甘肃省高等教育自学考试
课程考试大纲

专业名称：计算机应用技术（专科）

专业代码：510201

课程名称：信息安全基础（14481）

甘肃省高等教育自学考试委员会　　制定

2024 年 3 月

课程性质与课程目标

一、课程性质

《信息安全基础》是高等教育自学考试计算机应用技术专业中一门重要的专业课。本课程介绍主要的信息安全技术，包括密码技术、身份认证、授权与访问控制、信息隐藏技术、操作系统和数据库安全、网络与系统攻击、网络与安全防护及应急响应技术、安全审计与责任认定技术、Internet 安全、无线网络安全、恶意代码、内容安全技术等。设置本课程的主要目的是通过系统学习，使应考者能够在已有的计算机专业知识的基础上，对信息安全原理和技术有一个系统的、全面的了解，并能将理论与实际应用相结合，为将来的软件开发与应用打下基础。。

二、课程目标

本课程的主要目标是以信息技术体系为主线，系统介绍信息安全概念、技术框架、密码学基础、主机系统安全、网络攻击与防护、内容安全等内容。通过课程的学习，让学生全面掌握信息安全的基本理论及信息安全防护的主流工具与技术，更好培养和训练学生建立网络安全防护的基本技能。主流安全技术和应用。

课程内容与考核要求

第一章　绪论

一、课程内容

1.1 信息安全的概念

1.2 信息安全发展历程

1.3 信息安全技术体系

1.4 信息安全模型

1.5 信息安全保障技术框架

二、学习目的与要求

本章需要了解信息安全的基本概念和发展历程，对信息安全的发展历程有基本的了解、对信息安全技术体系和安全保障技术框架有初步的认识，为本课程以后几章的学习打下基础。本章在深度上不做要求。

本章的重点：了解信息安全技术体系

三、考核知识点与考核要求

1 信息安全的概念达到“识记” 层次

1.1 信息安全的基本概念，信息安全的重要性

1.2 信息安全发展发展的四个阶段

1.3 信息安全保障技术框架及其指导作用

1.4 信息安全模型:Dolev—Yao 信息安全模型的深远影响

2.信息安全技术体系，要求达到“领会”层次

2.1 5 类信息安全技术

2.2 每一类信息安全技术的具体技术

第二章　密码技术

一、课程内容

2.1 基本概念

2.2 对称密钥

2.3 公钥密钥

2.4 散列函数和消息认证

2.5 数字签名

2.6 密钥管理

二、学习目的与要求

密码学信息安全的重要基石。本章重点要求学生掌握密码技术的基本概念，深刻理解对称密钥、公钥密钥、散列函数和消息认证、数字签名及密钥管理等内容。本章有深度上的要求。

本章重点和难点是掌握对称密钥、公钥密钥、散列函数和消息认证、数字签名、密钥管理等技术的原理

三、考核知识点与考核要求

1、对密码技术的基本概念达到“识记” 层次

2.对密码技术达到“领会”层次

2.1 对称密钥中古典密钥的置换技术与代换技术、分组密码、序列密码

2.2 公钥密钥的原理和 RAS 算法

2.3 散列函数和消息认证码中散列函数的安全性和 SHA-1 算法，基于 MAC 和基于散列的消息鉴别码

2.4 基于公钥密码的数字签名原理和数字签名算法

2.5 密钥管理中的公钥分配、对称密钥体制的密钥分配、公钥密码用于对称密码体制的的密钥分配、Diffie-Hell 密钥交换。

第三章 身份认证

一、课程内容

3.1 用户认证

3.2 认证协议

3.3 Kerbeors

3.4 PKI 技术

二、学习目的与要求

本章学习的目的是要求考生了解身份认证的重要意义，熟悉身份认证的基本原理，掌握三个在网络上提供身份认证服务的标准：Kerbeors、X.509 和 PKI。

本章的重点是 Kerbeors、X.509 和 PKI 三个身份认证服务的标准的基本原理，他们同时也是本章难点。

三、考核知识点与考核要求

1、用户认证的基本方法达到“识记” 层次

1.1 基于口令认证：静态口令存储与传输、动态口令的产生方式

1.2 基于智能卡的认证：基于 USB-Key 认证的特点和几种常见方式

1.3 基于生物特征的认证的几种常见模式及优点

2.对认证协议达到“领会”层次

2.1 单向和双向认证协议

2.2Kerbeors 的工作原理和不同版本的差异性

2.3 PKI 的体系结构，包括 X.509、认证机构、相关协议及五种信任模型

第四章 授权与访问控制技术

一、课程内容

4.1 授权与访问控制策略的概念

4.2 自主访问控制

4.3 强制访问控制

4.4 基于角色的访问控制

4.5 基于属性的访问控制

4.6 PMI 技术

二、学习目的与要求

本章学习的目的是要求考生了解授权与访问控制的基本策略与常用技术。本章的学习重点是基于角色的访问控制、基于属性的访问控制。

三、考核知识点与考核要求

1、授权与访问控制概念、自主访问控制、强制访问控制等达到“识记” 层次

1.1 授权与访问的基本概念

1.2 自主访问控制的基本概念、授权管理、自主访问控制机制的完善

1.3 强制访问控制的基本概念

1.4 PMI 概念，PMI 授权管理模式、体系及模型

2.基于角色的访问控制、基于属性的访问控制、PMI 等达

到“领会”层次

2.1 RBAC 核心模型，用户、角色、许可的对应关系，授权策略等

2.2 ABAC 模型的核心概念、基于属性的加密机制 ABE

2.3 PMI 授权管理模式、体系及模型

第五章 信息隐藏技术

一、课程内容

5.1 信息隐藏的概念

5.2 信息隐藏的基本方法

5.3 数字水印

5.4 数字隐写

5.5 数字指纹

二、学习目的与要求

本章学习的目的是要求考生了解并掌握信息隐藏所涉及的基本理论与方法，熟悉信息隐藏、数字水印、数字隐写、数字指纹的基本方法与技术，使学生掌握信息隐藏的基本实践能力。为今后的工作和进一步学习，奠定信息隐藏的基础。

本章的学习重点是信息隐藏的基本方法、数字隐写和数字指纹的基本原理；本章学习的难点是数字水印。

三、考核知识点与考核要求

1、信息隐藏的基本概念达到“识记” 层次

1.1 信息隐藏的意义、分类

1.2 信息隐藏的基本方法

1.3 数字指纹的基本概念和模型

2.对信息隐藏的主流技术达到“领会”层次

2.1 数字隐写：隐写的技术模型、不同数字隐写算法的特点

2.2 数字水印：数字水印模型、数字水印的分类方法

第六章 主机系统安全技术

一、课程内容

6.1 操作系统安全技术

6.2 数据库安全技术

6.3 可信计算技术

二、学习目的与要求

本章学习的目的是要求考生了解并掌握主机系统安全所涉及的基本理论与方法，熟悉操作系统安全、数据库安全、可信计算的基本方法与技术，具有主机系统安全的思维与基本实践能力。为今后的工作和进一步学习，奠定基础。

本章的学习重点是操作系统的安全机制、传统数据库安全技术、TCG 可信计算系统。 学习的难点是 Linux 安全机制。

三、考核知识点与考核要求

1、主机系统安全的基本概念达到“识记” 层次

1.1 可信计算机评价标准（TCSEC）

1.2 云数据库/云存储安全

1.3 可信计算的概念和基本思想

2.主机系统安全主流技术和机制达到“领会”层次

2.1 操作系统安全的基本原理、操作系统的安全机制

2.2 传统数据库安全技术、外包数据库安全

2.3 TCG 可信计算系统

第七章 网络与系统攻击技术

一、课程内容

7.1 网络攻击概述

7.2 网络探测

7.3 缓冲区溢出攻击

7.4 拒绝服务攻击

7.5 僵尸网络

二、学习目的与要求

本章学习的目的是要求考生了解并掌握网络与系统攻击的基本理论与方法，熟悉网络攻击的一般流程、缓冲溢出的基本原理、僵尸网络的概念与结构，掌握网络扫描的过程和常见拒绝服务攻击的原理。具有网络与系统攻击防御的思维与基本实践能力。为今后的工作和进一步学习，奠定基础。

本章的学习重点是网络扫描祭器工具的应用和拒绝服务攻击的防范。

三、考核知识点与考核要求

1、网络与系统攻击的基本概念达到“识记” 层次

1.1 网络攻击的概念、网络攻击的一般流程

1.2 僵尸网络的概念

2.网络与系统攻击的原理与技术达到“领会”层次

2.1 网络扫描

2.2 缓冲区溢出的基本原理

2.3 拒绝服务攻击的基本原理

2.4 僵尸程序功能结构

3.网络与系统攻击的防范达到“简单应用”层次

2.1 网络扫描工具的应用

2.2 拒绝服务攻击的防范

2.3 缓冲区溢出的防范

第八章 网络与系统安全防护

一、课程内容

8.1 防火墙技术

8.2 入侵检测技术

8.3 蜜罐技术

8.4 应急响应技术

二、学习目的与要求

本章学习的目的是要求考生了解并掌握网络与系统安全防护的基本理论与方法，熟悉防火墙的概念、入侵检测的概念与分类模型、蜜罐的概念及分类、应急响应的概念。掌握包过滤技术、代理服务技术、状态检测技术。具有网络与系统安全防护的思维与基本实践能力。为今后的工作和进一步学习，奠定基础。

本章的学习重点是防火墙技术、入侵检测系统的分类模型和蜜罐技术的关键机制。

三、考核知识点与考核要求

1、网络与系统安全防护的基本概念达到“识记” 层次

1.1 熟悉防火墙的概念

1.2 蜜罐的概念及分类

1.3 入侵检测的概念与分类模型

1.4 僵尸网络的概念

1.5 应急响应的概念

2.网络与系统安全防护达到“领会”层次

2.1 防火墙的包过滤技术、代理服务技术、状态检测技术

2.2 入侵检测模型

2.3 蜜罐技术的关键机制

第九章 安全审计与安全责任认定技术

一、课程内容

9.1 安全审计

9.2 数字取证

9.3 数字取证关键技术和工具

二、学习目的与要求

本章学习的目的是要求考生了解并掌握安全审计与责任认定技术的基本理论与方法，熟悉安全审计的概念与审计系统的结构、数字取证的基本原理，掌握数字取证的关键技术和工具。具有安全审计与责任认定的思维与基本实践能力。为今后的工作和进一步学习，奠定基础。

本章的学习重点是数字取证的关键技术和工具。

三、考核知识点与考核要求

1、安全审计与安全责任认定的基本概念达到“识记” 层次

1.1 安全审计的概念与审计系统的结构

1.2 电子证据的特点和取证的基本原则

2.安全审计与安全责任认定的原理和技术达到“领会”层次

2.1 数字取证的基本原理

2.2 数字取证的关键技术

3.数字取证工具达到“简单应用”层次

第十章 Internet 安全

一、课程内容

10.1 OSI 安全体系结构

10.2 IPSec 协议

10.3 SSL/TLS 协议

10.4 安全电子交易

10.5 安全电子邮件

二、学习目的与要求

本章学习的目的是要求考生了解并掌握 Internet 安全的基本理论与方法，熟悉 OSI 安全体系结构、安全电子交易协议，掌握 TCP/IP 不同层次提供的安全机制，包括 IPSec 协议、SSL/TLS 协议、PGP 协议。具有 Internet 安全的思维与基本实践能力，为今后的工作和进一步学习，奠定基础。

本章的学习重点是 OSI 安全体系结构、IPSec 协议、SSL/TLS 协议、安全电子邮件协议。本章学习的难点是 SSL 的握手协

议、安全电子交易的支付处理和 PGP 协议。

三、考核知识点与考核要求

1. Internet 安全协议原理达到“领会”层次

1.1 OSI 安全体系结构

1.2 IPSec 协议

1.3 SSL/TLS 协议

1.4 安全电子邮件协议

第十一章 无线网络安全

一、课程内容

11.1 IEEE 802.11 无线网络安全

11.2 移动通信系统的安全

二、学习目的与要求

本章学习的目的是要求考生了解并掌握无线网络安全的基本理论与方法，熟悉 IEEE 802.11 系列部分标准和 GSM 安全机制，掌握 WEP 、GPRS 安全。具有无线网络安全安全的思维与基本实践能力，为今后的工作和进一步学习，奠定基础。

本章的学习重点是掌握 WEP 和 GPRS 安全，这也是本章学习的难点。

三、考核知识点与考核要求

1. 无线网络安全的概念与发展达到“识记”层次

1.1 IEEE 802.11 无线网络背景

1.2 3GPP 安全体制的总体架构

2. 无线网络安全的原理与技术达到“领会”层次

1.1 WEP

1.2 GPRS 安全

第十二章 恶意代码检测与防范技术

一、课程内容

12.1 恶意代码概述

12.2 常见恶意代码

12.3 恶意代码检测与分析技术

二、学习目的与要求

本章学习的目的是要求考生了解并掌握恶意代码检测与防范的基本理论与方法，熟悉恶意代码的种类、恶意代码的攻击流程、计算机病毒的特征及种类，掌握恶意代码的攻击技术、恶意代码分析与检测技术。具有恶意代码检测与防范的思维与基本实践能力，为今后的工作和进一步学习，奠定基础。

本章的学习重点是恶意代码检测与分析与技术。

三、考核知识点与考核要求

1.恶意代码检测与防范的基本知识达到“识记”层次

1.1 恶意代码的背景

1.2 计算机病毒的种类

1.3 计算机病毒的特征

2.恶意代码检测与防范的基本技术达到“领会”层次

2.1 恶意代码攻击技术

2.2 恶意代码生成技术

2.3 病毒预防技术

2.4 病毒预防技术

3. 恶意代码检测与分析与技术达到“简单应用”层次

第十三章 内容安全技术

一、课程内容

13.1 内容安全的概念

13.2 文本过滤

13.3 话题发现和跟踪

13.4 内容安全分级管理

13.5 多媒体内容安全技术简介

二、学习目的与要求

本章学习的目的是要求考生了解内容安全的概念，熟悉文本过滤的主要方法、话题发现的机理以及内容安全分级监管。具有内容安全的意识，为今后的工作和进一步学习奠定基础。

本章的学习重点是不良文本过滤的方法。

三、考核知识点与考核要求

1. 内容安全的概念与分级等达到“识记”层次

1.1 内容安全的概念及分级

1.2 内容安全分级监管

1.3 多媒体内容安全

2. 文本过滤技术达到“领会”层次

2.1 基于关键字的过滤方法

2.2 中文分词化

一、自学要求

本大纲的课程基本要求是依据专业考试计划和专业培

养目标而确定的。课程基本要求还明确了课程的基本内容以及对基本内容掌握的程度。基本要求中的知识点构成了课程内容的主体部分，因此，课程基本内容掌握程度、课程考核知识点是高等教育自学考试考核的主要内容。

为有效地指导个人自学和社会助学，本大纲已指明了课程的重点和难点，在各章的基本要求中也指明了各章内容的重点和难点。

信息安全是一个综合的、交叉的学科领域，涉及数学、信息、通信和计算机等诸多学科的长期知识积累，因此它的理论性比较强，同时信息安全也是一个实践性强的学科，仅仅通过书本，不可能全面深入地掌握信息安全的知识体系，必须理论与实践相结合，本大纲在教学参考书中也推荐了相关的实验指导教材。

考核目标

1、本课程要求考生学习和掌握的知识点内容都作为考核的内容。课程中各章的内容均由若干知识点组成，在自学考试中成为考核知识点。因此，课程自学考试大纲中的规定的考试内容是以分解为考核知识点的方式给出的。自学考试将各知识点分别按四个认知（能力）层次确定其考核要求。

2、四个能力层次从低到高依次是识记、领会、简单应用、综合应用。

识记：要求学生能够对大纲中的知识点，如定义、定理、公式、性质、法则等有清晰准确的认识，并能做出正确的判

断和选择。

领会：要求考生能够对大纲中的概念、定理、公式、法则等有一定的理解，清楚它与有关知识点的联系与区别，并能做出正确的表述和解释。

简单应用：要求考生能够运用本大纲中各部分的少数几个知识点，解决简单的计算、证明或应用问题。

综合应用：要求考生对大纲中的概念、定理、公式、法则熟悉和理解的基础上，会运用多个知识点，分析、计算或推导解决稍复杂的一些问题。

相关说明与实施要求

一、制定自学考试大纲的目的及其作用

本课程自学考试大纲是根据专业自学考试计划的要求，结合自学考试的特点而确定。其目的是对个人自学、社会助学和课程考试命题进行指导和规定。

本课程自学考试大纲明确了课程学习的内容以及深广度，规定了课程自学考试的范围和标准，因此，它是社会助学组织进行自学辅导的依据，是自学者学习教材、掌握课程内容知识范围和程度的依据，也是进行自学考试命题的依据。

二、自学要求

本大纲的课程基本要求是依据专业考试计划和专业培养目标而确定的。课程基本要求还明确了课程的基本内容以及对基本内容掌握的程度。基本要求中的知识点构成了课程内容的主体部分，因此，课程基本内容掌握程度、课程考核知识点是高等教育自学考试考核的主

要内容。

为有效地指导个人自学和社会助学，本大纲已指明了课程的重点和难点，在各章的基本要求中也指明了各章内容的重点和难点。

三、自学方法指导

信息安全是一个综合的、交叉的学科领域，涉及数学、信息、通信和计算机等诸多学科的长期知识积累，因此它的理论性比较强，同时信息安全也是一个实践性强的学科，仅仅通过书本，不可能全面深入地掌握信息安全的知识体系，必须理论与实践相结合，本大纲在教学参考书中也推荐了相关的实验指导教材。

四、助学建议

1、助学单位和老师应熟知本大纲的各项要求和规定。

2、教学过程中应以本大纲为依据，使用本大纲规定的教材为基础实施教学和辅导。

3、助学辅导时应重视基础知识和应用技术的培养，根据考生的特点，按照本大纲的具体要求制定并实施教学计划。

4、注意培养考生的自学能力，特别要培养考生自己提出问题，自己分析问题，自己解决问题的能力。

5、要使考生正确理解试题的难易程度和能力层次不是同一个概念，因此，每个能力层次都可能出现不同难度的试题。

6、助学单位应具备上机实习条件和环境。

五、命题考试的规定

1、考试方式为闭卷、笔试。考试时间为 120 分钟。评卷采用 100 分制，60 分为及格。考试时，只允许携带钢笔和

铅笔，答卷规定用钢笔完成。

2、本大纲在各章的考核知识点和考核要求中列出的所有细目都是考试的内容，试题覆盖到章，命题要突出重点章节，要加大重点内容的覆盖密度。

3、本课程对不同能力层次要求在试卷中所占比例大致如下：“识记”占 35%，“领会”占 55%，“简单应用”占 15%。

4、试卷中的难易程度比例大约为：易；较易；较难；难=2：3：3：2

5、试题题型有：单项选择题、填空题、名词解释题、简答题、计算题、算法阐述题。