**《信息系统安全》课程教学大纲**

执笔人：穆海冰 修订日期：2022年11月

**一、课程基本信息**

1．课程编号：M401148B

2．课程平台：专业教育平台

3．课程模块：专业拓展选修课程模块

4．课程性质：专业B类选修课程

5．学时/学分：32/2

6．先修课程：概率论与数理统计（B），线性代数，计算机类课程

7．适用专业：通信工程、自动控制、电子与信息科学专业

8．教学单位名称：网络安全教学团队

**二、课程教学目标及学生应达到的能力**

《信息系统安全》是工科高等学校电子信息类专业的一门专业课，在培养学生创造性思维、信息安全理念、综合设计能力和工程实践能力方面占有重要的地位。

本课程的主要任务是通过课堂教学和研究讨论等环节培养学生的创新意识与能力和信息安全科学知识的应用能力，使学生掌握信息与忘了安全的基本理论、基本知识和基本技能，常用信息安全算法与技术的分析与应用，具有基本的算法和方案方案设计能力，以及对信息系统安全问题进行分析和应对的能力，支撑毕业要求中的相应指标点。课程目标及能力要求具体如下：

**课程目标1.** 掌握与信息安全、计算机网络安全相关的技术，掌握信息系统安全协议与密码算法的数学基础，能运用整数论、随机过程等数学知识及分析方法，进行协议和算法的分析与设计，进行密码编码和密码分析的研究。

**课程目标2.** 掌握信息系统的安全性分析与协议算法设计的基本原理，包括了解和掌握计算机网络信息安全的主要防御手段、技术与方法，综合运用多种安全机制实现信息系统必要的安全服务，抵御多种攻击和威胁，建立多层次的安全体系结构。

**课程目标3.**由于课程内容的特殊性，在课堂教学中明确工程职业道德和规范，界定研究攻击与威胁的边界，培养学生正确的是非观和法律意识，使其成为能够承担社会责任，满足当前社会对信息安全的人才需求。

**三、课程教学目标和毕业要求的对应关系**

|  |  |  |
| --- | --- | --- |
| **毕业要求** | **毕业要求指标点** | **课程目标对毕业要求的支撑关系** |
| 1. 品德修养 | 1.2具有良好的思想品德和社会公德，具有家国情怀和社会责任感，树立并践行社会主义核心价值观。 | 课程目标3 |
| 2. 工程知识 | 2.3将数学、自然科学、工程基础和专业知识用于工程问题的计算分析。 | 课程目标1 |
| 5．研究 | 5.2 设计候选方案，考虑技术限制条件，评估方案可行性。 | 课程目标2 |
| 9. 职业规范 | 9.1具备人文社会科学素养，理解应担负的社会责任，愿意为社会服务。 | 课程目标3 |

**四、课程思政育人目标**

**目标1.** 介绍信息安全和密码学发展史和中外映照，特别是中国古代和现代密码学重要成果和贡献，让学生深切感受到发展历程的艰辛，坚定理想信念、厚植爱国主义情怀，以及民族自豪感、使命感和责任感。

**目标2.** 通过介绍课程中科学家的成就和贡献，培养学生坚忍不拔探索的奋斗精神和开拓精神，甘做冷板凳的踏实治学、严谨求实、不迷信不盲从的科学精神。

**目标3.** 引入信息安全有关法律法规和政策的讲解教学，培养学生职业素养和责任意识，知法守法，严守职业道德底线。

**五、课程教学教学内容和要求**

总学时 32学时，讲课32学时。

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **序号** | **知识单元（章节）** | **知识点** | **教学要求** | **推荐学时** | **教学方式** | **支撑课程目标** |
| 1 | 绪论 | 信息与网络安全现状以及课程的引入 | 了解 | 2 | 课堂讲授 | 5.2，9.1 |
| 信息安全，网络安全和系统安全等基本概念和定义 | 掌握 |
| OSI安全体系结构，包括威胁、服务和机制及其之间关系 | 掌握 | 2 | 课堂讲授 |
| 信息系统安全模型和防御体系；信息安全法律法规 | 理解 |
| 2 | 密码学基础知识 | 密码学概念和古典密码学 | 理解 | 2 | 课堂讲授 | 2.3 |
| 网络加密技术 | 掌握 |
| 对称加密技术，DES算法 | 掌握 | 4 | 课堂讲授 |
| 非对称加密技术，RSA算法 | 掌握 | 4 | 课堂讲授 |
| 3 | 信息系统安全协议 | 鉴别与数字签名 | 掌握 | 2 | 课堂讲授 | 5.2，2.3 |
| 身份认证与访问控制 | 掌握 | 2 | 课堂讲授 |
| 公钥基础设施PKI与CA | 掌握 | 2 | 课堂讲授 |
| 电子商务安全 | 掌握 | 2 | 课堂讲授 |
| 4 | 信息系统安全技术 | 防火墙 | 理解 | 2 | 课堂讲授 | 5.2 |
| 虚拟专网VPN | 掌握 |
| 入侵检测系统IDS | 掌握 | 2 | 课堂讲授 |
| 安全审计 | 了解 |
| 5 | 攻击与防范 | 恶意软件 | 掌握 | 2 | 课堂讲授 | 5.2，9.1 |
| 物理安全 | 理解 | 2 | 课堂讲授 |
| 数据库安全 | 理解 |
| 6 | 复习研讨 | 课堂复习总结和讨论 |  | 2 | 课堂讨论 | 2.3， 5.2 |

**六、课程教学安排**

**（一）知识讲授部分**

本课程是通信工程、信息工程专业的专业B类选修课，需要运用先修的概率论与数理统计、线性代数等专业数学知识和通信与计算等基础理论知识，又涉及到后续专业课程的多个领域，适宜采用灵活多样的教学方式，将理论教学、研讨、自主学习等有机结合。通过课堂理论教学讲解基础原理和分析方法，指导课后学生自学部分拓展知识并开展研讨。

教学方法设计及教学环节的安排建议和要求。其中，课堂讲授包括教学方法和手段设计；作业方面主要写明布置习题达到的目的与要求，题量、题型要求等，提倡按照教学的层次设计作业，包括结课小论文等形式。

**1．课堂讲授**

在教学过程中，教师应以建立概念、形成整体思路为基础，指出每章的重点和难点部分。上课时，适当提出一些问题，引导学生分析讨论，以调动学生的主动性，活跃课堂气氛提高课堂质量，集中学生注意力，培养学生发现问题和分析问题的能力。对教学媒体的运用须密切结合课程知识点的需要加以选择。

**2．习题及指导分析**

本课程理论与实际应用相结合，其中知识点需要作业支撑，一些实用技术需要课后自学整理。题型包括计算、画图、分析和设计等。通过习题巩固知识点的掌握，并适当布置自学作业，达到培养学生主动学习拓展知识的能力，锻炼其分析问题解决问题的能力。根据情况适当增设课堂习题指导及作业评述。

计算题集中在算法学习和设计中，例如RSA算法的计算过程；画图题可以用来复习DES以及相似结构的对称加密算法的设计；设计分析题目则是针对实际信息系统，分析其威胁，利用所学的技术和协议设计有效的防御体系。

**3．指导自学**

本课程与信息网络的日常应用息息相关，很多问题都来自于实际网络环境，而学时数有限，同时为了培养锻炼学生自学能力，对课程内容相关的实际安全问题，要求学生通过自学和调查研究，通过指导，使学生更好的掌握所学知识。内容可以是当前网络面临的主流威胁和防御手段，也可以是协议的发展各阶段各版本等。

**本课程学时数有限，实验以及专业讨论由相关课程支持。**

**（二）课程思政**

课程思政坚持正确的政治方向，紧紧围绕立德树人根本任务，针对《信息系统安全》课程理论性强、概念抽象、数学知识多的特点，细化分解课程思政育人主题，深挖知识点中隐含的思政元素，将课程思政案例（见下表）有机融入相关知识点和教学环节中，通过案例讲解、学生提问、课后调研、课堂展示、实验实践等方式，在进行知识传授、能力培养的同时，以“融盐与水、润物无声”的形式浸润学生心灵，使之内化为学生的精神追求、外化为学生的自觉行动。

表1《信息系统安全》思政案例

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 章节名称 | 知识点 | 所挖掘的思政元素 |
| 1 | 1 绪论1 | 安全体系架构，信息安全概况 | 【**知安全形势-担时代重任**】**-**讲解国内外安全案例，说明信息网络是国家的第五空间，让学生认识到自己肩负的责任，树立正确的学习的目标，未来建设国家信息安全保障体系，使我国成为网络强国。 |
| 2 | 1 绪论2 | 信息安全法律法规 | 【**工程伦理-法律意识**】**-**用实际案例向学生普及法律知识，让学生深刻认识到法律神圣，不容侵犯，网络不是法外之地，做为专业人员要知法懂法守法。 |
| 3 | 2 密码学基础知识 | 密码学发展史 | 【**中华文明-爱国主义精神**】**-**补充了中国的密码学发展内容，无论是孙子兵法理论还是戚继光戚家军的密码实践，到现在的量子计算和墨子卫星，都闪耀着中华文明的智慧，增强学生的民族自豪感。 |
| 4 | 3 信息系统安全协议 | 哈希函数 | 【**工匠精神-严谨治学-爱国情怀**】  引入王小云院士在哈希函数领域的研究工作，学习甘坐冷板凳的默默钻研精神、精益专注的工匠精神和科研报国的爱国主义精神，树立未来投身民族复兴伟业的正确志向和远大抱负。 |

**七、课程考核**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **课程成绩构成及比例** | **考核环节** | **目标分值** | **考核/评价细则** | **对应的课程目标** |
| 平时成绩1  占总评成绩的40% | 作业 | 100 | （1）主要考核学生对每章节知识点的复习、理解和掌握程度；  （2）每次作业单独评分，取各次成绩的平均值作为此环节的最终成绩。 | 1，2，3 |
| 平时成绩2  占总评成绩的30% | 随堂练习 | 100 | （1）开卷或者半开卷的方式，考核学生当堂内容或该章节应该掌握的内容。  （2）考核内容体现对于综合运用基本概念、基本原理和分析方法进行信息系统安全性设计和分析能力的考察,建议对应课程目标1的考查题型以填空题、作图题和计算题为主；对应课程目标2的考查题型以分析题、设计题为主。 | 2，3 |
| 结课论文  100分  占总评成绩的30% | 结课论文 | 100 | （1）考查学生自主学习、独立思考和拓展专业知识的能力。并且通过文字表达能力评价学生对自主学习能力的掌握程度。  （2）教师根据小论文的完成情况评定成绩。 | 1，2，3 |

根据以上三项成绩计算每名学生的综合成绩：

**综合成绩=作业×0.40+随堂练习×0.30 +结课论文×0.30**

**八、本课程与其它课程的联系与分工**

本课程与先修课程和后续课程联系都比较紧密，课程内容应避免重复。

先修课程：概率论和数理统计，计算机网络，通信基础理论课。

后续课程：通信工程其它信息安全类专业课，包括实验以及专题研讨课。

**九、建议教材及教学参考书**

1. 张基温，信息系统安全教程（第二版），清华大学出版社，2015.
2. 石文昌，信息系统安全概论（第二版），电子工业出版社，2014
3. 奥巴代特，布德里卡 著，毕红军，张凯 译，计算机网络安全导论，电子工业出版社，2009
4. 王育民，刘建伟， 通信网的安全--理论与技术，西安电子科技大学出版社出版，1999
5. 刘建伟，王育民， 网络安全：技术与实践(第2版)，清华大学出版社，2011
6. 斯托林斯　著，王张宜　等译，密码编码学与网络安全——原理与实践（第七版），电子工业出版社出版，2021
7. 有关信息系统安全的最新统计数据和信息网络安全应急响应网站发布的最新消息

**十、大纲审核人**

**十一、学院审核程序说明**

由通信系制定，负责本科教学工作的系主任审核，经学院教学指导委员会审核批准。

**十二、学院审定日期**

**附：达成度评价方法：**

课程目标达成度评价包括课程分目标达成度评价和课程总目标达成度评价，具体计算方法如下：





课程目标评价内容及符号意义说明如附表1，字母*A*、*B*、*C*则分别表示随堂练习、作业和结课论文的实际平均得分，其中，*A*= *A*1+*A*2，*B*= *B*1+*B*2，*C*= *C*1+*C*2；各部分成绩分别占总评成绩的30%、40%和30%。

附表1 课程评价考核基本信息表

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **课程目标评价内容** | **随堂练习** | | **作业** | | **结课论文** | | **课程总评成绩** |
| 基本概念  基本规律 | 分析和讨论 | 基础知识和计算 | 分析和问答 | 技术方案 | 心得体会 |
| 目标  分值 | 10 | 20 | 20 | 20 | 20 | 10 | 100 |
| 学生平均得分 | *A*1 | *A*2 | *B*1 | *B*2 | *C*1 | *C*2 | (*A*+*B*+*C*) |

课程目标达成度评价值计算具体说明如附表2。

附表2课程达成度评价计算方法

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **课程目标** | **考核环节** | **目标分值** | **学生平均得分** | **达成度计算示例** |
| 课程目标1 | 课堂问答（基本概念基本规律） | 10 | *A*1 | 课程目标1达成度=（*A*1 *+B*1）/30 |
| 作业（基础知识和计算） | 20 | *B*1 |
| 课程目标2 | 课堂问答（分析和讨论） | 20 | *A*2 | 课程目标2达成度=（*A*2+*B*2 *+C*1）/60 |
| 作业（分析和问答） | 20 | *B*2 |
| 结课论文（技术方案） | 20 | *C*1 |
| 课程目标3 | 结课论文（心得体会） | 10 | *C*2 | 课程目标3达成度=*C*2/10 |
| 课程总体目标 | 总评成绩 | 100 | *A*+*B*+*C* | 课程总目标达成度= *（A*+*B*+*C）/100* |