湖南省高等教育自学考试

课 程 考 试 大 纲

信息安全工程

（课程代码：07875）

湖南省教育考试院组编

2024 年 7 月

高等教育自学考试课程考试大纲

课程名称：信息安全工程　　课程代码：07875

第一部分　课程性质与目标

一、课程性质与特点

本课程是高等教育自学考试软件工程（本科）专业的选考课程。本课程全面地介绍信息安全基本概念、信息安全理论与技术体系、典型信息安全技术与应用，以及安全工程实现。主要内容包括：信息安全基本知识、安全体系结构、物理安全、系统安全、网络安全、数据安全、应用安全和安全管理等内容。

二、课程目标与基本要求

通过本课程的学习，应理解信息安全技术的基本概念、基本技能和安全意识，掌握密码技术、操作系统安全、物理安全、网络安全、软件安全和安全管理等关键技术，借助文献研究和应用必要的信息安全技术知识和所学技能，针对具体信息安全问题正确提出解决方案，分析过程的影响因素，获得有效结论，以培养对技术问题的理解能力、归纳总结的能力和提出问题的能力等。

本课程的学习目标是：

1. 培养问题分析能力。通过对信息安全意识、密码技术、操作系统安全、物理安全、网络安全、软件安全和安全管理等具有代表性的典型安全技术的分析，运用必要的信息安全技术知识和所学技能，针对具体信息安全问题正确提出解决方案，并分析论证所获结论。

2. 培养终身自主学习的能力。包括对安全技术问题的理解能力、归纳总结的能力和提出问题的能力等。

3. 培养终身学习的习惯。能在社会发展的大背景下，意识到信息安全技术是与时俱进的，认识到自主和终身学习的必要性，培养终身学习信息安全技术的习惯。

4. 通过对信息安全技术发展历史的了解，提升网络安全意识、树立网络强国的责任感和使命感。

三、与本专业其他课程的关系

本课程与许多专业课程有着密切的关系，先修课程为数据结构与算法、计算机网络技术。

第二部分　考核内容与考核目标

第一章　信息安全简介

一、学习目的与要求

通过本章的学习，了解信息安全的四个发展阶段，即保密通信、计算机系统、网络与信息安全和信息保障。同时，还需了解信息及其承载系统所面临的威胁和防护问题，明确信息安全的保护对象、保护目标和方法。最后通过对人、组织、管理、法规和社会道德等方面的讨论，强调安全意识、技术教育和管理的重要性。

二、考核知识点与考核目标

（一）信息安全的基本概念（重点）

识记：信息安全的定义

理解：信息安全的保护目标和方法

（二）信息安全的发展历史（次重点）

识记：信息安全发展的四个阶段

理解：1.通信保密科学的诞生

2.公钥密码学的原理

3.访问控制技术与可信计算机评估准则

4.网络信息安全的关键要素

（三）信息安全与其他学科（一般）

识记：我国信息安全方面相关的法律法规

理解：信息安全基本保障模型、安全属性、安全内在本质

第二章　信息安全体系结构

一、学习目的与要求

通过本章的学习，了解在特定环境下的安全目标和采用的安全机制，重点掌握两类最有影响的安全体系结构：一个是开放系统互连（OSI）体系结构，它描述了一种网络通信平台的技术安全体系；一个是 OSI 的高层安全协议模型，它描述了一种应用平台技术安全体系。熟悉物理环境安全体系和计算机系统平台安全体系，了解组织体系结构和管理体系结构与技术体系紧密关联。

二、考核知识点与考核目标

（一）应用体系结构（重点）

理解：1.安全交换与安全变换的区别

2.安全组件的类型

应用：应用服务元素（ASE）和应用服务对象（ASO）的区别

（二）体系结构概述（次重点）

理解：1.安全防护三棱锥

2.安全体系结构层次

3.网络通信平台安全体系概述

（三）安全机制（次重点）

识记：1. 安全机制的类别加密

2. 数字签名的两个过程
3. 访问控制机制的技术手段
4. 两类消息的数据完整性鉴别
5. 常用身份识别协议

理解：1. 保证的定义
2. 状态恢复的分类

（四）OSI 安全体系结构（次重点）

识记： OSI 的 7 层网络模型与 TCP/IP 模型

理解：1. OSI 安全体系结构的目标
2. 协议栈
3. 应用层常见的协议
4. OSI 安全服务的分类
5. 安全服务与安全机制的关系

（三）组织体系结构与管理体系结构（一般）

理解：1. 信息安全的组织保障系统
2. 信息系统安全的管理体系

第三章 数据加密

一、学习目的与要求

通过本章的学习，掌握密码学的基本概念和现实使用的加密算法。了解密码算法的主要编码思想和算法的原理，对它们的安全性分析仅进行了结论性描述。了解密码算法在信息安全中的作用，利用初等的数据加密算法知识解答实际问题。

二、考核知识点与考核目标

（一）对称加密算法（重点）

理解：1.三重 DES 的计算
2.其他分组密码算法的特点
3.序列密码算法 A5 的推导

应用：1.圈函数中的 E 变换, S-盒, P-盒置换
2.分组密码算法 AES 的基本特点

（二）数据加密模型与安全性（次重点）

识记：数据加密模型

理解：1.加密/脱密
2.破译的基本方法

（三）公钥加密算法（一般）

理解：1. RSA 加密算法的设计
2.有限域乘法群密码与椭圆曲线密码的比较
3.公钥密码算法难度的比较

第四章　数字签名

一、学习目的与要求

通过本章的学习，熟悉数字签名的基本概念和当前现实使用的算法，掌握数字签名方案，了解把数字签名方案和 Hash 函数进行结合实现对任意一个数据文件的签名。

二、考核知识点与考核目标

（一）数字签名算法（重点）

理解：1. RSA 签名算法的执行过程

2. ElGamal 签名算法的工作流程

3. DSA 签名算法的数字签名体制

（二）数字签名与安全性（次重点）

理解：1.一个数字签名方案的组成

2.数字签名系统需要满足的要求

3.攻击资源的分类

4.攻击目的

应用：数字签名模型的五元组

（三）Hash 函数（次重点）

识记：1.安全 Hash 函数的定义

2.强无碰撞性的性质

理解： MD4 的设计目标

（四）现实中的数字签名方案的构造（一般）

理解：与 Hash 函数结合的签名方案 DSA

第五章　身份识别与消息鉴别

一、学习目的与要求

通过本章的学习，掌握 4 种身份识别的技术和 4 种消息鉴别的技术，结合信息安全中出现的各种情况，分析每种技术应用的特点。

二、考核知识点与考核目标

（一）身份识别（重点）

理解：1. 身份识别的主要依据

2. 身份识别技术的分类

3. 随机数的主要作用

4. Needham-Schroeder 协议

5. 指纹识别处理的过程

应用： Markov 模型的实际操作

（二）消息鉴别（次重点）

识记：对称加密的鉴别方法

理解：1.数字签名机制的基本原理

2.无条件安全鉴别码的设计

应用：消息鉴别码实现消息鉴别

第六章　访问控制理论

一、学习目的与要求

通过本章的学习，掌握访问控制模型中的 BLP 模型。熟悉访问控制矩阵模型的基本概念；揭示访问控制的研究对象和方法。

二、考核知识点与考核目标

（一）Bell-LaPadula 模型（重点）

识记：1.主体对客体的访问模式

2. BLP 模型的安全策略

理解： Bell-LaPadula 模型的密级函数表

（二）访问控制矩阵模型（次重点）

识记：访问控制矩阵三元组的定义

应用：访问控制矩阵实操

（三）RBAC 模型（次重点）

理解：1. RBAC 的基本思想

2. RBAC 的安全原则

3. RBAC 的构件模型

4.职责分离（SD）概念

应用：RBAC 关系形式化的定义及映射关系

（四）授权与访问控制实现框架（一般）

理解：1. PMI 的权限管理模型

2.权限验证者决定访问的条件

3.PMI 访问控制实现流程

4.KDC 和 PMI 的访问控制框架功能组成

第七章　计算机系统安全

一、学习目的与要求

通过本章的学习，掌握可信计算基、操作系统安全、数据库安全、病毒防护、数据备份和可信计算平台等系统安全知识。熟悉安全问题与解决技术，重点了解介绍操作系统、数据库系统的安全机制，熟悉计算机病毒的机理与防护。

二、考核知识点与考核目标

（一）可信计算基（重点）

识记：1.访问监视器的组成与实现

2.访问验证机制设计的原则

理解：1.安全内核方法的定义

2.可信计算基的组成

应用：可信计算基安全保证的方法和措施

（二）操作系统安全（次重点）

识记：1.操作系统安全的主要目标

2.操作系统安全机制的设计原则

3. UNIX 操作系统的审计日志内容

理解：操作系统的安全控制与安全模型

（三）数据库安全（次重点）

识记：1.数据库系统的组成

2.数据库的特性

理解：1.数据库的安全策略

2.数据库安全技术的类型

（四）计算机病毒防护（一般）

识记：1.恶意软件的定义与分类

2.可执行文件的感染方式

3.计算机病毒防治的阶段

理解：1.计算机病毒的分类

2.计算机病毒的基本特性

应用：计算机病毒程序工作流程

（五）可信计算平台（一般）

识记：可信计算平台的基本思想

第八章　网络安全

一、学习目的与要求

通过本章的学习，构筑安全的网络系统，了解一些典型的网络安全技术，熟悉 IPSec、防火墙、VPN、入侵检测方面的知识。

二、考核知识点与考核目标

（一）网络安全概述（重点）

识记：网络的分类

理解： TCP/IP 的安全缺陷

（二）防火墙（重点）

识记：防火墙的功能

理解：1. 包过滤技术

2. 防火墙的基本控制策略

应用：防火墙的结构

（三）VPN（次重点）

理解：1. VPN 的定义

2.隧道技术的分类及其应用

3.PPTP 的报文

4.L2TP 的报文

应用： VPN 技术原理

（四）IPSec（次重点）

识记：IPSec 保护 IP 网络的数据方式

理解：1. IPSec 的工作模式

2. IPSec 提供的安全服务

3. 安全关联参数

4.了解鉴别报头与解释域

（五）入侵检测（次重点）

识记：入侵检测的主要分析模型和方法

理解：1.入侵检测的数据源的分类

2.入侵检测系统的功能模块

3.入侵检测的体系结构

第九章 数据安全

一、学习目的与要求

通过本章的学习，掌握隐私数据安全的基本概念，了解访问控制对计算机中数据安全的作用，了解加密和鉴别算法对数据安全的作用。

二、考核知识点与考核目标

（一）数据的机密性（重点）

识记：机密性保护的安全机制

理解：1.数据集的机密性

2.带标签数据的表示方式

应用：机密性保护的安全机制

（二）数据的完整性与备份（重点）

识记：数据完整性的保障技术

理解：1.数据完整性丧失原因

2.数据备份的方法

3.数据恢复策略

4.容错系统的设计

（三）数据安全概述（次重点）

理解：1.计算机系统中的数据安全

2.网络中的数据安全

3.其他载体的数据安全

（四）隐私保护（次重点）

识记：隐私的概念

理解：1.个人档案与隐私的关系

2.鉴别的基本方式

3.隐私的保护技术

第十章　事务安全与多方安全计算

一、学习目的与要求

通过本章的学习，掌握百万富翁问题的求解协议、平均薪水、数字货币等实例说明，了解用密码技术构造有用安全协议或实现事务的安全性。

二、考核知识点与考核目标

（一）安全多方计算（重点）

识记：密码协议的条件

应用：姚氏百万富翁问题的应用

（二）百万富翁问题的计算协议（次重点）

识记：百万富翁问题的计算协议实操

（三）平均薪水问题的计算协议（次重点）

识记：平均薪水问题的计算协议实操

（四）数字货币与区块链（一般）

理解：1.货币的安全协议

2.区块链技术的核心思想

3.比特币的操作流程

第十一章　应用安全

一、学习目的与要求

通过本章的学习，掌握 KDP、PKI、PMI 应用安全基础设施，Web 安全协议，以及邮件安全等内容。了解密码体制、安全协议、授权管理内容的应用系统安全基础等知识。

二、考核知识点与考核目标

（一）Web 安全（重点）

识记： Web 应用中存在的问题

理解：1. SSL 协议体系结构

2.SSL 握手协议的阶段

3.SET 协议的工作流程

应用：SET 协议的安全服务

（二）应用安全基础设施（次重点）

理解：1.密钥安全的重要环节
2.对称密钥设施的生成与分发
3.公钥基础设施的生成与分发
应用：KDP 协议的使用

（三）邮件安全（一般）
识记：电子邮件系统的工作原理
理解：1.电子邮件的安全目标
2.电子邮件安全的突出体现
3. PGP 的定义
4.S/MIME 的主要功能

第十二章　安全审计

一、学习目的与要求

通过本章的学习，掌握审计日志是安全审计的基础，熟悉安全审计与操作系统、应用软件、网络协议等相关知识的联系，了解计算机取证的基本概念，以及计算机取证的原则与步骤。

二、考核知识点与考核目标

（一）审计日志（重点）
识记：日志文件的概念
理解：1.审计日志的内容
2.日志系统的分类
应用：日志分析工具的操作

（二）安全审计（次重点）
识记：安全审计的类型
理解：1. 安全审计过程的实现步骤
2. 网络安全审计系统的问题
应用：安全审计的作用

（三）计算机取证（一般）
识记：计算机取证的基本概念
理解：1. 计算机取证的步骤
2. 计算机取证的原则
3. 计算机取证工具软件

第十三章　信息安全评估与工程实现

一、学习目的与要求

通过本章的学习，了解安全产品（系统）评估、安全工程方面相关内容，了解国家标准 GB 17859-1999 和可信计算机评估准则（TCSEC），重点掌握评估体系

（CC），并结合 SSE-CMM 了解安全工程体系构成。

二、考核知识点与考核目标

（一）信息安全评估（重点）

识记：系统安全保护等级的划分

理解：1.《准则》中的重要术语

2.计算机信息系统安全保护等级划分准则

3.安全需求的构造

应用：可信计算机系统评估准则

（二）信息安全工程（次重点）

识记：安全工程的主要目标

理解：1. SSE-CMM 概述与组成

2.能力成熟度的级别

应用： SSE-CMM 体系结构

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

信息安全概论（第 2 版），徐茂智，邹维，人民邮电出版社，2020 年版。

2．参考教材

信息安全导论，朱建明，王秀利，清华大学出版社，2022 年 8 月。

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。

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	章节名称	学 时
第一章	信息安全简介	2
第二章	信息安全体系结构	10
第三章	数据加密	8
第四章	数字签名	8
第五章	身份识别与消息鉴别	4
第六章	访问控制理论	6
第七章	计算机系统安全	10
第八章	网络安全	12
第九章	数据安全	10
第十章	事务安全与多方安全计算	6
第十一章	应用安全	8

第十二章	安全审计	4
第十三章	信息安全评估与工程实现	2
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 40 %、“理解”为 40%、“应用”为 20 %。

3．试题难易程度应合理：容易、中等、难比例为 3：4：3。

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、简答题、综合题。

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．下面算法中，不属于 Hash 算法的是

A．MD-4 算法　　B．MD-5 算法　　C．DSA 算法　　D．SHA 算法

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．安全机制的类别包括

A．保护机制　　B．检测机制　　C．恢复机制　　D．加密机制

三、填空题（本大题共■小题，每小题■分，共■分）

1．数字签名就是通过一个单向_____对要传送的报文进行处理。

四、简答题（本大题共■小题，每小题■分，共■分）

1．简述消息鉴别的主要目的。

五、综合题（本大题共■小题，每小题■分，共■分）

1．根据表 1 的对应关系，已知明文“E”对应密文“C"，明文“T”对应密文“F”，则相应的 key=(k1,k2)等于多少？

A	B	C	D	E	F	G	H	I	J	K	L	M
00	01	02	03	04	05	06	07	08	09	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

表 1　　英语字符与整数之间的对应关系表