信息安全基础 教学大纲

Information Security Subject Syllabus

一、课程信息 Subject Information

课程编号: Subject ID	3100213023	开课学期: Semester	2
课程分类: Category	专业教育 PA	所属课群: Section	工程能力 EA
课程学分: Credit Points	3	总学时/周: Total Hours/Weeks	48/8
理论学时: LECT. Hours	32	实验学时: EXP. Hours	16
PBL 学时: PBL Hours	0	实践学时/周: PRAC. Hours/Weeks	0
开课学院: College	东北大学 悉尼智能科技学院 Sydney Smart Technology College Northeastern University	适用专业: Stream	计算机科学与技术 CST
课程属性: Pattern	选修 Elective	课程模式: Mode	互认 EQV
中方课程协调人: NEU Coordinator	袁晓铭 Yuan Xiaoming	成绩记载方式: Result Type	百分制 Marks
先修课程: Requisites	计算机网络 Computer Networks		
英文参考教材: EN Textbooks	William Stallings (2020). Cryptography and Network Security – Principles and Practice (8th Edition).		
中文参考教材: CN Textbooks	Willliam Stallings 著，白国强等译，《网络安全基础-应用与标准（第6版）》，清华大学出版社，2019		
教学资源: Resources	www.WilliamStallings.com/Cryptography		
课程负责人(撰写人): Subject Director	于七龙 Yu Qilong	提交日期: Submitted Date	4/8/2023
任课教师(含负责人): Taught by	于七龙 Yu Qilong		
审核人: Checked by	韩鹏	批准人: Approved by	史闻博
		批准日期: Approved Date	4/8/2023

二、教学目标 Subject Learning Objectives (SLOs)

注：毕业要求及指标点可参照悉尼学院本科生培养方案，可根据实际情况增减行数

Note: GA and index can be referred from undergraduate program in SSTC website. Please add/reduce lines based on subject.

整体目标: Overall Objective	信息安全基础是计算机相关专业的专业选修课，其目的是使学生掌握信息安全的基本知识和概念以及安全理论与应用技术，树立信息安全防范意识，并在实际应用环境下能够运用所学信息安全技术和管理理论分析、判断和解决所遇到的信息安全问题。 Information security is a professional elective course of computer-related major, the purpose of which is to enable students to master the basic knowledge and concepts of information security, as well as the security theory and application technology, to establish the awareness of information security prevention, and to be able to use the information security technology and management theory to analyze, judge and solve the information security problems encountered in the actual application environment.	
（1）专业目标: Professional Ability	1-1	了解网络安全形势，增强网络安全防范意识，理解网络安全对个人与国家的影响。 Understand the network security situation, enhance the awareness of network security prevention, understand the impact of network security on individuals and countries
	1-2	了解信息安全的发展历史，理解信息安全的研究内容，掌握信息安全基本概念及信息安全的目标。 Understand the history of information security, understand the research content of information security, master the basic concept of information security and the goal of information security.
	1-3	掌握密码体制、消息认证、数字签名、用户认证、密钥管理、安全协议等信息安全的基本知识与技术。 Master the basic knowledge and technology of information security such as password system, message authentication, digital signature, user authentication, key management, security protocol, etc
	1-4	具备信息系统安全保障能力，能在实际应用环境下运用所学的信息安全知识分析、判断和解决所遇到的信息安全问题。 With information system security capability, can use the information security technology and theoretical analysis, judgment and solve the information security problems encountered in the practical application environment
	1-5	培养科学与工程应用的意识和素质，培养学生的探索精神和创新能力。 Cultivate the consciousness and quality of science and engineering application, and cultivate students' exploration spirit and innovation ability

（2）德育目标: Essential Quality	2-1	信息安全学习与实践过程中，应当遵循法律法规与工程伦理原则。 In the process of information security learning and practice, laws and regulations and engineering ethics principles should be followed.
	2-2	认知当前全球，信息安全的发展对提升中国工程关键技术及核心竞争力的重要意义。 Enhance the innovation and entrepreneurship ability of engineering science and technology talents and construct the education network of industry-university cooperation to improve the core competitiveness of China in the global development.

课程教学目标与毕业要求的对应关系 Matrix of GA & SLOs

毕业要求 GA	指标点 GA Index	教学目标 SLOs
1、 工程知识：能够将数学、自然科学、工程基础和专业知识用于解决复杂工程问题。 GA1. Engineering Knowledge: Apply knowledge of mathematics, natural science, engineering fundamentals and an engineering specialization to the solution of complex engineering problems.	指标点 1-5：掌握在计算机科学与技术专业的相关领域进行工程设计、技术创新的能力。	1-3，1-4，1-5
3、设计/开发解决方案：能够设计针对复杂工程问题的解决方案，设计满足特定需求的系统、单元或流程，并能够在设计环节中体现创新意识，考虑社会、健康、安全、法律、文化以及环境等因素。 Design/Development of Solutions: Design solutions for complex engineering problems and design systems, components or processes that meet specified needs with appropriate consideration for public health, and safety, cultural, societal and environmental considerations.	指标点 3-1：能够设计针对本专业相关复杂工程问题的解决方案，能够设计和开发实现特定功能、满足特定需求的计算机、软件或网络系统。 3-1: Capable of designing solutions to complex engineering problems related to the major, and capable of designing and developing computers, software or network systems that can function specifically and meet specific requirements.	1-3，1-4，1-5
	指标点 3-3：能够在设计和开发的各个环节中综合考虑社会、健康、安全、法律、文化以及环境等因素。 3-3: Capable of taking social, health, safety, legal, cultural and environmental factors in consideration during all aspects of design and development.	1-4，1-5，2-1，2-2

4、研究：能够基于科学原理并采用科学方法对复杂工程问题进行研究，包括设计实验、分析与解释数据、并通过信息综合得到合理有效的结论。 Investigation: Conduct investigations of complex problems using research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of information to provide valid conclusions.	指标点 4-1：能够基于科学原理并采用科学方法，在本专业相关理论指导下对复杂工程问题设计实验进行研究。 Capable of designing experiments and doing research on complex engineering problems based on scientific principles and scientific methods, under the guidance of related theories of the major.	1-5，2-2

三、教学内容 Content (Topics)

注：以中英文填写，各部分内容的表格可根据实际知识单元数量进行复制、扩展或缩减

Note: Filled in both CN and EN, extend or reduce based on the actual numbers of knowledge unit

(1) 理论教学 Lecture

知识单元序号: Knowledge Unit No.	1		支撑教学目标: SLOs Supported	1-2,1-3
知识单元名称 Unit Title	课程简介与绪论 Introduction			
知识点: Knowledge Delivery	课程简介 Introductions			
	网络安全形势与法律基础 Cybersecurity situation and legal basis			
学习目标: Learning Objectives	了解: Recognize	网络安全形势与相关法律基础 Cybersecurity landscape and the legal basis		
	理解: Understand	OSI 安全体系结构与信息安全目标 OSI security architecture and information security objectives		
	掌握: Master	信息安全基本概念 Basic concepts of information security		
德育目标 Moral Objectives	理解网络安全对个人与国家的影响 Understand the impact of cybersecurity on individuals and countries			
重点: Key Points	信息安全基本概念与目标 Basic concepts and objectives of information security			
难点: Focal points	攻击类型及分析 Type of attack and analysis			

知识单元序号: Knowledge Unit No.	2	支撑教学目标: SLOs Supported	1-2，1-3
知识单元名称 Unit Title	对称密码　Symmetric password		
知识点: Knowledge Delivery	密码学的发展历史，密码学的基本概念，密码系统的分类，经典密码学 The development history of cryptography, the basic concept of cryptography, the classification of cryptography system, classical cryptography		
	对称分组密码，数据加密标准 DES，3DES，高级加密标准 AES Symmetric grouping password, data encryption standard DES, 3DES, advanced encryption standard AES		
	分组密码工作模式 Group password working mode		
	随机数和伪随机数，流密码和 RC4 Random numbers and pseudo-random numbers, stream passwords and RC4s		
学习目标: Learning Objectives	了解: Recognize	密码学的发展历史 The history of cryptography	
	理解: Understand	理解代替与置换技术 Thesubstitution and replacement techniques	
	掌握: Master	对称密码，分组密码工作模式，随机数发生器 Symmetric password, group password working mode, random number generator	
德育目标 Moral Objectives	认知当前全球，信息安全的发展对提升中国工程关键技术及核心竞争力的重要意义。 Enhance the innovation and entrepreneurship ability of engineering science and technology talents and construct the education network of industry-university cooperation to improve the core competitiveness of China in the global development.		
重点: Key Points	对称密码，分组密码工作模式，随机数发生器 Symmetric password, group password working mode, random number generator		
难点: Focal points	对称密码，分组密码工作模式，随机数发生器 Symmetric password, group password working mode, random number generator		

知识单元序号: Knowledge Unit No.	3	支撑教学目标: SLOs Supported	1-2，1-3
知识单元名称 Unit Title	公钥密码 The public key password		
知识点: Knowledge Delivery	公钥密码体制基本原理 The basic principle of public key cryptography system		
	RSA 等公钥密码算法 Public key cryptography algorithms such as RSA		

	Diffie-Hellman 密钥交换 Diffie-Hellman key exchange	
学习目标: Learning Objectives	了解: Recognize	公钥密码 The basic principle of public key
	理解: Understand	公钥密码体制基本原理 The basic principle of public key cryptography system
	掌握: Master	掌握 RSA、Diffie-Hellman 等公钥算法 Master public key algorithms such as RSA and Diffie-Hellman
德育目标 Moral Objectives	认知当前全球，信息安全的发展对提升中国工程关键技术及核心竞争力的重要意义。 Enhance the innovation and entrepreneurship ability of engineering science and technology talents and construct the education network of industry-university cooperation to improve the core competitiveness of China in the global development.	
重点: Key Points	公钥密码体制原理及其与对称加密体制区别 The principle of public key cryptography and its difference from symmetric encryption system	
难点: Focal points	数论基础 The basis of number theory	

知识单元序号: Knowledge Unit No.	4	支撑教学目标: SLOs Supported	1-3，1-4，1-5
知识单元名称 Unit Title	数据完整性 Data integrity		
知识点: Knowledge Delivery	哈希函数 Hash function		
	消息认证码 MAC		
	数字签名 Digital signature		
学习目标: Learning Objectives	了解: Recognize	哈希函数原理应用 The principle of hash function is applied	
	理解: Understand	消息认证码原理及用途 The principle and purpose of message authentication code	
	掌握: Master	掌握数字签名方案 The digital signature scheme	
德育目标 Moral Objectives	认知当前全球，信息安全的发展对提升中国工程关键技术及核心竞争力的重要意义。 Enhance the innovation and entrepreneurship ability of engineering science and technology talents and construct the education network of industry-university cooperation to improve the core competitiveness of China in the global development.		

重点: Key Points	哈希函数 Hash function
难点: Focal points	数字签名方案 The digital signature

知识单元序号: Knowledge Unit No.	5	支撑教学目标: SLOs Supported	1-3，1-4，1-5
知识单元名称 Unit Title	互信 Mutual trust		
知识点: Knowledge Delivery	基于对称加密的密钥分配 Key allocation based on symmetric encryption		
	基于非对称加密的密钥分配 Key allocation based on asymmetric encryption		
	用户认证 User authentication		
学习目标: Learning Objectives	了解: Recognize	公钥接触设施 PKI	
	理解: Understand	理解利用非对称密码分配对称密钥的技术问题 Understand the technical problems of assigning symmetric keys using asymmetric passwords	
	掌握: Master	公钥分配的方法及风险 Methods and risks for public key allocation	
德育目标 Moral Objectives	认知当前全球，信息安全的发展对提升中国工程关键技术及核心竞争力的重要意义。 Enhance the innovation and entrepreneurship ability of engineering science and technology talents and construct the education network of industry-university cooperation to improve the core competitiveness of China in the global development.		
重点: Key Points	Kerberos 协议；X.509 证书 Kerberos, X.509		
难点: Focal points	Kerberos 协议；X.509 证书 Kerberos, X.509		

知识单元序号: Knowledge Unit No.	6	支撑教学目标: SLOs Supported	1-3，1-4，1-5
知识单元名称 Unit Title	网络与 Internet 安全 Network and Internet security		
知识点: Knowledge Delivery	网络访问控制 Network access control		
	传输层安全 The transport layer security		
	电子邮件安全 E-mail security		
	IP 安全		

	IP security	
学习目标: Learning Objectives	了解: Recognize	无线网络安全 Wireless network security
	理解: Understand	传输层安全、电子邮件安全、IP 安全机制原理机制 Transport layer security, e-mail security, IP security mechanism principle mechanism
	掌握: Master	SSL, S/MIME, IPSec SSL, S/MIME, IPSec
德育目标 Moral Objectives	认知当前全球，信息安全的发展对提升中国工程关键技术及核心竞争力的重要意义。 Enhance the innovation and entrepreneurship ability of engineering science and technology talents and construct the education network of industry-university cooperation to improve the core competitiveness of China in the global development.	
重点: Key Points	SSL, S/MIME, IPSec SSL, S/MIME, IPSec	
难点: Focal points	SSL, S/MIME, IPSec SSL, S/MIME, IPSec	

知识单元序号: Knowledge Unit No.	7	支撑教学目标: SLOs Supported	1-3，1-4，1-5
知识单元名称 Unit Title	系统安全 System security		
知识点: Knowledge Delivery	常见计算机病毒的特征及原理 Characteristics and principles of common computer viruses		
	入侵检测原理 IPS		
	防火墙的安全策略 Firewall		
学习目标: Learning Objectives	了解: Recognize	了解计算机病毒的定义、特征．病毒程序的构成；知道病毒的传播途径、类型等 The definition and characteristics of computer viruses. The composition of the virus program	
	理解: Understand	入侵检测 IPS	
	掌握: Master	防火墙的安全策略 Firewall	
德育目标 Moral Objectives	认知当前全球，信息安全的发展对提升中国工程关键技术及核心竞争力的重要意义。 Enhance the innovation and entrepreneurship ability of engineering science and technology talents and construct the education network of industry-university cooperation to improve the core competitiveness of China in the global development.		
重点:	防火墙的安全策略		

Key Points	Firewall
难点: Focal points	防火墙的安全策略 Firewall

四、教学安排 Teaching Schedule

注：可根据实际情况增减行数

Note: Please add/reduce lines based on subject.

教学内容 Teaching Content	学时(周)Hour(Week)			
	理论 LECT.	实验 EXP.	实践 PRAC.	PBL
绪论 Introduction	2	0	0	0
对称密码 Symmetric password	10	2	0	0
公钥密码 The public key password	6	0	0	0
数据完整性 Data integrity	2	0	0	0
互信 Mutual trust	4	0	0	0
网络与 Internet 安全 Network and Internet security	6	12	0	0
系统安全 System security	2	2	0	0
总计 Total	32	16	0	0

五、教学方法 Teaching Methodology

注：可根据实际情况增减行数或修改内容

Note: Please add/reduce lines or revise content based on subject.

勾选 Check	教学方法与特色 Teaching Methodology & Characters
☑	多媒体教学：基于信息化设备的课堂教学 Multi-media-based lecturing
☑	实践能力传授：理论与行业、实际案例相结合 Combining theory with industrial practical problems
☑	课程思政建设：知识讲授与德育相结合 Knowledge delivery with ethic education
☑	PBL 教学：问题驱动的分组学习与交流 Problem-based learning

□	其他:单击或点击此处输入文字。 Other:单击或点击此处输入文字。

六、成绩评定 Assessment

注：可根据实际情况增减行数或修改内容

Note: Please add/reduce lines or revise content based on subject.

考核环节: Assessment Content	平时 Behavior	环节负责人: Director	于七龙
给分形式: Result Type	百分制 Marks	课程总成绩比重(%): Percentage (%)	20
考核方式: Measures	满分 100 分，以学生平时考勤、课堂表现、课堂教师随机提问，学生平时作业完成情况综合评定，其中，学生考勤占比 50%，平时课堂表现、课堂教师随机提问占比 20%, 学生平时作业(课前预习作业、课后作业)完成情况占比 30%. The full score is 100. Students' attendance, classroom performance, random questions from teachers, and students' homework completion are comprehensively evaluated. Among them, students' attendance accounts for 50%, classroom performance and random questions from teachers account for 20%, and students' homework (preview homework before class and homework after class) accounts for 30%.		

考核环节: Assessment Content	实验 Experiment	环节负责人: Director	于七龙
给分形式: Result Type	百分制 Marks	课程总成绩比重(%): Percentage (%)	30
考核方式: Measures	满分 100 分，通过 PBL 实验报告记录学生成绩，按照学生的报告完成情况和贡献程度酌情给分，抄袭、给他人抄袭或未交实验报告不得分。 The full score is 100, and the students' scores are recorded through PBL experimental report. According to the students' report completion and contribution degree, the score is given. Plagiarism, plagiarism to others or failure to hand in the experimental report will not be scored.		

考核环节: Assessment Content	期末 Final	环节负责人: Director	于七龙
给分形式: Result Type	百分制 Marks	课程总成绩比重(%): Percentage (%)	50
考核方式: Measures	满分 100 分，通过批阅期末考试试卷给出学生成绩。 The full score is 100, and students' scores are given according to the final examination.		

七、改进机制 Improvement Mechanism

注：未尽事宜以教学团队以及学院教学指导委员会商定为准。

Note: Matters not covered in this file shall be determined by TAB of SSTC, NEU.

教学大纲改进机制 Subject Syllabus Improvement Mechanism			
考核周期(年): Check Period (YR)	4	修订周期(年): Revise Period (YR)	4
改进措施: Measures	课程负责人根据课程教学内容与人才培养目标组织课程团队讨论并修改教学大纲，报分管教学工作副院长审核后由执行院长批准。 The subject coordinator shall be responsible for the syllabus discussion and improvement, and the revised version shall be submitted to deputy dean (teaching affairs) for reviewing then to executive dean for improvement.		
成绩评定改进机制 Assessment Improvement Mechanism			
考核周期(年): Check Period (YR)	1	修订周期(年): Revise Period (YR)	1
改进措施: Measures	课程负责人根据课程教学内容、课堂教学效果以及成绩分布，对课程教学方法和成绩评定环节进行改进，并同步优化评定办法。 The subject coordinator shall revise the syllabus based on the teaching content, effect and result distribution while optimize the assessment measures.		