北京工业大学

本科课程教学大纲

Undergraduate Course Syllabi

信息学部

2020 版

信息安全专业

目　录

“离散数学”课程教学大纲

英文名称：The Discrete Mathematics

课程编号：0010121

课程性质：学科基础必修课

学分：2.5　　学时：45

面向对象：信息安全（实验班）专业本科生

先修课程：高等数学（工）、线性代数（工）

推荐教材及参考书：

[1] Kenneth H. Rosen，Discrete Mathematics and Its Applications: And Its Applications（英文影印版.第 6 版）,机械工业出版社, 2008 年 5 月.

[2] 邵学才，《离散数学(第 2 版)》，电子工业出版社，2009，4

[3] 邵学才，叶秀明，《离散数学 (第四版) 》，机械工业出版社，2011

[4] [美] Richard Johnsonbaugh 石纯一等译，离散数学，人民邮电出版社，2009

[5] [美] Kenneth H. Rosen 著，袁崇义等译，《离散数学及其应用》，机械工业出版社，2002

[6] 左孝凌等，离散数学，上海科学技术文献出版社，1982

[7] 屈婉玲、耿素云、张立昂，《离散数学（第 2 版)》，清华大学出版社，2008

[8] 王元元，离散数学，机械工业出版社，2010

[9] Bemard Kolman, Robert C．Busby，Sharon Ross．Discrete Mathematical Structures，高等教育出版社，2001

[10] 屈婉玲等，离散数学，高等教育出版社，2008

一、课程简介

离散数学属于理工科高等院校信息安全专业必修的、重要的学科基础课程，是以研究离散结构为对象的数学课程，与计算机科学理论、应用技术有着密切的联系。课程中的综合、分析、归纳、演绎、递推等方法在信息安全中有着广泛的应用，不仅为后续课程如：数据结构、操作系统、编译原理等做必要的理论准备，而且其课程内容中所提供的一些把科学理论应用于实践的范例可以培养学生逐步增强如何实施“科学理论一一技术——生产力”转化的观念和方法，提高学生在知识经济时代中的适应能力，培养学生具有一定的解决实际问题的能力和创新能力、抽象思维和概括能力、严谨的数学推理的能力。

二、课程地位与目标

（一）课程地位：本课程是理工科高等院校计算机专业必修的、重要的学科基础课程，在计算机专业人才培养中有着很大作用。本课程与计算机科学理论、应用技术有着密切的联系。通过学习这门课程，使学生能够正确理解和熟练掌握离散数学中的基本概念、基本定理及其证明方法，提高运用基本理论分析和解决实际问题的能力，为其进一步深入学习计算机专业相关知识打下良好的基础。

本课程支撑的毕业要求拆分指标点的具体描述。

2.1 能应用数学、自然科学和专业相关知识正确表示复杂工程问题。

2.2 能针对一个系统或过程选择或建立适当的描述模型。

3.1 能识别和判断信息安全复杂工程问题的关键环节和参数。

3.4 能正确表达一个工程问题的解决方案。

（二）课程目标

1 教学目标：写明课程拟达到的课程目标，指明学生需要掌握的知识、素质与能力及应达到的水平，本课程对毕业要求拆分指标点达成的支撑情况，详见表 1。

表 1 课程目标与毕业要求拆分指标点的对应关系

序号	课程目标	毕业要求拆分指标点			
		2.1	2.2	3.1	3.4
1	培养学生的数学思维能力，使学生得到良好的数学训练。	●			
2	培养学生的抽象思维和逻辑推理能力，使学生获得应用数学模型解决数学问题的技能。		●		
3	通过学习离散数学中各个原理在信息安全层面的应用，使学生获得把数学思维应用于信息安全的意识。			●	
4	使学生掌握处理离散结构所必须的描述工具和方法，获得应用数学知识解决信息安全具体问题的能力。				●

注：●：表示有强相关关系，◎：表示有一般相关关系，⊙：表示有弱相关关系

2 育人目标：课程不仅培养学生专业技能，更加培养学生的家国情怀、民族自信、责任担当、职业素养、行为规范等育人元素。我国一直将科教兴国、人才强国和创新驱动发展战略放在国家发展的核心位置,高度重视人才,重视科技。而本课程运用了引导学生独立思考、加强实践等教学方法，使学生牢固掌握离散数学知识并将其应用于实践，使离散数学教学为培养应用型人才服务。在信息化的时代，建设祖国不仅需要坚实的信息技术作为后盾，也需要卓越的应用能力。作为计算机相关专业的学生，不仅要学好专业知识，掌握应用技术，更要有民族自信和责任担当，在为祖国建设事业添砖加瓦的过程中实现人生理想。

三、课程教学内容

分章节列出课程教学内容及对课程目标的支撑，详见表 2。

表 2 教学内容与课程目标的对应关系

章节名称	教学内容及重点（▲）、难点（★）	课程目标（√）			
		1	2	3	4
第一章集合	集合的表示方法及子集、幂集基本概念▲★，集合的运算方法▲和集合等式的证明	√	√		
第二章二元关系与函数	二元关系的三种表示方法，二元关系的五种基本类型，传递关系的矩阵判定方法，等价关系与划分之间的关系▲，相容关系和覆盖的基本概念，偏序关系的概念▲、HASSE 图▲、特异元素，复合关系和逆关系，三种关系的闭包运算，集合论中的一般函数，特殊函数▲，复合函数和逆函数▲；	√	√		

第三章组合计数初步	容斥原理，鸽笼原理，递推关系；	√	√		
第四章图论	各种图的定义、图的同构、顶点的度、图的矩阵表示，通路、回路与连通图的定义，求赋权图中最短通路图的 Dijkstra 算法▲，用矩阵方法研究图的性质，欧拉图的性质及应用▲，哈密尔顿图的性质及应用▲，中国邮路问题和旅行推销员问题，二部图的定义、定理及应用▲，可平面图的判定★、库拉托夫斯基定理的应用，无向树的定义、生成树，无向树的性质及应用▲，有向树的性质及其应用▲；	√	√	√	√
第五章命题逻辑	命题的符号化方法[2]，对偶原理[3]，命题逻辑等价的证明[1]，永真蕴含式的证明▲，推理理论的规则和推理过程▲★，主析取范式和主合取范式▲。	√	√	√	√
第六章谓词逻辑	谓词的符号化方法★，谓词逻辑等价和永真蕴含式▲，推理理论的规则和推理过程▲★；	√	√	√	√
第七章代数系统简介	代数系统的定义，代数系统中的特殊运算与特殊元素，代数系统中同构的概念★，半群及其性质▲，群及其性质▲，子群的概念，循环群的概念及性质，置换群的概念及性质，拉格朗日定理及应用★，同态和同余★，群码的应用，环和域 ▲，格的定义及与偏序之间的关系▲，有补格、有界格、分配格。	√	√	√	√

四、教授方法与学习方法指导

教授方法：结合课程内容的教学要求以及学生认知活动的特点，以教师课堂讲授为主，所有的定理、定义做成课件，例题的讲解在黑板板书。经过本课程的课堂教学，首先要使学生掌握课程教学内容中规定的一些基本概念、基本理论和基本方法。特别是通过教师的讲授，使学生能够对这些基本概念和理论有更深入的理解，使之有能力将它们应用到一些问题的解决过程中。在此过程中尤其注意对其中的一些基本方法的核心思想的分析，使学生能够掌握其关键。

学习方法：教材上的习题较为丰富，着重选择概念题、证明题、计算题和综合分析题等题型，目的在于加强学生对知识的理解。通过课外作业，使学生重温课堂讲述的内容，自觉检验学习的效果，了解自己掌握的程度，思考一些相关的问题，进一步深入理解扩展的内容。

五、教学环节及学时分配

教学环节及各章节学时分配，详见表 3。

表 3 教学环节及各章节学时分配表

章节名称	教学内容	学时分配					合计
		讲授	习题	实验	讨论	其它	
第一章 集合	集合的表示方法及子集、幂集基本概念，集合的运算方法和集合等式的证明	2					2
第二章 二元关系与函数	二元关系的三种表示方法，二元关系的五种基本类型，传递关系的矩阵判定方法，等价关系与划分之间的关系，相容关系和覆盖的基本概念，偏序关系的概念、HASSE 图、特异元素，复合关系和逆关系，三种关系的闭包运算，集合论中的一般函数，特殊函数，复合函数和逆函数；	4	2				6
第三章 组合计数初步	容斥原理，鸽笼原理，递推关系；	2	1				3
第四章 图论	各种图的定义、图的同构、顶点的度、图的矩阵表示，通路、回路与连通图的定义，求赋权图中最短通路图的 Dijkstra 算法，用矩阵方法研究图的性质，欧拉图的性质及应用，哈密尔顿图的性质及应用，中国邮路问题和旅行推销员问题，二部图的定义、定理及应用，可平面图的判定、库拉托夫斯基定理的应用，无向树的定义、生成树，无向树的性质及应用，有向树的性质及其应用；	12	2				14
第五章 命题逻辑	命题的符号化方法，对偶原理，命题逻辑等价的证明，永真蕴含式的证明，推理理论的规则和推理过程，主析取范式和主合取范式。	5					5
第六章 谓词逻辑	谓词的符号化方法，谓词逻辑等价和永真蕴含式，推理理论的规则和推理过程；	4	1				5
第七章 代数系统简介	代数系统的定义，代数系统中的特殊运算与特殊元素，代数系统中同构的概念，半群及其性质，群及其性质，子群的概念，循环群的概念及性质，置换群的概念及性质，拉格朗日定理及应用，同态和同余，群码的应用，环和域 ，格的定义及与偏序之间的关系，有补格、有界格、分配格。	8	2				10
合计		37	8				45

六、考核与成绩评定

课程成绩包括：平时成绩 20%（作业 80%，其它 20%），考试成绩 80%。

平时成绩中的其它 20%主要反应学生的课堂表现、平时的信息接收、自我约束。成绩评定的主要依据包括：课程的出勤率、课堂的基本表现（如课堂测验、课堂互动）等；作业占 80%主要是课堂作业和课外作业，主要考察学生对已学知识掌握的程度以及自主学习的能力。

考试成绩 80%为对学生学习情况的全面检验，更具有重要的导向作用。考题要强调考查学生对基本概念的理解以及将其综合运用解决问题的能力，淡化考查一般知识、结论的死记硬背。

本课程各考核环节的比重及对毕业要求拆分点的支撑情况，详见表 4。

表 4 考核方式及成绩评定分布表

考核方式	占比（%）	主要考核内容及对毕业要求拆分指标点的支撑情况
平时成绩	20	主要考核内容：对已学知识掌握的程度以及自主学习的能力，包括课程的出勤率、课堂的基本表现（如课堂测验、课堂互动）等；作业（课堂作业和课外作业）。对毕业要求的支撑：2.1、2.2、3.1、3.4
考试成绩	80	主要考核内容：对基本概念、基本方法、基本理论等方面掌握的程度，及学生运用所学理论知识解决复杂问题的能力。对毕业要求的支撑：2.1、2.2、3.1、3.4

七、考核环节及质量标准

本课程各考核环节及质量标准，详见表 5。

表 5 考核环节及质量标准

考核方式	评　分　标　准				
	A	B	C	D	E
	90～100	80～89	70～79	60～69	< 60
作业	积极完成作业规定任务并提前提交作业；作业书写非常工整；简答题回答非常完整；计算题有步骤且结果正确。	按时完成作业规定任务；作业书写工整；简答题回答比较完整；计算题有步骤且结果比较正确。	大部分情况下能按时完成作业规定任务；作业书写比较工整；简答题回答比较完整；计算题有步骤且结果大部分正确。	基本按时完成作业规定任务；作业书写基本工整；简答题回答基本完整；计算题结果基本正确。	不满足 D 要求
研讨	能够准确、流利陈述相关概念和技术，能够将知识融会	能够准确陈述相关概念和技术，能够把知识联系起来，	能够比较准确地陈述相关概念和技术，能够把知识联系起来，在老师的	能够基本准确陈述相关概念和技术，在老师	不满足 D 要求

	贯通，能积极主动参与讨论，并能发表自己的观点，且观点正确。	能主动参与讨论，并发表自己的观点，且大部分观点正确。	引导下积极参与讨论并回答老师提出的大部分问题。	的引导下能参与讨论，能回答老师提出的部分问题。	
实验	无	无	无	无	不满足 D 要求
考试	完全掌握相关概念、原理及技术，能够运用理论知识解决各种复杂问题。卷面整洁、字迹工整，客观题回答非常正确，简答题回答非常完整、计算和分析非常正确。	掌握相关概念、原理及技术，能够运用理论知识解决多个复杂问题。卷面整洁、字迹工整，客观题回答大部分正确，简答题回答比较完整、计算和分析比较正确。	掌握大部分相关概念、原理及技术，能够运用理论知识解决若干复杂问题。卷面比较比较整洁、字迹比较工整，客观题回答大部分正确，简答题回答大部分、计算和分析大部分正确。	基本掌握相关概念、原理及技术，能够理论知识解决一些比较复杂的问题。卷面较整洁、字迹尚工整，简答题基本完整、计算和分析基本正确。	不满足 D 要求
评分标准（A～E）：主要填写对教学内容中的基本概念、理论、方法等方面的掌握，及综合运用理论知识解决复杂问题能力的要求。					

制定者：公备

批准者：张建标

2020 年 7 月

“网络空间安全导论”课程教学大纲

英文名称：Introduction to Cyberspace Security

课程编码：0010677

课程性质：学科基础必修课

学分： 2.0 学时：32

面向对象：信息安全（实验班）专业本科生

先修课程：

教材及参考书：

[1] 刘建伟等编著. 网络空间安全导论. 清华大学出版社. 2020.9

[2] 李剑 杨军主编. 网络空间安全导论. 机械工业出版社. 2020.12

[3] 沈昌祥等编著. 网络空间安全导论. 电子工业出版社. 2018.05

[4] 石文昌 编著. 网络空间系统安全概论（第 3 版）. 电子工业出版社. 2021.1

[5] 朱建明等编著. 信息安全导论. 清华大学出版社. 2015.9

[6] 黄波等编著. 网络空间安全素养导论. 清华大学出版社. 2019.8

[7] 教育部高等学校网络空间安全学科专业教学指导委员会 编制. 高等学校信息安全专业指导性专业规范. 清华大学出版社. 2019.12

一、课程简介

随着信息技术与产业的高速发展和广泛应用,人类社会进入信息化时代。在信息化时代,人类生活工作在网络空间中, 网络空间的信息安全事件不断发生，因此网络空间安全成为信息时代的基本需求。目前，我国已发展形成完整的网络空间安全学科和信息安全专业体系。本课程从信息化与网络空间的信息安全关系切入，介绍网络空间信息安全的内涵特点、信息安全与社会经济发展的关系、以及信息安全专业涉及的主要学科知识、课程体系和人才培养基本要求等，旨在帮助学生形成较系统的信息安全专业认识，帮助学生了解信息安全技术的发展历史和沿革，为后续其他专业课程的深入学习打好基础。

二、课程地位与目标

（一）课程地位：“网络空间安全导论”课程是信息安全专业本科生的必修课程，也是其他专业学习信息安全知识的入门课程，是信息安全专业完整知识体系的绪论，通过这门课程的学习，使学生了解和掌握网络空间安全学科的内涵特点、信息安全专业涉及的主要学科知识、课程体系和人才培养基本要求等，帮助学生了解网络空间安全技术的发展历史和沿革、树立信息安全专业的整体知识框架，帮助学生识别信息安全专业知识能解决的主要问题，帮助学生明确信息安全专业大学毕业生应该具备的素质和能力，培养学生追求科学真理、热爱祖国，为保护网络空间安全努力奋斗的情怀，为后续其他专业课程的学习打下坚实的基础。

本课程支撑的毕业要求拆分指标点的具体描述。

3.1：能识别和判断信息安全复杂工程问题的关键环节和参数

7.1：具有社会、健康、法律以及文化意识，能够认识到信息安全产业对他们的影响

8.1：具有环境保护和社会持续发展意识，能认识到信息安全系统的开发、运行、更新换代对环境保护和社会持续发展的影响

13.1：认识到网络空间安全学科是一个发展迅速的学科，具有自主学习和终身学习的意识

（二）课程目标

1 教学目标：本课程帮助学生了解和掌握网络空间安全学科内涵、信息安全的属性和概念，明确信息安全与社会、经济、文化发展和健康、法律等的关系；要求学生从整体上了解信息安全涉及的主要学科知识，帮助学生形成信息安全专业较为系统的全局知识框架；要求学生认识和理解信息安全专业的课程体系，帮助学生识别和判断不同信息安全专业知识能解决的复杂工程问题；引导学生了解国内外信息安全领域的最新发展动态和发展趋势，帮助学生认识信息安全专业大学毕业生应该具备的素质和能力。本课程对毕业要求拆分指标点达成的支撑情况，详见表 1。

表 1 课程目标与毕业要求拆分指标点的对应关系

序号	课程目标	毕业要求拆分指标点			
		3.1	7.1	8.1	13.1
1	让学生从整体上了解信息安全涉及的主要学科知识，树立全局知识框架，帮助学生识别和判断不同信息安全专业知识能解决的对应复杂工程问题。	◎			
2	通过学习和理解网络空间安全学科的内涵和信息安全专业特点，帮助学生明确信息安全与社会经济文化发展的关系，认识信息安全对社会安全、经济安全、文化安全以及健康、法律等的重要影响。		●		
3	通过学习和理解网络空间安全学科的内涵和信息安全专业特点，帮助学生认识信息安全专业大学毕业生应具备的素养和能力，包括应具有的环境保护和社会持续发展意识。			◎	
4	引导学生了解信息安全领域的最新动态，帮助学生认识到信息安全是发展迅速的，信息安全专业的毕业生应具有自主学习和终身学习的意识。				◎

注：●：表示有强相关关系，◎：表示有一般相关关系，⊙：表示有弱相关关系

2 育人目标： 在知识传授中强调主流价值引领，挖掘课程中蕴含的思政元素，通过讲述我国在网络空间信息安全技术的最新成果与应用，结合对我国网络空间安全的重要战略和政策的研讨互动，让学生了解我国在网络空间信息安全技术方面的需求、已取得的成果以及与世界先进国家的差距，鼓励学生树立奋起直追的意识，帮助学生树立科学的发展观，提升学生追求科学真理、热爱祖国、为保护网络空间安全努力奋斗的家国情怀，增强学生在网络命运共同体、网络空间治理和网络强国等方面的责任和担当。

三、课程教学内容

分章节列出课程教学内容及对课程目标的支撑，详见表 2。

表 2 教学内容与课程目标的对应关系

章节名称	教学内容及重点（▲）、难点（★）	课程目标（√）			
		1	2	3	4
第一章 绪论	课程介绍（课程目标、课程的教学内容、教材及参考文献和考核要求等）； 信息化发展与信息安全 信息化发展 信息安全威胁与热点事件 我国的信息安全工作▲ 网络空间安全学科浅谈 网络空间与网络空间安全的概念▲，★ 网络空间安全学科内涵▲，★ 网络空间安全与信息安全 信息安全基本概念与体系结构 信息的安全属性▲ 信息安全概念的演变 信息安全保障（定义、三要素）▲，★ 信息安全术语（脆弱性、威胁的定义及分类▲、攻击的定义及分类▲、风险的定义及决定因素▲） 信息安全专业知识体系▲，★	√	√	√	
第二章 计算系统、网络信息系统基础	计算机系统概述 计算机网络概述 计算机网络的定义与类别 计算机网络体系结构▲，★ 信息系统概述 信息系统的分类 信息系统的功能▲，★	√			
第三章 密码学 基础	密码学的概念▲ 密码机制 基本组成及分类▲ 对称密码的基本加解密原理▲ 非对称密码的基本加解密原理▲，★ Hash 函数与消息认证 Hash 基本概念和原理★ 消息认证技术的基本思想★ 数字签名技术 数字签名的特点和功能 数字签名的基本原理▲	√			√
第四章 系统安全 基础	系统安全的概念▲ 系统安全威胁 系统安全关键技术介绍 系统硬件平台安全技术	√			

	操作系统安全技术（身份认证、访问控制、数据加密和安全审计等）▲,★ 数据库安全技术（并发控制等）▲ 软件安全技术（恶意代码检测、逆向工程等）★ 系统可靠性技术（备份、恢复等）★				
第五章 网络安全基础	网络安全的概念 网络安全威胁▲ 网络安全关键技术介绍 入侵检测（基本概念、分类）▲ 网络安全协议（基本概念、作用和典型协议）▲ 网络安全防护（基本概念、网络安全扫描、防火墙▲、虚拟专用网等） 新兴网络及安全技术（工业互联网安全、移动互联网安全、物联网安全等）	√			√
第六章 内容安全基础	内容安全的概念▲ 内容安全威胁 内容安全关键技术介绍▲ 信息内容获取 信息内容识别和分析 信息内容控制和管理（信息过滤、信息隐藏、数字水印和版权保护等）★	√			
第七章 网络空间安全法律法规	中华人民共和国网络安全法▲ 中华人民共和国密码法 中华人民共和国计算机信息系统安全保护条例 中华人民共和国数据安全法▲		√		
第八章 新技术及新应用中的安全	云计算安全概述 云计算基本概念和基本原理 云计算安全问题★ 云计算安全技术现状▲ 大数据安全与隐私保护 大数据基本概念 大数据面临的安全威胁★ 大数据安全与隐私保护技术现状▲,★ 其他开放问题（如区块链及其安全、人工智能及其安全等）				√

四、教授方法与学习方法指导

教授方法： 以讲授为主，作业为辅。课内讲授采用探究教学、项目驱动、案例教学等多种教学方法与模式，结合多媒体、板书等教学手段，通过范例和视频演示讲授教学内容，以知识为载体，侧重传授相关的技术思想和方法。使学生在充分理解网络空间安全学科的内涵特点、信息安全专业涉及的主要学科知识、课程体系和人才培养基本要求的基础上，

形成信息安全专业的整体知识框架，了解现代密码学、系统安全、网络安全、内容安全和新型信息安全技术的基本方法，为学生理解专业方向基础知识、后续专业课程的学习以及从事网络空间安全相关领域的设计、分析、开发与管理等学习与工作打下坚实的基础。课外作业既包含对课内讲授重点难点知识的巩固，也包括扩展知识的课下自学，帮助学生拓展视野。

学习方法：养成探索和思考的习惯，特别是重视对基本理论的钻研和知识框架的构建，在理论指导下进行实践。明确学习各阶段的重点任务，做到课前预习，课中认真听课，课后认真复习，不放过疑点，充分利用好教师资源和同学资源。仔细研读教材，适当选读参考书的相关内容或利用国内外多所高校已开设的相关 MOOC 课程资源，从系统实现的角度深入理解概念，掌握方法的精髓和技术的原理。积极按时完成作业，通过作业加深对各种网络空间安全技术工作原理的理解。

五、教学环节及学时分配

教学环节及各章节学时分配，详见表 3。

表 3 教学环节及各章节学时分配表

章节名称	教学内容	学 时 分 配					合计
		讲授	习题	实验	讨论	其它	
第一章	绪论	4					4
第二章	计算系统、网络与信息系统基础	4					4
第三章	密码学基础	4					4
第四章	系统安全基础	6					6
第五章	网络安全基础	6					6
第六章	内容安全基础	2					2
第七章	网络空间安全法律法规	2					2
第八章	新技术及新应用中的安全	2					2
	总结复习和考试					2	2
合计		30				2	32

六、考核与成绩评定

课程成绩包括平时成绩、作业成绩和期末考试成绩三部分。

考核方式及成绩评定分布：

平时成绩占 10%，主要反应学生的课堂表现、平时的信息接收、自我约束。成绩评定的主要依据包括：课程的出勤率、课堂的基本表现（如课堂测验、课堂互动等）；

作业成绩占 20%（平时课后小作业占 5 %和课程大作业占 15%），平时课后小作业随堂布置，主要考察学生对已学知识点的掌握程度以及自主学习的能力。课程大作业为学生自拟题目或根据任课教师提出题目撰写的课程学习小论文，主要考核学生对网络空间安全特点及发展机遇的认识、对信息安全专业整体知识框架的掌握、对国内外信息安全发展动态的了解、对网络空间安全需要的个人素养和职业素养的认识等等，还包括学生的语言及文字表达能力。

考试成绩占 70%，是对学生学习情况的全面检验，书面考试形式，主要考核学生对网络空间安全中涉及的基本概念、基本方法、基本理论等方面掌握的程度， 涵盖所学内容 90%以上，题型包括填空题、选择题、问答题等。

本课程各考核环节的比重及对毕业要求拆分点的支撑情况，详见表 4。

表 4 考核方式及成绩评定分布表

考核方式	所占比例（%）	主要考核内容及对毕业要求拆分指标点的支撑情况
平时成绩	10%	考查学生课堂的参与度，对所讲内容的基本掌握情况，通过考核学生课堂练习参与度（含出勤情况）及其完成质量，对应课程目标 1 和课程目标 3 的考核。
作业成绩	20%	平时课后小作业随堂布置，主要考察学生对已学知识点的掌握程度以及自主学习的能力。课程大作业为学生自拟题目或根据任课教师提出题目撰写的课程学习小论文，主要考核学生对网络空间安全特点及发展机遇的认识、对信息安全专业整体知识框架的掌握、对国内外信息安全发展动态的了解、对网络空间安全需要的个人素养和职业素养的认识等等，还包括学生的语言及文字表达能力。对应课程目标 2 和课程目标 4 达成度的考核。
考试成绩	70%	是对学生学习情况的全面检验，书面考试形式，主要考核学生对网络空间安全涉及的基本概念、基本方法、基本理论等方面掌握的程度。对应课程目标 1 和课程目标 2 达成度的考核。

七、考核环节及质量标准

本课程各考核环节及质量标准，详见表 5。

表 5 考核环节及质量标准

考核方式	评分标准				
	A	B	C	D	E
	90～100	80～89	70～79	60～69	< 60
平时成绩	上课全勤、积极回答教师随堂提问、积极参与讨论	上课全勤、较积极回答教师随堂提问、较积极参与讨论	上课全勤、较积极回答教师随堂提问、能参与讨论	上课缺席不超过 2 次、能回答教师随堂提问、能参与讨论	不满足 D 要求
课程作业	平时小作业按时完成；课程大作业文档格式规范、文字规范；对网络空间安全特点及发展机遇认识准确；正确掌握信息安全专业整体知识框架；对国内外信息安全发展动态认识深入、	平时小作业按时完成；课程大作业文档格式较规范、文字较规范；对网络空间安全特点及发展机遇认识准确；正确掌握信息安全专业整体	平时小作业按时完成；课程大作业文档格式较规范、文字较规范；对网络空间安全特点及发展机遇认识准确；较好掌握信息安全专业整体知识框架；对国内外	平时小作业按时完成；课程大作业文档格式基本规范、文字基本规范；对网络空间安全特点及发展机遇认识基本准确；基本掌握信息安全专业整体知识框架；基本了解国内外信息安全	不满足 D 要求

	对网络空间安全个人素养和职业素养认识深入。	知识框架；对国内外信息安全发展动态认识较深入；对网络空间安全个人素养和职业素养的认识较深入。	信息安全发展动态认识较深入；对网络空间安全个人素养和职业素养的认识较深入。	发展动态；基本认识网络空间安全个人素养和职业素养。	
期末考试	很好地掌握教学内容涉及的基本概念、理论、方法，且具备很强的综合运用所学知识解决复杂问题的能力。	较好地掌握教学内容涉及的基本概念、理论、方法，且具备较强的综合运用所学知识解决复杂问题的能力。	较好地掌握教学内容涉及的基本概念、理论、方法，且具备一定的综合运用所学知识解决复杂问题的能力。	基本掌握教学内容涉及的基本概念、理论、方法，且基本能具备运用所学知识解决复杂问题。	不满足D要求
评分标准（A～E）：主要填写对教学内容中的基本概念、理论、方法等方面的掌握，及综合运用理论知识解决复杂问题能力的要求。					

制定者：林莉

批准者：张建标

2020 年 7 月

“计算机网络（双语）”课程教学大纲

英文名称：Computer Networks

课程编码：0010114

课程性质：学科基础必修课

学分：2.5　　学时：40

面向对象：信息安全（实验班）专业本科生

先修课程：计算机组成原理

教材及参考书：

[1] Andrew S. Tanenbaum , Davi J. Wetherall 编著.严伟，潘爱民译.计算机网络(第 5 版).清华大学出版社，2012 年 3 月第 1 版，2018 年 11 月第 17 次印刷

[2] 谢希仁. 计算机网络（第 7 版）. 电子工业出版社，2017.1

一、课程简介

《计算机网络》是信息安全专业的学科基础必修课。通过本课程的学习，使学生能够对计算机网络原理与技术有一个系统的、全面的了解；掌握计算机网络的概念、组成、网络体系结构、网络系统结构各层的作用，理解各种应用背后的基础技术和理论。该课程对培养学生的思维能力，树立工程观念，锻炼学生的动手能力，为今后的网络相关实践和开发工作打下良好的基础。

二、课程地位与目标

（一）课程地位：本课程是学科基础必修课，在信息安全本科生一门重要专业课程，在安全专业人才培养中起着举足轻重的作用。本课程既注重对计算机网络基本原理和概念的阐述，又力求反映计算机网络的新技术。通过学习这门课程，使学生掌握网络的基本工作原理、基本理论和基本技术，为进一步深入学习网络攻击与防护、安全协议等相关专业课程打下良好的基础。通过本课程的学习，可以从多个方面为后续的实习和毕业设计提供强有力的支持。

本课程支撑的毕业要求拆分指标点的具体描述。

2.4 具备应用相关知识对系统解决方案进行比较分析、改进的能力。

3.1 能识别和判断信息安全复杂工程问题的关键环节和参数的能力。

3.2 能认识到解决问题有多种方案可以选择的能力。

3.3 能利用多种资源开展文献检索和资料查询的能力。

11.2 具有一定的英语阅读能力，能够利用一门外语进行专业相关的口头和书面交流，能有效利用外文资料的能力。

（二）课程目标

1 教学目标：写明课程拟达到的课程目标，指明学生需要掌握的知识、素质与能力及应达到的水平，本课程对毕业要求拆分指标点达成的支撑情况，详见表 1。

表 1 课程目标与毕业要求拆分指标点的对应关系

序号	课程目标	毕业要求拆分指标点				
		2.4	3.1	3.2	3.3	11.2
1	掌握计算机网络的基本概念，了解网络的发展历史，培养学生利用网络、图书馆等各种资源能利用多种资源开展文献检索和资料查询。				●	
2	掌握各种链路层、网络层和传输层协议工作原理，培养学生采用多种方案解决问题的能力			●		
3	掌握各种网络设备组网和配置网络相关设备参数，掌握组网方法，培养识别和判断信息安全复杂工程问题的关键环节和参数能力		●			
4	分析不同网络协议的优缺点，掌握不同的网络协议特点，培养学生应用相关知识对系统解决方案进行比较分析、改进的能力。	◎				
5	通过布置相关英文资料文献阅读任务，培养学生利用外文资料阅读能力；通过课程讨论，培养学生的英文口头交流能力；通过布置英文作业，培养学生的英文交流能力。					●

注：●：表示有强相关关系，◎：表示有一般相关关系，⊙：表示有弱相关关系

2 育人目标：

课程不仅培养学生专业技能，更加培养学生的家国情怀、民族自信、责任担当、职业素养、行为规范等育人元素。通过这个课程将使学生认识到：网络空间是共享的，网络空间秩序是共建的；中国是当前世界主要网络大国，但是网络大国并不等于网络强国，中国正处于由网络大国向网络强国发展的关键时期。作为世界主要网络大国，中国除了维系大国间的均势外，还肩负着特殊的“正义”职责，即始终坚定维护全球网络空间安全。在未来构建网络空间国际合作体系过程中，中国只有持续发展网络空间软硬实力，才能更多承担起网络空间的大国责任。当然负责任的网络大国形象，不仅仅依靠法规或者契约即可以达成，还需要坚实的信息技术作为后盾。作为网络安全专业学生，不仅要学好网络知识，更要有民族自信、责任担当、职业素养，才能维护好网络空间的安全，实现人生理想。

三、课程教学内容

分章节列出课程教学内容及对课程目标的支撑，详见表 2。

表 2 教学内容与课程目标的对应关系

章节名称	教学内容及重点（▲）、难点（★）	课程目标（√）				
		1	2	3	4	5
第一章计算机网络概述	计算机网络定义▲、发展、分类及应用，计算机网络体系结构★▲，网络标准化工作及相关组织▲；	√				√
第二章物理层	数据通信的基础知识，传输介质及其特性▲，数字调制与复用技术▲， 数字传输系统；	√				
第三章数据链路层	数据链路层的功能与服务▲，差错处理技术▲，数据链路层协议的基本原理和典型协议▲★；		√	√		

第四章介质访问控制子层	多路访问协议▲★，以太网▲，无线局域网，数据链路层交换技术▲；		√	√		√
第五章网络层	网络层的功能与服务▲，路由算法及协议★，网络组网方式▲，Internet 的网络层协议▲★；	√	√	√	√	√
第六章传输层	传输层的功能与服务▲，UDP 协议、TCP 协议▲★；	√	√	√	√	√
第七章应用层	应用层的功能与服务▲，域名系统 DNS▲，电子邮件系统构成与协议▲， 万维网 WWW 原理与协议▲。	√				√

四、教授方法与学习方法指导

教授方法: 结合课程内容的教学要求以及学生认知活动的特点，采取包括讲授、研讨、小组合作、探究教学、项目驱动、案例教学、线上、线上线下混合等多种教学模式与方法。

（1） 教师讲授为主，配合小组研讨

教师采用多媒体教学，讲授 35 学时，课程设置 3 学时研讨，2 学时课堂练习，鼓励学生开展小组合作的研讨。

（2） 线上线下混合式教学

针对重点、难点知识点提前发放预习材料，实现线上线下混合教学。

（3） 项目驱动的案例教学

结合网络的特点，围绕学生经常使用的 QQ、收发邮件等功能，开展项目驱动的案例教学。

学习方法：根据课程及学生学习特点，给出学习该门课程的指导和建议。可以包括体现本门课程特点的学习策略、学习技巧、自主学习指导、课程延伸学习资料获取途径及信息检索方法、教学网站及学习注意事项、学习效果自我检查方法指导等内容。

（1） 利用日新学堂开展学习

课程为双语教学，利用学校的日新学堂提供一些英文的学习资料，供学生下载学习。利用日新学堂提供的作业平台，学生可以及时看到自己的作业对错得分，检查学习效果。

（2） 加强学生的自主学习能力

计算机网络为实践性比较强的课程，课堂安排一些协议工作原理的演示，学生可以自己安装相应工具，通过自主学习加深对课程内容的深入理解。

五、教学环节及学时分配

教学环节及各章节学时分配，详见表 3。

表 3 教学环节及各章节学时分配表

章节名称	教学内容	学时分配					合计
		讲授	习题	实验	讨论	其它	
第一章计算机网络概述	计算机网络定义、发展、分类及应用，计算机网络体系结构，网络标准化工作及相关组织；	6					6

第二章物理层	数据通信的基础知识，传输介质及其特性，数字调制与复用技术， 数字传输系统；	4					4
第三章数据链路层	数据链路层：数据链路层的功能与服务，差错处理技术，数据链路层协议的 基本原理和典型协议；	4					4
第四章介质访问控制子层	多路访问协议，以太网，无线局域网，数据链路层交换技术；	5			1		6
第五章网络层	网络层的功能与服务，路由算法及协议，网络组网方式，Internet 的 网络层协议；	6	2				8
第六章传输层	传输层的功能与服务，UDP 协议、TCP 协议；	5			1		6
第七章	应用层的功能与服务，域名系统 DNS，电子邮件系统构成与协议， 万维网 WWW 原理与协议。	5			1		6
合计		35	2		3		40

六、考核与成绩评定

课程考核以考核学生对课程目标达成为主要目的，检查学生对教学内容的掌握程度为重要内容。课程成绩包括平时成绩和考试成绩两部分。

平时成绩 20%（作业 80%，其它 20%），考试成绩 80%。

平时成绩中的其它 20%主要反应学生的课堂表现、平时的信息接收、自我约束。成绩评定的主要依据包括：课程的出勤率、课堂的基本表现（如课堂测验、课堂互动）等；作业占 80%主要是课堂作业和课外作业，主要考察学生对已学知识掌握的程度以及自主学习的能力。

考试成绩 80%为对学生学习情况的全面检验。强调考核学生对基本概念、基本方法、基本理论等方面掌握的程度，及学生运用所学理论知识解决复杂问题的能力。

本课程各考核环节的比重及对毕业要求拆分点的支撑情况，详见表 4。

表 4 考核方式及成绩评定分布表

考核方式	所占比例（%）	主要考核内容及对毕业要求拆分指标点的支撑情况
平时成绩	20	主要考核内容：对已学知识掌握的程度以及自主学习的能力，包括课程的出勤率、课堂的基本表现（如课堂测验、课堂互动）等；作业（课堂作业和课外作业）。 对毕业要求的支撑： 2.4、3.1、3.2、3.3、11.2
考试成绩	80	主要考核内容：对基本概念、基本方法、基本理论等方面掌握的程度，及学生运用所学理论知识解决复杂问题的能力。 对毕业要求的支撑： 2.4、3.1、3.2、11.2

七、考核环节及质量标准

本课程各考核环节及质量标准，详见表 5。

表 5 考核环节及质量标准

考核方式	评　分　标　准				
	A	**B**	**C**	**D**	**E**
	90～100	**80～89**	**70～79**	**60～69**	**< 60**
作业	积极完成作业规定任务并提前提交作业；作业书写非常工整；简答题回答非常完整；计算题有步骤且结果正确。	按时完成作业规定任务；作业书写工整；简答题回答比较完整；计算题有步骤且结果比较正确。	大部分情况下能按时完成作业规定任务；作业书写比较工整；简答题回答比较完整；计算题有步骤且结果大部分正确。	基本按时完成作业规定任务；作业书写基本工整；简答题回答基本完整；计算题结果基本正确。	不满足 D 要求
研讨	能够准确、流利陈述相关概念和技术，能够将知识融会贯通，能积极主动参与讨论，并能发表自己的观点，且观点正确。	能够准确陈述相关概念和技术，能够把知识联系起来，能主动参与讨论，并发表自己的观点，且大部分观点正确。	能够比较准确地陈述相关概念和技术，能够把知识联系起来，在老师的引导下积极参与讨论并回答老师提出的大部分问题。	能够基本准确陈述相关概念和技术，在老师的引导下能参与讨论，能回答老师提出的部分问题。	不满足 D 要求
实验	无	无	无	无	不满足 D 要求
考试	完全掌握相关概念、原理及技术，能够运用理论知识解决各种复杂问题。卷面整洁、字迹工整，客观题回答非常正确，简答题回答非常完整、计算和分析非常正确。	掌握相关概念、原理及技术，能够运用理论知识解决多个复杂问题。卷面整洁、字迹工整，客观题回答大部分正确，简答题回答比较完整、计算和分析比较正确。	掌握大部分相关概念、原理及技术，能够运用理论知识解决若干复杂问题。卷面比较比较整洁、字迹比较工整，客观题回答大部分正确，简答题回答大部分、计算和分析大部分正确。	基本掌握相关概念、原理及技术，能够理论知识解决一些比较复杂的问题。卷面较整洁、字迹尚工整，简答题基本完整、计算和分析基本正确。	不满足 D 要求
评分标准（A～E）：主要填写对教学内容中的基本概念、理论、方法等方面的掌握，及综合运用理论知识解决复杂问题能力的要求。					

制定者：段立娟

批准者：张建标

2020 年 7 月

“信息安全数学基础”课程教学大纲

英文名称：Mathematic Foundations of Information Security

课程编码：0008206

课程性质：学科基础必修课

学分：2.5　　学时：45

面向对象：信息安全（实验班）专业本科生

先修课程：高等数学（工）；线性代数（工）

教材及参考书：

[1] 陈恭亮 编著，信息安全数学基础，清华大学出版社，2018 年。

[2] 潘承洞 潘承彪 编著，《初等数论》，北京大学出版社，1992 年。

[3] 吴品三 编著，《近世代数》，人民教育出版社，1983 年。

[4] 李继国等 编著，《信息安全数学基础》，武汉大学出版社，2006 年。

[5] 谢敏 编著，《信息安全数学基础》，西安电子科技大学出版社，2006。

一、课程简介

为了解决信息系统的安全问题，信息安全技术广泛的用于通信系统的各个层面。从抽象的角度讲,信息安全技术是保障信息安全基本属性顺利实现的主要手段。而基本安全属性的实现需要较为深刻的数学理论支持。现有各学科教学体制中缺乏专门介绍密码以及信息安全所涉及的数学知识的课程。其中，数论和代数结构是解决现代密码关键技术的理论基础。而密码技术可以提供包括保密性在内的多种安全属性的实现。因此，为了适应信息技术发展的需求，将信息安全相关的数学作为一门独立的基础课程，为解决信息安全理论与实践问题提供数学基础。

二、课程地位与目标

（一）课程地位：本课程为信息安全专业以及与通信相关的各专业的本科生奠定一定的数学基础，提高他们认识、分析和解决信息安全问题的能力。

本课程是学科基础课，系统地介绍与密码技术相关的数学知识以及信息安全设计的主要思想，并通过一些应用实例使学生了解数学知识在信息安全中的应用。本课程属于应用数学的范畴，将通过实例激发学生学习抽象数学知识的积极性，为进一步应用数学知识解决信息安全领域的理论与实践问题奠定扎实的数学基础。写明本课程在人才培养体系中的地位和作用。

本课程支撑的毕业要求拆分指标点的具体描述。

2.1：培养学生应用数学知识正确表示信息安全复杂工程问题的能力。理解数学内在的性质和变化规律，锻炼从数学角度对信息安全问题的表达和分析的能力。

3.5 培养学生应用数学的基本原理证实解决方案的合理性，获得有效结论。从实际出发，能够抽象出相应的数学问题，并应用数学基本理论解决问题，进而验证方案的合理性。

4.2 能针对特定需求完成系统模块的设计与实现，测试验证模块的正确性，并进行性能优化。数学知识的系统性和逻辑性可以引导学生在系统模块的设计与实现，测试验证模

块的正确性，并进行性能优化方面提供支持。

4.5：能对已有复杂问题的解决方案进行研究，并提出新的替代方案。数学基础在工程领域的灵活应用有助于学生对已有复杂问题的解决方案进行深入研究，并通过文献阅读和数学知识的综合应用能够创新性的提出新方案。

（二）课程目标

1 教学目标：本课程通过讲解与密码技术相关的数学知识，奠定进一步学习信息安全专业知识的理论基础。本课程要求的基本教学内容，在授课中应完全涵盖，主讲教师可以根据学生的状况，自身的体会等在某些方面进行扩展和对学生进行引导，适当扩大学生的涉猎面, 使学生掌握“信息安全数学”中的基本概念、基本理论、基本方法，体验分析和解决问题的乐趣。本课程对毕业要求拆分指标点达成的支撑情况，详见表 1。

表 1 课程目标与毕业要求拆分指标点的对应关系

序号	课程目标	毕业要求拆分指标点			
		2.1	3.5	4.2	4.5
1	掌握信息安全数学的基本概念和基础理论	●			
2	了解密码学的基本思想,学习设计和分析安全问题的数学方法。		●		
3	加强数学思维能力的训练，为分析和解决实际问题提供系统性与逻辑性方面的支持。			◎	
4	增强应用数学能力，为分析和解决信息安全实际问题提供数学方法的支持。				◎

注：●：表示有强相关关系，◎：表示有一般相关关系，⊙：表示有弱相关关系

2 育人目标：通过本课程专业知识的学习，树立学生建设科技强国的理想信念和责任担当，通过课程的特点培养学生的职业素养和行为规范，通过基本原理等理论学习引导学生建立价值观。

三、课程教学内容

分章节列出课程教学内容及对课程目标的支撑，详见表 2。

表 2 教学内容与课程目标的对应关系

章节名称	教学内容及重点（▲）、难点（★）	课程目标（√）		
		1	2	3
第一章 整数的可除性	整除、最大公因数▲、最小公倍数、素数的概念；欧几里得除法、数学基本定理★；整数的表示、广义欧几里得除法。	√	√	
第二章 同余	同余、同余式的的概念▲；剩余类；欧拉定理★、费马小定理、一次同余式、中国剩余定理▲。	√	√	√
第三章 二次同余与平方剩余	二次同余式、平方剩余的概念▲；模为奇素数的平方剩余与平方非剩余、勒让德符号★；雅可比符号、模 p 平方。	√	√	√
第四章 原根与指标	指数、原根及基本性质▲；指标；高次同余式的求解★。	√	√	√

第五章 代数基础	群的定义和性质▲；陪集、置换群、商群；循环群、环和域的基本概念▲；理想和商环、多项式环、域的有限扩张；有限域的性质、有限域的表示★、有限域上的多项式。	√		√
第六章 椭圆曲线	椭圆曲线基本概念▲、椭圆曲线的加法原理、有限域的椭圆曲线。			√

四、教授方法与学习方法指导

教授方法：课内讲授推崇研究型教学，以知识为载体，传授相关的思想和方法，引导学生踏着大师们研究步伐前进。结合课程内容的教学要求以及学生认知活动的特点，采取包括讲授、研讨、探究教学、案例教学、线上、线上线下混合等多种教学模式与方法。

积极探索和实践研究型教学。通过学生身边看得见、摸得着的例子入手，将理论和实践结合起来，逐步过渡到信息安全的专业问题上，引导学生进行初步的科学研究。

学习方法：养成探索的习惯，特别是重视对基本理论的钻研，在理论指导下进行实践；明确学习各阶段的重点任务，做到课前预习，课中认真听课，积极思考，课后认真复习，不放过疑点，充分利用好教师资源和同学资源。仔细研读教材，适当选读参考书的相关内容，从应用的角度，深入理解概念，掌握方法的精髓和算法的核心思想，不死记硬背。

五、教学环节及学时分配

教学环节及各章节学时分配，详见表 3。

表 3 教学环节及各章节学时分配表

章节名称	教学内容	学 时 分 配					合计
		讲授	习题	实验	讨论	其它	
1	整数的可除性	6	1				7
2	同余	8					6
3	二次同余与平方剩余	6	2				8
4	原根与指标	6	2				10
5	代数基础	6	2				8
6	椭圆曲线	4	2				6
合计		36	9				45

六、考核与成绩评定

课程考核以考核学生对课程目标达成为主要目的，检查学生对教学内容的掌握程度为重要内容。课程成绩包括平时成绩和考试成绩两部分。

平时成绩 30%（作业 15%，其它 15%），考试成绩 70% 。

平时成绩中的其它 15%主要反应学生的课堂表现、平时的信息接受程度、自我约束。成绩评定的主要依据包括：课程的出勤率、课堂的基本表现（如课堂测验、课堂互动等；作业等的 15%主要是课堂作业和课外作业，主要考察学生对已学知识掌握的程度以及自主学习的能力。

考试成绩 70%为对学生学习情况的全面检验。强调考核学生对基本概念、基本方法、基本理论等方面掌握的程度，及学生运用所学理论知识解决复杂问题的能力。

本课程各考核环节的比重及对毕业要求拆分点的支撑情况，详见表 4。

表 4 考核方式及成绩评定分布表

考核方式	所占比例（%）	主要考核内容及对毕业要求拆分指标点的支撑情况
平时成绩	30	相关作业的完成质量，对应毕业要求 4.2 和 4.5 达成度的评价提供支持。
考试成绩	70	对培养目标的完成情况，对应毕业要求 2.1 和 3.5 达成度的评价提供支持。

七、考核环节及质量标准

本课程各考核环节及质量标准，详见表 5。

表 5 考核环节及质量标准

考核方式	评分标准				
	A	B	C	D	E
	90～100	80～89	70～79	60～69	< 60
作业	优	良	中	合格	不满足 D 要求
研讨	优	良	中	合格	不满足 D 要求
实验					不满足 D 要求
考试	按试卷评分标准执行				不满足 D 要求
评分标准（A～E）：主要填写对教学内容中的基本概念、理论、方法等方面的掌握，及综合运用理论知识解决复杂问题能力的要求。					

制定者：张兴兰

批准者：张建标

2020 年 7 月

“操作系统原理及安全”课程教学大纲

英文名称：Principle and Security of Operating System

课程编码：0010065

课程性质：学科基础必修课

学分：3.0　　学时：48

面向对象：信息安全专业本科生

先修课程：汇编语言程序设计、高级语言程序设计、计算机组成原理、数据结构与算法、网络空间安全导论

教材及参考书：

[1] Abraham Silberschatz、Peter Bear Galvin、Greg Gagne 著，郑扣根译、唐杰、李善平译. 《操作系统概念》（原书第 9 版）. 机械工业出版社. 2018 年 07 月.

[2] 费翔林、骆斌.《操作系统教程》（第 5 版）. 高等教育出版社. 2014 年 02 月.

[3] Tanenbaum.A.S、Herbert Bos 著，陈向群、马洪兵等译. 《现代操作系统》(原书第 4 版). 机械工业出版社. 2017 年 07 月.

[4] 汤小丹, 梁红兵, 哲凤屏, 汤子瀛.计算机操作系统(第四版). 西安: 西安电子科技大学出版社, 2014 年 05.

[5] William Stallings 著，陈向群，陈渝等译. 操作系统:精髓与设计原理（第八版）. 电子工业出版社. 2017 年 02 月.

[6] 卿斯汉, 刘文清, 刘海峰. 操作系统安全导论. 北京：科学出版社，2003 年 01 月.

[7] 刘克龙, 冯登国, 石文昌. 安全操作系统原理与技术. 科学出版社，2004 年 07 月.

[8] 石文昌. 信息系统安全概论（第 2 版）. 电子工业出版社，2014 年 02 月.

[9] 卿斯汉, 沈晴霓，刘文清. 操作系统安全(第 2 版). 清华大学出版社，2011 年 06 月；

一、课程简介

本课程是信息安全专业本科生学科基础必修课。课程主要围绕操作系统的进程管理、内存管理、文件管理、I/O 设备管理和安全机制进行讲授，旨在继程序设计、数据结构与算法、计算机组成原理和网络空间安全导论等课程后，引导学生在计算机系统上级再认识操作系统是如何管理和控制计算机系统中的所有软硬件资源，以及操作系统是如何为用户提供一个方便灵活、安全可靠的工作环境，并要求学生理解多用户、多任务操作系统的运行机制，系统资源管理的策略、方法和安全保障机制。通过设置进程创建及访问权、线程创建与同步、进程间通信和操作系统安全构建等实验课题，在系统软件级上使学生系统科学地受到分析问题和解决问题的训练，从而具备初步的操作系统分析、设计、开发的能力，同时启发和引导学生运用操作系统安全基本原理和方法，结合工作、学习和生活对操作系统安全的具体需求，配置和构建安全的操作系统。

二、课程地位与目标

（一）课程地位：

操作系统是计算机系统的核心系统软件，负责控制和管理计算机系统硬件和软件资源，

力求使各类资源高效利用且最大程度提高整个计算系统的工作效率，其安全性是保证上层应用软件高可靠性运行以及信息的完整性、机密性的基础。因此，本课程被列为信息安全专业的学科基础必修课，在计算机知识结构中有着重要的地位和作用，是信息安全专业课程的重要基础。

本课程支撑的毕业要求拆分指标点的具体描述。

2.3：能对系统设计方案和所建模型的正确性进行推理并能得出结论；

3.4：能正确表达一个工程问题的解决方案；

4.2：能针对特定需求完成系统模块的设计与实现，测试验证模块的正确性，并进行性能优化；

12.2 能够在信息安全项目的开发中考虑成本、质量、效率等目标；

（二）课程目标

1 教学目标：本课程要求学生掌握“操作系统原理及安全”中的基本概念、基本理论和基本方法，在操作系统级的资源管理层面上再认识计算机资源分配的相关工作原理、运行过程以及安全保障机制，培养学生初步具备操作系统分析、设计、开发的能力以及解决系统安全问题的能力。

本课程对毕业要求拆分指标点达成的支撑情况，详见表 1。

表 1 课程目标与毕业要求拆分指标点的对应关系

序号	课程目标	毕业要求拆分指标点			
		2.3	3.4	4.2	12.2
1	掌握操作系统原理及安全的基本概念、基本理论和基本方法，培养学生对较复杂的系统问题能正确性进行推理并得出结论。	●			
2	培养学生综合运用操作系统原理及安全的相关理论知识解决复杂问题的能力。		●		
3	培养学生具有根据实验要求完成方案设计和实现、验证实验结果正确性的能力。			●	
4	培养学生实验环节中方案设计及实现的优化能力。				⊙

注：●：表示有强相关关系，◎：表示有一般相关关系，⊙：表示有弱相关关系

2 育人目标：

学习操作系统原理，有利于学生正确、合理和更有效的使用计算机系统，对计算机系统出现的异常现象能准确的判断并能采取正确的应对措施；学习操作系统的安全机制，在保障计算机系统正常运行的情况下，增强学生保护计算机系统安全的防范意识以及如何保证计算机系统的安全性，更重要是让学生做一个计算机系统安全的“懂法守法人”。

三、课程教学内容

分章节列出课程教学内容及对课程目标的支撑，详见表 2。

表 2 教学内容与课程目标的对应关系

章节名称	教学内容及重点（▲）、难点（★）	课程目标（√）			
		1	2	3	4
第一章 引论	操作系统概念（操作系统的地位和作用、操作系统的主要功能和特性）；操作系统发展（手工操作系统、单道批处理系统、多道批处理系统▲★、分时系统▲★）、操作系统结构、CPU 状态/模式▲、中断▲★、异常机制▲★、系统调用▲★。	√			
第二章 进程管理	进程▲：进程的概念、进程控制块、进程状态及状态转化★、进程控制★； 线程：线程的引入及定义、线程的实现▲★； CPU 调度：基本概念、调度准则、调度算法▲★； 进程同步：进程同步背景、临界区▲★、软件/硬件实现方法、信号量▲★、管程▲★、利用信号量和管程实现进程同步实例▲★； 进程间通信▲；信号、管道、消息传递、共享内存 死锁：死锁的概念▲、死锁的四个必要条件、资源分配图；死锁的处理方法▲包括预防、避免（例子：银行家算法★）、检测★与恢复。	√	√		
第三章 内存管理	内存管理：基本概念（存储层次结构、地址重定位▲★）、连续内存管理（固定分区、可变分区）、非连续内存管理（页式▲★、段式▲★、段页式）、内存“扩充”技术（覆盖、交换、虚拟存储） 虚拟存储：局部性原理、基本概念（基本思想▲、实现方式、特性、支持技术）、虚拟页式存储（基本思想、页表设计★、地址转换、缺页异常★、页面置换算法★、抖动/颠簸） 页面置换算法：局部页面置换算法（最优算法★▲、先进先出算法★▲、最近最久未使用置换算法★▲、最不常用算法）、全部页面置换算法（工作集算法、缺页率算法）。	√	√		
第四章 文件管理	文件和文件系统概念、文件的逻辑结构▲★、文件存取方法▲★、文件目录； 虚拟文件系统、文件的物理结构▲★（连续分配、链接分配、索引分配）、空闲空间的管理； 磁盘结构、磁盘调度。	√	√		
第五章 I/O 设备管理	I/O 结构、I/O 设备的类型、设备控制器、I/O 控制方式▲、I/O 软件层次结构（设备独立性▲、设备驱动）、缓冲技术▲、SPOOLing 技术★▲。	√	√		
第六章 操作系统安全演化进程	由于共享问题引入操作系统的安全；操作系统安全演化进程、操作系统安全演化进程中的代表性思想▲★。	√			
第七章 操作系统安全机制	硬件安全机制：内存保护、运行保护、I/O 保护。 软件安全机制：身份认证机制、访问控制机制、加密机制、安全审计。 身份认证机制：认证技术的基本概念、操作系统中身份认证的实现方法；	√	√		

	访问控制机制：访问控制的基本概念、操作系统中自主访问控制访问的实现▲包括基于权限位的访问控制、进程的有效身份与权限★、细粒度的访问控制； 加密机制：加密文件系统（eCryptfs 和 EFS）、驱动加密机制 BitLocker、两种加密机制的对比； 安全审计：审计机制的结构、审计指令的配置▲、审计信息的分析实例★；				
实验一 进程创建及访问权	加深对进程概念的理解，进一步认识并发执行的实质，熟悉并发程序设计的基本结构，学习 Linux 系统中使用 fork()创建子进程的方法；明确进程与程序的区别，学习 fork()与 exec()的结合实现一个进程启动另一个程序的执行的方法；理解进程标识符与其安全标识符（即进程的身份标识）的概念以及进程有效身份的变化；			√	√
实验二 线程创建与同步	编写 Linux 环境下的多线程程序，了解多线程的程序设计方法，掌握最常用的三个函数 pthread_create，pthread_join 和 pthread_exit 的用法；理解 POSIX 线程（Pthread）互斥锁和 POSIX 信号量机制，学习它们的使用方法；编写程序，实现多个 POSIX 线程的同步控制。			√	√
实验三 进程间通信	本实验主要学习在 Linux 系统中进程间通信的几种方法：利用信号实现进程间通信的方法，掌握注册信号处理程序及 signal()调用方法；利用 pipe()实现进程之间的管道通信；利用 msgget()、msgsnd()、msgrcv()、msgctl()实现基于消息通信机制的进程间通信；利用 shmget()、shmat()、shmctl()实现基于共享存储区的进程间通信。			√	√
实验四 Linux 操作系统安全构建	熟悉 Linux 环境下的用户管理、进程管理以及文件管理的相关操作命令，掌握 Linux 操作系统中的相关安全配置方法，构建 Linux 操作系统的基本安全框架。			√	√

四、教授方法与学习方法指导

教授方法：教学过程中，合理使用多媒体课件、板书等教学手段。针对重点难点进行精讲详讲，帮助学生深入掌握操作系统原理及安全中涉及的一些基本概念、原理和方法；通过理论与实例分析相结合的方法，加深对操作系统原理及安全相关理论知识的理解；

以讲授为主实验为辅相结合的方法加深学生对操作系统原理及安全相关理论知识的理解；课内讲授推崇理论与实例相结合的教学方法，以知识为载体，通过实例传授相关的思想和方法，帮助学生理解抽象的基本概念及原理。实验教学则提出基本要求，引导学生独立完成实验的设计与实现。

学习方法：重视对基本理论的钻研，在理论指导下进行实践；明确学习各阶段的重点任务，做到课前预习，课中认真听课，积极思考，课后认真复习，不放过疑点，充分利用好教师资源和同学资源；选用适当的参考书，仔细研读，深入理解概念，掌握方法的精髓和算法的核心思想，不要死记硬背；积极参加实验，在实验中加深对理论知识的理解。

五、教学环节及学时分配

教学环节及各章节学时分配，详见表 3。

表 3 教学环节及各章节学时分配表

章节名称	教学内容	学 时 分 配					合计
		讲授	习题	实验	讨论	其它	
第一章	引论	3					
第二章	进程管理	14		10			
第三章	内存管理	6					
第四章	文件管理	4					
第五章	I/O 设备管理	2					
第六章	操作系统安全演化进程	1					
第七章	操作系统安全机制	5		2			
	总结与复习	1					
合计		36		12			48

六、考核与成绩评定

平时 10%，实验 20%，考试 70%。

平时：主要反映学生的课堂表现。成绩评定的主要依据包括：课堂的出勤和作业完成情况。

实验：主要考查学生方案设计、实现和验证实验结果正确性的能力。成绩评定的主要依据包括：平时表现和实验任务的完成情况。

期末考试：对学生学习情况的全面检验。强调考核学生对操作系统原理及安全的基本概念、基本方法、基本技术的掌握程度，进一步考核学生综合运用理论知识解决复杂问题能力。

本课程各考核环节的比重及对毕业要求拆分点的支撑情况，详见表 4。

表 4 考核方式及成绩评定分布表

考核方式	所占比例（%）	主要考核内容及对毕业要求拆分指标点的支撑情况
平时	10%	课堂的出勤率和作业完成情况，主要为毕业要求 2.3 达成度的评价提供支持；
实验	20%	实验环节的平时表现及实验任务的完成情况。主要为毕业要求 4.2 达成度的评价提供支持；同时对毕业要求 12.2 达成度的评价也提供一定参考价值的基础数据。
考试	70%	对规定考试内容掌握的情况，主要为毕业要求 2.3、3.4 达成度的评价提供支持。

七、考核环节及质量标准

本课程各考核环节及质量标准，详见表 5。

表 5 考核环节及质量标准

考核方式	评　分　标　准				
	A	**B**	**C**	**D**	**E**
	90～100	**80～89**	**70～79**	**60～69**	**< 60**
平时	课堂的出勤率和作业完成质量高。	课堂的出勤率和作业完成质量较高。	课堂的出勤率较高、作业完成质量一般。	课堂的出勤率较低、作业完成质量较差。	不满足 D 要求
实验	实验环节学生的整体表现好，实验任务完成质量高。	实验环节学生的整体表现较好，实验任务完成质量较高。	实验环节学生的整体表现一般，实验任务完成质量一般。	实验环节学生的整体表现一般，实验任务完成质量合格。	不满足 D 要求
考试	对教学内容中的基本概念、理论、方法等方面掌握的好，且综合运用理论知识解决复杂问题能力强。	对教学内容中的基本概念、理论、方法等方面掌握的较好，且综合运用理论知识解决复杂问题能力较强。	对教学内容中的基本概念、理论、方法等方面掌握的较好，且综合运用理论知识解决复杂问题能力一般。	对教学内容中的基本概念、理论、方法等方面掌握的一般，且综合运用理论知识解决复杂问题能力一般。	不满足 D 要求
评分标准（A～E）：主要填写对教学内容中的基本概念、理论、方法等方面的掌握，及综合运用理论知识解决复杂问题能力的要求。					

制定者：侍伟敏

批准者：张建标

2020 年 7 月

“密码学Ⅰ”课程教学大纲

英文名称：Cryptography

课程编码：0004864

课程性质：学科基础必修课

学分：2.5　　学时：40

面向对象：信息安全（实验班）专业本科生

先修课程：信息安全数学基础

教材及参考书：

[1] 杨波编著.现代密码学（第 4 版）. 清华大学出版社，2017,7

[2] 张仕斌，万武南，张金全.应用密码学.西安电子科技大学出版社，2017,1

[3] 张焕国,唐明编著，密码学引论（第 3 版）.武汉大学出版社，2015，7

[4] 胡向东，魏琴芳，胡蓉编著，应用密码学（第 4 版）.电子工业出版社，2019,6

[5] Christof Pear，Jan Petzl 著，马小婷译. 深入浅出密码学：常用加密技术原理与应用. 清华大学出版社，2012.9

一、课程简介

密码学是信息安全的基础，本课程的学习将为后续的信息安全课程打下基础，同时也为将来从事信息安全安全系统设计、开发与应用提供必要的基础。本课程主要讲授密码学的基本概念、基本理论和基本方法，要求学生理解和掌握古典密码体制、序列密码、分组密码体制、公钥密码体制、数字签名、消息认证、杂凑函数、密码协议的基本概念、基本理论以及基本应用，领会密码体制设计与分析的基本思想与方法，培养学生在实践中解决问题的能力。通过本课程的学习，使学生对密码学一个比较全面和系统的了解，掌握密码学的基本概念、理论、技术与方法，为培养解决复杂信息安全工程问题的能力奠定坚实的理论基础。

二、课程地位与目标

（一）课程地位：本课程是信息安全专业的学科基础必修课。旨在使学生理解并掌握密码学所涉及的基本理论和方法，具备密码学的基本能力。通过对本课程的学习，要求学生对密码学所涉及的基本理论和方法有比较深入的理解，熟悉和掌握主要的密码学方法与技术。通过配套的实验课程教学，使学生掌握密码学的基本实践能力。为今后的工作和进一步学习及解决信安复杂工程问题奠定基础。

本课程支撑的毕业要求拆分指标点的具体描述。

2.3：密码学属于信息安全专业的基础理论之一，通过学习密码学的基本概念和方法、各种密码模块的功能、特点，能基于这些知识对信息系统设计方案和所建模型的正确性进行推理并能得出系统安全与否的有效结论。

3.1 通过学习各种密码算法的原理、密钥长度、算法的轮数、分组长度等参数，能识别和判断信息安全复杂工程问题中所需要的关键环节和参数。

3.5 通过理解和掌握密码算法基于的代数、群、环、域等数论原理，能证实解决方案

的合理性，获得有效安全性结论。

4.1 通过学习密码协议的概念、密码协议的设计原则与方法，各种常用的密码协议，能够归纳描述用户的安全性需求，并能选择正确的方法确定设计目标。

4.5 通过学习各种密码模块受到的各种攻击及密码模块的抗攻击能力，能对已有复杂问题的安全性解决方案进行研究，并提出新的安全性更高、实用性更强的替代解决方案。

（二）课程目标

1 教学目标：

使学生掌握“密码学”中的基本概念、基本理论、基本方法，针对具体的信息系统，描述用户需求、分析和解决其中与密码相关的安全问题，选择解决方案，培养学生利用所学知识分析、描述、解决问题的基本能力。通过密码学课程的学习，学生具备使用密码学工具保护信息系统安全的基本素质，在实际网络环境中，具备信息安全意识。本课程对毕业要求拆分指标点达成的支撑情况，详见表 1。

表 1 课程目标与毕业要求拆分指标点的对应关系

序号	课程目标	毕业要求拆分指标点				
		2.3	3.1	3.5	4.1	4.5
1	掌握密码学的基本概念和方法、各种密码模块的功能及特点，培养学生对信息系统设计方案和所建模型的正确性进行推理并能得出系统安全与否的有效结论的能力	◎				
2	掌握各种密码算法的原理、关键参数，培养学生识别和判断信息安全问题的关键环节和参数选择能力		●			
3	掌握各种密码算法对应的数论原理，培养其利用代数、群、环、域等基本原理证明解决方案合理性的能力			●		
4	掌握密码协议的设计原则和主要的密码协议，培养学生根据用户描述，提炼用户需求，设计信息安全解决方案的能力				●	
5	熟悉各种密码模块、各种密码模块受到的各种攻击及密码模块的抗攻击能力，培养学生对已有方案进行分析，增强系统安全性的能力。					⊙

注：●：表示有强相关关系，◎：表示有一般相关关系，⊙：表示有弱相关关系

2 育人目标：

没有网络安全，就没有国家安全，习近平总书记把网络安全提升到国家安全的战略地位。而密码学是信息安全的基础，如果密码算法的安全性不能保证，就会严重影响到整个信息系统的安全，而现有的安全系统基本上都使用国外的密码算法，安全性不能得到保障。通过本课程的学习，培养学生自主可控的安全理念，树立民族自信和职业素养，在工作和信息系统开发过程中，自觉使用国产密码算法，保证系统的安全运行。

三、课程教学内容

分章节列出课程教学内容及对课程目标的支撑，详见表 2。

表 2 教学内容与课程目标的对应关系

章节名称	教学内容及重点（▲）、难点（★）	课程目标（√）				
		2.3	3.1	3.5	4.1	4.5

第一章 绪论	教学目标、课程的基本内容、密码学基本概念、密码学与信息安全的关系、密码学发展、密码体制与密码分析▲、密码体制的安全性★、古典密码体制▲	√				
第二章 分组密码	分组密码的基本概念、分组密码的设计原则、分组密码的结构、分组密码的安全性、SM4▲★、DES▲、AES▲★、分组密码的工作模式▲。	√	√	√		√
第三章 序列密码	序列密码的基本概念、线性反馈移位寄存器▲、伪随机序列评价、非线性序列▲★、典型的序列密码算法祖冲之密码▲★、RC4 密码▲	√	√			
第四章 公开密钥密码体制	公钥密码概述、SM2 密码▲★、RSA、ELGamal▲密码体制、椭圆曲线密码体制▲★。	√	√	√	√	√
第五章 散列函数和消息认证	散列函数概念及安全性、散列函数的构造方法、常用的散列函数（SM3、SHA3）▲★、消息认证码及其安全性▲。	√	√			
第六章 数字签名	数字签名的基本概念与性质、数字签名的分类、SM2 密码数字签名▲★、RSA 密码数字签名、ElGamal 密码数字签名▲、基于椭圆曲线的数字签名。	√	√	√		√
第七章 密码协议	密码协议的概念与特点、密码协议的安全问题、零知识认证协议、比特承诺协议、安全多方计算协议▲等。	√			√	√

四、教授方法与学习方法指导

教授方法: 结合课程内容的教学要求以及学生认知活动的特点，采取包括讲授、研讨、小组合作、探究教学、项目驱动、案例教学、线上、线上线下混合等多种教学模式与方法。

1. 课堂讲授

课堂教学首先要使学生掌握课程教学内容中规定的一些基本概念、基本理论和基本方法。特别是通过讲授，使学生能够对这些基本概念和理论有更深入的理解，使之有能力将它们应用到一些问题的求解中。要注意对其中的一些基本方法的核心思想的分析，使学生能够掌握其关键。

在授课过程中，通过启发式教学，可由常见的生活问题引出概念，揭示知识发生的过程，自然进入相关内容的讲授；通过讨论进一步掌握和巩固重点；通过学生身边看得见、摸得着的图像及视频加密算法入手，将理论和实践结合起来，增强学生对密码学算法感性理解。

多媒体和传统手段相结合，配合板书、范例和视频演示讲授课程内容。积极探索和实践研究型教学，重要概念术语给出英文表达，探索如何实现教师在对问题的求解中教，学生怎么在对未知的探索中学，通过提出问题，让学生去分析、讨论，设计解决方案，提高学生的独立和团队解决问题的能力。适当引导学生阅读外文书籍和资料，培养自学能力。

2. 实验教学

实验需要在掌握基本原理的基础上，在总体结构的指导下，完成古典密码、分组密码、公钥密码这样三个密码算法及简单应用的设计与实现，并提交规范的实验报告。

通过实验，引导学生体会密码学算法的主要流程，掌握密码学的典型方法，加深对理论的理解；其次是培养学生的系统能力（系统的视角，系统的设计、分析与实现）；第三是培养学生的软件实现能力；第四是培养学生查阅资料，获取适当工具、使用适当工具的能力；第五是培养学生表达能力。

（1）古典密码的编程实现：通过编程实现替代密码和置换密码算法，加深对古典密码体制对了解。

（2）分组密码编程实现：通过编程实现一种分组密码算法，并用分组密码算法的不同工作模式对不同类型的数据进行加、解密，深刻理解分组密码算法的设计机制、不同工作模式对安全性及性能的影响。

（3）公钥密码算法编程实现：通过编程理解公钥密码算法的加密和解密过程，公钥与分组算法安全性及性能的对比，加深对非对称密码算法的理解。

验收方式：现场验收。现场验收学生设计实现的系统，根据学生完成的时间及功能模块进行成绩评定。此外，学生必须提交实验报告，通过此环节训练其实验总结与分析等能力。

3. 作业

通过课外作业，引导学生检验学习效果，进一步掌握课堂讲述的内容，了解自己掌握的程度，思考一些相关的问题，进一步深入理解扩展的内容。

作业的基本要求：根据各章节的情况，包括思考题、计算题、研究性习题等，根据章节内容不同，布置适量的课外作业，完成这些作业需要的知识覆盖课堂讲授内容，包括基本概念题、解答题、证明题、综合题以及其它题型等。

学习方法：

密码学是一门理论性较强的基础课程，应养成探索的习惯，特别是重视对基本理论的钻研，在理论指导下进行实践；明确学习各阶段的重点任务，做到课前预习，课中认真听课，积极思考，课后认真复习，不放过疑点，充分利用好教师资源和同学资源，平时多通过中国大学 MOOC、超星学习通进行线上学习。仔细研读教材，适当选读参考书的相关内容，从系统实现的角度，深入理解概念，掌握方法的精髓和算法的核心思想，不死记硬背。课下通过同学之间、微信群、讨论组、信安竞赛等进行交流和提高。

五、教学环节及学时分配

教学环节及各章节学时分配，详见表 3。

表 3 教学环节及各章节学时分配表

章节名称	教学内容	学 时 分 配					合计
		讲授	习题	实验	讨论	其它	
1	绪论及古典密码	4		2			6
2	分组密码	8		4			12
3	序列密码	3					3
4	公开密钥密码体制	5	1	2			8

6	散列函数和消息认证	4					4
7	数字签名	4					4
8	密码协议	3					3
合计		31	1	8	0		40

六、考核与成绩评定

课程考核成绩包括平时成绩和考试成绩两部分。考核方式为期末考试及平时成绩两部分;，其中考试成绩占 70%，平时成绩占 30%。

期末考试是对学生学习情况的全面检验，要起到督促学生系统掌握包括基本思想方法在内的主要内容。强调考察学生对密码学的基本概念、基本方法、基本技术的掌握程度，包括计算、加解密算法应用、推理证明、根据需求选择密码算法等能力型考核内容，考核学生运用所学方法设计解决方案的能力。支持毕业指标点 2.3,3.1,3.5,4.1

平时成绩包括实验、作业及平时表现三部分（实验 15%、作业 10%、平时表现 5%）

实验成绩：主要反映学生在所学理论指导下如何设计和实现一个最终能够生成中间代码的复杂密码系统的能力，并能基于实现的密码算法实现对文件、文本、图像等数据的加密与解密，通过替代密码与置换密码两种古典密码的设计与实现，培养学生对现代密码模块的理解，引导学生发挥潜力，增强系统的功能；通过对 DES 密码算法的设计与实现，培养学生对对称密码系统架构、扩散、混淆、雪崩效应思想的理解，掌握其背后的理论基础，能选择不同的关键参数，识别、判断、解决信息安全中的复杂工程问题；通过对 RSA 算法的设计与实现，加深学生对代数理论的理解，培养学生基于数论原理，证明解决方案的合理性及增强学生设计解决方案的能力。成绩评定的主要依据包括完成时间、完成模块、选择的开发工具及实验效果等。支持毕业指标点 2.3、3.1、4.1

作业成绩：主要的形式为课外作业，通过完成一定数量的密码算法、方案设计等课后作业，巩固课程所学内容，主要考察学生对已学知识掌握的程度、计算能力、文献搜索及团队合作等自主学习的能力。支持毕业指标点 3.5,4.1

平时表现：主要反映学生的平时出勤、课堂表现、平时的信息接受程度等。支持毕业指标点 2.3,3.1,3.5,4.1

本课程各考核环节的比重及对毕业要求拆分点的支撑情况，详见表 4。

表 4 考核方式及成绩评定分布表

考核方式	所占比例（%）	主要考核内容及对毕业要求拆分指标点的支撑情况
平时成绩	30	实验系统的设计实现情况、作业的完成质量及平时表现，对毕业要求指标点 2.3,3.1,3.5，4.1 达成度的评价提供支持。
考试成绩	70	对课程内容全面掌握的情况，对课程目标 2.3,3.1,3.5,4.1,4.5 达成度的评价提供支持。

七、考核环节及质量标准

本课程各考核环节及质量标准，详见表 5。

表 5 考核环节及质量标准

考核方式	评　分　标准				
	A	**B**	**C**	**D**	**E**
	90～100	**80～89**	**70～79**	**60～69**	**< 60**
作业	表达准确、条理清晰、步骤详细、结果正确	表达较准确、条理较清晰、步骤较清晰、结果个别错误	表达、条理性、步骤及结果中有 2 项不够准确或清晰	表达一般、条理清晰度一般、步骤不详细、结果有稍许错误	不满足 D 要求
研讨					不满足 D 要求
实验	按时出勤、所有功能均已实现、提前完成、实验报告详实	按时出勤、完整功能实现、按时完成、实验报告较详实	不无故缺勤、完整功能实现、拖后完成、实验报告较一般	不无故缺勤、完整核心功能、拖后完成、实验报告较一般	不满足 D 要求
考试					不满足 D 要求
平时表现	不缺勤、课堂表现积极、抽查回答问题正确，有创新思想、积极提出问题	不缺勤、课堂表现较积极、抽查回答问题正确	不无故缺勤、课堂表现较积极、抽查回答问题正确	偶尔缺勤、课堂表现一般、抽查回答问题有稍许错误	不满足 D 要求
评分标准（A～E）：主要填写对教学内容中的基本概念、理论、方法等方面的掌握，及综合运用理论知识解决复杂问题能力的要求。					

制定者：周艺华

批准者：张建标

2020 年 7 月

“安全协议”课程教学大纲

英文名称：Network Security Protocols

课程编码：0004850

课程性质：学科基础必修课

学分：2.0　　学时：32

面向对象：信息安全（实验班）专业本科生

先修课程：计算机网络（双语）

教材及参考书：

[1] 赖英旭,杨震,刘静. 网络安全协议. 清华大学出版社，2012

[2] 寇晓蕤,王清贤. 网络安全协议：原理、结构与应用（第 2 版）. 高等教育出版社，2016

[3] 肖美华. 安全协议形式化分析与验证. 科学出版社，2019

[4] 刘天华,朱宏峰. 安全协议模型与设计. 科学出版社，2018

一、课程简介

本课程对数据链路层安全协议、网络层安全协议、传输层安全协议、会话层安全协议和应用层安全协议等方面进行了比较深入的分析，介绍了各层协议的安全缺陷、易受到的攻击、以及在相应层协议中所增强的安全机制。在网络安全协议应用方面，重点阐述了三种常见的 VPN 网络应用模式，并比较详细地介绍了 VPN 网络的工作原理和配置。教学内容重点：数据链路层安全协议、网络层安全协议、传输层安全协议、应用层安全协议。教学内容的难点：安全协议的应用场景，VPN 构建技术。

二、课程地位与目标

（一）课程地位：本课程是信息安全专业的学科基础课，可以作为其它计算机类专业的选修课。旨在继计算机网络基础等课程后，引导学生在系统上级再认识网络协议的安全性分析、协议安全关键技术、VPN 网络拓扑设计、配置等内容；给学生提供参与设计实现颇具规模的复杂系统的机会，培养其工程意识和能力。

主要为毕业要求第 3.1、4.1、5.1、9.2 的实现提供支持。

对于毕业要求 3.1，培养学生应用安全协议的基本原理，通过研究分析协议安全隐患，以获得有效结论。

对于毕业要求 4.1，强化学生网络安全核心意识，带着网络安全的出发点对经典网络协议进行掌握，培养其网络协议形式化描述、协议程序改进等复杂需求设计能力。

对于毕业要求 5.1，培养学生能够基于网络协议原理，采用科学的方法对其中存在的安全问题进行研究，并通过结合应用场景得到合理有效的结论。

对于毕业要求 9.2，培养学生解与本专业相关的重要法律、法规及方针与政策，并在实践中自觉遵守。

（二）课程目标

1 教学目标：

使学生掌握计算机网络中的基本概念、基本理论、基本方法，再认识网络协议的安全漏洞以及如何增强协议安全性的关键技术。本课程对毕业要求拆分指标点达成的支撑情况，详见表 1。

表 1 课程目标与毕业要求拆分指标点的对应关系

序号	课程目标	毕业要求拆分指标点			
		3.1	4.1	5.1	9.2
1	掌握协议安全分析基本概念，以及问题描述和处理方法。	●			
2	掌握协议安全增强的关键技术。		●		
3	增强理论结合实际能力，实现 VPN 网络配置。				◎
4	培养系统能力和面向系统构建的交流和团队协作能力。			◎	

注：●：表示有强相关关系，◎：表示有一般相关关系，⊙：表示有弱相关关系

2 育人目标：

网络是一把双刃剑，现有的网络协议在促进学生与外界交流的同时，也会给我们带来诸多不良的影响。随着智能手机日渐成为我国大学生标配，网络成为大学生日常生活、娱乐不可或缺的一部分。通过对案例的深入分析，引出习近平总书记在全国网络安全和信息化工作会议上的重要讲话精神、国家安全领域新理念与重大举措以及《中华人民共和国网络安全法》的重要性三大基本原则和重要法条进行详细解读。引导学生感受维护国家网络安全的重要意义，明确责任担当，今后要以身作则，率先垂范，共建健康安全文明的网络环境。

三、课程教学内容

分章节列出课程教学内容及对课程目标的支撑，详见表 2。

表 2 教学内容与课程目标的对应关系

章节名称	教学内容及重点（▲）、难点（★）	课程目标（√）			
		1	2	3	4
第一章 网络信息安全标准概况	主要讲授国内外主要的安全评价标准，国际上通用的信息技术安全性评价通用准则（CC），并通过介绍流行操作系统的等级使读者更加清晰地了解信息技术安全性评价通用准则的使用。主要内容包括：国内外网络安全标准现状★、国际组织制定的有关安全标准★、我国政府制定的有关安全标准★。	√			
第二章 数据链路层安全协议	讲授原有数据链路层协议的安全问题、局域网数据链路层安全协议 802.10 和 802.1q、广域网数据链路层安全协议 L2TF 和 PPTP、以及无线网数据链路层安全协议 802.11 和 802.1x。主要内容包括：局域网安全协议▲，IEEE802.10 标准、IEEE802.1Q 标准；远程通信安全协议▲，点到点协议 PPP★、点到点隧道协议 PPTP★、L2TP、PPTP 的应用★。	√	√		
第三章 网络层安全协议	讲授网络攻击的特点及危害和工作原理等，详细讲授网络安全协议 IPSec 的体系结构，IPSec 所包含的安全协议、安全联盟和密钥交换等关键技术。主要内容包括： IPSec 安全体系	√	√		

	结构▲、IPSec 实现模式、安全关联★、安全关联数据库★；认证头协议▲，AH 格式、AH 操作模式、完整性校验值的计算、AH 的处理；封装安全有效载荷协议▲，ESP 数据包格式、ESP 模式、ESP 处理；密钥管理，ISAKMP（安全关联密钥管理协议）★、 IKE 协议（密钥交换协议）★。				
第四章 传输层安全协议	分析传输层安全协议 SSL 的握手协议和记录协议，对 SSL 的安全性进行分析。主要内容包括：SSL 握手协议▲，SSL 的握手过程、SSL 的握手消息、会话和连接状态；SSL 记录协议▲，记录格式、记录压缩、记录加密、警告协议；SSL 协议安全性分析，握手协议的安全性★、记录协议的安全性★；SSL 协议的应用，认证中心、基于 SSL 的安全解决方案。	√	√		
第五章 应用层安全协议	讲授安全电子邮件协议和 S-HTTP 协议，为了降低应用层协议受到的攻击，在应用层安全协议中所采用的安全机制。主要内容包括：S-HTTP 协议▲，PGP 协议▲，PGP 概述[3]、PGP 的安全性▲★、PGP 的应用；S-MIME 协议▲★，MIME 协议、S-MIME 协议的应用、S-HTTP 应用。	√	√		
第六章 VPN 技术	讲授 VPN 技术。主要内容包括：VPN 工作原理▲、VPN 的应用模式▲、基于数据链路层的 VNP 构建技术、基于 IPSec 的 VPN 构建技术★、基于 SSL 协议的 VPN 构建技术★。			√	√

四、教授方法与学习方法指导

教授方法：以讲授、实验对半方式，采取小组合作、探究教学、案例教学、线上线下混合等多种教学模式与方法，进一步加强学生的实践能力。课内讲授推崇研究型教学，以知识为载体，传授相关的思想和方法，引导学生踏着大师们研究步伐前进。实验教学则提出基本要求，引导学生独立（按组）完成系统的设计与实现。

1. 课堂讲授

课堂教学首先要使学生掌握课程教学内容中规定的一些基本概念、基本理论和基本方法。特别是通过讲授，使学生能够对这些基本概念和理论有更深入的理解，使之有能力将它们应用到一些问题的求解中。要注意对其中的一些基本方法的核心思想的分析，使学生能够掌握其关键。

积极探索和实践研究型教学。注重可操作性和实用性。通过对典型 VPN 网络应用模式案例讲解，使学生能够举一反三。

使用多媒体课件，配合板书和范例演示讲授课程内容。适当引导学生阅读外文书籍和资料，培养自学能力。

2. 实验教学

通过实践环节增强学生对 IP 层、传输层和应用层安全协议的感性认识，培养学生分析问题、解决问题的能力以及理论联系实际的动手能力，同时还培养学生初步具备自我创新能力以及严谨认真的实验态度和分工协作的团队精神。

通过实验系统的设计与实现，引导学生经历构造系统的主要流程，具体体验如何将基本的原理用于系统设计与实现，加深对理论的理解；其次是培养学生系统能力（系统的视角，系统的设计、分析与实现）；第三是通过分小组，培养学生的团队合作精神与能力；第

四是培养学生查阅资料，获取适当工具、使用适当工具；第五是培养学生表达（书面语口头）能力。

学习方法：养成探索的习惯，特别是重视对基本理论的钻研，在理论指导下进行实践；注意从实际问题入手，归纳和提取基本特性，设计抽象模型，最后实现计算机问题求解——设计实现计算系统。明确学习各阶段的重点任务，做到课前预习，课中认真听课，积极思考，课后认真复习，不放过疑点，充分利用好教师资源和同学资源。仔细研读教材，适当选读参考书的相关内容，从系统实现的角度，深入理解概念，掌握方法的精髓和算法的核心思想，不要死记硬背。积极参加实验，在实验中加深对原理的理解。

五、教学环节及学时分配

教学环节及各章节学时分配，详见表 3。

表 3 教学环节及各章节学时分配表

章节名称	教学内容	学 时 分 配					合计
		讲授	习题	实验	讨论	其它	
1	网络信息安全标准概况	2					2
2	数据链路层安全协议	2		4			6
3	网络层安全协议	4		4			8
4	传输层安全协议	2					2
5	应用层安全协议	2	2	4			8
6	VPN 技术	2		4			6
合计		14	2	16			32

六、考核与成绩评定

课程考核以考核学生对课程目标达成为主要目的，检查学生对教学内容的掌握程度为重要内容。课程成绩包括平时成绩、实验成绩和考试成绩三部分。

考核方式及成绩评定分布：写明该门课程考核环节及各环节的成绩占比，各考核环节、考核内容对毕业要求拆分指标点的支撑情况。

平时成绩 10%（作业等 5%，其它 5%），实验成绩 15%，考试成绩 75%。

平时成绩中的其它 5%主要反应学生的课堂表现、平时的信息接收、自我约束。成绩评定的主要依据包括：课程的出勤率、课堂的基本表现（如课堂测验、课堂互动等；作业等的 5%主要是课堂作业和课外作业，主要考察学生对已学知识掌握的程度以及自主学习的能力。

实验成绩 15%为培养学生在网络设备的配置、设计与实现中的交流能力（口头和书面表达）、协作能力、组织能力。

考试成绩 75%为对学生学习情况的全面检验。强调考核学生对基本概念、基本方法、基本理论等方面掌握的程度，及学生运用所学理论知识解决复杂问题的能力。

本课程各考核环节的比重及对毕业要求拆分点的支撑情况，详见表 4。

表 4 考核方式及成绩评定分布表

考核方式	所占比例（%）	主要考核内容及对毕业要求拆分指标点的支撑情况
平时成绩	10	相关作业的完成质量，对应课程目标 1、课程目标 2 达成度的考核。课堂练习参与度及其完成质量，对应课程目标 1、课程目标 2 达成度的评价提供支持。
实验成绩	15	实验系统的设计实现情况。对对应课程目标 3 达成度的评价提供支持，同时对应课程目标 2、课程目标 3、课程目标 4 达成度的考核提供有一定参考价值的基础数据。
考试成绩	75	对规定考试内容掌握的情况，对应课程目标 1、课程目标 2、课程目标 3、课程目标 4 达成度的评价提供支持。

七、考核环节及质量标准

本课程各考核环节及质量标准，详见表 5。

表 5 考核环节及质量标准

考核方式	评　分　标　准				
	A	B	C	D	E
	90～100	80～89	70～79	60～69	< 60
作业	基本概念非常清晰	基本概念清晰	基本概念比较清晰	基本概念掌握一般	不满足 D 要求
其他	课堂表现积极、正确回答问题	课堂表现积极、踊跃回答问题	课堂表现较好、能够回答问题	课堂表现一般、能够回答部分问题	不满足 D 要求
实验	充分预习实验内容、动手能力强	提前预习实验内容、动手能力强	提前预习实验内容、动手能较好	提前预习实验内容、动手能一般	不满足 D 要求
考试	有优秀的综合运用理论知识解决复杂问题能力	有良好的综合运用理论知识解决复杂问题能力	有较好的综合运用理论知识解决复杂问题能力	综合运用理论知识解决复杂问题能力一般	不满足 D 要求
评分标准（A～E）：主要填写对教学内容中的基本概念、理论、方法等方面的掌握，及综合运用理论知识解决复杂问题能力的要求。					

制定者：赖英旭

批准者：张建标

2020 年 7 月

“网络攻击与防护”课程教学大纲

英文名称：Network Attack and Defense

课程编码：0008210

课程性质：学科基础必修课

学分：2.0　　学时：32

面向对象：信息安全（实验班）专业本科生

先修课程：计算机网络（双语）、计算机组成原理

教材及参考书：

[1]　赖英旭，刘思宇，杨震，刘静，叶超等（编著）. 计算机病毒与防范技术(第 2 版). 北京：清华大学出版社，2019 年 12 月

[2] 牛少彰，崔宝江，李剑（编著）. 信息安全概论(第 3 版)，　北京：北京邮电大学出版社，2016 年 08 月

一、课程简介

《网络攻击与防护》课程是面向信息安全专业开设的一门必修课程，共 32 学时。

信息时代，网络空间已成为陆、海、空、天之外人类活动的“第五空间”。政治、经济、文化、社会、军事等国家重要领域的基础设施与网络空间联系日益紧密，网络安全对国家安全牵一发而动全身，已成为国家安全体系的重要组成部分。要贯彻“总体国家安全观”，维护好网络空间这一非传统领域的安全，最关键的要素在于人。目前网络空间安全专业人才的缺口明显，特别是缺乏具有实际动手能力的实践型人才。

本课程以实践型教学为主要特色，面向信息安全专业高年级本科生开设。在学生掌握信息安全基本理论知识的基础上，以实践教学为抓手，培养具有实际动手能力的实践型人才。让学生能够了解网络中存在的常见安全威胁与攻击手段，学习和掌握网络防御技术的基本概念、理论与方法，学习和掌握网络异常的发现、响应与恢复方法。为学生从事网络安全、网络管理、信息保障等工作奠定基础。

本课程依据学生的特点，以总体结构为主线，选择网络安全态势分析、网络安全威胁解析、网络攻击防范实践作为主要内容，讨论网络攻击与防护相关的方法和原理。

二、课程地位与目标

（一）课程地位：本课程是信息安全专业的必修课，也可以作为其它计算机类专业的选修课，属于软件技术系列。旨在计算机网络、计算机组成原理等课程后，以实践教学为抓手，引导学生在实践中再认识网络相关基础知识、网络攻击基本形态、网络方法基本方法。除了学习知识外，还要学习自顶向下、自底向上、递归求解、模块化等典型方法；给学生提供参与设计实现颇具规模的复杂系统的机会，培养其工程意识和能力。

主要为毕业要求第 7.2、8.2、9.3、11.3 的实现提供支持。

对于毕业要求 7.2，网络攻击与防护是一门理论和实践相结合的课程，既能让学生掌握相关的网络安全知识，又能学以致用，培养解决复杂工程实际问题的能力。在实际案例设计过程中，同学能够基于信息安全专业相关背景知识进行合理分析、评价解决方案对社会、

健康、安全、法律以及文化的影响，并理解应承担的责任。

对于毕业要求 8.2，网络攻击与防护是一门理论和实践相结合的课程，要求学生设计满足信息安全需求的系统，并能够在设计环节中体现较强的创新意识和一定的创新能力。在设计环节中能够促使同学理解和评价针对安全问题的信息安全技术方案与实施对环境、社会可持续发展的影响，并将思考所得反映和体现到系统设计中。

对于毕业要求 9.3，网络攻击与防护通过课程教学使得同学能够了解企事业网络中存在的威胁，掌握网络安全策略的设计与实现、安全事故处理的基本方法。就必须要求同学具有人文社会科学素养、社会责任感，了解信息安全领域和信息安全产业的基本发展方针、政策和国家法律法规，能够在工程实践中理解并遵守职业道德和规范，履行责任。从而为学生从事企业安全网络设计与网络管理等工作奠定基础。

对于毕业要求 11.3，培养学生对于国内外研究前沿工作和发展情况的掌握能力，能够将现有学习和未来方向的选择与国际科技发展的大背景相结合。

（二）课程目标

1 教学目标：使学生理解网络攻击的基本形态，掌握常见网络攻击的防范方法。了解企事业网络中存在的威胁，掌握安全评测的基本理论与方法，掌握网络安全策略的设计与实现、网络安全事故处理的基本方法。为学生从事企业安全网络设计与网络管理等工作奠定基础。该目标分解为以下子目标：

课程目标 1：掌握网络攻击的基本概念、场景和方法。掌握网络防护的基本概念、原理与手段，支持指标点 7.2。

课程目标 2：通过案例分析，引导学生参与分析和讨论，逐步提高学生的网络安全意识，增强运用网络安全技术分析问题和解决问题的能力，体验分析和解决问题的乐趣，支持指标点 8.2。

课程目标 3：熟悉本学科各研究方向的最新研究成果和研究方法，支持指标点 11.3。

课程目标 4：通过专题研究讨论活动，锻炼学生的探索与研究能力。通过大量动手实验环境，培养学生网络安全与防护软件开发能力和应用能力，为进一步学习信息安全知识、以及进行信息安全的理论研究和应用开发打好基础。培养系统能力和团队协作能力，支持指标点 9.3。

本课程对毕业要求拆分指标点达成的支撑情况，详见表 1

表 1 课程目标与毕业要求拆分指标点的对应关系

序号	课程目标	毕业要求拆分指标点			
		7.2	8.2	9.3	11.3
1	掌握网络攻击的基本概念、场景和方法。掌握网络防护的基本概念、原理与手段	◎			
2	通过案例分析，引导学生参与分析和讨论，逐步提高学生的网络安全意识，增强运用网络安全技术分析问题和解决问题的能力，体验分析和解决问题的乐趣		●		
3	熟悉本学科各研究方向的最新研究成果和研究方法				◎
4	通过专题研究讨论活动，锻炼学生的探索与研究能力。通过大量动手实验环境，培养学生网络安全与防			●	

	护软件开发能力和应用能力，为进一步学习信息安全知识、以及进行信息安全的理论研究和应用开发打好基础。培养系统能力和团队协作能力				

注：●：表示有强相关关系，◎：表示有一般相关关系，⊙：表示有弱相关关系

2 育人目标：理念决定行动，世界上主要国家普遍对网络安全人才问题高度重视，并把人才发展作为国家关键基础设施网络安全保障的基础和先决条件。本课程能够提升学生对于信息安全技术重要性的理解，理解信息技术安全对于行业乃至国家安全的重要作用，在今后的学习、工作中能自觉地维护信息安全，以适应我国科技发展的需要。

三、课程教学内容

分章节列出课程教学内容及对课程目标的支撑，详见表 2。

表 2 教学内容与课程目标的对应关系

章节名称	教学内容及重点（▲）、难点（★）	课程目标（√）			
		1	2	3	4
第一章 网络攻击与防范的一般流程	课程教学目标、课程的基本内容、信息安全态势、主机安全与网络异常▲、网络攻击流程▲★、网络安全分析、常见网络攻击防范措施▲★。	√	√	√	√
第二章 木马造成的主机及网络异常	特洛伊木马的定义、特洛伊木马的组成和分类、特洛伊木马的基本原理▲、特洛伊木马的编程技术▲★、特洛伊木马的检查和清除▲★。	√	√	√	√
第三章 蠕虫造成的主机及网络异常	网络蠕虫的定义、网络蠕虫分类和组成、网络蠕虫的基本原理▲、网络蠕虫的行为特征▲★、网络蠕虫的检查和清除▲。	√	√	√	√
第五章 漏洞造成的主机及网络异常	漏洞的基本概念、理论和方法▲★、重要信息系统安全性分析、重要信息系统安全隐患及其防范▲、缓冲区溢出分析与防护▲★、SQL 注入分析与防护▲★	√	√	√	√
第四章 数据灾难备份与恢复机制	数据灾难备份和恢复机制、硬盘数据存储机制▲、手动数据备份和恢复▲★、利用工具进行数据备份和恢复▲★。	√	√	√	√
第六章 企业级网络整体安全规划与设计	企业网（工业互联网）中的安全需求应用场景、企业网中的安全威胁分析▲、企业网中的安全规划与设计▲★。	√	√	√	√

四、教授方法与学习方法指导

教授方法：以实践教学为主（30 学时），课堂教学为辅（课内 2 学时）。课内讲授推崇研究型教学，以知识为载体，传授相关的思想和方法，引导学生踏着大师们研究步伐前进。实验教学则提出基本要求，引导学生独立（按组）完成系统的设计与实现。

学习方法：养成探索的习惯，特别是重视对基本理论的钻研，在理论指导下进行实践；注意从实际问题入手，归纳和提取基本特性，设计抽象模型，最后实现计算机问题求解——设计实现计算系统。明确学习各阶段的重点任务，做到课前预习，课中认真听课，积极

思考，课后认真复习，不放过疑点，充分利用好教师资源和同学资源。仔细研读教材，适当选读参考书的相关内容，从系统实现的角度，深入理解概念，掌握方法的精髓和算法的核心思想，不要死记硬背。积极参加实验，在实验中加深对原理的理解。

五、教学环节及学时分配

教学环节及各章节学时分配，详见表 3。

表 3 教学环节及各章节学时分配表

章节名称	教学内容	学时分配					合计
		讲课	习题	实验	讨论	其他	
1	引论	2					2
2	网络攻击流程			4			4
3	主机病毒与网络异常			4			4
4	木马造成主机和网络异常实验			4			4
5	蠕虫造成主机和网络异常实验			4			4
6	漏洞造成主机和网络异常实验			4			4
7	数据灾难备份与恢复实验			4			4
8	企业级网络整体安全规划与设计			6			6
合计		2		30			32

注：课内 30 小时实验时间不足以完成系统的设计与实现，还需用更多的课外时间。实验环节也包含一半讲授内容。

六、考核与成绩评定

课程考核以考核学生对课程目标达成为主要目的，检查学生对教学内容的掌握程度为重要内容。课程成绩包括平时成绩、实验成绩和考试成绩三部分。

平时成绩 10%，实验成绩 40%，考试成绩 50%（以课程设计、综合答辩的形式进行开卷考核）。

本课程各考核环节的比重及对毕业要求拆分点的支撑情况，详见表 4。

表 4 考核方式及成绩评定分布表

考核方式	占比（%）	主要考核内容及对毕业要求拆分指标点的支撑情况
平时成绩	10	主要反应学生的课堂表现、平时的信息接受、自我约束。成绩评定的主要依据包括：课程的出勤情况、课堂的基本表现（含课堂测验）、作业情况，支撑毕业要求 7.2、9.3、11.3。
实验成绩	40	主要反映学生在所学理论指导下如何设计和实现一个最终能够生成中间代码的复杂系统的能力：掌握语言的描述模型，应用所掌握的方法。引导学生发挥潜力，尽量增强系统的功能。培养学生在该复杂系统的研究、设计与实现中的交流能力（口头和书面表达）、协作能力、组织能力，支撑毕业要求 7.2、8.2、9.3、11.3。
考试成绩	50	以课程设计、综合答辩的形式进行开卷考核。强调考核学生对基本概念、基本方法、基本技术的掌握程度，考核学生运用所学方法设计解决方案的能力，淡化考查一般知识、结论记忆，支撑毕业要求 7.2、8.2、9.3、11.3。

七、考核环节及质量标准

本课程各考核环节及质量标准，详见表 5。

表 5 考核环节及质量标准

考核方式	评分标准				
	A	**B**	**C**	**D**	**E**
	90～100	**80～89**	**70～79**	**60～69**	**< 60**
平时	课堂表现优秀、课程出勤率高、课堂互动积极、随堂测试成绩优异等。	课堂表现良好、课程出勤率良好、课堂互动良好、随堂测试成绩良好等。	课堂表现中等、课程出勤率中等、课堂互动积极、能完成随堂测试等。	课堂表现一般、课程出勤率一般、有课堂互动、能基本完成随堂测试等。	不满足 D 要求
实验	实验内容完成度高、实验报告撰写专业、思考题体现深入思考的结果等。	实验内容完成度良好、实验报告撰写较好、思考题体现思考的结果等。	实验内容完成度中等、实验报告撰写中等、思考题仅体现一般性结论等。	实验内容完成度一般、完成实验报告撰写、完成思考题撰写等。	不满足 D 要求或出现大面积实验报告抄袭现象
考试	课程设计：深入理解编程要求，能够通过广泛调研，完成程序设计、代码编写。程序通过验证，能够实现实验要求的功能。 答辩展示：答辩人口齿清晰、能够准确、完整、有逻辑的陈述自己的工作，能够介绍清楚工作的亮点、难度和工作量。 报告撰写：实验报告条理清晰、书写规范，相关文献综述完整。团队分工：分工合理、互相协助、每位成员都体现出自己的工作价值。	程序设计：深入理解编程要求，能够通过广泛调研，完成程序设计、代码编写。基本实现实验要求的功能。 答辩展示：答辩人口齿清晰、能够准确、完整、有逻辑的陈述自己的工作。报告撰写：实验报告条理清晰、书写规范，相关文献综述完整。团队分工：分工合理、互相协助、每位成员都基本体现出自己的工作价值。	程序设计：理解编程要求，能够通过广泛调研，部分完成程序设计、代码编写。 答辩展示：答辩人能够清楚工作的亮点、难度和工作量。报告撰写：实验报告书写较为规范，相关文献综述较为完整。团队分工：成员互相协助，完成综合课设工作。	程序设计。理解编程要求，能够通过调研，部分完成程序设计、代码编写。 答辩展示：答辩人说明自己的工作。 报告撰写：实验报告书写较为规范， 团队分工：成员有一定的分工。	不满足 D 要求或出现大面积课设报告抄袭现象
评分标准（A～E）：主要填写对教学内容中的基本概念、理论、方法等方面的掌握，及综合运用理论知识解决复杂问题能力的要求。					

制定者：杨震

批准者：张建标

2020 年 7 月

“数据库原理及安全”课程教学大纲

英文名称：Database Principle and Security

课程编码：0010652

课程性质：学科基础必修课

学分：2.0　　学时：32

面向对象：信息安全（实验班）专业本科生

先修课程：网络空间安全导论、计算机组成原理、操作系统原理及安全

教材及参考书：

[1]王珊，萨师煊. 数据库系统概论（第 5 版）. 高等教育出版社，2014.09

[2]陈越，寇红召，费晓飞，卢贤玲. 数据库安全. 国防工业出版社，2015.01

[3]邝劲筠，杜金莲. 数据库原理实践（SQL Server 2012）. 清华大学出版社，2015.07

[4]李月军，付良廷. 数据库原理及应用（MySQL 版）. 清华大学出版社，2019.10

[5]Abraham Silberschatz, Henry F. Korth , S. Sudarshan. 数据库系统概念（原书第 6 版）杨冬青等译. 机械工业出版社，2017.09

[6]刘晖，彭智勇等. 数据库安全. 武汉大学出版社，2007.10

[7]Patrick O'Neil, Elizabeth O'Neil. 数据库原理、编程与性能（原书第 2 版）周傲英等译. 机械工业出版社，2004.09

一、课程简介

随着信息技术的不断发展，数据库得到了越来越广泛的应用，数据库管理系统产品不断升级，由此可见，在不久的将来，数据库系统在准确性、效率和安全性等方面都会有更高的设计要求。本课程主要包括数据库概念、关系数据库和 SQL、关系数据理论、数据库设计和编程、数据库安全性和完整性。首先介绍数据库理论，并从信息安全专业的角度，引导学生理解数据库的工作原理，了解数据库在身份认证、访问控制、保密性、完整性、审计恢复技术及并发控制等方面的安全需求与应用措施。通过数据库的原理、技术和数据库安全的教学，提高学生分析和解决工程问题的能力，培养信息安全专业人才。

二、课程地位与目标

（一）课程地位

本课程是信息安全专业本科生的学科基础必修课。数据库是计算机领域中项目开发的重要模块，其运行稳定与安全等性能受到广泛关注。着眼当今，数据库技术不断升级，发展迅速，而数据库原理正是这些新技术的基础，而数据库安全为新技术提供保障。本课程与其他的计算机和信息安全专业课程密切相关，实际应用到数据结构与算法、高级语言程序设计等课程的内容，与计算机网络、计算机组成原理、操作系统原理及安全、网络空间安全导论、信息安全数学基础等课程关系密切，切实提高学生综合分析与解决问题的能力。

本课程支撑的毕业要求拆分指标点的具体描述如下：

2.4：具备应用相关知识对系统解决方案进行比较分析、改进的能力

3.2：能认识到解决问题有多种方案可以选择

3.4：能正确表达一个工程问题的解决方案

12.1：掌握信息安全相关项目的开发过程和管理方法

（二）课程目标

1 教学目标

本课程是关于数据库概念、数据库访问、关系数据模型、数据库安全、数据库操作、数据库编程、数据库设计的课程，其教学目标是使学生掌握关系数据库基础知识；掌握数据库系统结构；掌握简单数据库系统的基本设计和实现方法；了解数据库安全需求并掌握一定的数据库安全防护技术，培养学生的问题解决能力、实际编程能力和数据库安全诊断和防护能力；了解并初步掌握当前软件行业公认的数据库模型和应用。课程中将重点培养学生较熟练地使用关系数据模型进行关系数据库设计、编程解决实际问题、设计方案提升数据库应用安全的能力。

与课程目标相对应，本课程对毕业要求拆分指标点达成的支撑情况，详见表 1。

表 1 课程目标与毕业要求拆分指标点的对应关系

序号	课程目标	毕业要求拆分指标点			
		2.4	3.2	3.4	12.1
1	通过数据库建模的教学，使学生掌握数据库建模的核心概念，培养问题的抽象与归纳、问题求解方法、多种解决方案的对比与权衡等等系统分析与工程应用能力。	◎			
2	通过关系代数的教学，训练学生的逻辑思维能力；通过查询问题的多种解决方法的介绍，增强学生思维的灵活性，并理解查询优化的思路与必要性。		●		
3	通过范式理论、SQL 语言、事务处理等内容的教学，训练学生对问题的抽象与归纳能力，培养逻辑思维、工程思维以及软件应用与开发能力。			●	
4	通过数据库安全需求与应用措施的教学，使学生建立起对数据库系统原理及安全需要的本质认识，培养学生编程解决实际问题、设计方案提升数据库应用安全的能力。				●

注：●：表示有强相关关系，◎：表示有一般相关关系，⊙：表示有弱相关关系

2 育人目标

互联网、计算机领域的大量项目开发都离不开数据库技术，因此数据库安全技术对于网络安全至关重要。“没有网络安全就没有国家安全”，引导学生运用所学的专业技术，在不同的工作中为守护网络安全、保卫国家安全贡献自己的一份力量，培养学生建立良好的职业素养，树立学生守护国家安全的理想信念和责任担当。

三、课程教学内容

本课程的主要内容包括数据库概念、关系数据库和 SQL、关系数据理论、数据库设计和编程、数据库安全性和完整性。本课程的任务是通过数据库的原理、技术和数据库安全的教学，提高学生分析和解决工程问题的能力，培养信息安全专业人才。

教学内容的重点是培养学生较熟练地使用关系数据模型进行关系数据库设计、编程解决实际问题、设计方案提升数据库应用安全的能力。教学内容的难点在于关系规范化理论、

E-R 模型与关系模型的转换等抽象概念的理解。

本课程各章节教学内容及对课程目标的支撑，详见表 2。

表 2 教学内容与课程目标的对应关系

章节名称	教学内容及重点（▲）、难点（★）	课程目标（√）			
		1	2	3	4
第一章 绪论	教学内容：数据库的基本概念、数据模型的组成要素和常用的数据模型、数据库系统的三级模式结构和数据库系统的主要组成部分。 重点：数据库和数据模型的基本概念、数据库的系统结构和系统组成。 难点：数据库系统的系统结构及其实现原理。	√			
第二章 关系数据库和 SQL	教学内容：关系数据库的重要概念，包括关系模型和关系代数；关系数据库标准语言 SQL 的数据定义、数据查询和数据更新功能。 重点：关系模型、关系代数；SQL 语言的数据操作 难点：无		√	√	
第三章 关系数据理论	教学内容：关系数据规范化的需求背景，规范化需求与应用需求之间的联系和区别，关系规范化理论。 重点：关系数据理论 难点：关系规范化理论，数据依赖，范式。			√	
第四章 数据库安全	教学内容：数据库在身份认证、访问控制、保密性、完整性、审计恢复技术及并发控制等方面安全的需求与现状；现有商业数据库系统在上述方面的技术和方法；数据库安全防护新技术。 重点：身份认证、访问控制、保密性、完整性、审计恢复技术及并发控制等方面的安全需求及应对措施；数据库访问控制的技术和方法、完整性约束的定义方法。 难点：断言和触发器。				√
第五章 数据库设计和编程	教学内容：数据库的设计方法和步骤，概念结构设计、逻辑结构设计，数据库编程概念和方法。 重点：概念结构设计，逻辑结构设计 难点：E-R 模型和关系模型的转换。	√			√

四、教授方法与学习方法指导

教授方法：以讲授为主（26 学时），实验为辅（课内 6 学时）。通过启发式教学，介绍问题的背景以及解决的方案；借助实例，讲解相关概念与方法；对于相近或相反的概念和术语，进行对比与区分。探索如何将数据库原理、数据库安全相关内容与案例分析相结合，探索问题求解中的多种思路、不同解决方法的分析与对照；使学生养成理论联系实际的习惯。注重学生对问题和求解方案的分析、总结以及归纳能力的培养。结合使用多媒体课件和黑板板书等，不仅讲授课程内容，还要组织问题研讨，为学生提供参考资料，鼓励学生课下进行自主学习和研究。

学习方法：明确学习各阶段的重点任务，做到课前预习，课中认真听课，积极思考，课后认真复习，注重同学之间的讨论和与授课老师的交流，多问多想多练。在数据库原理课程的学习过程中，始终注重理论联系实际，用案例分析引导概念的理解、方法的学习。

重视数据库上机实验，在实验中加深对原理的理解，增强应用开发能力。

五、教学环节及学时分配

教学环节：第一部分是课堂讲授，其目标是使学生掌握数据库原理与安全课程中的基本概念、基本理论和基本方法，按照绪论、关系数据库和 SQL、关系数据理论、数据库安全、数据库设计和编程的章节顺序进行课堂讲授；第二部分是实验教学，包括三小部分内容，一是数据库设计、数据定义初步、数据更新与数据约束，二是查询、视图、索引与安全性，三是存储过程、触发器与完整性。

教学环节及各章节学时分配，详见表 3。

表 3 教学环节及各章节学时分配表

章节名称	教学内容	学时分配					合计
		讲授	习题	实验	讨论	其它	
第一章 绪论	数据库的基本概念、数据模型的组成要素和常用的数据模型、数据库系统的三级模式结构和数据库系统的主要组成部分。	2					2
第二章 关系数据库和 SQL	关系数据库的重要概念，包括关系模型和关系代数；关系数据库标准语言 SQL 的数据定义、数据查询和数据更新功能。	8		2			10
第三章 关系数据理论	关系数据规范化的需求背景，规范化需求与应用需求之间的联系和区别，关系规范化理论。	4					4
第四章 数据库安全	数据库在身份认证、访问控制、保密性、完整性、审计恢复技术及并发控制等方面安全的需求与现状；现有商业数据库系统在上述方面的技术和方法；数据库安全防护新技术。	8		2			10
第五章 数据库设计和编程	数据库的设计方法和步骤、概念结构设计、逻辑结构设计、数据库编程概念和方法。	4		2			6
合计		26		6			32

实验教学在学生掌握数据库原理及安全中基本的概念、理论和方法的基础上，指导学生从应用实例出发，对问题进行分析，设计数据库模式，创建数据库对象，进行各种数据更新，进行各种数据查询（包括：连接查询、嵌套查询、聚合函数的使用等），以及视图、索引、安全性、事务等相关内容的实验。注重学生在数据库设计方面的训练；要求学生熟练使用 SQL 语言和图形用户界面进行数据处理与数据库管理。要求学生记录实验过程，总结并提交规范的实验报告。

通过实验教学，使学生加深对理论的理解、培养学生系统能力（系统的视角，系统的设计、分析与实现）、培养学生的软件系统实现能力（算法、程序设计与实现）和总结归纳、表达以及撰写报告的能力。实验具体安排见表 4，包含三部分内容：

(1) 数据库设计与数据准备

给出实际应用背景的基本描述，学生根据个人的水平和爱好选择应用问题，重点在于概念模型设计以及数据模型设计的思路与方法；管理数据库以及管理基本表的方法，理解概念模式以及相关数据约束的概念；数据更新的方法，通过测试加深对于数据约束概念的理解。

(2) 查询、视图、索引与安全性

查询实验涉及到单表、多表连接、嵌套查询、聚集查询、综合查询等，也可以自行学习更多高级查询的方法；学习视图与索引的创建等，理解外模式的概念与用途，理解索引的概念与用途，学习授权机制的使用，理解对应安全机制。

(3) 存储过程、触发器与完整性

了解存储过程的作用和使用方法；理解和掌握触发器的分类，利用各类触发器实现用户自定义完整性约束的机制和方法，包括创建、使用、删除、激活等各种基本功能，并能设计和执行相应的 SQL 语句验证触发器的有效性。

表 4 实验的具体安排（6 学时）

数据库设计与数据准备	选择现实生活中的应用背景，给出简要的需求说明，如：实体集的属性及相应联系、约束、经常做的查询等操作。学生自己设计 E-R 图，并转换为达 3NF 的数据库模式。 根据设计好的数据库模式，建库、建表（含约束定义），输入基本数据。数据要足够后面的实验使用。进行合理的插入、删除、和修改操作。对表结构进行修改。
查询、视图、索引与安全性	单表查询、连接查询、嵌套查询、排序、分组、聚合以及综合查询等，视图的建立、删除与使用；索引的建立与使用；授权与收权的应用。
存储过程、触发器与完整性	建立和使用存储过程；理解和掌握各类触发器的设计与使用方法，包括创建、使用、删除、激活等各种基本功能。

实验部分的具体说明：

数据库的设计至少包含 3 个实体集，两个联系；一个多对多联系，另一个为一对一或多对一。能力强的学生可以设计更多实体集与联系，可以含多元联系、一元递归联系；可以含子类实体集、弱实体集。可以附加外层应用程序部分的设计，具体语言工具可由学生自行选择。

实验建议一人一组，任课教师亦可根据班级具体情况安排多人一组。

实验考核包括实验报告与上机检查。考核的几个方面：基本概念掌握情况；概念模型的表达与数据库设计能力；数据准备情况；数据库管理系统的操作能力；数据约束各种方法的掌握情况；SQL 句法的使用情况；查询方法的多样性以及逻辑思维能力；扩展实验情况。

六、考核与成绩评定

课程考核以考核学生对课程目标达成为主要目的，检查学生对教学内容的掌握程度为重要内容。课程成绩包括平时成绩和考试成绩两部分。

考核方式及成绩评定分布：

平时成绩 30%（课堂表现及作业等 10%，上机实验 20%），考试成绩 70%。

平时成绩中课堂表现及作业等占 10%，主要反映学生的课堂表现、平时的信息接收、自我约束，成绩评定的主要依据包括：课程的出勤率、课堂的基本表现（如课堂测验、课堂互动、课堂作业等）和课外作业，主要考察学生对已学知识掌握的程度以及自主学习的能力。上机实验占 20%，成绩评定的主要依据包括上机实验表现、任务完成情况和实验报告，主要考查学生数据库设计能力、上机实践能力、逻辑思维能力、表达能力。

考试成绩 70%为对学生学习情况的全面检验。强调考核学生对数据库原理基本概念、基本方法、基本技术和数据库安全基本需求、基本技术的掌握程度，考核学生运用所学知识设计解决方案的能力，强调数据库设计环节以及 SQL 查询的应用，尽量反映出学生的理论知识、逻辑思维能力、问题分析、归纳求解能力。

本课程各考核环节的比重及对毕业要求拆分点的支撑情况，详见表 5。

表 5 考核方式及成绩评定分布表

考核方式	占比（%）	主要考核内容及对毕业要求拆分指标点的支撑情况
课堂表现及作业等	10	课堂的基本表现情况、相关作业的完成质量，为毕业要求的 2.4、3.2、3.4 达成度的评价提供支持；
上机实验	20	实验系统的设计实现情况，为毕业要求 2.4、3.2、3.4 达成度的评价提供支持，同时为毕业要求 12.1 的达成度的评价也提供一定参考价值的基础数据。
考试成绩	70	规定考试内容的掌握情况，为毕业要求 2.4、3.2、3.4 达成度的评价提供支持。

七、考核环节及质量标准

本课程各考核环节及质量标准，详见表 6。

表 6 考核环节及质量标准

考核方式	评　分　标　准				
	A	B	C	D	E
	90～100	80～89	70～79	60～69	< 60
作业	熟练掌握数据库基本概念、数据模型等	较为熟练掌握数据库基本概念、数据模型等	掌握数据库基本概念、数据模型等	基本掌握数据库基本概念、数据模型等	不满足 D 要求
研讨	对数据库在身份认证、审计恢复技术等方面安全的需求有独立见解	对数据库在身份认证、审计恢复技术等方面安全的需求有较全面的认识	对数据库在身份认证、审计恢复技术等方面安全的需求有一定的认识	对数据库在身份认证、审计恢复技术等方面安全的需求有基本认识	不满足 D 要求
实验	上机实验任务完成情况优秀，实验报告内容完善	上机实验任务完成情况良好，实验报告内容较为完善	能够完成上机实验任务，实验报告内容完整	基本完成上机实验任务，实验报告内容较为完整	不满足 D 要求

考试	熟练掌握数据库原理与安全的基本概念、数据模型、数据库设计的规范和方法	较为熟练掌握数据库原理与安全的基本概念、数据模型、数据库设计的规范和方法	掌握数据库原理与安全的基本概念、数据模型、数据库设计的规范和方法	基本掌握数据库原理与安全的基本概念、数据模型、数据库设计的规范和方法	不满足 D 要求

制定者：李铮

批准者：张建标

2020 年 7 月

“信息系统安全”课程教学大纲

英文名称：Information System Security

课程编码：00107016

课程性质：学科基础必修课

学分：2.5　　学时：40

面向对象：信息安全专业本科生

先修课程：计算机网络（双语），密码学 I

教材及参考书：

[1] 张建标 编著. 网络安全体系结构. 北京：科学出版社. 2020 年待出版

[2] 张建标等 编著. 信息安全体系结构. 北京：北京工业大学出版社. 2011.9

[3] 中华人民共和国国家标准(GB/T 22239-2019). 信息安全技术 网络安全等级保护基本要求. 国家市场监督管理总局/中国国家标准化管理委员会发布.2019.5.10

[4] 中华人民共和国国家标准(GB/T 25070-2019). 信息安全技术 网络安全等级保护安全设计技术要求. 国家市场监督管理总局/中国国家标准化管理委员会发布.2019.5.10

一、课程简介

随着我国信息化建设不断推进，信息技术应用广泛深入，各种基础信息网络和重要信息系统快速普及。国民经济和社会发展对信息化的高度依赖，相伴而生带来信息安全事件不断增多，信息安全问题已愈发严峻。面对不断出现的信息安全事件，如何规划、设计和建设一个安全的网络信息系统已非常重要。本课程依据学生的特点，围绕如何构建一个安全的信息系统，从信息系统安全体系角度出发，完成安全体系的规划与设计、涉及的关键技术和产品、信息系统的安全管理和安全评估为主要内容，系统地讲述如何解决信息技术应用所带来的信息安全问题。

二、课程地位与目标

（一）课程地位：本课程是信息安全专业的学科基础必修课，可以作为其它计算机类专业的选修课，旨在以信息系统安全体系为主线，系统地引导学生了解信息安全涉及的各个层面，掌握信息安全的基本概念、基本理论、基本方法，认识如何构建一个安全的信息系统，包括信息系统的安全需求分析、信息系统安全体系的设计原则和方法等。除了学习知识外，给学生提供参与设计颇具规模的网络信息系统安全解决方案的机会，培养其工程意识和设计、分析和解决信息安全问题的专业能力。本课程系统性强、内容覆盖面广、体系化程度高，对信息安全涉及的各个层面进行了梳理和论证，并讨论了信息安全领域的最新研究进展和发展趋势。

本课程支撑的毕业要求拆分指标点的具体描述。

1.2：良好的人文社会科学素养，尊重生命，关爱他人，诚实守信，有科学精神

2.4：具备应用相关知识对系统解决方案进行比较分析、改进的能力

4.3：能针对特定需求设计并实现功能完整的系统，包括系统整体架构设计、各模块及交互实现或选择、正确性验证、部署、运行和维护等

10.3：能够在多学科团队中独立完成一个成员相应的任务，并能进行有效的合作

（二）课程目标

1 教学目标：让学生了解和掌握信息安全领域的基本概念、基本理论和基本方法，构建知识结构，形成信息安全科学素养，从整体上认识构建一个安全的信息系统需要解决的主要问题。通过结合具体的应用案例分析和分组式实验环节训练，使学生获得设计、分析和解决信息安全问题的综合体验。

表 1 课程目标与毕业要求拆分指标点的对应关系

序号	课程目标	毕业要求拆分指标点			
		1.2	2.4	4.3	10.3
1	掌握信息安全的基本概念、基本理论，以及问题描述和分析处理方法		●		
2	培养学生需求分析、系统设计、分析改进的综合设计能力			●	
3	培养学生在综合多因素的情况下，分析设计的能力	●			
4	培养学生的交流、团队协作能力				◎
5	培养学生的信息安全项目管理能力				⊙

注：●：表示有强相关关系，◎：表示有一般相关关系，⊙：表示有弱相关关系

2 育人目标：通过讲述我国的网络安全法律、标准和战略，培养学生的家国情怀和民族自信，通过讲述系统安全的关键技术及发展过程，培养学生的责任担当和职业素养，寓价值观引导于知识传授之中。

三、课程教学内容

分章节列出课程教学内容及对课程目标的支撑，详见表 2。

表 2 教学内容与课程目标的对应关系

章节名称	教学内容及重点（▲）、难点（★）	课程目标（√）				
		1	2	3	4	5
第一章 概述	教学目的、课程基本内容、信息安全发展阶段； 信息系统安全概念▲、信息化发展与信息系统安全的关系； 国家网络安全法和网络安全等级保护制度。	√				
第二章 网络和通信安全	网络模型、传输介质、网络互联及设备； 网络安全设备▲（防火墙、入侵检测系统、入侵防御系统、VPN、防病毒网关、漏洞扫描系统）	√				
第三章 信息系统安全体系	基本概念▲（脆弱性、威胁、攻击、安全风险、安全措施）； 安全体系★（PDRR 模型、P2DR 模型、IATF 框架，一个中心三重防护体系）； 信息系统安全需求，设计目标和原则★	√	√	√		
第四章 物理安全	设备物理安全（设备标记、防电磁信息泄露、抗电磁干扰）； 环境物理安全（场地选择、物理访问控制、供电系统、通信线路安全、温湿度控制、防火防水、机房屏蔽）； 系统物理安全（备份介质、设备备份、系统恢复）		√			
第五章	身份鉴别技术（口令、生物特征、数字证书）；		√			

系统安全技术	安全模型★（BLP、Biba、Clark-Wilson、无干扰）； 访问控制模型▲（矩阵模型，自主访问控制、强制访问控制、基于角色的访问控制、基于属性的访问控制）； 数据完整性保护，数据保密性保护，系统备份与恢复					
第六章 可信计算技术	可信计算概念，发展过程； 可信根★（TPM、TCM、TPCM），信任链技术★； 可信计算相关标准介绍▲		√			
第七章 安全管理	安全管理的概念，安全管理的内容，安全管理的原则； 信息安全管理体系；					√
第八章 等级保护	评估准则（TCSEC、通用评估准则）； 我国等级保护发展过程； 信息系统安全保护等级划分准则，等级划分原则；网络安全等级保护基本要求和设计要求▲				√	√

四、教授方法与学习方法指导

教授方法：以讲授为主。课内讲授采用探究教学、项目驱动、案例教学等多种教学方法与模式，以知识为载体，传授相关的思想和方法，引导学生掌握信息系统安全涉及的基本概念、基本理论和基本方法。能根据设计案例基本要求，引导学生根据场景要求分组完成网络信息系统及其安全解决方案的设计。

学习方法：养成探索和思考的习惯，特别是重视对基本理论的钻研，在理论指导下进行实践；注意从实际问题入手，根据信息系统面临的安全威胁分析其安全需求，遵循设计原则给出安全解决方案。明确学习各阶段的重点任务，做到课前预习，课中认真听课，课后认真复习，不放过疑点，充分利用好教师资源和同学资源。仔细研读教材，适当选读参考书的相关内容或利用国内外多所高校已开设的相关 MOOC 课程资源，从系统实现的角度深入理解概念，掌握方法的精髓和技术的原理。

五、教学环节及学时分配

教学环节及各章节学时分配，详见表 3。

表 3 教学环节及各章节学时分配表

章节名称	教学内容	学 时 分 配					合计
		讲授	习题	实验	讨论	其它	
第一章	概述	2					2
第二章	网络和通信安全	4					4
第三章	信息系统安全体系	6		8			14
第四章	物理安全	2					2
第五章	系统安全技术	8					8
第六章	可信计算技术	4					4
第七章	安全管理	2					2
第八章	等级保护	4					4
合计		32		8			40

六、考核与成绩评定

课程成绩包括平时成绩、作业成绩和期末考试成绩三部分。

考核方式及成绩评定分布：

平时成绩 10%，作业成绩 20%，期末考试成绩 70%。

平时成绩 10%主要反应学生的课堂表现、平时的信息接收、自我约束。成绩评定的主要依据包括：课程的出勤率、课堂的基本表现（如课堂测验、课堂互动等）。

作业成绩 20%主要是课后作业（5%）和课程设计报告（15%）。课后作业主要考察学生对已学知识掌握的程度以及自主学习的能力。课程设计报告主要反映学生在所学理论指导下如何根据场景要求设计和实现一个网络信息系统及其安全解决方案的能力，要求学生掌握信息系统安全体系的设计原则和各层面的关键安全技术和产品。培养学生在该系统及其安全解决方案的研究、设计与实现能力、协作能力、组织能力。

期末考试成绩 70%为对学生学习情况的全面检验。强调考核学生对“信息系统安全”的基本概念、基本理论和基本方法的掌握程度，考核学生运用所学方法设计信息系统安全解决方案的能力，要起到督促学生系统掌握课程主要教学内容的作用。

本课程各考核环节的比重及对毕业要求拆分点的支撑情况，详见表 4。

表 4 考核方式及成绩评定分布表

考核方式	所占比例（%）	主要考核内容及对毕业要求拆分指标点的支撑情况
平时成绩	10	考查学生课堂的参与度，对所讲内容的基本掌握情况，基本的问题解决能力，通过对课堂练习参与度（含出勤情况）及其完成质量的评价，对应毕业要求 1.4、3.3 达成度的考核。
作业成绩	20	按照教学的要求，课后作业将引导学生复习讲授的内容（基本概念、基本理论和基本方法），锻炼学生运用所学知识解决相关问题的能力，通过对相关作业完成质量的评价，对应毕业要求 1.4、3.3 达成度的考核。对学生综合运用信息安全需求分析、安全体系架构设计原则、各层次关键技术设计以及安全管理和安全评估等典型方法完成信息系统安全解决方案的检验。通过对课程设计完成情况的评价，对应毕业要求 3.3、8.1 和 9.3 达成度的考核。
考试成绩	70	对规定考试内容掌握的情况，对应毕业要求 1.4、3.3 达成度的考核。

七、考核环节及质量标准

本课程各考核环节及质量标准，详见表 5。

表 5 考核环节及质量标准

考核方式	评分标准				
	A	B	C	D	E
	90～100	80～89	70～79	60～69	< 60
平时成绩	上课全勤、积极回答教师提问、课堂练习	上课全勤、较积极回答教师提问、课堂练	上课全勤、较积极回答教师提问、课堂练	上课缺席不超过 2 次、能回答教师提问、	不满足 D 要求

	优	习良	习中	课堂练习中	
作业成绩	课后作业按时完成；课程设计报告文档格式规范，图表清晰；方案设计合理。	课后作业按时完成；课程设计报告文档格式较规范，图表清晰；方案设计较合理。	课后作业按时完成；课程设计报告文档格式较规范；方案设计基本合理。	课后作业按时完成；课程设计报告文档格式基本规范；方案设计基本合理。	不满足 D 要求
考试成绩	很好地掌握课程内容涉及的基本概念、理论、方法，且具备很强的综合运用所学知识解决复杂问题的能力。	较好地掌握课程内容涉及的基本概念、理论、方法，且具备较强的综合运用所学知识解决复杂问题的能力。	较好地掌握教学内容涉及的基本概念、理论、方法，且具备一定的综合运用所学知识解决复杂问题的能力。	基本掌握教学内容涉及的基本概念、理论、方法，且具备一定的综合运用所学知识解决复杂问题的能力。	不满足 D 要求
评分标准（A～E）：主要填写对教学内容中的基本概念、理论、方法等方面的掌握，及综合运用理论知识解决复杂问题能力的要求。					

制定者：张建标

批准者：张建标

2020 年 7 月

“信息论与编码”课程教学大纲

英文名称：Information Theory and Coding Theory

课程编码：0008211

课程性质：专业选修课

学分：2.0　　学时：32

面向对象：信息安全（实验班）专业本科生

先修课程：概率论与数理统计

教材及参考书：

[1] 姜楠，王健. 信息论与编码理论. 北京：清华大学出版社，2010 年 9 月

[2] 科尔曼. 信息论基础. 北京：机械工业出版社，2008 年 1 月

[3] 傅祖芸. 信息论：基础理论与应用. 北京：电子工业出版社，2015 年 2 月

[4] 沈世镒，陈鲁生. 信息论与编码理论. 北京：科学出版社，2010 年 10 月

一、课程简介

物质、能量和信息是组成世界的三大要素。信息论与编码要研究的就是信息，它运用概率论与数理统计的方法研究信息、信息熵、通信系统、网络传输、数据表示、数据压缩、密码学等问题，是整个信息学科的基础。通过本课程的学习，使学生对信息理论有一个初步的了解，熟悉用信息论的观点和方法来分析和解决问题的思路，掌握数据编码的基本方法，为从事信息安全的研究和应用打下基础。

二、课程地位与目标

（一）课程地位：本课程是信息安全专业的专业选修课。旨在引导学生用统计的观点看待信息的存储、传输和处理过程，培养其安全问题分析、设计/开发安全解决方案、信息安全相关研究等能力，为学生的终身学习增加知识储备。

本课程支撑的毕业要求拆分指标点的具体描述。

2.3：能对系统设计方案和所建模型的正确性进行推理并能得出结论。

3.1：能识别和判断信息安全复杂工程问题的关键环节和参数。

4.1：能归纳描述用户的需求，并能选择正确的方法确定设计目标。

（二）课程目标

1 教学目标：

总的教学目标是：使学生掌握“信息论与编码”中的基本概念、基本理论、基本方法，体验分析和解决问题的乐趣。该目标分解为以下子目标。

- ✧ 掌握信息论的基本概念和编码方法。
- ✧ 增强理论结合实际能力，体验分析和解决问题的乐趣。
- ✧ 培养系统能力和团队协作能力。

主要为毕业要求 2.3、3.1、4.1 的实现提供支持。

对于毕业要求 2.3，给定一个方案，能用信息论和编码理论的观点和方法，推导判断方案和模型的好坏。

对于毕业要求 3.1，信息论与编码是一门理论和实践相结合的课程，既能让学生掌握相关的数学知识和自然科学知识，又能学以致用，培养解决复杂工程实际问题的能力。

对于毕业要求 4.1，能从复杂的描述中抽象出问题的本质，并用信息论的观点进行解释、描述和设计。

表 1 课程目标与毕业要求拆分指标点的对应关系

序号	课程目标	毕业要求拆分指标点		
		2.3	3.1	4.1
1	掌握信息论的基本概念和编码方法	●		
2	增强理论结合实际能力，体验分析和解决问题的乐趣		●	
3	培养系统能力和团队协作能力			◎

注：●：表示有强相关关系，◎：表示有一般相关关系，⊙：表示有弱相关关系

2 育人目标：在信息论与编码理论的发展过程中，中国科学家做出了重要贡献，并且信息论在我国信息技术发展过程中发挥了巨大作用。授课过程中通过无缝引入中国科学家的成果，以及信息论发挥作用的经典案例，使学生树立起理想信念、家国情怀、民族自信和责任担当，寓价值观引导于知识传授之中。

三、课程教学内容

分章节列出课程教学内容及对课程目标的支撑，详见表 2。

表 2 教学内容与课程目标的对应关系

章节名称	教学内容及重点（▲）、难点（★）	课程目标（√）		
		1	2	3
第一章 绪论	教学目的、课程的基本内容、信息的概念▲、信息的性质▲、通信系统模型▲、信息论与编码的形成和发展。	√	√	
第二章 信息的统计度量	自信息、条件自信息、互信息、平均自信息（熵）▲、条件熵▲、联合熵、各种熵之间的关系、平均互信息▲。	√		
第三章 离散信源	离散信源的数学模型、信源的分类、离散无记忆信源▲、马尔科夫信源▲、马尔科夫链、马尔科夫信源的熵★。	√	√	
第四章 离散信道	离散信道的数学模型、信道的分类、离散无记忆信道▲、信道容量▲。	√	√	
第五章 无失真信源编码	编码的基本概念、无失真的本质、定长码、变长码▲、香农第一定理、霍夫曼编码▲。	√	√	√
第六章 限失真信源编码	失真的度量▲、信息率失真函数★、香农第三定理、量化编码、预测编码、变换编码。	√	√	√
第七章 信道编码	信道编码的基本概念、香农第二定理、奇偶校验码、线性分组码▲、生成矩阵和监督矩阵▲、循环码、BCH 码。	√	√	√

四、教授方法与学习方法指导

教授方法：课堂教学首先要使学生掌握课程教学内容中规定的一些基本概念、基本理论和基本方法。特别是通过讲授，使学生能够对这些基本概念和理论有更深入的理解，使之有能力将它们应用到一些问题的求解中。要注意对其中的一些基本方法的核心思想的分析，使学生能够掌握其关键。

积极探索和实践研究型教学。探索如何实现教师在对问题的求解中教，学生怎么在对未知的探索中学。通过学生身边看得见、摸得着的例子入手，将理论和实践结合起来，逐步过渡到信息安全的专业问题上，引导学生进行初步的科学研究。

使用多媒体课件，配合板书和范例演示讲授课程内容。在授课过程中，可由常见的生活问题引出概念，自然进入相关内容的讲授。适当引导学生阅读外文书籍和资料，培养自学能力。

学习方法：学生需要高效利用课堂教学时间，认真完成作业，鼓励学生和任课教师交流，仔细研读教材，适当选读参考书的相关内容，从系统实现的角度，深入理解概念，掌握方法的精髓和算法的核心思想，不要死记硬背。有余力同学可以额外阅读一些资料。

五、教学环节及学时分配

教学环节及各章节学时分配，详见表 3。

表 3 教学环节及各章节学时分配表

章节名称	教学内容	学 时 分 配					合计
		讲授	习题	实验	讨论	其它	
1	绪论	2					2
2	信息的统计度量	4					4
3	离散信源	4					4
4	离散信道	5	1				6
5	无失真信源编码	5					5
6	限失真信源编码	4					4
7	信道编码	5	1				6
	总结	1					1
合计		30	2	0	0	0	32

六、考核与成绩评定

课程考核以考核学生对课程目标达成为主要目的，检查学生对教学内容的掌握程度为重要内容。课程成绩包括平时成绩和考试成绩两部分。

平时成绩 50%（作业 30%，课堂 20%），考试成绩 50%。

平时成绩中的课堂 20%主要反应学生的课堂表现、平时的信息接收、自我约束。成绩评定的主要依据包括：课程的出勤率、课堂的基本表现；作业的 30%主要是课下作业，主要考察学生对已学知识掌握的程度以及自主学习的能力。

考试成绩 50%为对学生学习情况的全面检验。强调考核学生对基本概念、基本方法、基本理论等方面掌握的程度，及学生运用所学理论知识解决复杂问题的能力。

本课程各考核环节的比重及对毕业要求拆分点的支撑情况，详见表 4。

表 4 考核方式及成绩评定分布表

考核方式	所占比例（%）	主要考核内容及对毕业要求拆分指标点的支撑情况
作业	30	相关作业的完成质量，对应毕业要求 2.3、3.1、4.1 达成度的考核。
课堂	20	出勤和回答问题情况，对应毕业要求 3.1、4.1 达成度的考核。
考试成绩	50	对课程内容掌握的情况，对应毕业要求 2.3、3.1、4.1 达成度的考核。

七、考核环节及质量标准

本课程各考核环节及质量标准，详见表 5。

表 5 考核环节及质量标准

考核方式	评分标准				
	A	B	C	D	E
	90～100	80～89	70～79	60～69	< 60
课堂	全勤、积极回答问题、回答正确	缺勤 1 次，被提问到的时候能回答问题，基本正确	缺勤 2-3 次，被提问到的时候能回答问题，基本正确	缺勤 4-5 次，被提问到的时候回答“不会”或者基本错误	不满足 D 要求
作业	按时提交，完成情况良好	有 1 次未交，完成情况良好	有 2 次未交，作业不完整，有部分错误	有 3 次未交，作业不完整，错误较多	不满足 D 要求
考试	参考标准答案	参考标准答案	参考标准答案	参考标准答案	参考标准答案
评分标准（A～E）：主要填写对教学内容中的基本概念、理论、方法等方面的掌握，及综合运用理论知识解决复杂问题能力的要求。					

制定者：姜楠

批准者：张建标

2020 年 7 月

“信息内容安全”课程教学大纲

英文名称：Information Content Security

课程编号：0008217

课程类型：专业选修课

学分：2.0　　学时：32

面向对象：信息安全（实验班）本科生

先修课程：高等数学（工）

教材及参考书：

[1] 周学广等编著，信息内容安全，武汉大学出版社，2012 年 11 月

[2] 李建华主编，信息内容安全管理及应用. 机械工业出版社，2010 年 07 月

[3] 杨黎斌等编著，网络信息内容安全. 清华大学出版社，2017 年 02 月

一、课程简介

信息内容安全课程是一门专业选修课。该课程主要讲解信息内容安全的相关概念、理论基础和技术。通过本课程的学习，使学生能够对信息内容安全有一个比较全面和系统的了解，掌握信息内容安全的基本概念、原理和关键技术，涉及：网络媒体信息获取、网络媒体内容特征表达与分析、基于生物特征的身份认证、数字水印与版权保护、信息过滤与舆情监控等信息内容安全相关话题。并且，了解信息内容安全方面的最新研究成果。与此同时，帮助学生正确认识维护绿色网络空间的重要性，使学生树立正确的价值观，提升学生的社会责任感。本门课程的学习将为学生今后从事信息内容安全方向及相关方向的研究和产品研发奠定基础。

二、课程地位与目标

（一）课程地位：本课程是属于专业选修课。旨在使学生理解并掌握信息安全内容安全方向所涉及的基本概念、原理和关键技术，了解内容安全方向的应用场景、前景和技术现状，培养学生利用信息内容安全知识和技术解决问题的基本思路，使学生具备进行信息内容安全领域研究和技术开发的基本能力，助力学生价值观和社会责任感培养。为今后的工作和进一步学习，奠定基础。

本课程支撑的毕业要求拆分指标点：

5.4：培养学生针对问题计算结果数据进行分析和解释，验证所设计方案，并通过信息综合得到合理有效的结论。

9.1：帮助学生理解社会主义核心价值观，维护国家利益，培养学生良好的道德修养、社会责任感、道德操守。

10.1：通过组成团队共同合作完成编程作业，增强学生团队合作意识。

11.1：能够与同学和老师针对信息内容安全问题进行有效沟通和交流，包括撰写报告和设计文稿、陈述发言、清晰表达与回应。

（二）教学目标

1 教学目标：培养学生使用信息内容安全的基本知识和技术进行实际问题分析和解决

方案设计的能力，增强学生对实验结果数据进行分析和方案验证的能力。培养学生团队合作解决问题的能力。增强学生总结、交流和表达能力。培养学生的价值观、社会责任感。本课程对毕业要求拆分指标点达成的支撑情况，详见表 1。

表 1 课程目标与毕业要求拆分指标点的对应关系

序号	课程目标	毕业要求拆分指标点			
		5.4	9.1	10.1	11.1
1	培养学生使用所学基本知识和技术进行实际问题分析和解决方案设计的能力，增强学生对实验结果数据进行分析和方案验证的能力。	●			
2	培养学生团队合作解决问题的能力。			◎	
3	增强学生总结、交流和表达能力。				◎
4	培养学生的价值观、社会责任感。		⊙		

注：●：表示有强相关关系，◎：表示有一般相关关系，⊙：表示有弱相关关系

2 育人目标：互联网已经成为支撑中国经济社会发展的重要的基础设施。与此同时，互联网的开放、互动、共享特征，也容易成为暴力和色情的滋育地、谣言和极端言论的放大器。缺乏辨别力和抵抗力的青少年很容易在鱼龙混杂的虚拟世界迷失自我，继而在现实社会产生失范行为，甚至波及未来与人生。不激浊扬清无以正视听，不刮骨去腐无以养正气。只有维护积极健康、向上向善的网络文化，才能为大学生塑造正确的价值观和道德观，为国家输送正能量满满的建设者。本课程从维护绿色网络安全空间的实际应用需求出发，引导同学们树立正确的价值观，激发同学们的社会责任感，鼓励同学们学好专业知识和技术，加强个人专业素养，助力维护绿色网络空间。

三、课程教学内容

分章节列出课程教学内容及对课程目标的支撑，详见表 2。

表 2 教学内容与课程目标的对应关系

章节名称	教学内容及重点（▲）、难点（★）	课程目标（√）			
		1	2	3	4
第一章 内容安全概述	信息内容安全基本概念，信息内容安全需求与应用（▲），信息内容安全相关技术（▲），信息内容安全特点及其与相关学科的联系。				√
第二章 网络媒体信息内容的获取	互联网信息类型和特点，网络媒体信息获取原理（▲★），网络媒体信息获取方法（▲）。	√	√	√	
第三章 信息内容分析与识别	网络媒体特征表达（▲★）、选择与比较，信息聚类与分类（▲★）。	√	√	√	
第四章 信息过滤与	信息过滤的背景和意义，基于匹配的文本过滤（▲），垃圾邮件过滤原理与技术（▲★），舆情系统的背景和意义，网络舆情监测原理与技术	√	√	√	√

网络舆情监测	（▲★）。				
第五章 基于生物特征的身份认证	基于生物特征的身份认证的概念、原理（★）和方法（▲）。	√	√	√	√
第六章 数字水印与数字版权保护	数字水印与数字版权保护概述，数字水印理论与模型（★），数字图像水印技术（▲）。	√	√	√	√

四、教授方法与学习方法指导

教授方法：结合课程内容的教学要求以及学生认知活动的特点，采取包括启发式、层级递进式、分解式、问题驱动式的教学方法，以及小组合作、研讨的教学模式，采用多媒体可见，配合板书加范例演示的教学手段。

学习方法：课前预习、课上认真听讲，课后复习。平时生活中多观察信息内容安全的相关应用，并思考和探索其技术。养成自己发现问题和解决问题的习惯，充分锻炼编程能力。

五、教学环节及学时分配

教学环节及各章节学时分配，详见表 3。

表 3 教学环节及各章节学时分配表

章节名称	教学内容	学 时 分 配					合计
		讲授	习题	实验	讨论	其它	
1	内容安全概述	2	0	0	0	0	2
2	网络媒体信息内容获取	3	0	0	1	0	4
3	信息内容分析与识别	5	0	0	1	0	6
4	信息过滤与网络舆情监测	6	0	0	2	0	8
5	基于生物特征的身份认证	5	0	0	2	0	7
6	信息隐藏与数字水印	4	0	0	1	0	5
合计	32	25	0	0	7	0	32

六、考核与成绩评定

课程考核以考核学生对课程目标达成为主要目的，检查学生对教学内容的掌握程度为重要内容。课程成绩包括平时成绩和考试成绩两部分。

考核方式及成绩评定分布：考核包括期末考试（占比 60%）和平时作业成绩（作业 30%，其他 10%）。

平时成绩中，作业 30%，主要反应学生根据所学知识编程解决实际复杂问题的能力、团队合作能力、撰写报告和交流能力等。其他 10%，主要反应学生的课堂表现、自我约束，评定主要依据包括：课程的出勤率、课堂的基本表现（如课堂测验、课堂互动等）。

考试成绩为 60%，考查学生对内容安全基本概念及相关算法的理解以及将其综合运用

知识解决复杂问题的能力。

本课程各考核环节的比重及对毕业要求拆分点的支撑情况，详见表 4。

表 4 考核方式及成绩评定分布表

考核方式	所占比例（%）	主要考核内容及对毕业要求拆分指标点的支撑情况
平时成绩	40	以小组为单位对问题进行分析，给出解决问题的思路，并编程实现。出勤和课堂表现。对毕业要求 5.4、10.1、11.1 的达成度评价提供支持。
期末考试	60	通过对规定课程内容掌握的情况，对毕业要求 5.4、9.1 的达成度的评价提供支持。

七、考核环节及质量标准

本课程各考核环节及质量标准，详见表 5。

表 5 考核环节及质量标准

考核方式	评分标准				
	A	B	C	D	E
	90～100	80～89	70～79	60～69	< 60
作业	具备优秀的问题分析和方案设计能力，能够完整、正确的实现、验证和分析方案。团队合作、报告总结、课堂表达和交流优秀。	具备良好的问题分析和方案设计能力，能够较为完整和正确的实现、验证和分析方案。团队合作、报告总结、课堂表达和交流良好。	具备一般的问题分析和方案设计能力，能够基本完整和正确的实现、验证和分析方案。团队合作、报告总结、课堂表达和交流一般。	具备基本的问题分析和方案设计能力，通过部分完整和正确的实现、验证和分析方案。团队合作、报告总结、课堂表达和交流基本符合要求。	不满足 D 要求
考试	基本概念、理论、方法掌握扎实。	基本概念、理论、方法掌握较为扎实。	基本概念、理论、方法掌握一般。	基本概念、理论、方法掌握基本符合要求。	不满足 D 要求
评分标准（A～E）：主要填写对教学内容中的基本概念、理论、方法等方面的掌握，及综合运用理论知识解决复杂问题能力的要求。					

制定者：马伟

批准者：张建标

2020 年 7 月

“固件原理（双语）”课程教学大纲

英文名称： Principle of Firmware

课程编号：0008212

课程性质：专业选修课

学分：2.0 学时：32

面向对象：信息安全（实验班）专业本科生

先修课程：高级语言程序设计

使用教材及参考书：

[1]Vincent Zimmer. Beyond. BIOS: Developing with the Unified Extensible firmware(second edition).Intel press,2010

[2]戴正华.UEFI 原理与编程.机械工业出版社，2016.1

[3]Unified Extensible Firmware Interface Specification.2019.8

一、课程简介

BIOS 作为计算机上电后的第一部分代码，负责初始化硬件和启动操作系统，在整个计算机系统中起着承上启下的作用，是计算机体系中重要的一环，是信息安全研究中不可绕过的一个部分。

本课程培养学生掌握计算机固件的作用、固件的基本结构、UEFI 的概念、UEFI 的架构和原理以及 UEFI 各个主要部分具体工作。通过本课程的学习，学生可以在板级更深入地理解计算机工作机制，对固件相关知识有全面了解，并初步了解 BIOS 开发方法。

二、课程地位与目标

（一）课程地位：本课程是信息安全专业系统安全方向的专业限选课。目的在于在学习过计算机基础知识的基础上，通过对计算机固件原理的学习，以板级的视角进一步理解计算机工作机制，了解基于 UEFI 的计算机固件的体系，培养复杂系统的设计、开发能力。

信息安全离不开计算机基础设施的安全，在目前我国核心技术和核心设施受制于人的现状下，掌握计算机固件原理，初步具备计算机固件基本开发方法，为学生提供进入计算机设备的研制的机会，对提高学生在信息安全专业领域的竞争力、提升学生的就业质量有非常重要的作用。

本课程主要为毕业要求第 2.3、4.4、5.2 的实现提供支持。

毕业要求 2.3：掌握基于 UEFI 的固件的体系和机制，培养学生系统软件的设计、开发能力，用以解决信息安全领域复杂工程问题。

毕业要求 4.4：学习设计良好的 UEFI 体系以及参考实现，并通过一些实践活动，提高大型、系统软件的设计能力和设计水平，同时还可提升学生从问题到解决的能力。

毕业要求 5.2：在学习设计良好的 UEFI 体系以及参考实现过程中，学习并体会成熟的、工业化的设计成果，并通过一些实践活动，提高通过信息综合得到合理有效的结论的能力。

对毕业要求 11.1 的实现有一定支撑作用。

毕业要求 11.1，通过分组讨论和实践，培养学生团队合作和交流、表达能力；成果总

结时通过报告撰写、陈述发言等，提高学生专业表达和总结能力。

（二）课程目标

1 教学目标：使学生掌握计算机固件的基本概念、基本组成、基于 UEFI 的计算机固件的体系、机制及基本开发方法基本方法，在计算机板级更深入地理解计算机的工作机制，提高系统软件的开发水平，培养学生自主学习的能力，增强学生的竞争力。

本课程对毕业要求拆分指标点达成的支撑情况，详见表 1。

表 1 课程目标与毕业要求拆分指标点的对应关系

序号	课程目标	毕业要求拆分指标点			
		2.3	4.4	5.2	11.1
1	深入理解计算机固件概念、作用及在计算机体系中地位。	●			
2	掌握 UEFI 中核心数据结构、平台初始化流程。		●		
3	体会 UEFI 架构和设计思想，增强系统软件的开发水平设计能力。			●	
4	培养系统能力和工程设计能力。				◎

注：●：表示有强相关关系，◎：表示有一般相关关系，⊙：表示有弱相关关系

2 育人目标：了解我国在计算机核心部件方面的发展现状，增强民族自豪感和国家认同性，激发投入到国家计算机核心计算机研发的自信和热情。

三、课程教学内容

课程教学内容及对课程目标的支撑，详见表 2。

表 2 教学内容与课程目标的对应关系

章节名称	教学内容及重点（▲）、难点（★）	课程目标（√）			
		1	2	3	4
第零章 预备知识	概况介绍本门课程的教学目的▲、课程的基本内容，使学生对该门课程的基本情况有全面了解，为进一步学习做好思想准备。 计算机主板的典型结构▲，各个模块的主要功能，主板的主要流程，常用总线标准和设备管理方式。 引导学生自主阅读相关资料。	√			√
第一章 传统 BIOS 概述	BIOS 概念，BIOS 的作用▲、启动流程▲和发展历史，传统 BIOS 的服务接口，传统 BIOS 的不足。希望学生能够全面了解 BIOS 在整个计算机系统的地位和作用。	√	√		
第二章 UEFI 概述	UEFI 的提出和发展背景，UEFI 的特点，UEFI 层次结构▲★，系统启动流程和各阶段工作和实现方式▲。希望学生能够了解 UEFI 规范的发展过程，并能体会当一个产业的发展出现困难时，新技术如何产生以应对出现的问题。		√	√	
第三章 UEFI 基本架构和驱动模型	UEFI 基本架构▲★，主要数据结构▲★，UEFI 映像，驱动模型▲★，UEFI 协议▲★。UEFI 基本架构是重点，应当论述清楚框架如何做到在资源受限的环境下，如何实现对底层硬件的初始化，并能够保持可扩展性；在讲解 UEFI 各种对象时，重点说明相互关系和作用。学生应体会什么是好的设计。		√	√	√

第四章 PEI	PEI 的作用▲，工作流程▲，主要设计概念。PEI 和 DXE 阶段是固件初始化过程中的两个重要阶段，在讲述清楚基本概念和原理的基础上，分析阶段划分的思想、扩展性如何实现。				
第五章 DXE	基础框架▲，调度程序▲，驱动程序▲★，启动设备选择。		√	√	√
第六章 UEFI 开发	应用程序开发方法，EDK 原理及配置▲★。			√	√

四、教授方法与学习方法指导

教授方法：

（1）课堂讲授

课堂讲授应使学生能够理解 BIOS 的发展，全面了解 UEFI 规范，掌握 UFEI BIOS 的主要结构和关键环节，了解开发方法，为从事相关领域工作打下基础。

（2）实验环节

在掌握基本知识和原理的基础上，学会开发环境的搭建和基本的开发方法。开发环境涉及多个方面，注意引导学生“知其然更要知其所以然”，不能只停留在实验完成的层面。

（3）课外自学

因安排的学时为 28 学时，对于全面了解计算机固件远远不够，因此，在课堂上应重点讲清楚 UEFI 的机理和架构，细节和程序代码等方面可通过课下文献阅读和代码分析等手段补足。

对于相关的文献的学习，可进行总体介绍，引导学生课下阅读。

（4）线上线下混合

对于一些知识性、流程性的内容，提供线上资源供学生自学。

学习方法：BIOS 隐藏在计算机内部，日常很难感知到其在计算机系统所发挥的重要作用； BIOS 的工作与计算机硬件密切结合，实现语言为 C 和汇编；BIOS 代码非常庞大，在很多方面系统化不足；BIOS 开发涉及计算机的各个方面，如芯片、协议、操作系统等。因此，在学习和理解过程中存在较大难度，需要学生同时了解计算机硬件相关的多种知识，阅读相关规范文档。

五、教学环节及学时分配

教学环节及各章节学时分配，详见表 3。

表 3 教学环节及各章节学时分配表

章节名称	教学内容	学 时 分 配					合计
		讲授	习题	实验	讨论	其它	
0	预备知识	3					3
1	传统 BIOS 概述	2					2
2	UEFI 概述	2					2
3	UEFI 基本架构和驱动模型	6					6
4	PEI	2					2
5	DXE	8					8

6	UEFI 开发	3		4			7
	总结、研讨	2					2
合计		28		4			32

六、考核与成绩评定

本课程不进行卷面考试，建议成绩评定根据平时（20%）+实验（80%）。鼓励任课讲师采用更灵活的考核方式，以体现课程教学内容的特点。

本课程各考核环节的比重及对毕业要求拆分点的支撑情况，详见表 4。

表 4 考核方式及成绩评定分布表

考核方式	占比（%）	主要考核内容及对毕业要求拆分指标点的支撑情况
平时	20	教学过程参与度，自主学习效果，作业完成。对毕业要求 1.3、3.4 的达成度评价提供支持。
实验	80	实验完成情况，报告书写质量。对毕业要求 1.3、3.4、4.2、10.1 的达成度的评价提供支持。

七、考核环节及质量标准

本课程各考核环节及质量标准，详见表 5。

表 5 考核环节及质量标准

考核方式	评分标准				
	A	B	C	D	E
	90～100	80～89	70～79	60～69	< 60
作业	按时完成，概念深入理解，很好掌握解决问题的方法并能够扩展	按时完成，概念深入理解，很好掌握解决问题的方法	按时完成，概念深入理解，掌握解决问题的方法	及时完成，概念了解，基本了解解决问题的方法	不满足 D 要求
研讨	积极主动，能提出问题，解答问题圆满	积极主动，解答问题圆满	参与话题，解答问题圆满	能正确解答问题	不满足 D 要求
实验	按时完成任务，能够在基本要求基础上扩展；方法合理；自主解决问题；对工作进行很好的提炼；规范性良好	按时完成任务，能够在基本要求基础上扩展；方法合理；自主解决问题；对工作进的提炼；规范性良好	按时完成任务；方法正确；解决问题；符合规范	及时完成任务；解决问题；基本符合规范	不满足 D 要求
评分标准（A～E）：主要填写对教学内容中的基本概念、理论、方法等方面的掌握，及综合运用理论知识解决复杂问题能力的要求。					

制定者：王冠

批准者：张建标

2020 年 7 月

“网络协议分析与设计”课程教学大纲

英文名称：Network Protocol Analysis and Design

课程编码：0010679

课程性质：专业选修课

学分：2.0　　学时：32

面向对象：信息安全（实验班）专业本科生

先修课程：计算机网络（双语）

教材及参考书：

[1] 刘静 赖英旭. 网络协议分析. 北京：北京工业大学印刷厂, 2021

[2] 寇晓蕤 蔡延荣 张连成. 网络协议分析（第 2 版）. 北京：机械工业出版社, 2018

[3] 王晓卉 李亚伟. Wireshark 数据包分析实战详解. 北京：清华大学出版社, 2015

[4] 刘飚. 网络编程与分层协议设计:基于 Linux 平台实现. 北京：机械工业出版社, 2011

一、课程简介

网络协议即网络中传递、管理信息的一些规范。如同人与人之间相互交流是需要遵循一定的规矩一样，计算机之间的相互通信需要共同遵守一定的规则，这些规则就称为网络协议。网络协议是网络的基础，没有网络协议就没有互联网的发展。各个协议有其实际的应用及安全缺陷，是网络安全方向理论和实践结合最好的课程之一。本课程结合专业特点和学生特点，讲解主机从接入网络一刻信息被传递到其他网络中，各个层次所涉及的主要网络协议。深入分析主要网络协议的设计思想、流程、其所解决的问题及其面临的安全问题。每个网络协议注重原理、实践和安全隐患三个方面融会贯通。并且讲解如何设计和编写带有安全机制的网络协议，对编写的协议进行测试。

二、课程地位与目标

（一）课程地位：本课程是信息安全专业的专业限选课，旨在继计算机网络基础课程后，引导学生对网络协议有更深入的认识和理解，从发现问题出发，研究问题，解决问题，进一步发现安全问题。引导学生将理论和实践相结合，深入理解网络协议原理，并培养其工程实践能力。为安全协议课程的学习奠定坚实基础。

本课程主要为毕业要求第 3.2、5.2 的实现提供强支持，为毕业要求第 3.3、4.1 的实现提供中度支持，为毕业要求的第 4.4 的实现提供弱支持。

3.2：能认识到解决网络协议的安全问题有多种方案可以选择。

3.3：能利用多种资源开展文献检索和资料查询。

4.1：能归纳描述用户的网络设计需求，并能选择正确的方法确定组网设计目标。

4.4：能针对复杂系统问题，分析不同解决方案所涉及的相关因素、以及该问题对社会、安全、法律等的影响，在此基础上进行评价与权衡、并提出最终解决方案。

5.2：能基于专业理论和技术，针对设定的网络协议安全机制需求选择研究路线，设计实验方案。

（二）课程目标

1 教学目标：使学生掌握网络协议的基本理论、基本应用，在此基础上培养网络工程实践能力，进一步带着安全性的思维思考网络中存在的问题。培养学生发现问题、学习问题、解决问题的方法和思路。

该目标分解为以下子目标：

- 培养学生将网络协议的原理与实践相结合，能归纳描述用户的网络设计需求，并能选择正确的网络协议进行中小型网络的组网。
- 培养学生能够基于网络协议的工作原理，利用多种资源开展文献检索和资料查询，选取科学的方法对其中存在的安全问题进行解决。
- 培养学生灵活应用网络协议的工作原理，通过研究分析协议安全隐患，能够采用多种方法防御针对协议缺陷的攻击。
- 培养学生能基于专业理论和技术，对网络协议进行形式化描述，针对设定的网络协议安全机制等复杂需求选择研究路线，进行设计和改进。
- 强化学生网络安全核心意识，带着网络安全的出发点对经典网络协议进行掌握，评价出协议缺陷对社会和企业的影响，并通过结合应用场景得到合理有效的结论。

本课程对毕业要求拆分指标点达成的支撑情况，详见表 1。

表 1 课程目标与毕业要求拆分指标点的对应关系

序号	课程目标	毕业要求拆分指标点				
		3.2	3.3	4.1	4.4	5.2
1	培养学生将网络协议的原理与实践相结合，能归纳描述用户的网络设计需求，并能选择正确的网络协议进行中小型网络的组网			◎		
2	培养学生能够基于网络协议的工作原理，利用多种资源开展文献检索和资料查询，选取科学的方法对其中存在的安全问题进行解决		◎			
3	培养学生灵活应用网络协议的工作原理，通过研究分析协议安全隐患，能够采用多种方法防御针对协议缺陷的攻击	●				
4	培养学生能基于专业理论和技术，对网络协议进行形式化描述，针对设定的网络协议安全机制等复杂需求选择研究路线，进行设计和改进。					●
5	强化学生网络安全核心意识，带着网络安全的出发点对经典网络协议进行掌握，评价出协议缺陷对社会和企业的影响，并通过结合应用场景得到合理有效的结论				⊙	

注：●：表示有强相关关系，◎：表示有一般相关关系，⊙：表示有弱相关关系

2 育人目标：在传授知识的同时，重视培养学生严谨治学、力求上进的学习态度，培养学生分析和解决复杂工程问题的能力，培养学生的探索精神、创新意识和工程素质，培养学生的职业道德、社会责任感和社会主义核心价值观。在应用理论知识的同时，将知识上升到国家、社会、家庭的层面，讲解本行业中不同层次、不同分工的工作能力要求，使学生了解社会发展状况，跟上行业科技发展步伐，增强对国家和社会发展的理解，强化对社会与家庭的担当与使命，从多角度多维度进行思政教育，促进其提高自身实践能力的自觉性。

三、课程教学内容

课程教学内容及对课程目标的支撑，详见表 2。

表 2 教学内容与课程目标的对应关系

章节名称	教学内容及重点（▲）、难点（★）	课程目标（√）				
		1	2	3	4	5
第一章 数据链路层协议分析	地址解析协议、802.1Q 协议和生成树协议的工作原理、报文格式及封装▲，如何依据工作原理和相关软件发现协议存在的安全隐患▲。将理论与实践相结合，避免配置不当引发的安全问题，以及针对协议攻击的防御措施★。	√	√	√		
第二章 网络层协议分析	路由协议概述▲。距离矢量路由协议和链路状态路由协议的特点、工作原理和算法，适用场景▲。典型路由协议的特征和消息格式，在采用认证方式后消息格式的变化★。路由协议的攻击分析与安全防御措施★。ICMP 协议工作原理和消息格式，存在的安全问题，以及应用 ICMP 造成攻击▲。	√	√	√		
第三章 应用层协议分析	DHCP、NAT、TELNET 等应用层协议的工作原理和消息格式▲。协议存在的技术安全隐患▲。将理论与实践相结合，避免配置不当引发的安全问题，以及针对协议攻击的防御措施★。	√	√	√		√
第四章 网络协议设计与开发	掌握网络协议的设计方法▲，理解网络协议的形式化描述方式★，了解网络协议的测试方法和验证方法▲。		√		√	

四、教授方法与学习方法指导

教授方法：本课程以课堂讲授为主。积极探索和实践研究型教学。引导学生自主开展调查，自我学习、扩展、研讨，最大限度地激发学有余力的学生求知的欲望、探索的乐趣、创造的潜能，对防御措施进行研究性学习探索。

学习方法：在授课过程中，采用启发式教学和探究式教学，探索如何实现教师如何引导学生由现实问题探索科学问题，学生怎么在对未知的探索中学。赋予学生掌握学习方法的能力。通过实验设计和实现，让同学们运用自学知识自己动手解决实际问题。检查学生掌握已学知识的情况，进行查漏补缺。具体体验如何将基本的原理与实践相结合，加深对原理和消息格式的理解；其次是培养学生以安全视角看待网络协议的设计；第三是培养学生的网络协议设计与实现；第四是培养学生查阅资料，获取适当工具、使用适当工具；第五是培养学生表达（书面与口头）能力。

五、教学环节及学时分配

教学环节及各章节学时分配，详见表 3。

表 3 教学环节及各章节学时分配表

章节名	教学内容	学 时 分 配	合

称		讲授	习题	实验	讨论	其它	计
第一章数据链路层协议分析	地址解析协议、802.1Q 协议和生成树协议的工作原理、报文格式及封装▲，如何依据工作原理和相关软件发现协议存在的安全隐患▲。将理论与实践相结合，避免配置不当引发的安全问题，以及针对协议攻击的防御措施★。	4		4			8
第二章网络层协议分析	路由协议概述▲。距离矢量路由协议和链路状态路由协议的特点、工作原理和算法，适用场景▲。典型路由协议的特征和消息格式，在采用认证方式后消息格式的变化★。路由协议的攻击分析与安全防御措施★。ICMP 协议工作原理和消息格式，存在的安全问题，以及应用 ICMP 造成攻击▲。	4		4			8
第三章应用层协议分析	DHCP、NAT、TELNET 等应用层协议的工作原理和消息格式▲。协议存在的技术安全隐患▲。将理论与实践相结合，避免配置不当引发的安全问题，以及针对协议攻击的防御措施★。	4		4			8
第四章网络协议设计与开发	掌握网络协议的设计方法▲，理解网络协议的形式化描述方式★，了解网络协议的测试方法和验证方法▲。	4		4			8
合计		16		16			32

六、考核与成绩评定

平时成绩 60%（出勤等课堂表现 10%，实验 50%），期末报告 40%。

实验成绩 50%。主要反映学生在实验过程中是否真正掌握所学内容。培养学生实践能力，从实践中更加深入理解理论知识，发现问题，进行创新。以及实验过程中的沟通能力、协作能力、组织能力。

平时成绩中的 10%是出勤主要反应学生的课堂和实验过程中的表现、平时的信息接受、自我约束。

期末报告 40%主要是学生文献检索，综合归纳，书面表达能力和创新方案的可行性论证。给出的技术方案可以体现学生的自学能力以及终身学习能力，可以适应网络技术不断变化发展的需求。

本课程各考核环节的比重及对毕业要求拆分点的支撑情况，详见表 4。

表 4 考核方式及成绩评定分布表

考核方式	所占比例（%）	主要考核内容及对毕业要求拆分指标点的支撑情况
课堂表现	10	课堂展示的完成质量，对毕业要求 3.2、4.4 达成度的评价提供支持。
实验	50	运用理论解决实践问题的能力，对毕业要求 3.3、4.1、5.2 达成度的评价提供支持。
期末报告	40	具有良好报告撰写能力，对毕业要求 3.2、3.3、4.1、5.2 达成度的评价提供支持。

七、考核环节及质量标准

本课程各考核环节及质量标准，详见表 5。

表 5 考核环节及质量标准

考核方式	评分标准				
	A	**B**	**C**	**D**	**E**
	90～100	**80～89**	**70～79**	**60～69**	**＜60**
课堂研讨	课堂和实验过程中表现积极，信息接受能力强，能针对老师的问题提出给出合理答案，具有自我约束能力。	课堂和实验过程中表现较为积极，信息接受能力较强，能针对老师的问题提出进行思考，具有自我约束能力。	课堂和实验过程中表现较为积极，信息接受能力较强，具有自我约束能力。	课堂和实验过程中表现较为一般，信息接受能力不强，具有自我约束能力。	不满足D要求
实验	设计、实验方案科学合理；数据采集、计算、处理正确；论据可靠，分析、论证充分。实验结果无错误，回答问题正确。	设计、实验方案科学较为合理；数据采集、计算、处理较为正确；论据可靠，分析、论证较为充分。实验结果无错误，回答问题较为正确。	设计、实验方案科学较为合理；数据采集、计算、处理较为正确；论据可靠，分析、论证不够充分。实验结果无错误，回答问题不够正确。	设计、实验方案科学不够合理；数据采集、计算、处理较为正确；论据可靠，分析、论证不够充分。实验结果有错误，回答不够正确	不满足D要求
期末报告	综述简练完整，有见解；立论正确，论据充分，结论严谨合理；文理通顺，技术用语准确，符合规范；图表完备、正确。阐述过程语言清晰、表达和描述问题具备逻辑性，展示文档美观。设计方案有创新意识；对前人工作有改进、突破，或有独特见解，有一定应用价值。	综述简练完整，有见解；立论正确，论据充分，结论严谨合理；文理通顺，技术用语准确，符合规范；图表完备、正确。阐述过程语言清晰、表达和描述问题具备逻辑性，展示文档美观。设计方案有一定应用价值。	综述简练完整，有见解；论据较为充分，结论较为严谨合理；文理通顺，技术用语较为准确；图表完备、正确。阐述过程语言清晰、表达和描述问题具备逻辑性，展示文档美观。	论据较为充分，结论较为严谨合理；文理通顺，技术用语不够准确；图表不够规范。阐述过程语言清晰、表达和描述问题具备逻辑性。	不满足D要求
评分标准（A～E）：主要填写对教学内容中的基本概念、理论、方法等方面的掌握，及综合运用理论知识解决复杂问题能力的要求。					

制定者：刘静

批准者：张建标

020 年 7 月

“安全软件开发”课程教学大纲

英文名称：Building Security for Developing Software

课程编号：0008208

课程性质：专业选修课

学分：2.0　　学时：32

面向对象：信息安全（实验班）专业本科生

先修课程：高级语言程序设计、网络空间安全导论

教材及参考书：

[1] 陈波、于伶.软件安全技术　机械工业出版社，2018.08

[2] 张剑等. 软件安全开发　电子科技大学出版社，2015.02

[3] 任伟等.软件安全 National Defense Industry Press，2010.07

[4] John Viega 著殷丽华译安全软件开发之道机械工业出版社，2014.03

[5] Michael Howard.软件安全开发生命周期电子工业出版社，2008.01

一、课程简介

安全软件开发是一门工程实践技术课程，致力于找出软件安全漏洞问题根源的一般性趋势，并通过可行的方法，如采用相关工具或过程以防止同类或相似问题再次发生在软件开发中。与各种程序开发技术和软件工程技术贯穿在一起应用，以创建在遭受恶意攻击时依然安全可靠且运行正确的软件。其本质是将安全开发过程和信息安全专业知识集成到软件工程实践中。信息安全包括很多方面的内容，但软件安全是信息安全的首要和关键安全因素。由于各种原因，软件中存在着很多漏洞和缺陷，本课程的内容就是介绍如何通过行之有效的方法减少这些问题给信息安全带来的影响。

二、课程地位与目标

（一）课程地位：本课程是信息安全专业的专业选修课，亦可作为其它计算机类专业的选修课，属于信息系统安全方向。旨在学习了程序设计、数据结构与算法和信息安全相关课程后，引导学生在系统工程级别上，广泛了解掌握安全软件开发相关的方法、工具和过程；引导学生从问题出发，通过实施一系列的安全软件开发措施，强化学生关注软件安全的意识，减少软件内在的安全问题；除了学习知识和技术外，还要学习使用软件工具进行代码审核和安全测试的方法，向学生提供参与设计实现安全软件开发的过程，培养其工程意识和能力。

本课程支撑的毕业要求拆分指标点的具体描述

2.4：能正确表达一个工程问题的解决方案。安全软件开发作为一种工程技术，培养学生在掌握通常的软件安全设计原则基础上，构建威胁模型，分析软件面临的威胁，找出能消除或减少这些威胁的方法和技术，使用文档正确表达安全软件开发中的解决方案。

3.2：能针对特定需求完成系统模块的设计与实现，测试验证模块的正确性，并进行性能优化。掌握与软件工程结合的典型安全软件开发方法，具有根据软件安全要求和具体情况，运用适合安全软件开发的技术手段进行系统设计和实施编码及测试其正确性的能力。

5.2：开发、选择与使用适当的技术、资源和工具，对安全软件开发工程问题进行预测与模拟。培养学生对多种技术、工具的应用。实现需求分析、建立威胁模型的方法；实现过程选择：软件安全风险评估、使用最新软件工具进行代码自动或人工审核和测试。

9.1：认识合作的重要性，具有合作意识，明了自己在多学科团队中的责任和任务。安全软件开发是一个团队整体实施的任务，通过分组完成实验任务，培养学生具备初步的团队合作意识和承担自己的责任。学生需要从分工、设计、交流讨论、实现和书面报告等环节中相互协调、相互配合。

（二）课程目标：

1 教学目标：按照信息安全专业总体培养目标的要求，使学生掌握“安全软件开发”中的基本概念、基本理论、基本方法、过程、工具和技术，认识软件安全对信息安全的意义，提升开发软件的安全性水平，增强安全意识和法律意识。本课程对毕业要求拆分指标点达成的支撑情况，详见表 1。

表 1 课程目标与毕业要求拆分指标点的对应关系

序号	课程目标	毕业要求拆分指标点			
		2.4	3.2	5.2	9.1
1	掌握安全软件开发基本概念和原则，以及过程、方法、工具和技术等，能用文档表述以上内容如何应用在软件开发过程中	●			
2	了解现行网络环境下软件受到的威胁来源，并分析其危害和制定应对削减这些威胁的策略。能与软件工程相结合，进行安全软件开发工程实践		●		
3	开发、选择与使用适当的技术、资源和工具，对安全软件开发工程问题进行预测与模拟。培养学生理解安全软件开发生命周期的概念，以及在开发过程各个阶段对多种技术、工具的应用。			◎	
4	掌握和应用工具对软件进行有效的安全审核和测试，处理安全事件，同时在实验中培养团队合作意识				⊙

注：●：表示有强相关关系，◎：表示有一般相关关系，⊙：表示有弱相关关系

2 育人目标：培养学生的社会责任感和使命感，致力于开发出更加安全的软件，为社会提供安全且符合法律法规的软件产品。

三、课程教学内容

表 2 教学内容与课程目标的对应关系

章节名称	教学内容及重点（▲）、难点（★）	课程目标（√）			
		1	2	3	4
第一章软件安全概述	讲授软件安全的概念、软件安全问题的来源（▲），信息安全的发展对软件安全方面的要求（▲）	√			
第二章安全软件开发	讲授在程序设计和软件工程的基础上提升软件的安全性（▲），安全软件开发从软件需求分析阶段开始的各个组成阶段（▲），安全软件开发模型（★）	√			

第三章常见软件安全漏洞	讲授软件漏洞和缺陷（▲），典型的恶意代码利用软件漏洞实施攻击的模式（★），Windows 应用程序典型的安全漏洞（▲），Web 应用安全漏洞的几种形态分析（★）			√	
第四章安全风险分析	讲授如何根据软件功能需求和面临的安全环境创建威胁模型（▲），威胁模型审核（★）	√	√	√	
第五章安全设计原则	讲授通用的安全软件设计原则▲），基于安全模型的软件安全设计所涉及的工作	√	√	√	
第六章安全编码实践	讲授应用安全编码策略包括使用编译器内置防御特性（▲），代码分析（▲）、减少潜在可被利用的编码结构或设计（▲）、使用安全编码检查清单（▲）。	√	√	√	
第七章软件安全审核	讲授对威胁模型的审核，对源代码的人工和自动审核（▲）	√		√	√
第八章软件安全测试	讲授如何测试软件的安全性（▲）、测试技术的重要性（▲） 、各种测试技术和工具的运用和有效性（★）、测试结果的反馈作用		√	√	√
第九章最终安全审核与安全响应	讲授发布前的所需最终安全审核过程，确保对已知安全威胁的抵御能力，如何在交付后培训用户和应对安全问题			√	√

四、教授方法与学习方法指导

教授方法：

1. 课堂讲授

课堂教学首先要使学生掌握课程教学内容中的安全软件开发概念、基本技术和基本方法。通过讲授，使学生能够对这些基本概念和理论有更深入的理解，使之有能力将它们应用到一些问题的求解中。要注意对实现软件安全的一些基本方法与核心思想的分析，使学生能够掌握其关键。具体来说，从当前软件面临的威胁和自身的漏洞开始，阐述软件安全的重要性和相关概念，引导学生对安全软件开发的兴趣，逐步扩展安全软件开发所涉及的各个方面的内容，说明安全软件开发必须贯穿在整个软件开发过程中。然后介绍行之有效的过程、方法技术和工具

积极探索如何实现教师在对问题的解决过程中教学，学生怎样在对未知的探索中学习。从提出问题，到问题来源分析，再到用有效的方法和技术解决问题。从开始向学生介绍软件开发需要具备安全的观念，到安全软件开发涉及的各个方面的问题和解决之道，进一步培养学生解决问题的工程能力，从系统的角度向学生展示安全软件开发的一般原则，同时考虑不同软件的差异、解决具体问题的方案和技术。通过不同开发阶段时对多种技术的运用，培养学生的工程开发和能力。

使用多媒体课件，配合板书和实例演示讲授课程内容。在授课过程中，可由常见的软件面临的安全问题引出概念，自然进入相关内容的讲授。积极引导学生阅读外文书籍和资料，培养自学能力。

2. 实验教学

实验需要在了解掌握所学知识的基础上，在实验教学大纲的指导下，首先通过设计出攻击行为作用于程序，了解软件可能受到的攻击，确定软件的漏洞和薄弱之处。接下来进

行测试软件的安全性能，实现安全编码和安全审核。要求学生完成相关实验方案的选择，并使用适当的技术实现目标。每组最后提交规范的实验报告。

通过实验系统的实现，引导学生经历安全软件开发的主要流程，具体体验如何将基本的原则用于安全软件开发过程，加深对原则的理解；其次是培养学生系统能力（系统的视角，系统的设计、分析与实现）；第三是培养学生的软件系统实现能力（方法、技术的应用）；第四是通过分小组，培养学生的团队合作精神与能力；第五是培养学生查阅资料，获取适当工具、使用适当工具；第六是培养学生书面表达能力。

实验分组进行，2 人一组，协同完成系统的设计与实现。

（1）实验内容

程序安全漏洞寻找和分析

对一个肯定存在已知安全漏洞的程序，找出一个可利用通过输入进行攻击的方案，使得程序面对攻击时无法按正常流程执行。分析产生安全漏洞的原因。

安全测试

使用测试软件和框架，生成测试用例，对选定的程序进行安全测试，得到结果和生成反馈应对方案。

安全编码实践

以 C/C++语言为准，按照最新编译器提供的方案。进行代码编写实验，提升程序的安全水平，消除在程序分析和测试中发现的安全漏洞。

安全审核实践

对一个小型软件开发工程，实践对各个阶段的安全审核，产生结论(审核报告)。

以上均要求系统能有完整的源代码和输入序列，输出预期的结果。

（2）验收与评价

验收方式 1：现场验收。现场验收学生实验的成果，确定有无重大设计和实施错误而需要重做的情况，并给出现场初步评定。评定级别分合格、不合格，不合格者须重新完成实验和初评，合格的学生必须在稍后时间提交实验报告，通过此环节训练和检验其实验设计与执行能力。

验收方式 2：综合验收。现场验收合格后,学生撰写并按时提交打印版书面实验报告。对实验过程加以考核，通过此环节培养其实验分析与总结等能力。以此为准进行最终实验评分。

评分建议：总分为 85 分，主要依据书面报告验收标准评分，现场验收曾为不合格而重做的，最终分数会适当扣除 1-5 分，每缺席一次实验，将扣除 1 分；

3．作业

通过课外作业，引导学生检验学习效果，进一步掌握课堂讲述的内容，了解自己实际掌握的程度，思考一些相关的问题，进一步深入理解扩展的内容。

作业的基本要求：根据各章节的情况，包括练习题、思考题等，每一章布置适量的课外作业，完成这些作业需要的知识覆盖课堂讲授内容，包括基本概念题、解答题、综合题以及其它题型等。

每章题量参考数为 2-4 题。主要支持毕业要求 2.4、3.2 的实现。

学习方法：养成探索的习惯，特别是重视对基本方法的掌握，在信息安全理论指导下进行实践；注意从实际问题入手，了解软件现存的漏洞和缺陷、面临的威胁，从建立威胁模型开始，到最后实现安全的软件开发。明确学习各阶段的重点任务，做到课前预习，课中认真听课，积极思考，课后认真复习，不遗漏知识点，充分利用好教师资源和同学资源。仔细研读教材，适当选读参考书的相关内容，从系统实现的角度，深入理解概念，掌握方法的精髓和技术的核心思想。积极参加实验，加深对开发过程、方法和技术的理解。

五、教学环节及学时分配

教学环节及各章节学时分配，详见表 3。

表 3 教学环节及各章节学时分配表

章节	主要内容	学时分配					合计
		讲课	习题	实验	讨论	其他	
1	软件安全问题和对策	1					2
2	安全软件开发基础	1					2
3	软件安全漏洞分析	2		4			6
4	软件安全风险分析	2					2
5	软件安全设计	2					2
6	软件安全编码	2		4			6
7	软件安全审核	2					2
8	软件安全测试	2		4			6
9	最终审核和安全响应	2		4			6
合计		16		16			32

注：课内 16 小时的实验时间仅是在实验室集中进行的工作，学生还需要用更多的课外时间预习准备。

六、考核与成绩评定

作业：主要反应学生的课堂表现、平时对信息接受、自我学习和掌握情况。成绩评定的主要依据包括：课程的出勤情况，作业能否按时完成，质量情况。

实验：主要反映学生在运用所学知识进行安全软件开发工程实践的能力,培养学生在该复杂系统的研究、设计与实现中的交流能力（口头和书面表达）、协作能力、组织能力、总结能力。

表 4 考核方式及成绩评定分布表

考核方式	所占比例（%）	主要考核内容及对毕业要求拆分指标点的支撑情况
平时成绩	20	课堂出勤听讲状况，相关作业的完成质量，对毕业要求 2.4、3.2 达成度的评价提供支持。
实验成绩	80	实验系统的设计实现情况。对毕业要求 2.4、3.2 的达成度的考核，同时对毕业要求 5.2、9.1 的达成度的评价提供有一定参考价值的评分依据

七、考核环节及质量标准

本课程各考核环节及质量标准，详见表 5。

表 5 考核环节及质量标准

考核方式	评　分　标准				
	A	**B**	**C**	**D**	**E**
	90～100	**80～89**	**70～79**	**60～69**	**< 60**
作业	圆满完成作业要求，分析问题结论正确，有好的解决方法。反映出对教学内容中的基本概念和方法等方面的掌握很好	完成作业要求，分析问题结论较正确，有良好的解决方法。反映出对教学内容中的基本概念和方法等方面的掌握较好。	完成作业要求，分析问题结论基本正确，有可行的解决方法。反映出对教学内容中的基本概念和方法等方面的掌握一般	基本完成作业要求，分析问题结论基本正确，有基本可行的解决方法。反映出对教学内容中的基本概念和方法等方面有基本掌握	不满足 D 要求
实验	设计实验方案合理可行，功能设计符合实验要求，实验结果与设计相符，善于合作。综合运用理论知识解决复杂问题的能力很好。	设计实验方案合理可行，功能设计比较符合实验要求，实验结果与设计相符，善于合作。综合运用理论知识解决复杂问题的能力较好。	设计实验方案比较合理可行，功能设计比较符合实验要求，实验结果与设计比较相符，能够合作。综合运用理论知识解决复杂问题的能力一般。	设计实验方案基本合理可行，功能设计基本符合实验要求，实验结果与设计基本相符，能够合作。综合运用理论知识解决复杂问题的能力不足。	不满足 D 要求
报告	对实验过程叙述清楚、详略得当，结论清楚、图表齐全有说明效果	对实验过程叙述较清楚、详略得当，结论较清楚、图表较齐全有说明效果	对实验过程叙述基本清楚、详略较合适，结论基本清楚、图表基本齐全有说明效果	对实验过程叙述基本清楚、详略基本合适，结论不够清楚、图表不够齐全有说明效果不足	不满足 D 要求
评分标准（A～E）：主要填写对教学内容中的基本概念、理论、方法等方面的掌握，及综合运用理论知识解决复杂问题能力的要求。					

制定者：陈健中

批准者：张建标

2020 年 7 月

“信息安全法律基础Ⅰ”课程教学大纲

英文名称：Law about Information Security

课程编码：0004886

课程性质：专业选修课

学分：2.0　　学时：32

面向对象：信息安全（实验班）专业本科生

先修课程：思想道德修养与法律基础

教材及参考书：

[1] 陈忠文、麦永浩. 信息安全标准与法律法规（第三版）.武汉大学出版社. 2017.9.1

[2] 夏冰. 网络安全法和网络安全等级保护 2.0. 电子工业出版社. 2017.01

[3] 黄波，刘洋洋，李锦. 信息安全法律法规汇编与案例分析(公安院校招录培养体制改革试点专业系列教材). 清华大学出版社. 2012.

[4] 中华人民共和国保密法律法规汇编（第二版）. 法律出版社. 2019.07.

一、课程简介

描述课程概况（250-300 字）。信息安全法律基础是信息学部计算机学院为全校本科生开设的专业选修课程。本课程的任务是通过对信息安全相关法律条款和经典案例的介绍向学生传授信息安全相关法律知识，使学生较系统地掌握信息安全的相关法律法规，具备能正确处理相关信息安全法律问题的能力。教学内容重点：犯罪的概念、类型、计算机犯罪、网络安全法、密码法、域名权、隐私权、名誉权、网络虚拟财产权、电子证据、著作权法、计算机软件保护条例、信息网络传播权保护条例、电子合同、数据电文、电子签名法、电子商务法。教学内容的难点：犯罪的概念、犯罪的类型、计算机犯罪的类型、网络安全法、密码法、电子证据、计算机软件保护条例、信息网络传播权保护条例、电子商务法。

二、课程地位与目标

（一）课程地位：本课程是全校本科生专业选修课，它是继《思想道德修养与法律基础》课程之后开设的课程。《思想道德修养与法律基础》课程是帮助大学生树立正确的世界观、人生观、价值观、道德观和法治观，提高自我修养，而本课程主要侧重于使学生了解本专业相关的法律法规，培养良好的职业道德，具备正确处理信息安全法律问题的能力。

本课程支撑的毕业要求拆分指标点的具体描述。

7.1：掌握信息安全的相关法律法规，培养学生分析、评价计算机、信息安全相关产业对社会、健康、安全、法律、文化的影响的能力;

8.1：具有环境保护和社会持续发展意识，能认识到信息安全系统的开发、运行、更新换代对环境保护和社会持续发展的影响;

9.2：掌握与信息安全相关的重要法律、法规及方针与政策，培养学生良好的职业道德，具备正确处理信息安全法律问题并在实践中自觉遵守的能力。

（二）课程目标

1 教学目标：通过对信息安全相关法律条款和经典案例的介绍，向学生传授信息安全

相关法律知识，使学生较系统地掌握信息安全的相关法律法规，培养学生良好的信息安全法律意识，具备正确处理信息安全法律问题并在实践中自觉遵守的能力。本课程对毕业要求拆分指标点达成的支撑情况，详见表 1。

表 1 课程目标与毕业要求拆分指标点的对应关系

序号	课程目标	毕业要求拆分指标点		
		7.1	8.1	9.2
1	培养学生分析、评价计算机、信息安全产业对社会、健康、安全、法律以及文化的影响的能力	◎		
2	培养学生环境保护和社会持续发展意识，能认识到信息安全系统的开发、运行、更新换代对环境保护和社会持续发展的影响的能力		⊙	
3	培养学生良好的信息安全法律意识，具备正确处理信息安全法律问题并在实践中自觉遵守的能力			●

注：●：表示有强相关关系，◎：表示有一般相关关系，⊙：表示有弱相关关系

2 育人目标：本课程通过学习信息安全法律知识，可以了解计算机、信息安全相关的重要法律、法规及方针与政策，具备良好的人文社会科学素养、社会责任感，增强学生信息安全法律意识，培养学生理想信念、具有家国情怀、民族自信、法律意识、有责任担当，具有职业素养、良好行为规范的人，并在社会实践中自觉遵守法律。

三、课程教学内容

分章节列出课程教学内容及对课程目标的支撑，详见表 2。

表 2 教学内容与课程目标的对应关系

章节名称	教学内容及重点（▲）、难点（★）	课程目标（√）			
		1	2	3	4
第一章 信息安全法律基础概述	教学目标、课程的基本内容、法的产生▲、部门法的产生、信息安全/计算机法律的产生▲、两大法系▲★	√	√	√	
第二章 计算机犯罪	犯罪的概念▲、犯罪的类型▲；计算机犯罪的产生、原因、特点、发展趋势、定义与特点、立法；计算机犯罪的类型▲；非法侵入计算机信息系统罪▲★；破坏计算机信息系统罪▲★；案例分析▲★；传统犯罪计算机化	√	√	√	
第三章 网络法律制度	域名权▲、隐私权▲、名誉权、网络虚拟财产权▲；网络社会中的纠纷解决方式；中国互联网络域名争议解决办法▲★；网络安全法▲★；案例分析▲★	√	√	√	
第四章 计算机软件的法律保护	计算机软件保护条例▲★；信息网络传播权保护条例▲；案例分析▲★；计算机软件其它法律：专利法、商标法、反不正当竞争法；密码法▲★	√	√	√	
第五章 电子商务法律	电子商务带来的安全风险和相关法律问题、电子合同、数据电文以及电子签名的概念▲、数据电文的法律效力▲；《电子签名法》▲★；《电子商务法》▲★、案例分析▲★	√	√	√	

四、教授方法与学习方法指导

教授方法：以讲授为主，讨论作业为辅。课内讲授采用探究教学、案例教学等多种教学方法与模式，结合多媒体、板书等教学手段，通过范例和视频演示讲授课程内容。以知识为载体，传授相关的思想和方法，引导学生掌握信息安全相关的法律法规的基本内容，以及培养学生利用信息安全相关的法律法规知识分析案例解决信息安全相关法律问题的能力。

学习方法：在学习信息安全相关法律法规时，在理解和研究上遵循“法魂主义”的方法，即遵循法律公平和正义的精神，在这个前提下学习信息安全相关法律。结合相关信息安全法律实践案例，以更深刻地理解信息安全法律条文的内涵。

五、教学环节及学时分配

教学环节及各章节学时分配，详见表 3。

表 3 教学环节及各章节学时分配表

章节名称	教学内容	学时分配					合计
		讲授	习题	实验	讨论	其它	
第一章 绪论	教学目标、课程的基本内容、法的产生、部门法的产生、信息安全/计算机法律的产生、两大法系	2					2
第二章 计算机犯罪	犯罪的概念、犯罪的类型；计算机犯罪的产生、原因、特点、发展趋势、定义与特点、立法；计算机犯罪的类型；案例分析；传统犯罪计算机化	4			2		6
第三章 网络法律制度	域名权、隐私权、名誉权、网络虚拟财产权；网络社会中的纠纷解决方式；网络安全法；密码法；案例分析	8			2		10
第四章 计算机软件的法律保护	计算机软件保护条例；信息网络传播权保护条例；案例分析；计算机软件其它法律：专利法、商标法、反不正当竞争法	6			2		8
第五章 电子商务法律	电子商务带来的安全风险和相关法律问题、电子合同、数据电文以及电子签名的概念、数据电文的法律效力；《电子签名法》；《电子商务法》；案例分析	4					4
	总结和复习	2					
合计		26			6		32

六、考核与成绩评定

课程成绩包括平时成绩和考试成绩两部分。

考核方式及成绩评定分布：期末考试占 80%。涵盖所学内容 90％以上；分为概念题（理论题）和案例分析题两部分。考试环节是对学生学习情况的全面检验，考查学生对信息安全法律法规基础知识的掌握以及对信息安全法律案例分析的能力，起到督促学生系统掌握课程主要教学内容的作用。平时成绩占 20%，反映学生的课堂表现、平时的信息接受、自我约束，考察学生对已学知识掌握的程度以及自主学习的能力。成绩评定的主要依据包括：

课程的出勤情况、课堂的基本表现（含课堂作业、课堂互动等）以及课外作业情况。

本课程各考核环节的比重及对毕业要求拆分点的支撑情况，详见表 4。

表 4 考核方式及成绩评定分布表

考核方式	所占比例（%）	主要考核内容及对毕业要求拆分指标点的支撑情况
平时成绩	20	课程的出勤率、课堂的基本表现、课堂作业和课外作业的完成质量，对课程目标 1、课程目标 2、课程目标 3 达成度的评价提供支持。
考试成绩	80	对规定考试内容掌握的情况，对课程目标 1、课程目标 2、课程目标 3 达成度的评价提供支持。

七、考核环节及质量标准

本课程各考核环节及质量标准，详见表 5。

表 5 考核环节及质量标准

考核方式	评分标准				
	A	B	C	D	E
	90～100	80～89	70～79	60～69	< 60
作业	作业格式规范、文字规范、术语准确；案例分析准确	作业格式较规范、文字较规范、术语较准确；案例分析较准确	作业格式较规范、文字较规范、术语较准确；案例分析基本准确	作业格式基本规范、文字基本规范、术语基本准确；案例分析基本准确	不满足 D 要求
研讨	上课全勤、积极回答教师随堂提问、积极参与讨论	上课全勤、较积极回答教师随堂提问、较积极参与讨论	上课全勤、较积极回答教师随堂提问、能参与讨论	上课缺席不超过 2 次、能回答教师随堂提问、能参与讨论	不满足 D 要求
考试	很好地掌握教学内容涉及的基本概念、理论、方法，且具备很强的综合运用所学知识解决复杂问题的能力。	较好地掌握教学内容涉及的基本概念、理论、方法，且具备较强的综合运用所学知识解决复杂问题的能力。	较好地掌握教学内容涉及的基本概念、理论、方法，且具备一定的综合运用所学知识解决复杂问题的能力。	基本掌握教学内容涉及的基本概念、理论、方法，且基本能具备运用所学知识解决复杂问题。	不满足 D 要求
评分标准（A～E）：主要填写对教学内容中的基本概念、理论、方法等方面的掌握，及综合运用理论知识解决复杂问题能力的要求。					

制定者：杨宇光

批准者：张建标

2020 年 7 月

“信息隐藏”课程教学大纲

英文名称：Information Hiding

课程编码：0004923

课程性质：专业选修课

学分：2.0　　学时：32

面向对象：信息安全（实验班）专业本科生

先修课程：无

教材及参考书：

[1] 陆哲明，聂廷远，吉爱国. 信息隐藏概论. 北京：电子工业出版社，2014 年 11 月

[2] 张立和. 透视信息隐藏. 北京：国防工业出版社，2007 年 2 月

[3] 葛秀慧. 信息隐藏原理及应用. 北京：清华大学出版社，2009 年 10 月

[4] 王丽娜，张焕国. 信息隐藏技术与应用. 武汉：武汉大学出版社，2003 年 8 月

一、课程简介

信息隐藏技术是一种重要的信息安全技术，本课程以图像信息隐藏为主，介绍载体的基本知识、隐写术、数字水印、信息隐藏的应用（版权保护、图像的篡改与防伪鉴别等）等内容。通过本课程的学习，使学生对信息隐藏有一个基本的了解，掌握信息隐藏的基本概念和方法，为从事信息隐藏的研究和应用打下一个坚实的基础。

二、课程地位与目标

（一）课程地位：本课程是信息安全专业的专业选修课。旨在使学生理解并掌握信息隐藏所涉及的基本理论和方法，具备信息隐藏和数字水印的基本能力。通过对本课程的学习，要求学生对信息隐藏和数字水印所涉及的基本理论和方法有初步了解，并熟悉和掌握几种主要的信息隐藏和数字水印方法与技术。通过配套的实验课程教学，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，奠定基础。

本课程支撑的毕业要求拆分指标点的具体描述。

2.4：具备应用相关知识对系统解决方案进行比较分析、改进的能力。

3.3：能利用多种资源开展文献检索和资料查询。

4.2：能针对特定需求完成系统模块的设计与实现，测试验证模块的正确性，并进行性能优化。

（二）课程目标

1 教学目标：总的教学目标是：使学生掌握“信息隐藏”中的基本概念、基本理论、基本方法，体验分析和解决问题的乐趣。该目标分解为以下子目标。

- ✧ 掌握信息隐藏的基本概念和方法。
- ✧ 增强理论结合实际能力，体验分析和解决问题的乐趣。
- ✧ 培养系统能力和团队协作能力。

主要为毕业要求 2.4、3.3、4.2 的实现提供支持。

对于毕业要求 2.4，信息隐藏是一门理论和实践相结合的课程，既能让学生掌握相关的

数学知识和自然科学知识，又能学以致用，培养解决复杂工程实际问题的能力。

对于毕业要求 3.3，信息隐藏处在快速发展过程中，需要学生查找最新资料，能为学生通过文献研究分析信息安全领域问题，获得有效结论提供支撑。

对于毕业要求 4.2，信息隐藏是一门理论和实践相结合的课程，可以促使学生设计满足信息安全需求的系统，并能够在设计环节中体现较强的创新意识和一定的创新能力。

表 1 课程目标与毕业要求拆分指标点的对应关系

序号	课程目标	毕业要求拆分指标点		
		2.4	3.3	4.2
1	掌握信息隐藏的基本概念和方法	●		
2	增强理论结合实际能力，体验分析和解决问题的乐趣		●	
3	培养系统能力和团队协作能力			◎

注：●：表示有强相关关系，◎：表示有一般相关关系，⊙：表示有弱相关关系

2 育人目标：信息隐藏类似于密码学，是敌我双方角力的战场，已经有一些恐怖组织和个人利用信息隐藏传递非法信息。因此在授课过程中通过无缝引入经典案例，使学生树立起理想信念、家国情怀、民族自信、责任担当、职业素养、行为规范等，寓价值观引导于知识传授之中。

三、课程教学内容

分章节列出课程教学内容及对课程目标的支撑，详见表 2。

表 2 教学内容与课程目标的对应关系

章节名称	教学内容及重点（▲）、难点（★）	课程目标（√）		
		1	2	3
第一章 绪论	教学目的、课程的基本内容、信息隐藏的基本理论▲、古典信息隐藏、应用、信息隐藏技术的发展现状、载体基本知识。	√	√	
第二章 隐写术	隐写术的发展、隐写术与密码的关系、隐写系统模型、隐写术特点、隐写算法设计▲、LSB 隐写▲、隐写检测技术。	√	√	√
第三章 数字水印	数字水印的定义和分类、数字水印的主要特征、数字水印嵌入技术、DCT 数字水印算法▲、数字水印检测技术、数字水印的攻击和对抗策略、数字水印评估	√	√	√
第四章 图像取证	知识产权保护的概念、版权标记技术的发展、基于数字水印的版权保护、图像篡改检测▲、图像篡改定位▲、图像篡改恢复▲。	√	√	

四、教授方法与学习方法指导

教授方法：

1.课堂讲授：课堂教学首先要使学生掌握课程教学内容中规定的一些基本概念、基本理论和基本方法。特别是通过讲授，使学生能够对这些基本概念和理论有更深入的理解，使之有能力将它们应用到一些问题的求解中。要注意对其中的一些基本方法的核心思想的分析，使学生能够掌握其关键。

积极探索和实践研究型教学。探索如何实现教师在对问题的求解中教，学生怎么在对未知的探索中学。通过学生身边看得见、摸得着的例子入手，将理论和实践结合起来，逐步过渡到信息安全的专业问题上，引导学生进行初步的科学研究。

使用多媒体课件，配合板书和范例演示讲授课程内容。在授课过程中，可由常见的生活问题引出概念，自然进入相关内容的讲授。适当引导学生阅读外文书籍和资料，培养自学能力。

2.实验教学：实验需要在掌握基本原理的基础上，在总体结构的指导下，完成 LSB、基于 LSB 的篡改检测和定位、DCT 数字水印这样三个实验，并提交规范的实验报告。

通过实验，引导学生体会信息隐藏的主要流程，掌握信息隐藏的典型方法，加深对理论的理解；其次是培养学生的系统能力（系统的视角，系统的设计、分析与实现）；第三是培养学生的软件实现能力；第四是培养学生查阅资料，获取适当工具、使用适当工具的能力；第五是培养学生表达（书面、口头）能力。

（1）实现 LSB 图像信息隐藏算法：用所给的载体和消息图像，完成灰度图像的 LSB 算法。

（2）DCT 数字水印算法：实现课上讲过的 DCT 水印算法。载体 8*8 分块，用(5,2)、(4,3)这两个 DCT 系数的相对大小来表示隐藏的信息，每个 8*8 的块隐藏 1 比特信息。

（3）脆弱水印算法：基于实验 1 的 LSB 算法，实现一个奇偶校验的脆弱水印算法，能标示出图像被篡改的位置。

验收方式：现场验收。现场验收学生设计实现的系统，并给出现场评定。评定级别分优秀、良好、合格、不合格。此外，学生必须提交实验报告，通过此环节训练其实验总结与分析等能力。

学习方法：学生需要高效利用课堂教学时间，认真完成实验，鼓励学生和任课教师交流，仔细研读教材，适当选读参考书的相关内容，从系统实现的角度，深入理解概念，掌握方法的精髓和算法的核心思想，不要死记硬背。有余力同学可以额外阅读一些资料。

五、教学环节及学时分配

教学环节及各章节学时分配，详见表 3。

表 3 教学环节及各章节学时分配表

章节名称	教学内容	学 时 分 配					合计
		讲授	习题	实验	讨论	其它	
1	绪论	4					4
2	隐写术	6		2			8
3	数字水印	7		4			11
4	图像取证	6		2			8
	总结	1					1
合计		24	0	8	0	0	32

六、考核与成绩评定

课程成绩包括三部分：实验成绩 30%，课堂成绩 20%，考试成绩 50%。

实验成绩 30%要求学生通过编写程序，再现课堂所讲授的关键知识，并能灵活运用所学知识，从而得到实验结果。

课堂成绩 20%主要反应学生的课堂表现、平时的信息接收、自我约束。成绩评定的主要依据包括：课程的出勤率、课堂的基本表现。

考试成绩 50%为对学生学习情况的全面检验。强调考核学生对基本概念、基本方法、基本理论等方面掌握的程度，及学生运用所学理论知识解决复杂问题的能力。

本课程各考核环节的比重及对毕业要求拆分点的支撑情况，详见表 4。

表 4 考核方式及成绩评定分布表

考核方式	占比（%）	主要考核内容及对毕业要求拆分指标点的支撑情况
实验	30	实验的完成质量，对应毕业要求 2.4、3.3、4.2 达成度的考核。
课堂	20	出勤和回答问题情况，对应毕业要求 2.4、3.3、4.2 达成度的考核。
考试成绩	50	对课程内容掌握的情况，对应毕业要求 2.4、4.2 达成度的考核。

七、考核环节及质量标准

本课程各考核环节及质量标准，详见表 5。

表 5 考核环节及质量标准

考核方式	评　分　标　准				
	A	B	C	D	E
	90～100	80～89	70～79	60～69	< 60
实验	全部实验自主完成，按时提交，程序运行结果良好，能流畅回答老师的问题，按时提交实验报告	全部实验自主完成，个别实验有拖后提交现象，程序运行结果良好，基本能回答出老师的问题，按时提交实验报告	需要教师或者同学的一些指导，实验有拖后提交现象，程序能运行出结果，对老师的提问，有个别问题回答错误或者不知如何回答，按时提交实验报告	需要教师或者同学的指导，实验拖后提交，程序能运行出结果，对老师的提问，回答错误或者不知如何回答，按时提交实验报告	不满足 D 要求
课堂	全勤、积极回答问题、回答正确	缺勤 1 次，被提问到的时候能回答问题，基本正确	缺勤 2-3 次，被提问到的时候能回答问题，基本正确	缺勤 4-5 次，被提问到的时候回答“不会”或者基本错误	不满足 D 要求
考试	参考标准答案	参考标准答案	参考标准答案	参考标准答案	参考标准答案
评分标准（A～E）：主要填写对教学内容中的基本概念、理论、方法等方面的掌握，及综合运用理论知识解决复杂问题能力的要求。					

制定者：姜楠

批准者：张建标

2020 年 7 月

“深度网络与 AI 技术安全”课程教学大纲

英文名称：Security of Deep Neutral Network and AI Technology

课程编码：0010146

课程性质：专业选修课

学分：2.0　　学时：32

适用对象：信息安全专业本科生

先修课程：信息安全数学基础

教材及参考书：

[1] 周志华，机器学习，清华大学出版社，2016 年 1 月

[2] 伊恩·古德费洛（Ian Goodfellow），深度学习，人民邮电出版社，2017 年 8 月

[3] 弗朗索瓦·肖莱（Francois Chollet），Python 深度学习，人民邮电出版社，2018 年 8 月

[4] 安德鲁·特拉斯克（Andrew W. Trask）著，王晓雷、严烈译，深度学习图解，清华大学出版社，2019 年 12 月

[5] Aurélien Gér 著，Scikit-Learn 与 TensorFlow 机器学习实用指南，东南大学出版社，2017 年 1 月

一、课程简介

深度网络及 AI 技术安全是计算机学院（部）为信息安全专业本科生开设的专业选修课程类型。本课程的任务是对神经网络中的数据隐私和数据安全进行了分析。主要介绍了基于同态加密的神经网络，能够让服务器在不知道用户原始数据的情况下，对密文进行挖掘，从而得到一个基于密文的结果。首先介绍常用的同态加密方法，然后再介绍基于同态加密的神经网络。教学内容重点：同态加密的原理，神经网络的基础知识，基于同态加密的神经网络模型，常见的基于同态加密的神经网络。教学内容的难点：同态加密算法的实现，神经网络的训练流程，在数据集上测试基于同态加密的神经网络。

二、课程地位与目标

（一）课程地位：本课程是信息安全专业的限选课，可以作为其它计算机类专业的选修课。旨在引导学生对于深度神经网络上的数据安全和数据隐私进行认识；给学生提供参与设计实现能保护数据安全和数据隐私的深度网络模型，培养学生的工程意识和动手能力。

本课程支撑的毕业要求拆分指标点的具体描述。

3.5：能应用数学、自然科学和工程科学的基本原理证实解决方案的合理性，获得有效结论

4.5：能对已有复杂问题的解决方案进行研究，并提出新的替代方案

5.2：能基于专业理论和技术，选择研究路线，设计实验方案

6.1：针对信息安全工程问题，分析其所需的相关技术、资源和工具

（二）课程目标

1 教学目标：理解基于同态加密的深度学习的概念，理论和方法。在此之上再进一步了解如何在保护数据安全和数据隐私的前提下进行深度学习。该目标分解为以下子目标，

如表 1 所示。

表 1 课程目标与毕业要求拆分指标点对应关系

序号	课程目标	毕业要求拆分指标点			
		3.5	4.5	5.2	6.1
1	能应用数学、工程科学的基本原理证实已有的解决方案的合理性	●			
2	能对已有保护神经网络相关的数据安全和数据隐私问题的解决方案进行研究		◎		
3	能基于神经网络和数据安全及隐私理论和技术特点，选择研究路线，设计实验方案			⊙	
4	对于神经网络中相关的数据安全和数据隐私问题，分析其所需的相关技术、资源和工具				◎

● 表示表示有强相关关系， ◎： 表示有一般相关关系，⊙： 表示有弱相关关系

2 育人目标：目前主流的神经网络架构都是国外开发的，安全套件也是国外开发的，引导学生爱国主义情怀：通过图灵与恩格玛机器的故事；提升民族自信心：王小云教授的成就。

三、课程教学内容

分章节列出课程教学内容及对课程目标的支撑，详见表 2。

表 2 教学内容与课程目标的对应关系

章节名称	教学内容及重点（▲）、难点（★）	课程目标（√）			
		1	2	3	4
第一章 同态加密算法	首先介绍课程的主要目标，主要介绍同态加密的基本概念（▲），以及实现原理（★），所谓的同态加密是一种加密方式，允许对密文进行某种操作，得到的结果仍然是加密的结果，并且对这个加密的结果进行解密操作，得到的结果相当于对明文进行同样操作的结果。在这个基础之上介绍 Palier 同态加密，基于格的同态加密以及同态加密的原理以及实现（★）。并在此基础之上对下文要介绍的基于同态加密的神经网络模型所使用的同态加密进行介绍。	√			√
第二章 神经网络	对神经网络的基本原理和基本概念进行介绍。感知器、Sigmoid 神经元、激励函数、神经网络的结构代价函数等基本概念，以及神经网络的训练流程。此外还需要介绍一些矩阵的基本知识矩阵的加法、减法、乘法矩阵的转置，向量的 Hadamard 乘积向量的模等概念的回顾。			√	
第三章基于同态加密神经网络模型	Dowlin 等人于 2016 年提出的基于同态加密的网络模型。他们首先使用同态加密（▲）来保护数据安全和隐私。他们的方案包括卷积层，最大池化层，平均池化层，Sigmoid 等（▲）。他们提出了两种方案：训练神经网络和简化神经网络，简化神经网络用于预测（★）。主要贡献是提出了一种简单的在使用同态加密情况下保持神经网络正确性的方法。		√		√
第四章	详细分析 CryptoDL（★）、Faster CryptoNets（▲）、等基于同		√		

常见的基于同态加密的神经网络	态加密的神经网络，对比原理，实现方式。并且对运行结果和运行效率的对比。CryptoDL 重点关注 CNN，一种最流行的深度学习算法。Faster CryptoNets 基于 CryptoNets，对神经网络的激活功能进行了讨论。				

四、教授方法与学习方法指导

教授方法：以讲授、实验对半方式，进一步加强学生的实践能力。课内讲授推崇研究型教学，以知识为载体，传授相关的思想和方法。实验教学则提出基本要求，引导学生独立（按组）完成系统的设计与实现。

学习方法：养成探索的习惯，特别是重视对基本理论的学习和理解，在理论指导下进行动手操作；注意从实际问题入手，归纳和提取基本特性，能够将实际问题和理论结合起来，用理论来指导实践，并且解决实际生活中的问题。明确学习各阶段的重点任务，做到课前预习，课中认真听课，积极思考，课后认真复习，不放过疑点，充分利用好教师资源和同学资源。仔细研读教材，适当选读参考书的相关内容，并且需要积极参加实验，在实验中加深对原理的理解，提高自己的动手能力，对学习过的理论进行验证。能够对学习过的内容主动进行扩展，能够主动学习课堂相关内容，养成良好的学习习惯。

五、教学环节及学时分配

教学环节及各章节学时分配，详见表 3。

表 3 考核环节及质量标准

章	主要内容	学时分配					合计
		讲课	习题	实验	讨论	其他	
1	同态加密原理及常见同态加密	2	0	2	0	0	4
2	神经网络基本概念	4	0	4	0	0	8
3	基于同态加密的神经网络模型	6	0	6	0	0	12
4	常见的基于同态加密的神经网络	4	0	0	4	0	8
合计		16	0	12	4	0	32

1. 课堂讲授

课堂教学首先要使学生掌握一些基本概念、基本理论和基本方法。特别是通过讲授，使学生能够对这些基本概念和理论有更深入的理解，使之有能力将它们应用到一些问题的求解中。首先对学生的已经掌握的知识进行回归，发现学生对圣经网络基础概念的掌握情况，在此基础之上进行基础概念的复习。

注重可操作性和实用性。通过对典型神经网络案例讲解，使学生能够举一反三。在课堂介绍的知识之外学习主动学习新的知识，并能够把知识自己实践。适当引导学生阅读外文书籍和资料，培养自学能力。培养学生初步的科研能力。

2. 实验教学

通过实践环节增强学生对同态加密、常用的神经网络、以及基于同态加密的神经网络，培养学生分析问题、解决问题的能力以及理论联系实际的动手能力，同时还培养学生初步具备自我创新能力以及严谨认真的实验态度和分工协作的团队精神。

通过实验系统的设计与实现，引导学生经历构造系统的主要流程，具体体验如何将基

本的原理用于系统设计与实现，加深对理论的理解；其次是培养学生系统能力（系统的视角，系统的设计、分析与实现）；第三是通过分小组，培养学生的团队合作精神与能力；第四是培养学生查阅资料，获取适当工具、使用适当工具；第五是培养学生表达（书面语口头）能力。实验分组进行，3-4 人一组，协同完成系统的设计与实现。基本内容如下：

编号	实验内容	具体要求
1	同态加密的基本原理	掌握基于加法和乘法的同态加密原理和实现
2	常用的神经网络模型	在数据集上面实现常用的神经网络的数据挖掘
3	基于同态加密的神经网络	掌握基于同态加密的能保护数据隐私神经网络：基于同态加密的神经网络

验收方式：现场验收学生设计实现的系统，并给出现场评定。评定级别分优秀、良好、一般、合格、不合格；按照要求，撰写并按时提交书面实验报告（电子版）。最后根据具体情况按照满分 20 分折算。此外，学生须提交实验报告，通过此环节训练其实验总结与分析等能力。

六、考核与成绩评定

课程考核以考核学生对课程目标达成为主要目的，检查学生对教学内容的掌握程度为重要内容。课程成绩包括平时成绩和考试成绩两部分。

考核方式及成绩评定分布：写明该门课程考核环节及各环节的成绩占比，各考核环节、考核内容对毕业要求拆分指标点的支撑情况。

平时成绩 20%（作业等 10%，其它 10%），考察成绩 60%。

平时成绩中的其它 10%主要反应学生的课堂表现、平时的信息接收、自我约束。成绩评定的主要依据包括：课程的出勤率、课堂的基本表现（如课堂测验、课堂互动等；作业等的 10%主要是课堂作业和课外作业，主要考察学生对已学知识掌握的程度以及自主学习的能力。

实验成绩 20%主要是培养学生在深度神经网络环境的配置、设计与实现中的交流能力（口头和书面表达）、协作能力、组织能力。

考察成绩 60%为对学生学习情况的全面检验。强调考核学生对基本概念、基本方法、基本理论等方面掌握的程度，及学生运用所学理论知识解决复杂问题的能力。

表 4 考核环节及质量标准

考核方式	比例（%）	主要考核内容
作业	10	相关作业的完成质量，对应课程目标 1、课程目标 2 达成度的考核。
随堂练习	10	课堂练习参与度及其完成质量，对应课程目标 1、课程目标 2 达成度的评价提供支持。
实验	20	实验系统的设计实现情况。对应课程目标 3 达成度，以及学生动手能力的考查。
期末考察	60	对规定考试内容掌握的情况，对应课程目标 1、课程目标 2、课程目标 3、课程目标 4 达成度的评价提供支持。

七、考核环节及质量标准

本课程各考核环节及质量标准，详见表 5。

表 5 考核环节及质量标准

	评 分 标 准				
	A	**B**	**C**	**D**	**E**
	90～100	**80～89**	**70～79**	**60～69**	**< 60**
作业	高质量完成平时作业，格式规范内容充实严谨。	较好的完成平时作业，格式基本规范。	能够的完成平时作业，格式基本规范。	能够的完成平时作业，格式稍有不规范。	不满足D要求
随堂练习	能够完整准确地介绍一种基于同态神经网络或者其他神经网络安全相关地问题，并且说明方案的合理性。	能够完整地介绍一种基于同态神经网络或者其他神经网络安全相关地问题，能够说明方案的合理性。	能够完整地介绍一种方案，但是与安全问题的相关性不高，不能够说明方案的合理性。	不能够完整准确地介绍一种方案，并且这种方案与安全问题的相关性不高。不能够说明方案的合理性。	不满足D要求
实验	全勤，完成三次高质量实验内容	全勤，完成三次实验内容	全勤，有一次实验没有完成，并且剩余实验完成质量一般。	全勤，有两次及以上实验没有完成。	不满足D要求
期末考察	很好的掌握教学神经网络中的数据安全和隐私的基本概念、理论、方法，且具备很强的综合运用所学知识分析问题和解决复杂问题的能力。	掌握教学神经网络中的数据安全和隐私的基本概念、理论、方法，且具备综合运用所学知识分析问题和解决复杂问题的能力。	基本掌握教学神经网络中的数据安全和隐私的基本概念、理论、方法，具备一定的综合运用所学知识分析问题和解决复杂问题的能力。	基本理解教学神经网络中的数据安全和隐私的基本概念、理论、方法，具备一定的综合运用所学知识分析问题和解决复杂问题的能力。	不满足D要求

制定者：陈渝文

批准者：张建标

2020 年 7 月

“可信计算基础”课程教学大纲

英文名称：Introduction of trusted computing

课程编号：0004863

课程性质：专业选修课

学分：2.0　　学时：32

适用对象：信息安全专业本科生

先修课程：密码学 I、计算机组成原理、操作系统原理及安全

使用教材及参考书：

[1] 胡俊，沈昌祥，公备，《可信计算 3.0 工程初步（第二版）》，人民邮电出版社，2018

[2] 邹德清，羌卫中，金海 《可信计算技术原理与应用》，科学出版社，2011

[3] 冯登国 徐震 张立武《可信计算平台：设计与应用》，清华大学出版社，2006

[4] 沈昌祥 《信息安全导论》 电子工业出版社，2009 年

[5] 刘克龙 冯登国 石文昌《安全操作系统原理与技术》，科学出版社，2004

[6] Trusted Computing Group, TCG Software Stack(TSS) Specification Version 1.2 2006.1 http://www.trustedcomputinggroup.org

一、课程简介

在云计算、物联网、大数据等现代信息系统环境下，网络安全机制自身的安全性受到了严峻挑战，必须从体系化层面来提出解决方案。可信计算就是为安全体系提供支撑的重要技术。可信计算研究系统中可信计算环境的构建以及通过可信计算支撑系统安全问题，其内容涉及信息系统和信息安全的多个层面，是一个安全理论、密码学技术和工程实现高度结合的学科。

二、课程地位和教学目的

（一）课程地位：本课程是信息安全专业的限选课，是信息安全的重要专业课程，是北京工业大学计算机学院的特色课程。课程除教授可信计算的基础知识和技能外，还引导学生从整体上了解信息系统和信息安全的关系，了解安全的可信属性，重新梳理各种安全机制在系统中的作用，了解通过可信计算保障安全机制的体系化集成的方法。强化学生体系化、综合解决安全问题的思维方式以及相互配合、协作开发的意识。

本课程支撑的毕业要求拆分指标点的具体描述：

4.1： 培养学生根据安全需求，选择合适的可信计算 3.0 技术设计解决方案的能力，包括可信密码机制的选择以及对安全策略的可信支撑。

4.2：要求学生根据安全功能需求，开发具有通用性的可信计算模块，实现这些模块，并对模块进行功能测试，对功能达不到要求的模块则应根据测试情况寻找功能瓶颈并给与优化。

4.5：要求学生分析给出的示范安全应用，通过可信计算技术对安全应用进行改进，以增强其中安全机制的保障能力，应对潜在的安全威胁。

6.2：要求学生使用可信计算软件框架和可信根模拟器，模拟问题的实际环境，并验证

学生提出的解决方案的可行性。

（二）课程目标：

1 教学目标：总的教学目标是：使学生掌握可信计算的基本概念，在系统级上认识安全机制，了解安全机制的可信保障需求，学习可信计算基本功能的原理和使用方法，以及利用可信计算功能支撑安全机制的设计和开发方法，了解可信计算对系统安全的支撑作用，体验通过可信计算加固系统，改进系统安全方案的过程，增强开发过程中分析问题和持续改进的意识。该目标分解为以下子目标。

课程目标 1：了解可信计算的需求，理解可信根和可信链的基本概念，理解主动可信架构和被动可信架构的区别，可提出基于主动可信控制的安全解决方案。

课程目标 2：了解可信计算技术细节，能够开发实现可信计算具体功能的模块，并能将模块用于可信计算工程项目。

课程目标 3：增强从体系化角度寻找系统设计上的安全漏洞的能力，并训练学生通过改进安全功能模块，通过可信计算技术防范安全漏洞。支持毕业要求 3.5。

课程目标 4：要求学生们搭建可信计算模拟用例来模拟实际环境，并通过模拟用例的运行验证方案的可行性，支持毕业要求 5.2。

表 1 课程目标与毕业要求拆分指标点的对应关系

序号	课程目标	毕业要求拆分指标点			
		4.1	4.2	4.5	6.2
1	理解可信计算的基本概念	●			
2	掌握可信计算功能模块开发方法		◎		
3	了解通过可信计算技术防范安全漏洞能力			●	
4	通过可信计算模拟用例模拟实际环境，验证可信计算方案可行性				●

注：●：表示有强相关关系，◎：表示有一般相关关系，⊙：表示有弱相关关系

2 育人目标：本课程通过国内可信计算发展史以及国内外可信计算技术对比的讲解，来让学生了解自主发展的重要性，增强对国内信息安全技术发展的信心，加强学生对国内信息安全面临问题的关注和参与国内网络空间安全建设的意愿，并培养学生们参与网络空间安全工作，解决网络空间安全问题时从实际出发、严谨负责的态度。

三、课程教学内容

分章节列出课程教学内容及对课程目标的支撑，详见表 2。

表 2 教学内容与课程目标的对应关系

章节名称	教学内容及重点（▲）、难点（★）	课程目标（√）				
		1	2	3	4	5
第一章 安全可信网络安全观	网络空间安全面临的挑战[1]，网络安全脆弱性的根源[2] （▲），传统安全防护方法的局限性[2]，主动免疫机制的原理[3] （▲★），国内法规标准对安全可信的要求[2]、国外可信计算研究发展[1]。	√				
第二章	可信计算的历史发展 [2]，密码学对可信计算的支撑作	√		√		

可信计算理论基础	用 [2] （▲★） ,我国创新的主动可信架构 [2]（▲★），可信扩展的过程 [2],静态可信机制[2],动态可信机制[2] （★）。					
第三章 可信密码机制	可信密码模块概念(TPM,TCM 与 TPM2.0) [2] （▲），可信软件栈（TSS 与 TSM）[2], 可信软件基中的可信支撑机制[2],可信密码功能（可信认证、可信存储与可信报告） [3] （▲★），基于可信密码模块的可信密码管理 [3] （★）。		√			
第四章 可信对系统安全的支撑	系统主动监控机制的原理 [2]，Linux 环境执行程序可信验证 [3]，平台可信策略部署 [2]，平台可信度量机制 [2] （▲），平台可信报告机制 [3] （▲★），可信软件基在系统安全中的作用[2] （★）		√	√		
第五章 可信计算的应用	可信计算对等级保护系统的支持[2] （▲），可信网络连接 [2] （▲★），云计算环境的可信 [2] （★），新型信息系统中的可信计算应用 [1]。				√	

四、教授方法与学习方法指导

教授方法：通过启发式教学，揭示知识发生过程；通过讨论课和习题课，进一步掌握和巩固重点；多媒体和传统手段相结合，多使用教学模型；重要概念术语给出英文表达。课堂上以讲授为主（24 学时），习题讲解为辅(6 学时)，通过开放教学平台为学生们提供 24 小时开发的环境。课外习题 10 题，主要是名词解释、技术问答以及问卷调查题，用来补充可信计算相关的背景知识。

课堂讲授将以可信计算开发环境作为背景来讲解，注重课程内容的可体验性。第一章让学生从宏观上了解可信计算的意义，第二章让学生了解可信计算的基本概念与原理，第三章介绍可信密码机制的详细内容，第四章在第三章基础上进一步探讨可信计算对系统安全的支撑作用，第五章则是结合实际，对前面学习内容进行综合应用，从第三章到第五章在可信开发环境有相互衔接的练习内容，让学生们可以迅速把学到的东西付诸实践，以增强学生们的实践能力。

学习方法：课程要求学生结合线上资源自行进行实验，线上资源通过网络上的开放教学平台提供，学生在课下通过网络环境完成习题练习，并在开放教学平台上直接提交作业。

学生学习时需要养成动手验证的习惯，特别是重视在框架环境下定制和集成模块的能力，在理论指导下进行实践；注意从实际场景出发，分析安全过程，归纳可信需求，并灵活应用可信技术解决实际问题。

五、教学环节及学时分配

表 3 教学环节及各章节学时分配表

章节	主要内容	学时分配					合计
		讲课	习题	实验	讨论	其他	
1	安全可信网络安全观	4					4
2	可信计算理论基础	5					5
3	可信密码机制	5	2				7
4	可信计算对安全的支撑	4	2				6
5	可信计算应用	4	4				8
合计		24	8				32

注：本课程不设实验课，学生们需要使用课外时间在开放可信平台上完成实践过程。习题课实际上是讲解学生们课外时间在开放可信平台上的开发中遇到的问题。

六、考试与成绩评定

平时成绩 30%（学生出勤 10%，平时作业 20 %），期中成绩 30%，期末成绩 40%。

平时成绩包括学生出勤（10%）和平时作业（20%），平时作业主要考察学生们对可信计算相关概念的了解和体会程度

期中成绩需要学生们在网络上完成可信密码实训和可信系统安全实训两个实训任务，并提交实训报告，以考察学生对可信计算基础知识和工程开发能力的掌握。

期末成绩需要学生们选择应用背景并进行研讨，在网络上完成应用安全方案的可信加固，包括安全问题分析、安全改进措施设计以及改进措施的实现，并提交报告，以考察学生对可信计算作用的理解及对技术的灵活运用能力。

表 4 考核方式及成绩评定分布表

考核方式	占比（%）	主要考核内容
学生出勤	10	学生按时上课，认真听讲，为课程目标 1，课程目标 2，课程目标 3，课程目标 4 的达成度提供支持。
平时习题	20	学生们对可信计算相关的知识的了解情况和自学情况，为课程目标 1、课程目标 3 的达成度提供支持
期中实训	30	可信密码技术和可信系统安全技术的掌握，可信计算模块开发能力，为课程目标 1，课程目标 2 的达成度提供支持。
期末课设	40	应用可信计算技术改进信息系统安全解决方案的能力。为课程目标 1，课程目标 2，课程目标 3，课程目标 4 的达成度提供支持。

七、考核环节及质量标准

本课程各考核环节及质量标准，详见表 5。

表 5 考核环节及质量标准

考核方式	评　分　标　准				
	A	**B**	**C**	**D**	**E**
	90～100	**80～89**	**70～79**	**60～69**	**< 60**
平时习题	概念理论掌握全面，问题回答正确，有自己的思考	概念理论掌握全面，问题回答正确	核心概念理论基本掌握，问题回答基本正确	核心概念理论基本掌握，问题回答方向正确	不满足 D 要求
期中实训	解题思路正确，模块说明文档完整准确，运行正确，测试用例完整，测试结果正确	解题思路正确，模块说明文档准确，模块运行基本正确，测试用例比较完整，测试结果正确	解题思路基本正确，模块说明文档基本准确，模块主要功能运行正确，模块核心功能具备测试用例，测试结果正确，	解题思路大致正确，模块说明文档可用，模块主要功能具备，核心功能具备测试用例，用例测试结果正确。	不满足 D 要求
期末课设	应用背景安全分析准确，可信支撑方案合理有效，可信模块开发、测试、文档说明完整正确，课设内容有创新之处	应用背景安全分析准确，可信支撑方案合理有效，可信模块开发、测试、文档说明完整正确。	应用背景安全分析基本正确，可信支撑方案合理有效，可信模块测试通过，文档说明基本正确。	应用背景安全分析找到了问题，可信支撑方案有一定作用，可信模块测试基本通过，文档说明基本内容具备。	不满足 D 要求
评分标准（A～E）：主要填写对教学内容中的基本概念、理论、方法等方面的掌握，及综合运用理论知识解决复杂问题能力的要求。					

制定者：胡俊

批准者：张建标

2020 年 7 月

“边缘计算安全”课程教学大纲

英文名称：Edge Computing Security

课程编码：0010062

课程性质：专业选修课

学分： 2.0 学时：32

面向对象：信息安全（实验班）专业本科生

先修课程：计算机网络（双语）、安全协议

教材及参考书：

[1] Chris Hurley 等著，杨青译. 无线网络安全. 科学出版社，2009

[2] 施巍松, 刘芳, 孙辉, 裴庆祺. 边缘计算. 科学出版社，2018

[3] 苗刚中, 罗永龙, 陶陶, 陈付龙. 网络安全攻防技术--移动安全篇. 科学出版社，2018

[4] 张骏. 边缘计算方法与工程实践. 电子工业出版社，2019

一、课程简介

随着万物互联时代的到来，网络边缘设备产生的数据量飞速增长，由此产生了一系列新的应用场景，而边缘计算成为这些新兴万物互联应用的重要支撑，同时，边缘计算也将面临更多、更大的安全威胁，因此亟需引入大量相关安全人才。“边缘计算安全”课程涉及较为复杂的系统安全抽象概念和实际信息安全工程能力，是理论与应用结合比较紧密的信息安全专业课程。该课程对边缘计算的安全架构、安全概念、关键安全技术进行了系统的介绍和分析。

二、课程地位与目标

（一）课程地位：本课程是信息安全专业的专业限选课。旨在继计算机网络、安全协议等课程后，引导学生认识信息安全理论与技术如何落实到边缘计算中，从边缘计算网络、边缘计算终端、边缘计算应用三个层面进一步认识信息系统的安全性，培养学生系统安全、网络安全两大专业基本能力。帮助学生深入理解边缘计算安全的基本概念与原理，增强其对边缘计算安全机制的理解和应用能力，培养理论联系实际、知识转移层面的创新能力；帮助学生掌握边缘计算基础知识和安全技术，增强其对边缘计算安全状态的分析和设计能力，培养其工程意识和能力。

本课程支撑的毕业要求拆分指标点具体描述如下。

对于毕业要求 3.3，边缘计算安全属于一门比较综合的课程，因此其中许多问题的相关知识需要学生自己补充，培养学生有针对性地进行文件检索、资料查询及运用现代信息技术获取相关信息的基本能力。

对于毕业要求 4.1，边缘计算安全所要解决的问题都属于工程方面的问题，且紧跟技术发展潮流，紧密结合实际，培养学生运用所学理论和技术，结合实际问题，综合设计开发，解决工程实际问题的基本能力。

对于毕业要求 5.1，培养学生能够运用已学原理及协议，对边缘计算应用中出现的安全问题进行分析，能够基于已学的实验方法和工具设计出正确的方案，找出并理解问题本质

的能力。

对于毕业要求 9.2，通过课程中讲授和讨论真实的信息安全案例，让学生了解信息安全相关法律、法规及方针与政策，在实践中自觉遵守，并在实践中遵守信息安全专业职业道德和规范，履行责任，避免侵犯他人的信息资产。

（二）课程目标

1 教学目标：使学生掌握“边缘计算安全”中的基本概念、基本理论、基本方法，从边缘计算网络、边缘计算终端、边缘计算应用三个层面认识边缘计算的安全性，增强工程能力。该目标分解为以下子目标：

- 课程目标 1：掌握边缘计算相关的概念及安全方法，培养学生在边缘计算中应用信息安全基本方法，识别、判断复杂工程问题的能力，支撑指标点 3.3。
- 课程目标 2：掌握边缘计算安全框架和实际的应用场景、关键技术，培养学生应用专业知识进行系统设计实现和安全验证的能力，支撑指标点 4.1。
- 课程目标 3：掌握保障边缘计算安全所需的系统、网络安全分析方法，培养学生选择实验方案，以及进行实验数据分析的能力，支撑指标点 5.1。
- 课程目标 4：了解边缘计算安全相关的职业道德要求，培养学生遵守信息安全行业职业道德规范的责任意识，支撑指标点 9.2。

表 1 课程目标与毕业要求拆分指标点的对应关系

序号	课程目标	毕业要求拆分指标点			
		3.3	4.1	5.1	9.2
1	掌握边缘计算相关的概念及安全方法，培养学生在边缘计算中应用信息安全基本方法，识别、判断复杂工程问题的能力	●			
2	掌握边缘计算安全框架和实际的应用场景、关键技术，培养学生应用专业知识进行系统设计实现和安全验证的能力		●		
3	掌握保障边缘计算安全所需的系统、网络安全分析方法，培养学生选择实验方案，以及进行实验数据分析的能力			●	
4	了解边缘计算安全相关的职业道德要求，培养学生遵守信息安全行业职业道德规范的责任意识				◎

注：●：表示有强相关关系，◎：表示有一般相关关系，⊙：表示有弱相关关系

2 育人目标：随着万物互联时代的到来，网络边缘设备产生的数据量飞速增长，由此产生了一系列新的应用场景，而边缘计算成为这些新兴万物互联应用的重要支撑，同时，边缘计算也将面临更多、更大的安全挑战，因此亟需引入大量相关安全人才。

本课程能够引导学生关注我国前沿科技的发展，对我国目前取得的相关科技成果产生认同感、自豪感和使命感，同时，掌握边缘计算安全相关的职业道德要求和责任意识，为今后的发展打下坚实基础。

三、课程教学内容

分章节列出课程教学内容及对课程目标的支撑，详见表 2。

表 2 教学内容与课程目标的对应关系

章节名称	教学内容及重点（▲）、难点（★）	课程目标（√）			
		1	2	3	4
第一章 边缘计算 基础	教学目标，课程基本内容； 边缘计算的概念▲ 边缘计算的发展历程 边缘计算的优势与挑战 边缘计算的基本架构▲ 边缘计算系统实例▲ 边缘计算的关键技术▲ 边缘计算的典型应用▲ 边缘计算的通信基础▲	√			
第二章 边缘计算 安全概述	边缘计算相关的安全事件； 边缘计算面临的安全威胁； 边缘计算安全技术概述； 边缘计算安全防护体系▲	√			√
第三章 边缘计算 节点安全	边缘计算节点概述； 边缘计算节点安全▲； 移动终端安全技术▲★	√	√	√	
第四章 边缘计算 网络安全	边缘计算网络概述； 边缘计算网络安全▲； 无线网络安全技术▲★	√	√	√	
第五章 边缘计算 安全技术	边缘计算身份认证技术▲★； 边缘计算访问控制方法和模型▲★； 边缘计算隐私保护技术▲★；	√	√	√	
第六章 边缘计算 应用安全	边缘计算新生应用案例分析★； 边缘计算安全技术案例分析★	√	√	√	√

四、教授方法与学习方法指导

教授方法： 采用以课堂讲授为主，实验教学和讨论教学为辅的教授方法。课堂讲授推崇研究型教学，以知识为载体，传授相关的思想和方法，引导学生踏着大师们的步伐前进。实验教学则提出基本要求，引导学生独立（按组）完成。同时，结合课程内容的教学要求以及学生认知活动的特点，采取包括讲授、研讨、小组合作、探究教学、项目驱动、案例教学、线上、线上线下混合等多种教学模式与方法。

1、课堂讲授

课堂教学首先要使学生掌握课程教学内容中规定的一些基本概念、基本理论和基本方法。特别是通过讲授，使学生能够对这些基本概念和理论有更深入的理解，使之有能力将它们应用到一些问题的求解中。本课程为理论结合实践课程。通过教师引导，帮助学生深入理解边缘计算安全基本概念与原理，掌握总体安全方案的设计、关键安全技术的选择、以及系统安全性分析的能力，达到理论联系实际、知识转移层面的创新能力的培养。

积极探索和实践研究型教学。探索如何实现教师在对问题的求解中教，学生怎么在对

未知的探索中学。在提出、分析和解决问题的过程中，进一步培养学生实践工程能力；从边缘计算网络安全和边缘计算节点安全两个层面向学生展示安全技术在边缘计算中的应用，通过不同级别对象和问题的分析，培养学生的整体安全意识和能力。

教学过程中，采用多媒体教学手段，结合传统板书、范例演示等讲解手段，针对重点难点进行精讲详讲，以点带面，帮助学生深入掌握边缘计算安全相关的关键技术。在授课过程中，可由边缘计算的最新趋势以及安全的最新技术开始，增加学生的感性认识，自然地进入到相关内容的讲授，从而培养学生的学习兴趣。适当引导学生阅读外文书籍和资料，培养学生的自学能力。通过启发式教学，加强师生交互，启发学生面对真实环境与具体需求时分析问题、解决问题的能力，提高教学效果。

2、实验教学

实验需要在掌握信息安全关键技术原理及方法的基础上，通过移动终端系统漏洞利用分析、移动终端应用分析与防护、基于权限的 Web 攻击与防护、边缘计算环境下的隐私泄露实验，进一步理解边缘计算安全的原理、方法、特点，掌握具体安全技术和工具。另外，学生若有自己的想法，在现有开发平台基础上可以进行自己想法的验证。要求学生完成相关安全方法的设计，每组最后提交规范的实验报告。

通过实验系统的设计与实现，引导学生理解边缘计算安全防护体系，体验如何将基本的原理用于实践，加深对理论概念的理解；通过分组，培养学生的团队合作精神与能力；培养学生查阅资料，选择和使用合适的工具的能力；培养学生表达（书面、口头）能力。

实验分组进行，2 人一组，协同完成实验。

（1）移动终端系统漏洞利用分析：基于移动终端系统的基本安全架构，掌握系统漏洞利用的实现方法，分析系统的漏洞，设计并实现终端系统的漏洞利用。

（2）移动终端应用分析与防护：基于终端应用的属性，对终端应用进行分析检测，设计并实现基于代码分析的移动终端应用的防护系统。

（3）移动终端 Web 攻击与防护：基于 Web 漏洞，设计基于权限的 Web 攻击防护方案。

（4）隐私泄露：针对边缘计算环境下的隐私泄露问题，设计相应的隐私防护方案。

验收与评价：

验收方式 1：现场验收。现场验收学生设计实现的方法和系统，并给出现场评定。评定级别分优秀、良好、合格、不合格，最后根据具体情况按照满分 30 分折算。此外，学生必须提交实验报告，通过此环节训练其实验总结与分析等能力。

验收方式 2：综合验收。采取集体报告（制作报告、准备演示内容，每组报告 10-15 分钟）、按组、按要求评价其他各组的实验成果；按照要求，撰写并按时提交书面实验报告（电子版）。

评分建议：总分为 30 分；现场按照完备性、组织、创意、表达与展示进行分组评价，记录完成的质量（A-好、B-中、C-差、D-无），过后各组内商议给出个人综合评分。本组组长不给自己评分。教师根据各组的评分和表现给出每个学生的得分。

3、边缘计算安全讨论

讨论紧随最新边缘计算安全理论与技术进展，对课堂已讲述内容的深度和广度进行扩

展。要求学生提前根据教师提供的资料分组进行报告制作、准备演示内容，在课上进行边缘计算安全防护方案演示。

通过对边缘计算安全领域进展的学习，引导学生体验本领域的最新发展趋势，加深对理论概念的理解；通过分小组，培养学生的团队合作精神与能力；培养学生查阅资料，获取适当工具、使用适当工具的能力；培养学生表达（书面语口头）能力。

实验分组进行，2-4 人一组，协同完成。

验收与评价：综合验收。采取集体报告（制作报告、准备演示内容，每组报告 10-15 分钟）、按组、按要求评价其他各组的实验成果。

评分建议：总分为 20 分；现场按照完备性、组织、创意、表达与展示进行分组评价，记录完成的质量（A-好、B-中、C-差、D-无）。教师根据各组的评分和表现给出每个学生的得分。

学习方法：根据课程及学生学习特点，给出学习该门课程的指导和建议。可以包括体现本门课程特点的学习策略、学习技巧、自主学习指导、课程延伸学习资料获取途径及信息检索方法、教学网站及学习注意事项、学习效果自我检查方法指导等内容。

养成积极探索的习惯，特别是重视对基本理论的钻研，在理论指导下进行实践；注意从实际问题入手，验证设计实现测试系统。明确学习各阶段的重点任务，做到课前预习，课中认真听课，积极思考，课后认真复习，不放过疑点，充分利用好教师资源和同学资源。积极参加实验和讨论，加深对原理的理解。

五、教学环节及学时分配

教学环节及各章节学时分配，详见表 3。

表 3 教学环节及各章节学时分配表

章节名称	教学内容	学 时 分 配					合计
		讲授	习题	实验	讨论	其它	
1	边缘计算基础	4					4
2	边缘计算安全概述	2			2		4
3	边缘计算节点安全	4		4			8
4	边缘计算网络安全	4		2			6
5	边缘计算安全技术	4		2	2		8
6	边缘计算应用安全	2					2
合计		20		8	4		32

六、考核与成绩评定

课程考核以考核学生对课程目标达成为主要目的，检查学生对教学内容的掌握程度为重要内容。课程成绩包括平时成绩和考试成绩两部分。

考核方式及成绩评定分布：本课程期末成绩由平时成绩 50%（讨论演示成绩 20%，实验 30%），考试成绩 50%两部分组成。

平时成绩中的讨论演示成绩 20%主要反应学生的查阅文献、扩展思维、信息接受、协作交流能力。通过分组讨论演示边缘计算安全防护方案的方式考察学生的工程能力和专业

意识；实验成绩 30%主要反映学生在所学理论方法指导下如何基于具体安全技术实现边缘计算安全防护的工程能力。引导学生发挥潜力，尽量强化对工业互联网安全性的理解。培养学生在设计与实现中的交流能力（口头和书面表达）、协作能力、组织能力。

考试成绩 50%是对学生学习情况的全面检验，要起到督促学生系统掌握包括基本思想方法在内的主要内容的目的。强调考核学生对边缘计算安全基本概念、基本方法、基本技术的掌握程度，考核学生运用所学方法设计安全方案、运用所学理论知识解决复杂问题的能力，淡化考查一般知识、结论记忆，采用开卷考试形式，包含选择、填空、简答题、设计和论述题。

毕业要求拆分点的支撑情况详见表 4。

表 4 考核方式及成绩评定分布表

考核方式	占比（%）	主要考核内容及对毕业要求拆分指标点的支撑情况
考试成绩	50	对规定考试内容掌握的情况，对课程目标 1、课程目标 2 达成度的评价提供支持。
讨论演示成绩	20	课堂讨论参与度及演示完成质量，对课程目标 1、课程目标 4 达成度的评价提供支持；
实验成绩	30	实验设计实现情况，对课程目标 2、课程目标 3 达成度的评价提供支持。

七、考核环节及质量标准

本课程各考核环节及质量标准，详见表 5。

表 5 考核环节及质量标准

考核方式	评分标准				
	A	B	C	D	E
	90～100	80～89	70～79	60～69	< 60
研讨	完全掌握教学内容中的基本方法，能够清楚识别、判断复杂工程问题，并给出完备解决方案，具备遵守信息安全行业职业道德规范的责任意识	掌握教学内容中的基本方法，能够较清楚地识别、判断复杂工程问题，并给出较完备的解决方案，具备遵守信息安全行业职业道德规范的责任意识	基本掌握教学内容中的基本方法，能够识别、判断复杂工程问题，并给出解决方案，具备遵守信息安全行业职业道德规范的责任意识	部分掌握教学内容中的基本方法，能够识别、判断复杂工程问题，并给出基本解决方案，具备遵守信息安全行业职业道德规范的责任意识	不满足 D 要求
实验	能够综合运用理论知识，解决并优化复杂问题，能应用专业知识进行	能够运用理论知识解决复杂问题，能应用专业知识进行系统设计实现	经过少量提示，能够运用理论知识解决复杂问题，能应用专业知识	经过较多提示，基本能够运用理论知识解决复杂问题，能应用专	不满足 D 要求

	完善的系统设计实现和安全验证，进行全面分析	和安全验证，进行分析	进行系统设计实现和安全验证，进行分析	业知识进行系统设计实现和安全验证，进行分析	
考试	完全掌握教学内容中的基本概念、理论、方法，能够综合运用理论知识解决复杂问题	掌握教学内容中的本概念、理论、方法，能够综合运用理论知识解决复杂问题	基本掌握教学内容中的大部分基本概念、理论、方法，能够运用理论知识基本解决复杂问题	部分掌握教学内容中有限的基本概念、理论、方法，能够运用理论知识部分解决复杂问题能力	不满足 D 要求
评分标准（A～E）：主要填写对教学内容中的基本概念、理论、方法等方面的掌握，及综合运用理论知识解决复杂问题能力的要求。					

制定者：庄俊玺

批准者：张建标

2020 年 7 月

“工业互联网安全”课程教学大纲

英文名称：Industrial Internet Security

课程编码：0010093

课程性质：专业选修课

学分： 2.0　　学时：32

面向对象：信息安全专业本科生

先修课程：计算机网络（双语）

教材及参考书：

[1] 赖英旭, 杨震, 范科峰, 刘贤刚, 刘静, 杨胜志. 工业控制系统信息安全. 西安电子科技大学出版社，2019

[2] 闫怀志. 工业互联网安全体系理论与方法. 科学出版社. 2019

[3] 姚羽, 祝烈煌, 武传坤. 工业控制网络安全技术与实践. 机械工业出版社. 2017

一、课程简介

随着新一代信息技术与制造业深度融合，“中国制造 2025”的推进，工业互联网成为推动制造业转型升级的新型网络基础设施，面临严峻安全挑战，亟需引入大量安全人才。“工业互联网安全”课程对工业互联网面临的安全威胁，相关安全概念，关键安全技术和案例进行了系统介绍和分析，是理论与应用结合较为紧密的信息安全专业课程。本课程以安全为主线，理论与实践结合，从工业控制系统、工业互联网平台二个层次分别讨论相关安全理论和方法。

二、课程地位与目标

（一）课程地位：本课程是信息安全专业的专业限选课。旨在继计算机网络基础、安全协议等课程后，引导学生认识信息安全理论与技术如何落实到具体的工业控制应用中，从工业控制系统和互联网平台两个角度再认识信息系统安全性，培养系统安全、网络安全两大专业基本能力。帮助学生深入理解工业互联网安全基本概念与原理，增强对工业互联网安全机制的理解和应用能力，培养理论联系实际、知识转移层面的创新能力，帮助学生掌握工业互联网基础知识和安全技术的应用、工具的使用和对工业互联网安全状态的分析评估能力，培养其工程意识和能力。

本课程支撑的毕业要求拆分指标点具体描述如下。

对于毕业要求 3.1，培养选择适当的安全方法及参数，分析判断工业互联网复杂系统的安全性，应对信息安全攻防复杂形势的能力。

对于毕业要求 4.2，培养根据工业互联网用户的特定需求，应用适当的安全模型和方法进行安全系统设计与实现，能测试其正确性和一定的优化能力。

对毕业要求 5.4，培养基于所学理论和技术知识，通过对现有工业互联网信息系统安全方案进行模拟和实验数据分析，规范表述结论的能力。

对毕业要求 9.2，通过课程中讲授和讨论真实的信息安全案例，让学生了解信息安全相关法律、法规及方针与政策，在实践中自觉遵守，并在实践中遵守信息安全专业职业道德

和规范，履行责任，避免侵犯他人的信息资产。

（二）课程目标

1 教学目标：写明课程拟达到的课程目标，指明学生需要掌握的知识、素质与能力及应达到的水平，本课程对毕业要求拆分指标点达成的支撑情况，详见表 1。

使学生掌握“工业互联网安全”中的基本概念、基本理论、基本方法，在工业控制系统和互联网平台角度上认识工业互联网信息系统安全性，增强工程能力。该目标分解为以下子目标：

- 课程目标 1：掌握工业互联网相关的安全方法、关键参数，培养学生在工业互联网中应用信息安全基本方法，识别、判断复杂工程问题的能力，支撑指标点 3.1。
- 课程目标 2：掌握工业互联网安全相关标准和实践的应用场景、核心技术，培养学生应用专业知识进行系统设计实现和安全验证的能力；支撑指标点 4.2。
- 课程目标 3：掌握保障工业互联网安全所需的系统、网络安全分析方法，培养学生选择实验方案，以及进行实验数据分析的能力；支撑指标点 5.4。
- 课程目标 4：掌握工业互联网安全相关的职业道德要求，培养学生遵守信息安全行业职业道德规范的责任意识；支撑指标点 9.2。

表 1 课程目标与毕业要求拆分指标点的对应关系

序号	课程目标	毕业要求拆分指标点			
		3.1	4.2	5.4	9.2
1	掌握工业互联网相关的安全方法、关键参数，培养学生在工业互联网中应用信息安全基本方法，识别、判断复杂工程问题的能力	●			
2	掌握工业互联网安全相关技术的应用场景、核心技术，培养学生应用专业知识进行系统设计实现和安全验证的能力		●		
3	掌握保障工业互联网安全所需的系统、网络安全分析方法，培养学生选择实验方案，以及进行实验数据分析的能力			●	
4	掌握工业互联网安全相关的职业道德要求，培养学生遵守信息安全行业职业道德规范的责任意识				●

注：●：表示有强相关关系，◎：表示有一般相关关系，⊙：表示有弱相关关系

2 育人目标：写明课程对培养学生的理想信念、家国情怀、民族自信、责任担当、职业素养、行为规范等育人元素，寓价值观引导于知识传授之中。

随着新一代信息技术与制造业深度融合，“中国制造 2025”的推进，工业互联网成为推动我国制造业转型升级的新型网络基础设施，面临严峻安全挑战，亟需引入大量安全人才。

本课程能够引导学生关注影响我国将来高速发展的重大机遇和挑战，对我国目前取得的工业和安全产业成就产生认同感、自豪感和使命感，掌握工业互联网安全相关的职业道德要求和责任意识，为今后的发展打下坚实基础。

三、课程教学内容

分章节列出课程教学内容及对课程目标的支撑，详见表 2。

表 2 教学内容与课程目标的对应关系

章节名称	教学内容及重点（▲）、难点（★）	课程目标（√）		
		1	2	3
第一章 工业互联网基础	教学目标，课程基本内容；工业互联网的概念▲；工业互联网的发展历程；工业互联网的主流平台；工业互联网的基本架构▲；工业控制系统的概念▲；工业控制系统的种类▲；工业控制网络的概念▲；工业控制网络协议▲	√		
第二章 工业互联网信息安全概述	工业互联网常见攻击及安全事件；工业互联网面临的安全风险；；工业互联网安全防护体系▲	√		
第三章 工业互联网入侵检测	传统网络入侵检测系统；入侵检测技术概述；工业互联网入侵检测技术▲★	√	√	√
第四章 工业互联网漏洞扫描与挖掘	系统漏洞的概念；漏洞扫描技术概述；工业互联网相关安全漏洞▲；工业互联网相关漏洞挖掘技术▲★	√	√	√
第五章 工业互联网访问控制	网络访问控制的概念；工业互联网的网络访问控制方法和模型▲★；工业控制防火墙的选择及部署；工业控制防火墙与传统防火墙的区别与联系★	√	√	√
第六章 工业互联网安全防护案例分析	面向行业的工业控制系统案例分析★；工业互联网安全案例分析★	√	√	√

四、教授方法与学习方法指导

教授方法：结合课程内容的教学要求以及学生认知活动的特点，采取包括讲授、研讨、小组合作、探究教学、项目驱动、案例教学、线上、线上线下混合等多种教学模式与方法。

1、课堂讲授：课堂教学首先要使学生掌握课程教学内容中规定的一些基本概念、基本理论和基本方法。特别是通过讲授，使学生能够对这些基本概念和理论有更深入的理解，使之有能力将它们应用到一些问题的求解中。本课程为理论结合实践课程。通过教师引导，帮助学生深入理解工业互联网安全基本概念与原理，掌握总体安全方案的设计、关键安全技术的选择、应用和安全性分析的能力，达到理论联系实际、知识转移层面的创新能力的培养。

积极探索和实践研究型教学。探索如何实现教师在对问题的求解中教，学生怎么在对未知的探索中学。在提出、分析和解决问题的过程中，进一步培养学生实践工程能力；从工业互联网本地工业控制系统和互联网平台两个重要层次向学生展示安全技术在工业互联网环境中的应用，通过不同级别对象和问题的分析，培养学生的整体安全意识和能力。

本课程采用多媒体教学手段，结合传统板书、讲解手段，通过启发式教学，揭示知识发生过程。通过实验课，进一步掌握和巩固重点。在授课过程中，可由常用的程序设计语言问题引出概念，自然进入相关内容的讲授。适当引导学生阅读外文书籍和资料，培养自学能力。

2、实验教学：实验需要在掌握信息安全关键技术原理及方法的基础上，通过工业控制网络及协议安全实验、工业控制应用与服务安全实验，进一步理解工业互联网安全的原理、方法、特点，掌握具体安全技术和工具，要求学生完成相关安全方法的验证或设计，每组最后提交规范的实验报告。

通过实验系统的验证、设计与实现，引导学生理解工业互联网安全防护体系，具体体验如何将基本的原理用于实践，加深对理论概念的理解；通过分小组，培养学生的团队合

作精神与能力；培养学生查阅资料，获取适当工具、使用适当工具的能力；培养学生表达（书面语口头）能力。

实验分组进行，2-4 人一组，协同完成实验。

（1）工业控制网络及协议安全实验：基于通用的网络扫描与欺骗技术，分析网络安全漏洞，设计和验证工业控制网络扫描与欺骗攻击检测方案；在此基础上，基于一种工业控制网络通用或专有协议，分析工控相关的安全问题，设计和验证工控控制防火墙安全防护规则。

（2）工业控制应用与服务安全实验：基于逆向工程和调试技术，分析应用软件面临的安全漏洞，设计和验证工业控制应用漏洞利用方案；基于操作系统、Web 系统渗透方法，设计和实现工业互联网数据库及 Web 服务安全检测方法。

验收与评价：

验收方式 1：现场验收。现场验收学生设计实现的方法和系统，并给出现场评定。评定级别分优秀、良好、合格、不合格，最后根据具体情况按照满分 40 分折算。此外，学生必须提交实验报告，通过此环节训练其实验总结与分析等能力。

验收方式 2：综合验收。采取集体报告（制作报告、准备演示内容，每组报告 10-15 分钟）、按组、按要求评价其他各组的实验成果；按照要求，撰写并按时提交书面实验报告（电子版）。

评分建议：总分为 40 分；现场按照完备性、组织、创意、表达与展示进行分组评价，记录完成的质量（A-好、B-中、C-差、D-无），过后各组内商议给出个人综合评分。本组组长不给自己评分。教师根据各组的评分和表现给出每个学生的得分。

3、工业互联网安全讨论：讨论紧随最新工业互联网安全理论与技术进展，对课堂已讲述内容的深度和广度进行扩展。要求学生提前根据教师提供的资料分组进行报告制作、准备演示内容，在课上进行工业互联网安全防护方案演示。

通过对工业互联网安全领域进展的学习，引导学生体验本领域的最新发展趋势，加深对理论概念的理解；通过分小组，培养学生的团队合作精神与能力；培养学生查阅资料，获取适当工具、使用适当工具的能力；培养学生表达（书面语口头）能力。

实验分组进行，2-4 人一组，协同完成。

验收与评价：综合验收。采取集体报告（制作报告、准备演示内容，每组报告 10-15 分钟）、按组、按要求评价其他各组的实验成果。

评分建议：总分为 20 分；现场按照完备性、组织、创意、表达与展示进行分组评价，记录完成的质量（A-好、B-中、C-差、D-无）。教师根据各组的评分和表现给出每个学生的得分。

学习方法：养成探索的习惯，特别是重视对基本理论的钻研，在理论指导下进行实践；注意从实际问题入手，验证设计实现测试系统。明确学习各阶段的重点任务，做到课前预习，课中认真听课，积极思考，课后认真复习，不放过疑点，充分利用好教师资源和同学资源。积极参加实验和讨论，加深对原理的理解。

五、教学环节及学时分配

教学环节及各章节学时分配，详见表 3。

表 3 教学环节及各章节学时分配表

章节名称	教学内容	学 时 分 配					合计
		讲授	习题	实验	讨论	其它	
1	工业互联网基础	4					4
2	工业互联网信息安全概述	2					2
3	工业互联网入侵检测	4					4
4	工业互联网漏洞扫描与挖掘	4					4
5	工业互联网访问控制	4					4
6	工业互联网安全防护案例分析	2					2
7	工业互联网安全实验			8			8
8	工业互联网安全讨论				4		4
合计		20		8	4		32

六、考核与成绩评定

课程考核以考核学生对课程目标达成为主要目的，检查学生对教学内容的掌握程度为重要内容。课程成绩包括平时成绩和考试成绩两部分。

考核方式及成绩评定分布：写明该门课程考核环节及各环节的成绩占比，各考核环节、考核内容对毕业要求拆分指标点的支撑情况。

平时成绩 60%（讨论演示成绩 20%，实验 40%），考试成绩 40%。

平时成绩中的讨论演示成绩 20%主要反应学生的查阅文献、扩展思维、信息接受、协作交流能力。通过分组讨论演示工业互联网安全防护方案的方式考察学生的工程能力和专业意识；实验成绩 40%主要反映学生在所学理论方法指导下如何基于具体安全技术实现工业互联网安全防护的工程能力。引导学生发挥潜力，尽量强化对工业互联网安全性的理解。培养学生在设计与实现中的交流能力（口头和书面表达）、协作能力、组织能力。

考试成绩 40%是对学生学习情况的全面检验，要起到督促学生系统掌握包括基本思想方法在内的主要内容的目的。强调考核学生对工业互联网安全基本概念、基本方法、基本技术的掌握程度，考核学生运用所学方法设计安全方案、运用所学理论知识解决复杂问题的能力，淡化考查一般知识、结论记忆，采用开卷考试形式，包含选择、填空、简答题和论述题。

毕业要求拆分点的支撑情况详见表 4。

表 4 考核方式及成绩评定分布表

考核方式	占比（%）	主要考核内容及对毕业要求拆分指标点的支撑情况
讨论演示成绩	20	课堂讨论参与度及演示完成质量，对课程目标 1、课程目标 4 达成度的评价提供支持；
实验成绩	40	实验设计实现情况，对课程目标 2、课程目标 3 达成度的评价提供支持。
考试成绩	40	对规定考试内容掌握的情况，对课程目标 1、课程目标 2 达成度的评价提供支持。

七、考核环节及质量标准

本课程各考核环节及质量标准，详见表 5。

表 5 考核环节及质量标准

考核方式	评　分　标　准				
	A	**B**	**C**	**D**	**E**
	90～100	**80～89**	**70～79**	**60～69**	**< 60**
研讨	完全掌握教学内容中的基本方法，能够清楚识别、判断复杂工程问题，并给出完备解决方案，具备遵守信息安全行业职业道德规范的责任意识	掌握教学内容中的基本方法，能够较清楚地识别、判断复杂工程问题，并给出较完备的解决方案，具备遵守信息安全行业职业道德规范的责任意识	基本掌握教学内容中的基本方法，能够识别、判断复杂工程问题，并给出解决方案，具备遵守信息安全行业职业道德规范的责任意识	部分掌握教学内容中的基本方法，能够识别、判断复杂工程问题，并给出基本解决方案，具备遵守信息安全行业职业道德规范的责任意识	不满足 D 要求
实验	能够综合运用理论知识，解决并优化复杂问题，能应用专业知识进行完善的系统设计实现和安全验证，进行全面分析	能够运用理论知识解决复杂问题，能应用专业知识进行系统设计实现和安全验证，进行分析	经过少量提示，能够运用理论知识解决复杂问题，能应用专业知识进行系统设计实现和安全验证，进行分析	经过较多提示，基本能够运用理论知识解决复杂问题，能应用专业知识进行系统设计实现和安全验证，进行分析	不满足 D 要求
考试	完全掌握教学内容中的基本概念、理论、方法，能够综合运用理论知识解决复杂问题	掌握教学内容中的本概念、理论、方法，能够综合运用理论知识解决复杂问题	基本掌握教学内容中的大部分基本概念、理论、方法，能够运用理论知识基本解决复杂问题	部分掌握教学内容中有限的基本概念、理论、方法，能够运用理论知识部分解决复杂问题能力	不满足 D 要求
评分标准（A～E）：主要填写对教学内容中的基本概念、理论、方法等方面的掌握，及综合运用理论知识解决复杂问题能力的要求。					

制定者：詹静

批准者：张建标

2020 年 7 月

“数据安全与隐私保护”课程教学大纲

英文名称：Data security and Privacy Protection

课程编码：0008213

课程性质：专业选修课

学分： 2.0 学时：32

面向对象：信息安全（实验班）专业本科生

先修课程：密码学Ⅰ、网络空间安全导论

教材及参考书：

[序号] 作者. 教材名称. 出版社，出版年月

[1]《大数据安全与隐私保护》 冯登国等 编著，清华大学出版社，2018.12

[2]《大数据安全技术与应用》张尼等著，人民邮电出版社，2014.5

[3]《大数据治理与安全：从理论到开源实践》刘驰，机械工业出版社，2017.9

[4]《网络空间安全导论》 沈昌祥 左晓栋编著，电子工业出版社，2018.4

[5]《网络隐私保护与信息安全》 康海燕著，北京邮电大学出版社，2016.1

[6]《大数据时代个人数据隐私规制》王忠著，社会科学文献出版社，2014.9

[7]《通用数据保护规范》（General Data Protection Regulation ， GDPR）欧盟，https://gdpr-info.eu/，2018.5

一、课程简介

随着云计算、大数据等信息技术的飞速发展，数据已成为网络空间中重要的战略性资源，各类数据驱动的应用在金融、交通、能源和电信等重要行业、重大基础设施中发挥着重要作用，大量数据资源的融合分析、开放共享与应用开发给用户带来前所未有的数据安全以及隐私泄露威胁。大数据时代的数据安全和隐私保护问题已成为当前国家、社会和公民共同关注的热点问题。本课程从大数据的基本概念和随之带来的新型安全挑战，大数据安全与隐私保护技术框架设计、数据安全存储、数据安全检索、数据安全处理、隐私保护各项关键技术以及法律保障等方面讲述如何解决大数据时代的数据安全与隐私保护问题。

二、课程地位与目标

（一）课程地位： “数据安全与隐私保护”是信息安全专业本科生的专业限选课，旨培养学生应对大数据环境下数据安全和隐私保护问题的能力，是一门理论及应用均很强的专业课程，包括大数据安全与隐私保护技术框架、数据安全存储、数据安全检索、数据安全处理、隐私保护各项关键技术以及法律保障等。

本课程支撑的毕业要求拆分指标点的具体描述。

2.4：具备应用相关知识对系统解决方案进行比较分析、改进的能力

3.4：能正确表达一个工程问题的解决方案

5.2：能基于专业理论和技术，选择研究路线，设计实验方案

7.2：具有在社会背景和约束中，开展信息安全理论、技术及工程创新的方法和意识，并能够在工程开发中明确自己的社会责任

9.2：了解与本专业相关的重要法律、法规及方针与政策，并在实践中自觉遵守

（二）课程目标

1 教学目标： 本课程要求学生了解大数据、云计算及社会信息化对数据安全和公民隐私的安全威胁，掌握“数据安全和隐私保护”中的大数据、云计算、大数据安全等基本概念；了解国内外数据安全与隐私保护相关的法律法规，建立对大数据安全和隐私保护问题的宏观认识；掌握大数据安全存储、安全检索、安全处理和隐私保护的基本理论和基本方法，培养学生应用数据安全和隐私保护技术分析、解决和研究数据安全和隐私保护问题的能力。本课程对毕业要求拆分指标点达成的支撑情况，详见表 1。

表 1 课程目标与毕业要求拆分指标点的对应关系

序号	课程目标	毕业要求拆分指标点				
		2.4	3.4	5.2	7.2	9.2
1	让学生掌握数据安全与隐私保护基本概念，掌握数据安全存储、安全检索、安全处理和隐私保护的基本方法，又能学以致用，比较分析、改进数据安全和隐私保护实际问题的解决方案。	●				
2	涉及对同态加密、密文检索以及隐私信息的匿名、泛化等技术，具有良好的数学训练，能够培养学生应用数学和工程科学的基本理论，准确识别、表达数据安全与隐私保护问题。		●			
3	让学生掌握数据安全与隐私保护技术的基本原理，培养学生应用数据安全和隐私保护技术思路研究解决数据安全和隐私保护实际问题的能力。			●		
4	让学生了解大数据、云计算及社会信息化对数据安全和公民隐私的威胁，建立对大数据安全和隐私保护的宏观认识，帮助学生明确社会责任。				◎	
5	大数据时代的数据安全和隐私保护需求也不是纯技术能解决的，需要法律、法规制度的约束，通过学习大数据安全和隐私保护相关法律法规，帮助学生了解与本专业相关的重要法律、法规及方针与政策，并在实践中自觉遵守。					●

注：●：表示有强相关关系，◎：表示有一般相关关系，⊙：表示有弱相关关系

2 育人目标： 大数据时代的数据安全和隐私保护问题已成为当前国家、社会和公民共同关注的热点问题。本课程包括数据安全和隐私保护相关的法律法规保障专题，内容涉及《中华人民共和国网络安全法》（2017 年）、《通用数据保护法案》（2018 年）等国内、国际重要的法律法规。通过对这些法律法规解读和案例分析，使学生理解数据安全和隐私保护问题不是可有可无的，随意泄露或窥探别人的隐私问题会受到法律的惩罚，有利于让学生充分认识到泄密可能造成的严重危害和后果，从价值观层面进一步树立学生的数据安全与隐私保护的意识，强化他们对信息安全乃至总体国家安全观的认识和理解。

三、课程教学内容

分章节列出课程教学内容及对课程目标的支撑，详见表 2。

表 2 教学内容与课程目标的对应关系

章节名称	教学内容及重点（▲）、难点（★）	课程目标（√）

		1	2	3	4	5
第一章 绪论	课程介绍（课程目标、课程的教学内容、教材及参考文献和考核要求等）；大数据基本知识；大数据来源；大数据应用；大数据技术框架▲；大数据安全与隐私保护需求▲,★；大数据生命周期安全风险分析；大数据安全与隐私保护技术框架▲,★；大数据服务于信息安全；基本密码学工具▲；加密技术；数字签名技术；Hash 和 MAC 技术；密钥交换技术；	√			√	√
第二章 数据安全存储技术	产生动机；技术分类▲；基于可信引用监控器的访问控制；早期访问控制技术（DAC\MAC\RBAC）；角色挖掘▲,★；风险自适应访问控制技术▲,★；基于密码学的访问控制；基于密钥管理的访问控制；基于属性加密的访问控制▲,★	√		√		
第三章 数据安全检索技术	产生动机；技术分类▲；早期安全检索技术；PIR▲,★；ORAM★；对称密文检索；基于全文扫描的方案▲,★；基于文档关键词检索的方案★；非对称密文检索；BDOP-PEKS 方案▲,★；KR-PEKS 方案；密文区间检索▲,★	√		√		
第四章 数据安全处理技术	产生动机；技术分类▲；同态加密技术；同态加密▲,★；自举加密；类同态加密；全同态加密；可验证计算技术；基于承诺的可验证计算▲,★；基于交互的可验证计算；安全多方计算技术；安全两方计算▲,★；安全多方计算；函数加密技术；外包计算技术；具有多个服务器的外包计算；具有单一服务器的外包计算▲,★	√	√	√		
第五章 隐私保护技术	基本知识； 隐私的定义和分类▲；隐私泄露途径和表现形式；隐私保护需求；关系型数据隐私保护；身份匿名▲,★；属性匿名；社交图谱中的隐私保护：节点匿名▲,★；边匿名；位置轨迹隐私保护；基于政策法的 LBS 隐私保护；基于扭曲法的 LBS 隐私保护▲,★；基于加密法的 LBS 隐私保护；差分隐私；形式化定义★；拉普拉斯机制；指数机制	√	√	√	√	
第六章 数据安全与隐私保护的法律保障	国外的法律法规；通用数据保护条例（GDPR）▲,★；电子通讯隐私法（ECPA）；金融服务现代化法案；国内的法律法规；中华人民共和国网络安全法▲,★					√

四、教授方法与学习方法指导

教授方法：以讲授为主，讨论和课设作业为辅。课内讲授采用探究教学、项目驱动、案例教学等多种教学方法与模式，结合多媒体、板书等教学手段，通过范例和视频演示讲授课程内容，以知识为载体，传授相关的思想和方法，引导学生掌握数据安全与隐私保护涉及的基本概念、基本理论和基本方法。同时，也可聘请相关领域的企业专家进课堂介绍诸如脱敏等隐私保护技术专题，通过学生与企业专家、老师的共同讨论，学生能学到企业最新的数据安全和隐私保护技术案例，能更充分了解数据安全和隐私保护技术的技能要求，在拓宽学生眼界的同时，能有效培养学生的信息安全职业道德及专业素养，更好地提高学生的技能水平。课设作业则提出基本要求，引导学生根据场景要求分组完成一个具体数据

安全与隐私保护问题解决方案的设计与实现。

学习方法： 养成探索和思考的习惯，特别是重视对基本理论的钻研，在理论指导下进行实践；注意从实际问题入手，根据信息系统面临的数据安全和隐私泄露威胁分析其安全需求，遵循设计原则给出安全解决方案。明确学习各阶段的重点任务，做到课前预习，课中认真听课，课后认真复习，不放过疑点，充分利用好教师资源和同学资源。仔细研读教材，适当选读参考书的相关内容或利用国内外多所高校已开设的相关 MOOC 课程资源，从系统实现的角度深入理解概念，掌握方法的精髓和技术的原理。积极参加课设作业，在课设作业中加深对各种数据安全和隐私保护技术工作原理的理解。

五、教学环节及学时分配

教学环节及各章节学时分配，详见表 3。

表 3 教学环节及各章节学时分配表

章节名称	教学内容	学 时 分 配					合计
		讲授	习题	实验	讨论	其它	
第一章	绪论	4					4
第二章	数据安全存储技术	6					6
第三章	数据安全检索技术	6					6
第四章	数据安全处理技术	4					4
第五章	隐私保护技术	8					8
第六章	数据安全与隐私保护的法律保障	2					2
	总结和复习	2					2
合计		32					32

六、考核与成绩评定

期末考试占 75%。涵盖所学内容 90%以上；分为概念题（理论题）和设计分析题两部分。考试环节是对学生学习情况的全面检验，考查学生对数据安全与隐私保护基本概念、基本理论、基本方法的了解和掌握，起到督促学生系统掌握课程主要教学内容的作用。

平时成绩占 10%，反映学生的课堂表现、平时的信息接受、自我约束，课下的自主学习等，考查学生对已学知识掌握的程度以及自主学习的能力。成绩评定的主要依据包括：课程的出勤情况、课堂的基本表现（含课堂测验）、课外线上资源的预习情况。

课设作业占 15%，反映学生对课程主要教学内容的理解深度和实际应用能力，考查学生设计、分析和解决一个具体数据安全和隐私保护问题的能力。

本课程各考核环节的比重及对毕业要求拆分点的支撑情况，详见表 4。

表 4 考核方式及成绩评定分布表

考核方式	占比（%）	主要考核内容及对毕业要求拆分指标点的支撑情况
课设成绩	15%	引导学生复习和深入理解讲授的内容（解决数据安全和隐私保护问题的基本方法、基本理论、基本工具），锻炼运用所学知识选择一个具体大数据安全和隐私保护问题设计和实现解决方案，通过对课设作业的文档评审、需求分析、算法设计、实现源码和效果展示的完成质量评价，对

		应课程目标 1,2 和 3 达成度的考核。
平时成绩	10%	考查学生课堂的参与度，对所讲内容的基本掌握情况以及课外线上资源的自主学习情况，通过考核学生课堂练习参与度（含出勤情况）及其完成质量，对应课程目标 1 和课程目标 4 达成度的考核。
考试成绩	75%	对规定考试内容掌握的情况，对应课程目标 1、课程目标 2、课程目标 4 和课程目标 5 达成度的考核。

七、考核环节及质量标准

本课程各考核环节及质量标准，详见表 5。

表 5 考核环节及质量标准

考核方式	评分标准				
	A	**B**	**C**	**D**	**E**
	90～100	**80～89**	**70～79**	**60～69**	**< 60**
课设作业	报告文档格式规范、文字规范、术语准确、注释齐全；问题分析准确；提出算法完全解决问题需求；源码符合算法设计、齐全；效果展示符合预期	报告文档格式较规范、文字较规范、术语较准确、、注释较齐全；问题分析较准确；提出算法较好解决问题需求；源码较符合算法设计或较齐全；效果展示较符合预期	报告文档格式较规范、文字较规范、术语较准确、注释较齐全；问题分析较准确；提出算法基本解决问题需求；源码基本符合算法设计或较齐全；效果展示基本符合预期	报告文档格式基本规范、文字基本规范、术语基本准确、注释基本齐全；问题分析基本准确；提出算法基本解决问题需求；源码基本符合算法设计或较齐全；效果展示基本符合预期	不满足D要求
平时成绩	上课全勤、积极回答教师随堂提问、积极参与讨论、开展课外线上资源自主学习	上课全勤、较积极回答教师随堂提问、较积极参与讨论、开展课外线上资源自主学习	上课全勤、较积极回答教师随堂提问、能参与讨论、开展课外线上资源自主学习	上课缺席不超过 2 次、能回答教师随堂提问、能参与讨论、开展课外线上资源自主学习	不满足D要求
期末考试	很好地掌握教学内容涉及的基本概念、理论、方法，且具备很强的综合运用所学知识解决复杂问题的能力。	较好地掌握教学内容涉及的基本概念、理论、方法，且具备较强的综合运用所学知识解决复杂问题的能力。	较好地掌握教学内容涉及的基本概念、理论、方法，且具备一定的综合运用所学知识解决复杂问题的能力。	基本掌握教学内容涉及的基本概念、理论、方法，且基本能具备运用所学知识解决复杂问题。	不满足D要求
评分标准（A～E）：主要填写对教学内容中的基本概念、理论、方法等方面的掌握，及综合运用理论知识解决复杂问题能力的要求。					

制定者：林莉

批准者：张建标

2020 年 7 月

“逆向工程”课程教学大纲

英文名称：Reverse Engineering

课程编码：0008209

课程性质：专业选修课

学分：2.0　　学时：32

面向对象：信息安全（实验班）专业本科生

先修课程：高级语言程序设计、汇编语言程序设计

教材及参考书：

[1] 李承远著，武传海译. 逆向工程核心原理.：人民邮电出版社 2014 年 5 月

[2] 宁书林著. 软件逆向分析实用技术：北京理工大学出版社 2013 年 3 月

一、课程简介

逆向工程是信息学部为信息安全专业本科生开设的专业限选课。本课程的任务是引导学生从低阶视角再认识程序代码，深入了解程序代码的相关知识。培养其逆向思维、掌握逆向工程的核心原理和概念。除了学习知识外，还要学习静态和动态代码分析、特定信息查找等典型技术；给学生提供参与逆向工程的机会，培养其工程意识和能力。逆向工程重点是学习分析技术和软件调试分析检测工具的应用，为理解软件代码的复杂度和弄清“真相”提供了切实可行的方法。难点在于从全新的低阶视角审视现有的程序，以便评价软件的安全等级，改进提高安全等级，检查软件中的恶意代码，发现软件产品中的安全漏洞，在开发安全产品时与已存在的程序兼容等。

二、课程地位与目标

（一）课程地位：本课程是计算机信息安全专业的学科限选课，旨在继高级和汇编语言程序设计、汇编语言程序设计、数据结构与算法等与程序设计相关的课程后，引导学生在系统上级再认识程序代码，深入了解程序代码的相关知识。培养其逆向思维、掌握逆向工程的核心原理和概念；除了学习知识外，还要学习静态和动态代码分析、特定信息查找等典型技术；给学生提供参与逆向工程的机会，培养其工程意识和能力。

本课程支撑的毕业要求拆分指标点的具体描述。

5.1：能用基本的实验方法和工具在适当的环境下对系统特性进行实验。选择实现逆向工程目标的方法和技术。

5.2：能基于专业理论和技术，选择研究路线，设计实验方案。

10.1：认识合作的重要性，具有合作意识，明了自己在多学科团队中的责任和任务。学生需要从分工、运用逆向工程的各种技术实现、总结和书面报告等环节中相互协调、相互配合。

（二）课程目标

1 教学目标：使学生掌握“逆向工程”中的基本概念、基本理论、基本方法，在系统级上再认识逆向工程，提升计算机程序代码求解的水平，增强综合分析能力，体验实现逆向工程的乐趣。该目标分解为以下子目标：

表 1 课程目标与毕业要求拆分指标点的对应关系

序号	课程目标	毕业要求拆分指标点		
		5.1	5.2	10.1
1	掌握逆向工程基本概念，具备对各种逆向工程方法、工具、技术的比较、评价、选择和使用的能力。能按任务要求选择合适的工具软件，选择实现逆向工程目标的方法和技术，完成关键部分的逆向工程任务。	●		
2	增强综合运用静态分析和动态分析方法等技术、工具能力，实施完整的逆向工程		●	
3	了解逆向工程过程中涉及的法律问题。培养经验积累、系统能力和面向系统构建的交流和团队协作能力			◎

注：●：表示有强相关关系，◎：表示有一般相关关系，⊙：表示有弱相关关系

2 育人目标：通过逆向工程这门课，学生可以从低阶视角认识程序的另一面，通过对程序的分析可以了解国内外程序的差距，从低阶视角弥补高阶视角的不足。学生树立正确逆向工程有关的法律法规意识，正确运用所学知识报效祖国。同时也为日后从事信息安全行业打下坚实的基础。

三、课程教学内容

分章节列出课程教学内容及对课程目标的支撑，详见表 2。

表 2 教学内容与课程目标的对应关系

章节名称	教学内容及重点（▲）、难点（★）	课程目标（√）		
		1	2	3
第一章 引论	教学目的▲、课程的基本内容▲、逆向工程的适用对象、软件运行环境和组件层次、逆向工程的层次结构★、逆向工程的法律问题。	√		√
第二章 逆向工程的工具使用	“逆向工具”的开发与利用。▲	√		
第三章 可执行程序逆向的基本知识	Windows、Linux 的可执行文件格式▲、组件及基本架构、内存、核心对象，应用程序接口、数据分配和输入输出▲★。	√		
第四章 逆向工程的方法和技术	可执行文件的静态和动态代码分析方法▲、信息获取。 静态和动态代码分析的主要思路、功能、所需工具、应用特点和功能局限性★。 使用工具进行静态和动态代码分析的技术、获取相关信息的技术		√	
第五章 逆向工程的应用	主要是涉及逆向工程在信息安全方面的具体应用。 程序代码的分析和安全性审查▲、程序功能修补★，突破密钥保护；恶意软件的分析识别	√	√	
第六章 总结	逆向工程的知识综合、发展方向、反编译技术			√

四、教授方法与学习方法指导

教授方法：以课堂讲授为主（18 学时），总结讨论（2 学时），实验为辅（课内 12）。课内讲授推崇研究型教学，以知识为载体，传授相关的思想和方法，引导学生扎实掌握基本原则，学会应用各种方法、技术和工具。实验教学则提出基本要求，引导学生分组独立完成实验目标。

学习方法：养成探索的习惯，特别是重视对基本原则的掌握，在理论指导下进行实践；注意从实际问题入手，引导出总体原则，各种方法和技术、适用的工具，最后通过综合运用实现工程目标。明确学习各阶段的重点任务，做到课前预习，课中认真听课，积极思考，课后认真复习，不放过疑点，充分利用好教师资源和同学资源。仔细阅读教材，适当选读参考书的相关内容，从系统实现的角度，深入理解概念，掌握方法的核心思想，多动手实践。积极参加实验，在实验中加强对方法、技术和工具的掌握。

五、教学环节及学时分配

教学环节及各章节学时分配，详见表 3。

表 3 教学环节及各章节学时分配表

章节名称	教学内容	学时分配					合计
		讲授	习题	实验	讨论	其它	
第一章 引论	教学目的▲、课程的基本内容▲、逆向工程的适用对象、软件运行环境和组件层次、逆向工程的层次结构★、逆向工程的法律问题。	4					
第二章 逆向工程的工具使用	“逆向工具”的开发与利用。▲	2					
第三章 可执行程序逆向的基本知识	Windows、Linux 的可执行文件格式▲、组件及基本架构、内存、核心对象，应用程序接口、数据分配和输入输出▲★。	4		2			
第四章 逆向工程的方法和技术	可执行文件的静态和动态代码分析方法▲、信息获取。 静态和动态代码分析的主要思路、功能、所需工具、应用特点和功能局限性★。 使用工具进行静态和动态代码分析的技术、获取相关信息的技术	2		2			
第五章 逆向工程的应用	主要是涉及逆向工程在信息安全方面的具体应用。 程序代码的分析和安全性审查▲、程序功能修补★，突破密钥保护；恶意软件的分析识别	6		8			
第六章 总结	逆向工程的知识综合、发展方向、反编译技术				2		
合计		18		12	2		

六、考核与成绩评定

平时成绩占 20%（作业等 20%）。

平时成绩中的 5%主要反应学生的出勤听棵，15%反映在总结讨论环节，学生以小组为单位，网络调研为主，自行选题，课上每组完成 15 分钟左右的报告。

实验成绩占 80%。主要考查学生在所学理论知识指导下如何设计，引导学生发挥潜力和想象力，尽量完善实验的效果。培养学生综合运用所学知识进行探索、设计与实现中的交流能力（口头和书面表达）、协作能力、组织能力。

本课程各考核环节的比重及对毕业要求拆分点的支撑情况，详见表 4。

表 4 考核方式及成绩评定分布表

考核方式	占比（%）	主要考核内容及对毕业要求拆分指标点的支撑情况
平时成绩	20	相关报告的完成质量，对应毕业要求 5.1、9.1 达成度的考核。
考试成绩	80	实验系统的设计实现情况。对应毕业要求 5.1、5.2、9.1 达成度的考核.

七、考核环节及质量标准

本课程各考核环节及质量标准，详见表 5。

表 5 考核环节及质量标准

考核方式	评分标准				
	A	B	C	D	E
	90～100	80～89	70～79	60～69	< 60
出勤	全勤	少出勤 1-2 次	少出勤 3-4 次	少出勤 5 次以上	不满足 D 要求
研讨	有很好的表达能力和创新能力	有较好的表达能力和创新能力	有一般的表达能力和创新能力	有一般的表达能力，无创新能力	不满足 D 要求
实验	独立、自主、创新能力完成实验，且实验报告撰写优秀	独立、自主、有一定创能力新完成实验，且实验报告撰写较为优秀	独立、自主完成实验，且实验报告撰写一般	完成实验，且完成实验报告	不满足 D 要求
评分标准（A～E）：主要填写对教学内容中的基本概念、理论、方法等方面的掌握，及综合运用理论知识解决复杂问题能力的要求。					

制定者：王昱波

批准者：张建标

2020 年 7 月

“区块链安全技术”课程教学大纲

英文名称：Blockchain Security Technology

课程编码：0010135

课程性质：专业选修课

学分：2.0　　学时：32

面向对象：信息安全（实验班）专业本科生

先修课程：

教材及参考书：

[1] 朱建明, 高胜, 段美姣等. 区块链技术与应用. 机械工业出版社，2018.

[2] 王飞跃, 袁勇. 区块链理论与方法. 清华大学出版社, 2019.

[3] Rajneesh Gupta 著, 孙国梓译. 区块链安全实战. 机械工业出版社，2019

[4] 黄连金, 吴思进, 曹锋, 季宙栋等. 区块链安全技术指南. 机械工业出版社，2018

一、课程简介

本课程对区块链核心技术、区块链安全机制、区块链与安全技术等方面进行了比较深入的分析和介绍。在核心技术方面重点介绍了区块链的密码学基础、共识机制、智能合约以及典型项目。在安全机制方面介绍了针对区块链中的数据、交易、隐私、监管等方面的安全机制。在区块链与安全技术方面，重点阐述了区块链在大数据、身份认证、物联网、分布式存储等方面的安全技术中的典型应用。

二、课程地位与目标

（一）课程地位： 本课程是信息安全专业的限选课，可以作为其它计算机类专业的选修课。旨在引导学生在全面的理解区块链核心技术的基础上，深入了解区块链内部安全机制和区块链对于其他安全技术的作用；给学生学习并思考新技术的内在和外在安全的意识和能力。

主要为毕业要求第 2.4、3.1、4.1 的实现提供支持。

对于毕业要求 2.4，培养学生应用区块链核心技术，比较区块链不同方案的特点，并基于不同场景给出改进建议。

对于毕业要求 3.1，培养学生通过学习区块链安全机制，研究分析区块链的安全隐患，以获得有效结论。

对于毕业要求 4.1，强化学生信息安全核心意识，培养其在不同的安全场景需求下正确应用区块链技术的复杂需求设计能力。

（二）课程目标

1 教学目标：使学生掌握区块链中的基本概念、基本理论、基本方法，再认识区块链的安全机制，最后理解区块链在信息安全技术中的作用。该目标分解为以下子目标：

课程目标 1：掌握区块链技术基本概念和核心技术。

课程目标 2：掌握区块链核心安全机制。

课程目标 3：掌握区块链的安全特性及在安全技术中的作用。

本课程对毕业要求拆分指标点达成的支撑情况，详见表 1。

表 1 课程目标与毕业要求拆分指标点的对应关系

序号	课程目标	毕业要求拆分指标点		
		2.4	3.1	4.1
1	掌握区块链技术基本概念和核心技术	◎		
2	掌握区块链核心安全机制		◎	
3	掌握区块链的安全特性及在安全技术中的作用			●

注：●：表示有强相关关系，◎：表示有一般相关关系，⊙：表示有弱相关关系

2 育人目标：本课程能够培养学生对于技术安全的良好意识，理解技术安全对于行业乃至国家安全的重要作用，在今后的学习、工作中能自觉地维护信息安全，以适应我国科技发展的需要。

三、课程教学内容

分章节列出课程教学内容及对课程目标的支撑，详见表 2。

表 2 教学内容与课程目标的对应关系

章节名称	教学内容及重点（▲）、难点（★）	课程目标（√）		
		1	2	3
第一章 区块链概述	主要介绍区块链安全思想▲★，区块链分类和区块链技术原理▲，介绍区块链和信息安全、密码技术的关系，介绍区块链的发展史、能解决的行业问题以及未来的发展趋势。	√	√	
第二章 密码学基础	首先介绍区块链中密码学基础工具▲★，包括哈希函数、公钥密码体制、数字签名等。然后介绍密码算法的原理与应用▲，区块链与密码学的关系，最后介绍密码学与信息安全的关系。	√		
第三章 共识机制	主要介绍典型共识算法的原理与实现▲，包括工作量证明（POW）★，权益证明（POS）★，实用拜占庭容错（PBFT）等算法，介绍分布式及共识机制的思想，并简要介绍零知识证明协议。	√		
第四章 智能合约	主要介绍比特币脚本的原理和编写，以太坊智能合约的原理及意义▲★，以及超级账本链码（Chaincode）的原理和编写★。	√		
第五章 典型项目	主要介绍比特币的原理★和发展历程，重点介绍以太坊的原理▲★和发展历程，以及超级账本项目的核心框架▲和发展历史。	√		
第六章 区块链安全机制	主要介绍区块链内部的安全威胁，重点介绍区块链在数据、共识算法、隐私、智能合约、内容方面额安全机制▲和技术原理★。		√	
第七章 区块链与安全技术	主要介绍区块链技术在现有信息安全领域的主要作用★▲，包括区块链对大数据、身份认证、版权保护、分布式存储等领域的安全技术的影响★。			√

四、教授方法与学习方法指导

教授方法：以讲授为主，练习为辅的方式，进一步加强学生的学习和思辨能力。课内讲授推崇研究型教学，以知识为载体，传授相关的思想和方法，引导学生踏着大师们研究步伐前进。课下练习则提出开放问题，引导学生完成自学，学会对开放问题的多种角度的思考。

学习方法： 养成探索的习惯，特别是重视对基本理论的钻研，在理论指导下进行实践；注意从实际问题入手，归纳和提取基本特性，最后实现对实际问题的解答。明确学习各阶段的重点任务，做到课前预习，课中认真听课，积极思考，课后认真复习，不放过疑点，充分利用好教师资源和同学资源。仔细研读教材，适当选读参考书的相关内容，从系统实现的角度，深入理解概念，掌握方法的精髓和算法的核心思想，不要死记硬背。

五、教学环节及学时分配

教学环节及各章节学时分配，详见表 3。

表 3 教学环节及各章节学时分配表

章节名称	教学内容	学 时 分 配					合计
		讲授	习题	实验	讨论	其它	
第一章	区块链概述	2	0	0	0	0	2
第二章	密码学基础	2	0	0	0	0	2
第三章	共识机制	4	0	0	0	0	4
第四章	智能合约	2	0	0	0	0	2
第五章	典型项目	2	0	0	0	0	2
第六章	区块链安全机制	10	0	0	0	0	10
第七章	区块链与安全技术	10	0	0	0	0	10
合计		32	0	0	0	0	32

六、考核与成绩评定

平时成绩 40%（作业等 30%，其它 10%），考试成绩 60%。

平时成绩中的其它 10%主要反应学生的课堂表现、平时的信息接收、自我约束。成绩评定的主要依据包括：课程的出勤率、课堂的基本表现（如课堂测验、课堂互动等；作业等的 30%主要是课堂作业和课外作业，主要考察学生对已学知识掌握的程度以及自主学习的能力。

考试成绩 60%为对学生学习情况的全面检验。强调考核学生对基本概念、基本方法、基本理论等方面掌握的程度，及学生运用所学理论知识解决复杂问题的能力。

本课程各考核环节的比重及对毕业要求拆分点的支撑情况，详见表 4。

表 4 考核方式及成绩评定分布表

考核方式	占比（%）	主要考核内容及对毕业要求拆分指标点的支撑情况
平时成绩	40	相关作业的完成质量，对应课程目标 1、课程目标 2 达成度的考核，支撑毕业要求 2.4 和 3.1

考试成绩	60	对规定考试内容掌握的情况，对应课程目标 1、课程目标 2、课程目标 3 达成度的评价提供支持，支撑毕业要求 2.4、3.1 和 4.1

七、考核环节及质量标准

本课程各考核环节及质量标准，详见表 5。

表 5 考核环节及质量标准

考核方式	评　分　标　准				
	A	**B**	**C**	**D**	**E**
	90～100	**80～89**	**70～79**	**60～69**	**< 60**
平时成绩	课堂表现优异，作业完成质量高	课堂表现较好，作业完成质量较高	课堂表现一般，作业完成质量一般	课堂表现差，作业完成质量低	不满足 D 要求
考试成绩	考试内容掌握出色	考试内容掌握较好	考试内容掌握一般	考试内容掌握有限	不满足 D 要求
评分标准（A～E）：主要填写对教学内容中的基本概念、理论、方法等方面的掌握，及综合运用理论知识解决复杂问题能力的要求。					

制定者：于海阳

批准者：张建标

2020 年 7 月

“信息安全标准”课程教学大纲

英文名称：Information Security Standard

课程编码：0008216

课程性质：专业选修课

学分：2.0　　学时：32

面向对象：信息安全（实验班）专业本科生

先修课程：无

教材及参考书：

[1] 郭启全.信息安全等级保护政策培训教程.北京：电子工业出版社.2016

[2] 信息安全等级保护管理办法，公通字 43 号文

[3] 国家标准《计算机信息系统安全等级保护划分准则》（GB17859-1999）

[4] 国家标准《信息安全技术 信息系统安全等级保护定级指南》（GB/T22240-2010）

[5] 国家标准《信息安全技术 网络安全等级保护基本要求》（GB/T22239-2019）

[6] 国家标准《信息安全技术 网络安全等级保护安全设计技术要求》（GB/T 25070-2019）

[7] 国家标准《信息安全技术信息系统通用安全技术要求》（GB/T 20271-2006）

[8] 国家标准《信息安全技术操作系统安全技术要求》（GB/T 20272-2006）

[9] 国家标准《信息安全技术数据库管理系统通用安全技术要求》（GB/T 20273-2006）

[10] 国家标准《信息安全技术信息系统安全管理要求》（GB/T20269-2006）

一、课程简介

信息安全是一个涉及面相当广泛的学科，尤其是信息安全工程，更是保罗万象。培养信息安全人才，需要让学生了解信息安全工程的方方面面。“信息安全标准”课程根据学生的特点，以信息安全工程实施为主线，以国家等级保护政策为核心，通过对国内外典型的、核心的安全需求类、安全建设与实施类、安全评估类、安全管理类等信息安全标准的讲解与讨论，向学生传授信息安全工程的有关知识和方法，培养学生的宏观把控能力。要求学生掌握标准的制定背景、相关术语、核心内容、关联关系等，使其对国际和国内信息安全领域相关标准有一个基本了解，从而整体上对信息安全有一个宏观认识。

二、课程地位与目标

（一）课程地位：本课程不仅是信息安全专业限选课，而且是信息学部跨专业选修课。旨在继密码学、系统安全、网络安全等课程后，以信息安全工程为主线，以国内外典型的信息安全标准为切入点，系统地引导学生综合理解和应用所学知识，掌握信息安全工程的基本思路、方法和政策，认识如何构建一个安全的信息系统，包括信息系统的安全需求分析、信息系统安全体系结构的设计、信息系统安全评估及信息安全管理体系等。本课程系统性强、内容覆盖面广、体系化程度高，对信息安全涉及的各个层面进行了梳理和论证，并讨论了信息安全领域的最新研究进展和发展趋势。

本课程支撑的毕业要求拆分指标点的具体描述。

2.3：能对系统设计方案和所建模型的正确性进行推理并能得出结论

4.1：能归纳描述用户的需求，并能选择正确的方法确定设计目标

9.2：了解与本专业相关的重要法律、法规及方针与政策，并在实践中自觉遵守

（二）课程目标

1 教学目标：本课程要求学生了解国内外信息安全行业的政策，尤其是我国等级保护相关政策法规，使其树立正确的网络安全观，正确处理网络安全领域的攻防博弈；要求学生了解国内外网络安全主体标准，包括信息系统的安全需求分析、信息系统安全体系结构的设计、信息系统安全评估及信息安全管理体系等，掌握标准的制定背景、相关术语、核心内容、关联关系等，从而理论联系实际，让学生在信息安全工程实践层面更综合的理解和应用所学知识，提升学生的认知水平和工程实践能力，为学生的未来职业规划提供依据。本课程对毕业要求拆分指标点达成的支撑情况，详见表 1。

表 1 课程目标与毕业要求拆分指标点的对应关系

序号	课程目标	毕业要求拆分指标点		
		2.3	4.1	9.2
1	要求学生了解国内外信息安全行业的政策，尤其是我国等级保护相关的政策法规，培养学生正确的网络安全观			●
2	要求学生了解国内外信息系统安全需求分析类网络安全主体标准，掌握网络安全需求分析方法。		●	
3	要求学生了解国内外网络安全体系结构的设计、信息系统安全评估及信息安全管理体系等主体标准，掌握网络安全体系、工程方案设计的能力。	◎		

注：●：表示有强相关关系，◎：表示有一般相关关系，⊙：表示有弱相关关系

2 育人目标：信息安全已成为当前国家、社会和公民共同关注的热点问题，本课程包括信息安全行业，尤其是我国等级保护制度相关的主体标准法规，内容涉及安全需求分析、安全体系设计、安全风险评估、安全管理体系设计等网络安全工程需要的诸多内容。通过对这些标准的讲解，使学生理解网络安全工程的政策、方法及要求，有利于让学生树立正确的网络安全观，提升其网络安全工程能力，强化他们对网络安全乃至国家安全观的认识和理解。

三、课程教学内容

分章节列出课程教学内容及对课程目标的支撑，详见表 2。

表 2 教学内容与课程目标的对应关系

章节名称	教学内容及重点（▲）、难点（★）	课程目标（√）		
		1	2	3
第一章 绪论	信息安全标准概述 标准化概述、标准化意义、国内外信息安全标准化组织、国内外信息安全标准体系▲★。 等级保护总体介绍 等级保护背景、等级保护政策▲、等级保护内涵▲★、等级保护标	√		

	准架构、等级保护关键标准概述。			
第二章 安全需求 分析标准	定级指南 相关术语、定级依据、定级方法▲★ 基本要求 物理安全要求、计算环境安全要求▲★、通信网络安全要求▲★、 区域边界安全要求▲★ 行业特殊要求 介绍典型行业的信息安全需求类标准，如金融行业、医疗行业 等。		√	
第三章 安全体系 建设标准	设计技术要求 设计理念、信息安全架构设计▲、技术体系设计▲★、多级互联▲ ★ 安全管理体系 管理体系定义、管理体系内涵、管理体系方法论▲★ 安全工程实施 工程实施过程、过程实施任务			√
第四章 安全功能 机制标准	主机安全机制 安全操作系统标准、安全审计 应用安全机制 WAF▲、RASP 数据安全机制 DLP▲、电子文档加密 集中管理平台 SOC、态势感知▲		√	√
第五章 安全风险 评估标准	风险评估 相关术语、风险评估意义、风险评估方法▲★、风险控制▲★ 等级测评 安全测评方法、安全测评要求▲★。		√	√

四、教授方法与学习方法指导

教授方法：以讲授为主，讨论和课设作业为辅。课内讲授采用探究教学、项目驱动、案例教学等多种教学方法与模式，结合多媒体、板书等教学手段，通过范例和视频演示讲授课程内容，以知识为载体，传授相关的思想和方法，引导学生掌握信息安全涉及的基本概念、基本理论和基本方法。同时，也可聘请相关领域的企业专家进课堂介绍诸如等级保护政策、网络安全功能机制等技术专题，通过学生与企业专家、老师的共同讨论，学生能学到企业最新的信息安全政策、技术及案例，能更充分了解信息安全相关技术和要求，在拓宽学生眼界的同时，能有效培养学生的信息安全职业道德及专业素养，更好地提高学生的技能水平。课设作业则提出基本要求，引导学生根据场景要求分组完成一个具体等级保护解决方案的设计与实现。

学习方法：养成探索和思考的习惯，特别是重视对基本理论的钻研，在理论指导下进行实践；注意从实际问题入手，根据信息系统面临的安全威胁分析其安全需求，遵循设计原则给出安全解决方案。明确学习各阶段的重点任务，做到课前预习，课中认真听课，课

后认真复习，不放过疑点，充分利用好教师资源和同学资源。仔细研读教材，适当选读参考书的相关内容或利用国内外多所高校已开设的相关 MOOC 课程资源，从系统实现的角度深入理解概念，掌握方法的精髓和技术的原理。积极参加实验，在实验中加深对各种安全技术工作原理的理解。

五、教学环节及学时分配

教学环节及各章节学时分配，详见表 3。

表 3 教学环节及各章节学时分配表

章节名称	教学内容	学 时 分 配					合计
		讲授	习题	实验	讨论	其它	
第一章	绪论	4					4
第二章	安全需求分析标准	4					4
第三章	安全体系建设标准	12					12
第四章	安全功能机制标准	4					4
第五章	安全风险评估标准	2			4		6
	考试					2	2
合计		26			4	2	32

六、考核与成绩评定

课程成绩包括期末考试成绩和平时成绩两部分。

考核方式及成绩评定分布：

期末考试占 80%。涵盖所学内容 90%以上；分为概念题（理论题）和设计分析题两部分。考试环节是对学生学习情况的全面检验，考查学生对信息安全标准基本概念、理论、技术及系统的分析与设计的能力，起到督促学生系统掌握课程主要教学内容的作用。

平时成绩占 20%（分组讨论占 15%，随堂练习占 5%），反映学生的课堂表现、平时的信息接受、自我约束，考察学生对已学知识掌握的程度以及自主学习的能力。成绩评定的主要依据包括：课程的出勤情况、课堂的基本表现（含课堂测验）、分组讨论情况。

本课程各考核环节的比重及对毕业要求拆分点的支撑情况，详见表 4。

表 4 考核方式及成绩评定分布表

考核方式	所占比例（%）	主要考核内容及对毕业要求拆分指标点的支撑情况
平时成绩	分组讨论 15%	引导学生分组，查资料了解各种网络安全攻击，进行集中讨论。使其建立网络安全攻防博弈的概念，对网络安全需求、风险有更深入的认识，从而梳理正确的网络安全观。对应课程目标 1,2 和 3 达成度的考核。
	随堂练习 5%	考查学生课堂的参与度，对所讲内容的基本掌握情况，通过考核学生课堂练习参与度（含出勤情况）及其完成质量，对应课程目标 1,2 和 3 达成度的考核。
考试成绩	80%	对规定考试内容掌握的情况，对应课程目标 1,2 和 3 达成度的考核。

七、考核环节及质量标准

本课程各考核环节及质量标准，详见表 5。

表 5 考核环节及质量标准

考核方式	评　分　标　准				
	A	**B**	**C**	**D**	**E**
	90～100	**80～89**	**70～79**	**60～69**	**< 60**
分组讨论	攻击背景介绍清晰；攻击原理分析准确；攻击过程描述完善；攻击效果展示符合预期；	攻击背景介绍清晰；攻击原理分析较准确；攻击过程描述较完善；攻击效果展示较符合预期；	攻击背景介绍较清晰；攻击原理分析基本准确；攻击过程描述较完善；攻击效果展示基本符合预期；	攻击背景介绍基本清晰；攻击原理分析基本准确；攻击过程描述基本完善；攻击效果展示基本符合预期；	不满足 D 要求
随堂练习	上课全勤、积极回答教师随堂提问、积极参与讨论	上课全勤、较积极回答教师随堂提问、较积极参与讨论	上课全勤、较积极回答教师随堂提问、能参与讨论	上课缺席不超过 2 次、能回答教师随堂提问、能参与讨论	不满足 D 要求
期末考试	很好地掌握教学内容涉及的基本概念、理论、方法，且具备很强的综合运用所学知识解决复杂问题的能力。	较好地掌握教学内容涉及的基本概念、理论、方法，且具备较强的综合运用所学知识解决复杂问题的能力。	较好地掌握教学内容涉及的基本概念、理论、方法，且具备一定的综合运用所学知识解决复杂问题的能力。	基本掌握教学内容涉及的基本概念、理论、方法，且基本能具备运用所学知识解决复杂问题。	不满足 D 要求
评分标准（A～E）：主要填写对教学内容中的基本概念、理论、方法等方面的掌握，及综合运用理论知识解决复杂问题能力的要求。					

制定者：赵勇

批准者：张建标

2020 年 7 月

“新生研讨”课程教学大纲

英文名称：Freshman Seminars

课程编码：0009394

课程性质：自主课程

学分：1.0　　学时：16

面向对象：信息安全（实验班）专业本科生

先修课程：无

教材及参考书：

[1] 张建标、赖英旭、侍伟敏. 信息安全体系结构. 北京工业大学出版社. 2011 年 09 月.

[2] 杨义先、钮心忻. 安全简史. 机械工业出版社. 2017 年 03 月.

[3] [美] F.G.Major. 现代导航的演进——量子技术的兴起. 国防工业出版社. 2018 年 06 月.

[4] 陈晖. 密码前沿技术--从量子不可精确克隆到 DNA 完美复制. 国防工业出版社. 2015 年 06 月.

[5] 华为区块链技术开发团队. 区块链技术及应用. 清华大学出版社. 2019 年 03 月.

[6] 黄连金、吴思进、曹锋、季宙栋等. 区块链安全技术指南. 机械工业出版社. 2018 年 05 月.

[7] 杨东晓、张锋、陈世优. 云计算及云安全. 清华大学出版社. 2020 年 05 月 .

[8] [美] 布莱恩.罗素（Brian Russell）、 德鲁.范.杜伦（Drew Van D）. 物联网安全. 机械工业出版社. 2020 年 04 月.

[9] 牛少彰. 移动互联网安全. 机械工业出版社. 2020 年 05 月.

[10] 石瑞生. 大数据安全与隐私保护. 北京邮电大学出版社. 2019 年 05 月.

[11] 范渊. 智慧城市与信息安全(第 2 版). 电子工业出版社. 2016 年 09 月.

一、课程简介

信息安全是指信息网络的硬件、软件及其系统中的数据受到保护，不受偶然的或者恶意的原因而遭到破坏、更改、泄露、否认等，系统连续可靠正常地运行，信息服务不中断。广义的信息安全是一门综合性学科，安全不在是单纯的技术问题，而是将管理、技术、法律等问题相结合的产物；狭义的信息安全是建立在以密码技术为基础的计算机安全领域，辅以通信技术、计算机技术与网络技术等方面的内容。

本课程主要围绕“走进信息安全专业”、“浅谈信息安全技术”、“量子技术与信息安全”、“区块链技术及安全”、“新型计算环境下的信息安全”五个专题，针对大学新生特点，通过教师讲授、学生演讲、共同研讨等教学形式，让学生理解信息安全在社会、经济发展中的地位与作用；了解专业培养目标、毕业要求和课程体系；了解专业发展过程、现状和就业前景；初步了解信息安全的关键技术和前沿技术；熟悉和掌握专业文献的来源及获取方法。同时，本课程以探索、讨论和研讨为导向、强调师生互动和学生自主学习，对同学们在掌握知识、开拓视野、合作精神、交流表达、写作技能等诸多方面进行整体上的培养与训练。新生研讨课不仅让新生学习知识，更重要的是让新生体验认知过程，强调教师的引导与学生的充分参与和交流，启发学生的研究和探索兴趣，培养学生发现问题、提出问题、解决

问题的意识和能力。

二、课程地位与目标

（一）课程地位：

新生研讨课是信息专业的自主课程，是新生入学教育的深化和发展的必要，也是为建设研究型大学、开展研究性教与学的方法与之相匹配的一项重要改革举措。旨在帮助新生进行专业认知，激发学习兴趣，从新生一入校开始就构建起新生与专业教师见面与交流的平台，可使学生了解本专业学科，培养大学生积极探索知识的精神，使大学生从被动的学习者转变为主动学习的“发现者、研究者、探索者”。

本课程支撑的毕业要求拆分指标点的具体描述。

1.1：了解前沿技术的国内外发展现状以及国内技术的国际地位，引导学生爱国敬业，培养学生的社会责任感；

10.1：认识合作的重要性，具有合作意识，明了自己在多学科团队中的责任和任务；

11.1：能通过口头、书面与同行和相关人员进行有效沟通和交流；

11.3：了解专业的国际、国内发展情况，将系统设计开发置于国际发展的背景下；

（二）课程目标

1 教学目标：本课程旨在引导学生理解信息安全在社会、经济发展中的地位与作用；帮助学生了解专业培养目标、毕业要求、课程体系、专业发展过程、现状和就业前景；初步了解信息安全的关键技术和前沿技术；熟悉和掌握专业文献的来源及获取方法，培养学生文献检索和分析的能力，掌握正确的学习方法；培养学生的专业意识，使学生明确本专业的学习任务，为后续课程教学和培养良好的学习方法打下基础。同时，可使新生体验一种全新的以探索和研究为基础、师生互动、激发学生自主学习的研讨性教学的理念与模式，为其创造一个在合作环境下进行探究式学习的机会，从而激发学生专业学习兴趣，培养学生自主学习能力和积极探索的精神，锻炼学生表达和交流能力。

本课程对毕业要求拆分指标点达成的支撑情况，详见表 1。

表 1 课程目标与毕业要求拆分指标点的对应关系

序号	课程目标	毕业要求拆分指标点			
		1.1	10.1	11.1	11.3
1	帮助学生了解前沿技术的国内外发展现状及国内技术的国际地位，引导学生爱国敬业，培养学生的社会责任感。	◎			
2	培养学生具有合作意识。		⊙		
3	培养学生表达和交流能力。			●	
4	帮助学生了解专业的国际、国内发展情况，引导学生积极探索国际发展背景下的前沿技术。				●

注：●：表示有强相关关系，◎：表示有一般相关关系，⊙：表示有弱相关关系

2 育人目标：

通过了解信息系统面临的安全风险以及安全问题可能造成的后果，当前主流的安全技术和手段，以及新型技术所面临的安全问题，使学生充分认识到信息安全的重要性，激发学生对专业学习的热情，增强学生的安全防范意识，更重要的是做一个信息安全的“懂法守

法人”。

三、课程教学内容

分章节列出课程教学内容及对课程目标的支撑，详见表 2。

表 2 教学内容与课程目标的对应关系

章节 名称	教学内容及重点（▲）、难点（★）	课程目标（√）		
		1	2	3
第一章 走进信息安全专业	信息安全专业概况（专业的重要性、专业方向、专业特色）；本科生培养▲（专业培养目标、毕业要求和课程体系）；师资队伍建设；教学成果展示；就业前景展望。			√
第二章 浅谈信息安全技术	信息系统存在的安全威胁、信息系统存在的安全隐患、目前所采取的安全技术▲。			√
第三章 量子技术与信息安全	量子技术的产生背景和发展现状、量子技术的相关理论、量子技术在信息安全中的应用▲。	√	√	√
第四章 区块链技术及安全	区块链技术的产生、发展、关键技术和典型应用；区块链技术存在的安全问题以及采取的安全技术▲。	√	√	√
第五章 新型计算环境下的信息安全	“云、物、移、大、智”新型计算环境的产生背景、发展现状、应用和关键性技术；新型计算环境下存在的安全问题以及采取的安全技术▲。	√	√	√

四、教授方法与学习方法指导

在教学过程中采用教师讲授、学生演讲、共同研讨等教学形式，围绕师生共同感兴趣的专题，进行老师与学生之间、学生与学生之间的交流互动、口头及协作训练。通过边学习、边讨论，以灵活、多样的方式鼓励学生参与，激发学生的兴趣和主动参与意识。根据需要，可以安排聘请业界人员开展专题讲座。

五、教学环节及学时分配

教学环节及各章节学时分配，详见表 3。

表 3 教学环节及各章节学时分配表

章节名称	教学内容	学 时 分 配					合计
		讲授	习题	实验	讨论	其它	
第一章	走进信息安全专业	2					
第二章	浅谈信息安全技术	2					
第三章	量子技术与信息安全	1			1		
第四章	区块链技术及安全	1			1		
第五章	新型计算环境下的信息安全	4			4		

合计		10			6		16

六、考核与成绩评定

考核和成绩评定主要以平时和报告为依据，其中平时占 20%，主要反映学生的课堂表现，包括是否进入课堂听课、演讲内容符合度、表达清晰度、与教师或同学互动性等考核指标；报告占 80%，主要反映报告的完成情况，包括报告主题的符合度、内容的饱满性、结构的完整性、表达的清晰度以及格式是否规范等考核指标。

本课程各考核环节的比重及对毕业要求拆分点的支撑情况，详见表 4。

表 4 考核方式及成绩评定分布表

考核方式	所占比例（%）	主要考核内容及对毕业要求拆分指标点的支撑情况
平时	20%	课堂表现情况。主要为毕业要求 11.1 达成度的评价提供支持。
报告	80%	报告的完成情况。主要为毕业要求 11.3 达成度的评价提供支持。同时对毕业要求 1.1、10.1 达成度的评价也提供一定参考价值的基础数。

七、考核环节及质量标准

本课程各考核环节及质量标准，详见表 5。

表 5 考核环节及质量标准

考核方式	评 分 标 准	
	通过	不通过
平时	进入课堂听课、课堂演讲和研讨符合要求。	不满足通过的要求
报告	报告撰写符合要求。	不满足通过的要求
评分标准（A～E）：主要填写对教学内容中的基本概念、理论、方法等方面的掌握，及综合运用理论知识解决复杂问题能力的要求。		

制定者：侍伟敏

批准者：张建标

2020 年 7 月

“密码应用”课程教学大纲

英文名称：Cryptographic Applications

课程编码：0010122

课程性质：自主课程

学分：2.0　　学时：32

面向对象：信息安全（实验班）专业本科生

先修课程：密码学 I

教材及参考书：

[1] 胡向东，魏琴芳，胡蓉 著. 应用密码学（第 4 版）. 电子工业出版社，2019-05-01

[2] [美] 理查德 E. 布拉胡特（Richard E. Blahut） 著，黄玉划，薛明富，许娟 译. 现代密码学及其应用. 机械工业出版社，2018-05-01

[3] 吴世忠，祝世雄，张文政等 应用密码学：协议、算法与 C 源程序（原书第 2 版），机械工业出版社，2014-1

一、课程简介

密码应用是信息学部计算机学院为信息安全专业本科生开设的自主课程。本课程的任务是以工程技术为主线，在讲述面向特定应用的密码协议基本原理的同时，注重密码算法的应用，通过精选贴近生活以及新应用的密码学典型应用案例，使学生了解国内外密码算法的应用现状，增强学生对密码应用的现实感和信息安全的紧迫性，强化信息安全意识，培养学生密码学工程实践能力。本课程从密码的基本概念和技术、特殊数字签名技术、密钥管理、电子现金与电子支付系统、安全电子选举系统、安全多方计算等密码应用以及密码法律保障等方面讲述如何解决密码学工程实践问题。

二、课程地位与目标

（一）课程地位：本课程是信息安全专业本科生的自主课程，它是继《密码学》课程之后开设的课程。《密码学》课程主要侧重于介绍密码算法和密码协议的基本原理，而本课程主要侧重密码算法的应用，培养学生密码学工程实践能力。

本课程支撑的毕业要求拆分指标点的具体描述。

2.4：能够应用相关密码学算法和协议的相关知识对具体应用系统解决方案进行比较分析、改进。

4.5：能对已有密码学复杂问题的解决方案进行研究，并提出新的密码学解决方案。

6.1：针对特定信息安全工程问题，分析其所需的相关密码技术、资源和工具。

9.2：了解密码相关的重要法律、法规及方针与政策，并在实践中自觉遵守。

（二）课程目标

1 教学目标：本课程要求学生掌握“密码应用”中的密码算法和协议的基本原理，了解国内外密码相关的法律法规，培养学生运用所学密码学算法和协议的相关知识，分析、解决和研究密码学工程实践问题的能力。本课程对毕业要求拆分指标点达成的支撑情况，详见表 1。

表 1 课程目标与毕业要求拆分指标点的对应关系

序号	课程目标	毕业要求拆分指标点			
		2.4	4.5	6.1	9.2
1	培养学生能够应用相关密码学算法和协议的知识对具体应用系统解决方案进行比较分析、改进的能力。	⊙			
2	培养学生能对已有密码学复杂问题的解决方案进行研究，并提出新的密码学解决方案的能力。		●		
3	培养学生能够针对特定信息安全工程问题，分析其所需的相关密码技术、资源和工具的能力。			⊙	
4	通过学习密码相关法律法规，帮助学生了解与本课程相关的重要法律、法规及方针与政策，并在实践中自觉遵守。				⊙

注：●：表示有强相关关系，◎：表示有一般相关关系，⊙：表示有弱相关关系

2 育人目标：本课程通过精选贴近生活以及新应用的密码学典型应用案例，使学生了解国内外密码算法的应用现状，增强学生信息安全意识。本课程包括密码法等相关法律法规专题，内容涉及《中华人民共和国网络安全法》（2017 年）、《密码法》（2020 年）等重要的法律法规。通过对这些法律法规解读和案例分析，使学生理解纯粹的密码技术不是绝对保障信息安全的，法律是保障信息安全的重要方式。有利于让学生充分认识到密码技术使用不当可能造成的严重危害和后果，从价值观层面进一步树立了学生的信息安全法律意识，培养学生理想信念、具有家国情怀、民族自信、有责任担当，具有职业素养、良好行为规范的人。

三、课程教学内容

分章节列出课程教学内容及对课程目标的支撑，详见表 2。

表 2 教学内容与课程目标的对应关系

章节名称	教学内容及重点（▲）、难点（★）	课程目标（√）			
		1	2	3	4
第一章 密码应用绪论	课程介绍（教学目的、教学内容和考核要求等）； 密码学基本知识（密码应用、分类、模型及密码分析）▲； 密码应用服务于信息安全； 基本密码学工具（加密技术、数字签名技术、Hash 函数、零知识证明、安全多方计算、MAC 技术和密钥交换技术等）▲。	√			
第二章 特殊数字签名技术	产生动机； 技术分类▲； 盲签名▲,★；代理签名；群签名▲,★；多重数字签名；同时签约；前向安全数字签名；不可否认签名▲,★；失败－终止数字签名；指定确认人的数字签名；批量签名、在线/离线签名、群盲签名、前向安全的群签名等。	√	√	√	
第三章 密钥管理技术	产生动机； 技术分类▲； 密钥管理的基本概念；密钥的协商与分发▲,★；密钥分割与共享▲,★；具	√	√	√	

	有等级性的密钥管理方法；具有真实性树的管理方法；密钥托管。				
第四章 电子现金与电子支付系统	产生动机； 电子现金系统▲,★：电子现金基础知识、电子现金协议、电子现金系统的安全需求； 电子支付系统安全概述▲,★：电子支付系统模型、电子支付系统分类、电子支付系统安全； 安全支付协议（SET 协议）▲,★：SET 安全支付系统组成、SET 支付安全性分析、SET 工作流程及应用； 应用案例。	√	√	√	
第五章 安全电子选举系统	产生动机； 技术分类▲； 简单投票协议；带有两个中央机构的投票协议；无需投票中心的投票协议； 经典协议：1、FOO 协议，2、Sensus 协议。	√	√	√	
第六章 安全多方计算	产生动机； 技术分类▲； 安全多方计算问题； 安全多方计算定义与模型； 一般安全多方计算协议▲,★：基于可验证秘密共享的 SMPC 协议、基于不经意传输的 SMPC 协议、基于同态加密的 SMPC 协议、基于 Mix-Match 的 SMPC 协议； 特殊安全多方计算及应用▲,★：电子投票、加密数据计算。	√	√	√	
第七章 密码相关法律	密码法▲,★等。				√

四、教授方法与学习方法指导

教授方法：以讲授为主，讨论和课设作业为辅。课内讲授采用探究教学、项目驱动、案例教学等多种教学方法与模式，结合多媒体、板书等教学手段，通过范例和视频演示讲授课程内容。以知识为载体，传授相关的思想和方法，引导学生掌握密码工程实践中涉及的密码协议和算法。课外作业则提出基本要求，引导学生根据场景要求分组完成一个具体密码工程实践问题解决方案的设计与实现。

学习方法：根据课程及学生学习特点，给出学习该门课程的指导和建议。可以包括体现本门课程特点的学习策略、学习技巧、自主学习指导、课程延伸学习资料获取途径及信息检索方法、教学网站及学习注意事项、学习效果自我检查方法指导等内容。

五、教学环节及学时分配

教学环节及各章节学时分配，详见表 3。

表 3 教学环节及各章节学时分配表

章节名称	教学内容	学时分配					合计
		讲授	习题	实验	讨论	其它	

第一章密码应用绪论	密码学基本知识（密码应用、分类、模型及密码分析）；密码应用服务于信息安全；基本密码学工具（加密技术、数字签名技术、Hash 函数、零知识证明、安全多方计算、MAC 技术和密钥交换技术）。	2					2
第二章特殊数字签名技术	产生动机；技术分类；盲签名；代理签名；群签名；多重数字签名；同时签约；前向安全数字签名；不可否认签名；失败－终止数字签名；指定确认人的数字签名；批量签名、在线/离线签名、群盲签名、前向安全的群签名等。	4			2		6
第三章密钥管理技术	产生动机；技术分类；密钥管理的基本概念；密钥的协商与分发；密钥分割与共享；具有等级性的密钥管理方法；具有真实性树的管理方法；密钥托管。	4			2		6
第四章电子现金与电子支付系统	产生动机；电子现金系统：电子现金基础知识、电子现金协议、电子现金系统的安全需求；电子支付系统安全概述：电子支付系统模型、电子支付系统分类、电子支付系统安全；安全支付协议（SET 协议）：SET 安全支付系统组成、SET 支付安全性分析、SET 工作流程及应用；应用案例。	4			2		6
第五章安全电子选举系统	产生动机；技术分类；简单投票协议；带有两个中央机构的投票协议；无需投票中心的投票协议；经典协议：1、FOO 协议，2、Sensus 协议。	2					2
第六章安全多方计算	产生动机；技术分类；安全多方计算问题；安全多方计算定义与模型；一般安全多方计算协议：基于可验证秘密共享的 SMPC 协议、基于不经意传输的 SMPC 协议、基于同态加密的 SMPC 协议、基于 Mix-Match 的 SMPC 协议；特殊安全多方计算及应用：电子投票、加密数据计算。	6					6
第七章密码相关法律	密码法等。	2					2
	总结和复习	2					2

合计		26			6		32

六、考核与成绩评定

课程成绩包括平时成绩和考试成绩两部分。

考核方式及成绩评定分布：期末考试占 80%。涵盖所学内容 90％以上；分为概念题（理论题）和设计分析题两部分。考试环节是对学生学习情况的全面检验，考查学生对密码应用基本概念、理论、技术及系统的分析与设计的能力，起到督促学生系统掌握课程主要教学内容的作用。平时成绩占 20%，反映学生的课堂表现、平时的信息接受、自我约束，考察学生对已学知识掌握的程度以及自主学习的能力。平时成绩评定的主要依据包括：课程的出勤情况、课堂的基本表现（含课堂测验）、课外大作业情况。

本课程各考核环节的比重及对毕业要求拆分点的支撑情况，详见表 4。

表 4 考核方式及成绩评定分布表

考核方式	所占比例（%）	主要考核内容及对毕业要求拆分指标点的支撑情况
平时成绩	课设作业 15%	引导学生复习和深入理解讲授的内容（基本方法、基本理论、基本工具），锻炼运用所学知识选择一个具体密码学应用问题设计和实现解决方案，通过对课设作业的文档评审、需求分析、算法设计、实现源码和效果展示的完成质量评价，对应课程目标 1,2 和 3 达成度的考核。
	随堂练习 5%	考查学生课堂的参与度，对所讲内容的基本掌握情况，通过考核学生课堂练习参与度（含出勤情况）及其完成质量，对应课程目标 1,2 和 3 达成度的考核。
考试成绩	80	对规定考试内容掌握的情况，对课程目标 1、课程目标 2、课程目标 3、课程目标 4 达成度的评价提供支持。

七、考核环节及质量标准

本课程各考核环节及质量标准，详见表 5。

表 5 考核环节及质量标准

考核方式	评　分　标　准				
	A	**B**	**C**	**D**	**E**
	90～100	**80～89**	**70～79**	**60～69**	**< 60**
课设作业	报告文档格式规范、文字规范、术语准确、注释齐全；问题分析准确；提出算法完全解决问题需求；源码符合算法设计、齐全；效果展示符合预期	报告文档格式较规范、文字较规范、术语较准确、注释较齐全；问题分析较准确；提出算法较好解决问题需求；源码较符合算法设计或较齐全；效果展示较符合预期	报告文档格式较规范、文字较规范、术语较准确、注释较齐全；问题分析较准确；提出算法基本解决问题需求；源码基本符合算法设计或较齐全；效果展示基本符合预期	报告文档格式基本规范、文字基本规范、术语基本准确、注释基本齐全；问题分析基本准确；提出算法基本解决问题需求；源码基本符合算法设计或较齐全；效果展示基本符合预期	不满足 D 要求
随堂练习	上课全勤、积极回答教师随堂提问、积极参与讨论	上课全勤、较积极回答教师随堂提问、较积极参与讨论	上课全勤、较积极回答教师随堂提问、能参与讨论	上课缺席不超过 2 次、能回答教师随堂提问、能参与讨论	不满足 D 要求
期末考试	很好地掌握教学内容涉及的基本概念、理论、方法，且具备很强的综合运用所学知识解决复杂问题的能力。	较好地掌握教学内容涉及的基本概念、理论、方法，且具备较强的综合运用所学知识解决复杂问题的能力。	较好地掌握教学内容涉及的基本概念、理论、方法，且具备一定的综合运用所学知识解决复杂问题的能力。	基本掌握教学内容涉及的基本概念、理论、方法，且基本能具备运用所学知识解决复杂问题。	不满足 D 要求
评分标准（A～E）：主要填写对教学内容中的基本概念、理论、方法等方面的掌握，及综合运用理论知识解决复杂问题能力的要求。					

制定者：杨宇光

批准者：张建标

2020 年 7 月

“学术写作”课程教学大纲

英文名称：Academic Writing

课程编号：0010711

课程性质：自主课程

学分：1.0　　学时：16

适用对象：信息安全（实验班）专业本科生

先修课程：

教材及参考书：

[1] 张孙玮，吕伯昇，张 迅，科技论文写作入门(第五版)，化学工业出版社，2017 年 2 月

[2] 李玉浩，Writing English Research Papers 英语学术写作概论，知识产权出版社，2013 年 8 月

[3] 罗伊娜·默里等，学术写作手册：一种新方法，上海教育出版社，2011 年 6 月

[4] 王雨磊，学术论文写作与发表指引， 中国人民大学出版社，2017 年 9 月

[5] 海伦· 索德，学术写作指南：100 位杰出学者的写作之道，人民教育出版社，2018 年 12 月

一、课程简介

学术写作是计算机学院为信息安全专业本科生开设的专业选修课课程类型。本课程的任务是通过学习学术写作，为学生最后撰写毕业论文和发表科技论文打下良好基础，并掌握撰写毕业论文方法、技巧和能力。论文是展现研究成果的一种重要方式，也是科研工作者与同行交流的一个重要途经，学术论文写作方法和规范是学生应该掌握的基本知识和基本技能，为将来从事科学研究打下基础。并且掌握口头、书面与同行和相关人员进行有效沟通和交流的能力。教学内容重点：期刊评价标准，论文管理工具的使用, 如何写综述，撰写开题报告，毕业论文的写作。教学内容的难点：论文管理工具的使用, 摘要的主要内容,如何提取关键词。

二、课程地位与教学目标

（一）课程地位：学术论文写作是科研成果展现，与学术同行交流的重要途经之一。学术论文的写作方法和规范是学生应该掌握的基本知识和基本技能。通过学习本课程，掌握学术论文写作，英文论文写作以及毕业论文写作的要求，学会如选题，如何搜集和管理文献，如何写摘要，如何提取关键词，如何发表论文，如何回答编辑的问题，以及如何撰写毕业论文。

3.3 能利用多种资源开展文献检索和资料查询

10.3 能够在多学科团队中独立完成一个成员相应的任务，并能进行有效的合作

11.1 能通过口头、书面与同行和相关人员进行有效沟通和交流

11.2 具有一定的英语阅读能力，能够利用一门外语进行专业相关的口头和书面交流，能有效利用外文资料

（二）课程目标

教学目标：使学生掌握学术写作中的基本概念、基本理论、基本方法，在学会如何撰写学术论文。该目标分解为 4 个子目标，子目标与毕业要求拆分指标点得关系如下表所示。

表 1 课程目标与毕业要求拆分指标点对应关系

序号	课程目标	毕业要求拆分指标点			
		3.3	10.3	11.1	11.2
1	学会收集，管理和使用学术论文。	⊙			
2	掌握学术写作的方法。		⊙		
3	掌握英文论文写作以及与编辑和同行交流的能力				●
4	掌握毕业论文写作的方法，包括如何开题和毕业答辩			●	

● 表示表示有强相关关系， ◎： 表示有一般相关关系，⊙： 表示有弱相关关系

2 育人目标：科技论文写作能够将我们国家科技工作者的成果展示给国内外科技工作者、为后来者研究提供基础，促进我国科技工作的进步，让学生在学习中有名族自豪感和自信心。

三、课程教学内容

分章节列出课程教学内容及对课程目标的支撑，详见表 2。

表 2 教学内容与课程目标的对应关系

章节名称	教学内容及重点（▲）、难点（★）	课程目标（√）			
		1	2	3	4
第一章如何搜集和使用材料	论文的搜集主要包括两方面，一方面是搜索引擎的使用（▲）。另一方面是期刊和会议的评价标准。主要介绍了三种搜索引擎的使用：CNKI 中文中国知网，Web of science 搜索引擎以及 IEEE 搜索引擎。介绍论文评价标准（▲），论文的引用量、期刊的影响引子、JCR 期刊分区、中科院期刊分区表以及中国计算机学会推荐国际学术期刊目录。会议论文的评价标准主要是中国计算机学会推荐国际学术会议目录。材料的使用方面主要介绍了论文管理工具 Zotero、Citavi、Endnote、Mendele 的使用（▲）（★），如何管理文献，如何同步数据，如何导出参考目录。	√			
第二章论文的综述摘要关键词	综述主要介绍研究的背景（▲），研究的问题的关键性，拟解决的关键问题，解决关键问题重要意义，结合科学研究发展趋势来论述科学意义等等。摘要主要提炼出本文的主要研究内容（▲）（★），主要的研究方法或者使用的技术以及方法或者技术主要的优点是什么。论文的关键词（▲）一般要体现研究的内容、使用的方法、突破点等等。		√	√	
第三章英文学术论文写作	英文论文写作之前的准备，尽早的学会阅读英文论文（▲）。英文论文写作中可以使用的工具（▲），百度翻译的使用，grammarly 等英语写作检查工具的使用，曼彻斯特大学学术短语库等等。科技英语写作（★）中要注意的问题（▲），比如英语的语态与句式。在这个过程中要求学生完成一篇英文论			√	√

	文摘要的写作。				
第四章投稿与改稿	详细介绍论文投稿的流程，如何查询和使用特定期刊的模板（▲）。回复审稿人的问题的时候主要将审稿人的问题一一提炼出来并分别回答（▲）。当审稿人要求修改的时候，如何回应审稿人的意见。如何使用审阅功能来保存修改痕迹，那些修改痕迹需要被保留，那些痕迹不需要被保留。如何像编辑申诉，当论文质量很高却被审稿人拒绝的时候，如何才能向编辑申诉，并且和写申诉信（▲）（★）。			√	√
第五章毕业论文撰写	开题报告（▲）、文献综述的写作方法（▲），掌握学校规范编制毕业论文的注释、参考文献以及引文的主要方法（▲）（★）。			√	

四、教授方法与学习方法指导

教授方法：主要以讲授的方式进行，同时让学生自己同学动手写作来体验学术写作。课内讲授推崇研究型教学，以知识为载体，传授相关的思想和方法，引导学生学会学术写作。

学习方法：养成探索的习惯，特别是重视对基本自主学习，能够主动的学习各种内容，在理论指导下进行实践，注意从实际问题入手，能够自己动手来实践。明确学习各阶段的重点任务，做到课前预习，课中认真听课，积极思考，课后认真复习，不放过疑点，充分利用好教师资源和同学资源。认真阅读参考书的相关内容，从全局的角度，深入理解概念，不要死记硬背。

五、教学环节及学时分配

教学环节及各章节学时分配，详见表 3。

表 3 教学环节及各章节学时分配表

章	主要内容	学时分配				合计
		讲课	习题	讨论讨	其他	
1	如何搜集和使用材料	2	0	0	0	2
2	论文的综述摘要关键词	2	2	0	0	4
3	英文学术论文写作	4	2	0	0	6
4	投稿与改稿	2	0	0	0	2
5	毕业论文撰写	2	0	0	0	2
合计		12	4	0	0	16

六、考核与成绩评定

课程考核以考核学生对课程目标达成为主要目的，检查学生对教学内容的掌握程度为重要内容。课程成绩包括平时成绩和考察成绩两部分。

考核方式及成绩评定分布：写明该门课程考核环节及各环节的成绩占比，各考核环节、考核内容对毕业要求拆分指标点的支撑情况。

平时成绩 40%（作业等 20%，其它 20%），期末考察 60%。

平时成绩中的其它 20%主要反应学生的课堂表现、平时的信息接收、自我约束。成绩评定的主要依据包括：课程的出勤率、课堂的基本表现（如课堂测验、课堂互动等；作业

等的 20%主要是课堂作业和课外作业，主要考察学生对已学知识掌握的程度以及自主学习的能力。

考察成绩 60%为对学生学习情况的全面检验。强调考核学生对基本概念、基本方法、基本理论等方面掌握的程度，及学生运用所学理论知识解决复杂问题的能力。

本课程各考核环节的比重及对毕业要求拆分点的支撑情况，详见表 4。

表 4 考核方式及成绩评定分布表

考核方式	比例（%）	主要考核内容
作业	20	相关作业的完成质量，对应课程目标 1、课程目标 2 达成度的考核。
随堂练习	20	课堂练习参与度及其完成质量，对应课程目标 1、课程目标 2 达成度的评价提供支持。
期末考察	60	对规定学习内容掌握的情况，对应课程目标 1、课程目标 2、课程目标 3、课程目标 4 达成度的评价提供支持。

七、考核环节及质量标准

本课程各考核环节及质量标准，详见表 5。

表 5 考核环节及质量标准

考核方式	评分标准				
	A	B	C	D	E
	90～100	80～89	70～79	60～69	< 60
作业	语言流畅有明确表达中心，关键词中心思想对应	语言基本流畅，有表达出中心思想，关键词能够没有明确对应关系	语言基本流畅，但看不出表达中心，关键词能不能明确	语言不够流畅，有语法错误，没有明确中心思想，关键词不明确	不满足 D 要求
随堂练习	全勤，完成两次高质量课堂练习	全勤，完成两次课堂练习	全勤，完成一次课堂练习，完成质量一般。	全勤，没有完成课堂练习。	不满足 D 要求
期末考察	格式规范，各部分内容比例协调，有明确表达中心。	格式基本规范，各部分内容比例基本协调，能看出表达中心。	格式基本规范，各部分内容比例不够协调，能看出明确表达中心。	格式不规范，各部分内容比例不够协调，不能看出明确表达中心。	不满足 D 要求

制定者：陈渝文

批准者：张建标

2020 年 7 月

“学科前沿”课程教学大纲

英文名称：Academic Frontiers

课程编码：0010709

课程性质：自主课程

学分：1.0　　学时：16

面向对象：信息安全（实验班）专业本科生

先修课程：

教材及参考书：

本课程为前沿讲座，讲授内容随着本学科个研究方向的发展动态而不断调整，无固定教材，参考书主要为本学科国内外核心期刊和会议集。

一、课程简介

本课程主要介绍信息安全领域的各个分支方向，深入介绍每个方向的前沿理论和前沿工作，重点涉及密码学、网络安全、数据安全、软件安全、人工智能安全、分布式安全等方向的前沿。

二、课程地位与目标

（一）课程地位：本课程是信息安全专业的专业必修课。旨在引导学生对本专业的不同方向的前沿科技动态和科研工作有一定的认识；给学生提供了解科技前沿、与高水平学者对话、思考科技发展和未来研究方向的机会，培养其对于科研工作的理解，提升其科技发展的眼界。

主要为毕业要求第 3.3、7.1、11.3、13.1 的实现提供支持。

对于毕业要求 3.3，培养学生通过多种查询手段，开展文献检索和资料查询，从而对前沿领域有一定认识和理解。

对于毕业要求 7.1，使学生了解前沿发展对于社会和产业的影响。

对于毕业要求 11.3，培养学生对于国内外研究前沿工作和发展情况的掌握能力，能够将现有学习和未来方向的选择与国际科技发展的大背景相结合。

对于毕业要求 13.1，培养学生对于前沿的关注能力，让学生认识到信息安全学科是一个发展迅速的学科，能够拥有自主学习和终身学习的意识。

（二）课程目标

1 教学目标：使学生掌握信息安全的主要分支、前沿方向、前沿理论、前沿工作，深入理解学科前沿和学科基础之前的区别和联系。该目标分解为以下子目标：

课程目标 1：掌握信息安全的研究方向和前沿领域的主要分支以及基本概念。

课程目标 2：掌握信息安全各研究方向的最新发展方向及其影响。

课程目标 3：熟悉本学科各研究方向的最新研究成果和研究方法。

课程目标 4：培养学术视野和创新精神，启发科研思路，提高学生的科研能力。

本课程对毕业要求拆分指标点达成的支撑情况，详见表 1。

表 1 课程目标与毕业要求拆分指标点的对应关系

序号	课程目标	毕业要求拆分指标点			
		3.3	7.1	11.3	13.1
1	掌握信息安全的研究方向和前沿领域的主要分支以及基本概念	●			
2	掌握信息安全各研究方向的最新发展方向		●		
3	熟悉本学科各研究方向的最新研究成果和研究方法			⊙	
4	培养学术视野和创新精神，启发科研思路，提高学生的科研能力				◎

注：●：表示有强相关关系，◎：表示有一般相关关系，⊙：表示有弱相关关系

2 育人目标：本课程能够提升学生对于信息安全技术重要性的理解，理解信息技术安全对于行业乃至国家安全的重要作用，在今后的学习、工作中能自觉地维护信息安全，以适应我国科技发展的需要。

三、课程教学内容

分章节列出课程教学内容及对课程目标的支撑，详见表 2。

表 2 教学内容与课程目标的对应关系

章节名称	教学内容及重点（▲）、难点（★）	课程目标（√）			
		1	2	3	4
第一章 密码学讲座	介绍密码学方向的主流理论和研究方法★，重点介绍密码学界的热点问题和前沿工作▲★，介绍密码学界的国内外知名学者，最后对密码学的应用有初步介绍。	√	√	√	√
第二章 网络安全讲座	介绍网络安全面临的主要威胁及安全事件，重点介绍网络安全防护的主流手段和前沿领域▲★，可以介绍网络安全界的国内外知名公司等最新内容。	√	√	√	√
第三章 数据安全讲座	介绍数据安全的核心要素，介绍最新的大数据安全热点问题▲★，以及数据安全的未来发展方向。	√	√	√	√
第四章 软件安全讲座	介绍软件安全的主要理论和分支，软件安全目前面临的困境，重点介绍软件安全研究在学术界和工业界的进展以及未来方向▲★。	√	√	√	√
第五章 人工智能安全讲座	介绍人工智能的发展历程和最新的发展浪潮，重点介绍目前人工智能技术应用所面临的安全风险▲★。	√	√	√	√
第六章 分布式安全讲座	介绍分布式系统的安全概念，关键问题，重点介绍以区块链为代表的新一代分布式技术的热点安全问题▲★。	√	√	√	√

四、教授方法与学习方法指导

教授方法：以讲座方式，进一步加强学生的自学能力和信息获取能力。讲座讲授推崇研究型教学，以知识为载体，传授相关的思想和方法，引导学生踏着大师们研究步伐前进。

学习方法：养成探索的习惯，明确学习各阶段的重点任务，做到课前预习，课中认真听课，积极思考，课后认真总结和拓展，充分利用好教师资源和同学资源。仔细研读文献，适当选读参考书的相关内容，深入理解相关领域。

五、教学环节及学时分配

教学环节及各章节学时分配，详见表 3。

表 3 教学环节及各章节学时分配表

章节名称	教学内容	学时分配					合计
		讲授	习题	实验	讨论	其它	
第一章	密码学方向讲座	4	0	0	0	0	4
第二章	网络安全方向讲座	4	0	0	0	0	4
第三章	数据安全方向讲座	2	0	0	0	0	2
第四章	软件安全方向讲座	2	0	0	0	0	2
第五章	人工智能安全方向讲座	2	0	0	0	0	2
第六章	分布式安全方向讲座	2	0	0	0	0	2
合计		16	0	0	0	0	16

六、考核与成绩评定

讲座报告：主要培养学生对讲座方式的学习能力以及课下进行自学的能力。本课程各考核环节的比重及对毕业要求拆分点的支撑情况，详见表 4

表 4 考核方式及成绩评定分布表

考核方式	占比（%）	主要考核内容及对毕业要求拆分指标点的支撑情况
讲座报告	100	相关报告的完成质量，对应课程目标达成度的考核，支撑毕业要求 3.3、7.1、11.3、13.1

七、考核环节及质量标准

本课程各考核环节及质量标准，详见表 5。

表 5 考核环节及质量标准

考核方式	评分标准				
	A	B	C	D	E
	90～100	80～89	70～79	60～69	< 60
报告	讲座理解透彻，课下查询文献丰富且质量较高，自我思考深入，在讲座基础上有很多个人自学内容，对于讲座涉及相关技术有很强的个人见解	讲座理解深入，课下查询文献丰富，对讲座内容有深入思考，有一定的个人见解	能够理解讲座核心内容，课下查询文献有一定积累，对讲座相关前沿技术做了较多整理归纳，对讲座相关内容有一定思考	讲座有一定理解，课下查询文献有限，对讲座相关前沿技术做了一定的整理归纳	不满足 D 要求
评分标准（A～E）：主要填写对教学内容中的基本概念、理论、方法等方面的掌握，及综合运用理论知识解决复杂问题能力的要求。					

制定者：于海阳

批准者：张建标

2020 年 7 月