）电子钱包的功能

（十一）电子钱包的分类

（十二）电子钱包网上购物基本流程

（十三）电子钱包的购物实例

（十四）智能卡概述

（十五）智能卡的工作过程

（十六）智能卡的应用实例

（十七）第三方支付的定义

（十八）第三方支付的产生背景和起源

（十九）第三方支付的特点与流程

（二十）第三方支付的法规与支付牌照

二、考核要求

识记：①银行卡的分类；②银行卡支付参与各方；③电子现金的定义和起源；④电子现金的属性和特点；⑤加密货币的起源和定义；⑥加密货币的技术基础；⑦央行数字货币的定义；⑧电子钱包的含义；⑨第三方支付的定义、产生背景和起源。

领会：①银行卡网上支付模式分类；②电子现金的工作原理；③电子现金的发展——加密货币；④央行数字货币的特点；⑤第三方支付的特点与流程；⑥第三方支付的法规和支付牌照。

应用：①无安全措施的信用卡支付模式流程和特点；②通过第三方代理人的信用卡支付模式的流程和特点；③基于 SSL 协议的信用卡支付模式的流程和特点；④基于 SET 协议的支付模式使用技术和流程。

第十一章 移动商务与移动支付

一、考核知识点

（一）移动商务的含义

（二）移动商务的特点

（三）移动商务技术

（四）移动支付的定义与应用

（五）移动支付的应用类别

（六）移动支付的商业模式

（七）支付宝

（八）微信支付

（九）“云闪付”

二、考核要求

识记：①移动商务的含义、特点；②移动商务技术概述；③移动支付的定义。

领会：①移动支付的应用类别；②移动支付的商业模式；③移动支付开展实例支付宝、微信支付等概述。

Ⅳ　关于大纲的说明与考核实施要求

为使本大纲的规定在个人自学、社会助学和考试命题中得到贯彻和落实，兹对有关问题作如下说明，并进而提出具有要求。

一、关于“课程内容与考核目标”中有关提法的说明

在大纲的考核要求中，提出了“识记”、“领会”、“应用”等三个能力层次的要求，它们的含义是：

识记：要求考生掌握有关的知识点，正确理解和记忆相关内容的原理、方法步骤等。

领会：要求考生能够记忆规定的有关知识点的主要内容，并能够领会和理解规定的有关知识点的内涵与外延，熟悉其内容要点和它们之间的区别与联系，并能根据考核的不同要求，做出正确的解释、说明和阐述。

应用：要求考生能够运用本大纲中各部分的少数几个知识点，解决简单的解释说明并应用。

二、自学教材

本课程使用教材为：《网络支付与安全》，徐利敏编著，清华大学出版社，2020 年。

教材特色：二维码新形态教材，教材的大多数知识点都有相应的二维码，微信扫描后可以观看当前知识点的视频讲解。

三、自学方法的指导

本课程作为一门专业基础课程，综合性强、内容多、难度大，考生在自学过程中应该注意以下几点：

1.学习前，应仔细阅读课程大纲的第一部分，了解课程的性质、地位和任务，熟悉课程的基本要求以及本课程与有关课程的联系，使以后的学习紧紧围绕课程的基本要求。

2.在阅读某一章教材内容前，应先认真阅读大纲中该章的考核知识点、自学要求和考核要求，注意对各知识点的能力层次要求，以便在阅读教材时做到心中有数。

3.阅读教材时，应根据大纲要求，要逐段细读，逐句推敲，集中精力，吃透每个知识点。对每个知识点建议阅读的同时打开二维码视频进行观看，加深对基

本概念的深刻理解，同时基本原理必须牢固掌握。

4.学完教材的每一章节内容后，应认真完成教材中的习题，这一过程可有效地帮助考生理解、消化和巩固所学的知识，增加分析问题、解决问题的能力。

注意：本门课程在中国大学 MOOC 平台和学银平台都开设有线上开放课程，为了提高学习效率，强烈建议考生到平台上自主学习，两个平台的课程链接如下：

平台	网络链接	二维码入口
中国大学 MOOC 平台	https://www.icourse163.org/course/HSNUFE-1451759178	
学银平台	https://www.xueyinonline.com/detail/235970223	

四、对社会助学的要求

1.应熟知考试大纲对课程所提出的总的要求和各章的知识点。

2.应掌握各知识点要求达到的层次，并深刻理解各知识点的考核要求。

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

4.辅导时应对考生进行学习方法的指导，提倡考生“认真阅读教材，刻苦钻研教材，主动提出问题，依靠自己学懂”的学习方法。

5.辅导时要注意基础、突出重点，要帮助考生对课程内容建立一个整体的概念，对考生提出的问题，应以启发引导为主。

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、做出判断和解决问题。

7.要使考生了解试题难易与能力层次高低两者不完全是一回事，在各个能力层次中都存在着不同难度的试题。

五、关于命题和考试的若干规定

1.本大纲各章所提到的考核要求中，各条细目都是考试的内容，试题覆盖到

章，适当突出重点章节，加大重点内容的覆盖密度。

2.试卷对不同能力层次要求的试题所占的比例大致是：识记占40%，领会占40%，应用占20%。

3.试题难易程度要合理，可分为四档：易、较易、较难、难，这四档在各份试卷中所占的比例约为2：3：3：2。

4.本课程考试试卷可能采用的题型有：单项选择题、填空题、名词解释题、简答题、作图说明题及论述题。

5.考试方式为闭卷、笔试，考试时间为150分钟。评分采用百分制，60分为及格。考生只准携带0.5毫米黑色墨水的签字笔、铅笔、圆规、直尺、三角板、橡皮等必需的文具用品。不可携带计算器。

附录　题型举例

一、单项选择题

1.按开展电子商务的实体性质分类，网络支付可以分为(　　)

A.B TO C型和B TO B型络支付方式　　B.支付指令型支付和电子现金传递型支付

C.小额支付和中大额支付　　D.现金支付与非现金支付

参考答案：A

二、填空题

1.网络支付系统需要保证网络上资金结算数据不被随意篡改，也即保证相关网络支付结算数据的_____。

参考答案：完整性

三、名词解释题

1.对称密钥密码体制

参考答案：对称密钥密码体制，也叫作私有密钥密码体制或秘密密钥密码体制，即加密密钥与解密密钥相同的密码体制。

四、简答题

1.简要描述数字信封的优点。

参考答案：

①加密和解密的速度较快，可以满足实用特别是网络支付中的即时处理需要。

②通信双方在传输的密文中携带用RSA公钥加密的DES密钥，不用为交换DES密钥而费

尽周折，减小了 DES 密钥在传输过程中泄密的风险。

③具有数字签名和认证的功能。

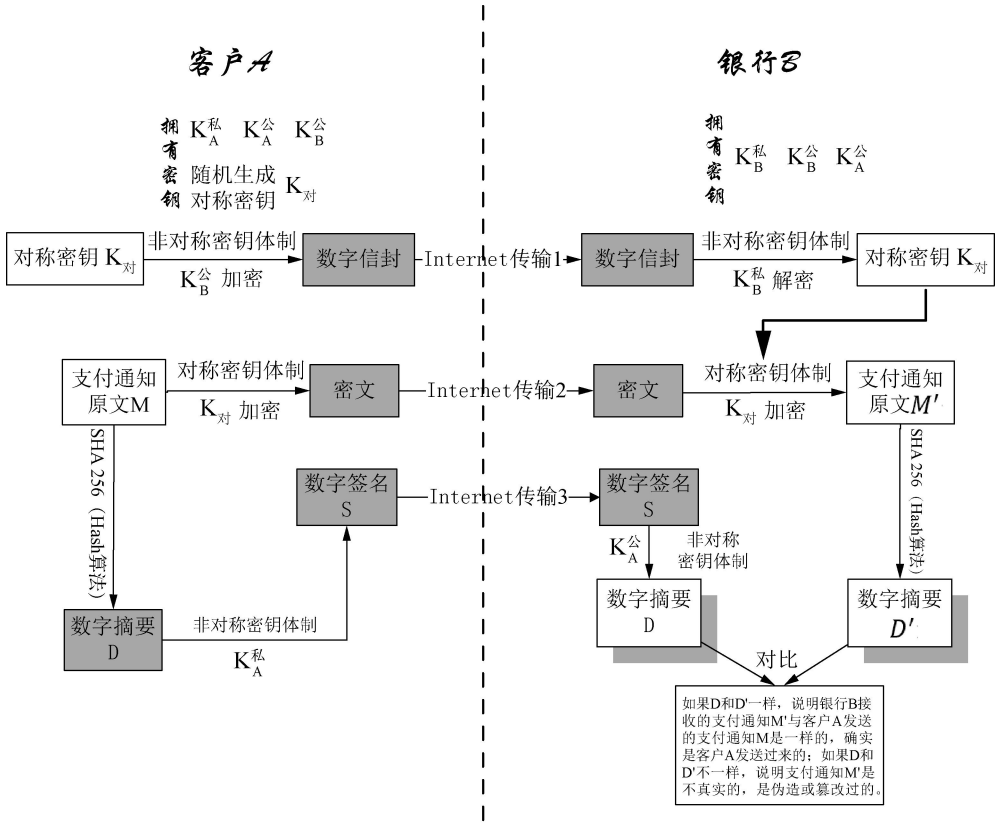
④密钥管理方便。

⑤保证通信的安全。

五、作图说明题

1.作图说明数字签名如何实现数据的机密性和完整性。

参考答案：



①发送方借助数字摘要技术，使用公开的单向 Hash 函数对信息报文 M 进行变换，得到数字摘要 A。

②发送方借助公开密钥加密法，利用自己的私钥对数字摘要 A 进行加密，得到一个特殊的字符串，即数字标记或直接称为数字签名。

③发送发把产生的数字标记附在信息报文 M 之后，一同通过网络发给接收方。

④接收方受到数字标记和信息报文 M’。

⑤接收方利用发送发的公开密钥对收到的数字标记进行解密，得到数字摘要 A。

⑥接收方再将得到的信息报文 M’利用与发送方一样的单向 Hash 函数进行变换，产生数字摘要 A’。

⑦接收方将数字摘要 A 和 A'进行比较，如果相同，说明信息报文是真实的，签名有效，否则报文不真实，签名无效。

六、论述题

1.在基于 Internet 电子商务安全技术中，保证网络支付信息的安全传送可以单独使用对称密码体制吗？如果不可以，主要问题出在哪里，请详细论述。

参考答案：不可以

主要存在问题：

①如果单独使用对称密钥体制，当网络用户有 n 个时，需要密钥 n*(n-1)/2，而 Internet 网络用户众多，所需的密钥个数过多。

②网络中每个用户都需要跟其他 n-1 个用户进行通信，这时跟其他的每个用户通信的对称密钥又不能相同，因此对于每个用户要保存的密钥太多，而且管理也不方便，当网络用户达到一定程度时，这种方法几乎不可能。

③每个对称密钥都是通讯双方共同拥有的，因此，一方泄露了，密钥就失效了。

④对称密钥双方共同拥有，因此也不能作为个人标记用作身份认证。