《信息安全技术》课程教学大纲

课程英文名	**Information Security Technology**				
课程代码	**B0504870**	课程类别	专业课	课程性质	专业选修
学　分	**3**		总学时数	**48**	
开课学院	计算机学院		开课基层教学组织	网络与信息安全课程组	
面向专业	计算机科学与技术、智能财务(软件工程)		开课学期	第 6 学期	

注：课程类别是指学科基础课/专业课/实践环节/通识公共课/公共基础课/其他；

课程性质是指通识必修/通识选修/学科必修/专业必修/专业选修/实践必修/实践选修。

一、课程目标

信息化、网络化是当今世界经济与社会发展的大趋势。同时，由于计算机网络所具有的开放性与共享性，使信息安全成为人们日益关切的问题。信息的传输通过脆弱的公共信道，信息储存于不设防的计算机系统中，如何保护信息的安全，使之不被窃取及不至于被篡改或破坏，以成为当今普遍关注的重大问题。信息安全密码技术是有效而可行的办法。引导学生思考网络安全对社会、法律、文化以及可持续发展的影响，树立正确的价值观和责任意识。

通过理论教学和实践活动，达到以下课程目标：

1. 能够运用分组密码、公钥密码、数字签名、鉴别与认证等密码技术，解决信息系统中信息的安全与保密问题。
2. 具备运用网络安全协议来增强网络通信安全保障的能力。
3. 具备网络攻击分析能力，并初步具备设计安全网络体系结构的能力。

二、课程目标与毕业要求对应关系

本课程的课程目标对计算机科学与技术专业毕业要求指标点的支撑情况如表 1 所示：

表 1. 课程目标与计算机科学与技术毕业要求对应关系

毕业要求	指标点	课程目标及支撑权重
1.工程知识：掌握数学、自然科学、工程基础、计算机专业领域的知识，并能应用于计算机领域复杂工程问题的解决方案中。	1-3 能够运用计算机专业知识，对计算机领域复杂工程问题解决方案进行分析与优化。	目标 1：0.4 目标 2：0.4 目标 3：0.2
	1-4 掌握计算机系统、物联网、人工智能、大数据、网络安全等某个专业领域的知识，并用于解决计算机领域	

	的复杂工程问题。	
2.问题分析：能够应用数学、自然科学和工程科学的基本原理，以及科学思维方法，对计算机领域的复杂工程问题进行识别、表达和分析，并通过文献查阅与研究获得有效结论。	2-1 能够应用数学、自然科学、工程科学和计算科学的基本原理识别、表达计算机领域的复杂工程问题。	目标 1：0.5 目标 2：0.5
3.设计/开发解决方案：能够设计计算机领域复杂工程问题的解决方案，设计与开发满足特定需求的软硬件系统、算法或部件，在设计中考虑社会、健康、安全、法律、文化以及环境等因素，并体现一定的创新意识。	3-1 具备计算思维和程序设计能力，能够针对计算机复杂系统设计与开发满足特定需求的模块或算法。	目标 1：0.5 目标 2：0.5
4.研究：能够基于包括计算学科在内的科学原理，采用科学方法研究计算机领域的复杂工程问题，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。	4-1 能够运用计算机科学原理与方法，对计算机领域复杂工程问题进行研究分析。	目标 1：0.4 目标 2：0.4 目标 3：0.2

本课程的课程目标对计算机科学与技术(计算机科学英才班)专业毕业要求指标点的支撑情况如表 2 所示：

表 2. 课程目标与计算机科学与技术(计算机科学英才班)毕业要求对应关系

毕业要求	指标点	课程目标及支撑权重
1.工程与科学知识：能够掌握数学、自然科学、工程基础、计算机科学理论知识，并应用在计算机相关领域的复杂工程问题和基础科学问题的解决方案中。	1-3 能够运用计算机专业知识，对复杂工程问题解决方案进行分析与优化。 1-4 掌握计算机系统、人工智能、大数据、网络安全等某个专业领域的知识，并用于解决计算机相关领域的复杂工程问题。	目标 1：0.4 目标 2：0.4 目标 3：0.2
2.问题分析：能够应用数学、自然科学和工程科学的基本原理，以及计算科学思维方法，对计算机相关领域的复杂工程问题进行抽象分析与识别、建模表达和形式化论证，并通过文献查阅与研究获得有效结论。	2-1 能够应用数学、自然科学、工程科学和计算科学的基本原理识别、表达计算机相关领域的复杂工程问题。	目标 1：0.5 目标 2：0.5
3.设计/开发解决方案：能够设计计算机相关领域复杂工程问题的解决方案，能够设计与开发满足特定需求的计算机软硬件系统、模块或算法，在设计中考虑社会、健康、安全、法律、文化以及环境等因素，并体现较强的创新意识，具备基本的创新能力。	3-1 具备计算思维和程序设计能力，能够针对计算机复杂系统设计与开发满足特定需求的模块或算法。	目标 1：0.5 目标 2：0.5
4.研究：具有基本的科学素养和研究意识，具备良好的科学思维能力，对未知事物有探	4-1 能够运用计算机科学原理与方法，对计算机复杂工程问题进行研究	目标 1：0.4 目标 2：0.4

索精神和研究兴趣。具有运用数学和自然科学方法解决复杂问题的能力，能够采用科学方法研究计算机相关领域的复杂问题，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。	分析。	目标 3：0.2

本课程的课程目标对智能计算与数据科学(计算机科学与技术)专业毕业要求指标点的支撑情况如表 3 所示：

表 3. 课程目标与智能计算与数据科学(计算机科学与技术)专业毕业要求对应关系

毕业要求	指标点	课程目标及支撑权重
1.工程知识：能够掌握数学、自然科学、工程基础、计算机软硬件知识、人工智能、智能计算和数据科学的基础理论及专业知识，并应用在人工智能、智能计算和大数据专业领域及其他相关交叉领域的复杂工程问题的解决方案中。	1-3 能够运用计算机专业知识，对计算机领域复杂工程问题解决方案进行分析与优化。 1-4 掌握人工智能、智能计算、大数据等某个专业领域的知识，并用于解决计算机领域的复杂工程问题。	目标 1：0.4 目标 2：0.4 目标 3：0.2
2.问题分析：能够应用数学、自然科学、工程科学、人工智能、智能计算和大数据的基本原理，对人工智能和大数据专业领域及其他相关交叉领域的复杂工程问题进行识别、表达、分析和抽象建模，并通过文献查阅与研究获得有效结论。	2-1 能够应用数学、自然科学、工程科学和计算科学的基本原理识别、表达计算机领域的复杂工程问题。	目标 1：0.5 目标 2：0.5
3.设计/开发解决方案：能够设计人工智能、智能计算和大数据专业领域及其他相关交叉领域复杂工程问题的解决方案，能够设计与开发满足特定需求的计算机软硬件系统、模型或算法，在设计中考虑社会、健康、安全、法律、文化以及环境等因素，并体现一定的创新意识。	3-1 具备计算思维和程序设计能力，能够针对计算机复杂系统设计与开发满足特定需求的模块或算法。	目标 1：0.5 目标 2：0.5
4.研究：具有基本的科学素养和研究意识，能够采用科学方法研究人工智能、智能计算和大数据专业领域及其他相关交叉领域的复杂工程问题，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。	4-1 能够运用计算机科学原理与方法，对计算机领域复杂工程问题进行研究分析。	目标 1：0.4 目标 2：0.4 目标 3：0.2

本课程的课程目标对智能财务(软件工程)专业毕业要求指标点的支撑情况如表 4 所示：

表 4. 课程目标与智能财务(软件工程)专业毕业要求对应关系

毕业要求	指标点	课程目标及支撑权重

1. 工程知识：掌握数学、自然科学、工程基础、财务领域基础知识和软件工程专业领域知识，并能应用在智能财务软件领域复杂工程问题的解决方案中。	1-3 能够运用软件工程专业知识和财务领域专业知识，对智能财务软件工程领域复杂工程问题解决方案进行分析与优化。 1-4 掌握某个专业领域知识，并用于解决智能财务软件工程领域复杂工程问题。	目标 1：0.4 目标 2：0.4 目标 3：0.2
2. 问题分析：能够应用数学、自然科学、财务领域基础知识和工程科学的基本原理，以及计算科学思维方法，对智能财务软件领域复杂工程问题进行识别、表达和分析，并通过文献查阅与研究获得有效结论。	2-1 能够应用数学、自然科学、工程科学、财务领域和软件工程的基本原理识别、表达智能财务软件工程领域复杂工程问题。	目标 1：0.5 目标 2：0.5
3. 设计/开发解决方案：能够设计智能财务软件领域复杂工程问题的解决方案，设计与开发满足特定需求的软件系统、模块或算法，在设计中考虑社会、健康、安全、法律、文化以及环境等因素，并体现一定的创新意识。	3-1 具备计算思维和程序设计能力，能够针对复杂智能财务软件系统设计与开发满足特定需求的模块或算法。	目标 1：0.5 目标 2：0.5
6.工程与社会：能够基于软件工程相关背景知识进行合理分析、认识和评价工程实践和复杂工程问题解决方案对社会、健康、安全、法律以及文化的影响，并理解应承担的责任。	6-1 能够基于智能财务软件工程相关背景知识，合理分析、认识与评价智能财务软件工程实践和复杂工程问题解决方案对社会、健康、安全、法律及文化的影响。	目标 1：0.4 目标 2：0.4 目标 3：0.2
7.环境和可持续发展：了解国家信息产业发展的宏观政策，能够理解和评价智能财务软件领域复杂工程问题解决方案及专业工程实践对环境、社会可持续发展的影响。	7-2 能够在智能财务软件工程领域复杂工程问题解决方案中，考虑工程实践与环境、社会的和谐可持续发展等因素。	目标 1：0.4 目标 2：0.4 目标 3：0.2

三、课程目标与教学内容和方法的对应关系

课程教学内容对课程目标的支撑关系、教学方法如表 5 所示：

表 5. 课程目标与教学内容、教学方法的对应关系

教学内容	教学方法	课程目标
1.信息安全概述	课堂讲授、自学	1,2,3
2.密码学基础	课堂讲授、课堂练习、案例分析设计	1,2,3
3.认证理论与技术	课堂讲授、课堂练习、案例分析设计	1,2,3
4.网络安全协议	课堂讲授、课堂练习、案例分析设计	1,2,3
5.网络攻防技术	课堂讲授、案例分析设计	1,2,3

课程教学的详细内容与要求如下：

1. 信息安全概述

（1） 教学内容：

- 信息安全的基本概念

（2） 教学重点：信息系统安全定义的内涵，以及从网络、自控、信息处理等不同角度对信息系统安全的理解。

（3） 教学难点：信息系统安全产生威胁和攻击的手段。

（4） 教学要求：使学生能够应用信息安全中攻击、服务和机制等基本概念分析网络安全性。

思政融合点 1：引入中共中央成立网络安全和信息化领导小组的重要意义，学习习总书记关于网络安全和信息化的重要讲话，让学生体会到网络安全和信息化是事关国家安全和国家发展、事关广大人民群众工作生活的重大战略问题，要从国际国内大势出发，总体布局，统筹各方，创新发展，努力把我国建设成为网络强国。

2. 密码学基础

（1）教学内容：

- 对称密码算法、非对称密码算法、序列密码体制、分组密码体制的概念
- 密码算法、DES 密码算法，高级加密标准 AES 算法， RSA 算法
- 对称密钥的管理，密钥分发中心 KDC 的概念
- 公钥管理和公钥设施基 PKI 的概念
- 密钥协商协议

（2）教学重点：对称密码 DES 算法、非对称密码 RSA 算法等加密算法的基本原理和过程；密钥管理的概念；公钥设施基 PKI；密钥协商协议的基本原理。

（3）教学难点：密码学基本数学基础和现代密码算法的实现技术，理解数字证书的基本原理。

（4）教学要求：能够通过基础知识的学习及查阅研究分析文献等方式，使学生能够运用密码算法的基本思想和原理；能够运用 DES 分组加密算法和 RSA 算法解决软件工程中的数据加密问题；能够应用公钥设施基 PKI 解决公钥管理问题；能够应用密钥协商协议解决通信中密钥协商问题。

3. 认证理论与技术

（1）教学内容：

- 鉴别技术：鉴别的定义，鉴别机制的特征：对称/非对称特性、使用密码/非密码技术特性，鉴别的 3 种类型：单向鉴别、双向鉴别、鉴别确认；
- 数字签名技术：数字签名的的定义，RSA 和 DSA 数字签名方案；

（2）教学重点：鉴别机制、数字签名机制的基本原理。

（3）教学难点：DSA 数字签名算法、基于密码技术的安全认证协议。

（4）教学要求：能够分析数字签名的基本原理和方法；能够分析 DSA 数字签名算法的基本过程，能够分析身份鉴别协议的基本方法；能够运用数字签名算法解决软件工程中抗抵赖问题；能够运用鉴别机制实现软件工程中的身份人认证功能。

思政融合点 2：引导学生了解我国王小云院士破解 MD5、SHA 等散列算法取得令世人瞩目的成就，激发学生的爱国主义热情、自豪感与使命感。

4. 网络安全协议

（1） 教学内容：

网络层安全协议 Ipsec：密钥管理协议 ISAKMP、AH 协议和 ESP 协议；

- IPsec 的安全体系结构、工作原理；
- 传输层安全协议 TLS 工作原理、工作流程；
- TLS 记录协议和 TLS 握手协议；

（2） 教学重点：IPsec 的安全体系结构、工作原理、工作流程，传输层安全协议 TLS 的构成方式、工作原理。

（3） 教学难点：安全关联 SA、密钥交换机制 IKE 概念。

（4） 教学要求：能够分析网络层安全协议 Ipsec；能够分析传输层安全协议 TLS；能够应用网络层安全协议 Ipsec 实现网络层的安全通信；能够应用 TLS 协议实现应用程序传输安全。

5. 网络攻防技术

（1） 教学内容：

- 网络攻击技术：网络扫描、嗅探技术、网络欺骗与会话劫持、缓冲区溢出攻击、木马与后门等技术的基本原理；
- 防火墙技术：防火墙的基本实现类型，防火墙的体系结构；
- 入侵检测技术：入侵检测系统的基本原理，入侵检测框架，入侵检测的基本技术；

（2） 教学重点：网络攻击技术的基本原理、防火墙的基本原理、入侵检测的基本技术。

（3） 教学难点：缓冲区溢出攻击、防火墙实现方式、入侵检测技术。

（4） 教学要求：能够分析网络攻击的基本原理，能够应用防火墙技术过滤数据包；能够将防火墙、入侵检测运用于网络设计中。

思政融合点 3：引导学生学习《中华人民共和国网络安全法》，让学生了解其是我国规范网络空间安全管理方面问题的基础性法律，是依法治网、化解网络风险的法律重器，是让互联网在法治轨道上健康运行的重要保障。

四、实践环节及基本要求

1．实验项目和基本要求

通过实验，要求学生能够掌握密码算法、数字签名技术以及网络安全技术。

序号	实验项目	时数	每组人数	内容提要	实验要求
1	分组密码实验	3	1	DES加密算法的实现与应用	掌握运用DES分组密码算法。
2	公钥密码实验	3	1	RSA公钥密码算法的实现	掌握运用RSA公钥密码算

				与应用	法。
3	数字签名实验	3	1	DSA数字签名算法的实现与应用	掌握运用DSA数字签名算法。
4	网络安全技术实验	3	1	网络攻击与安全防护	掌握网络攻击与防护的基本方法。

2．实验报告基本要求

实验报告至少包含以下几个部分：⑴实验目的；⑵实验过程（含算法思想、程序等）；⑶实验结果及结果分析；⑷实验总结。

五、与其它课程的联系

先修课程：程序设计基础、计算机网络、操作系统。

六、学时分配

教学内容	讲课时数	实验时数	实践学时	上机时数	自学时数	习题课	讨论时数
1、信息安全概述	3						
2、密码学基础	12				1		
3、认证理论与技术	9				1		
4、网络安全协议	6				1		
5、网络攻防技术	6						
6、实验				12			
合　　计	36			12	3		
总　　计	总学时 48 学时，其中讲课 36 学时，上机 12 学时、自学 3 学时						

七、课程目标达成途径及学生成绩评定方法

1. 课程目标达成途径

各个课程目标的达成途径如表 6 所示，但不仅限于此。

表 6. 课程目标与达成途径

课程目标	达成途径
课程目标 1：能够运用分组密码、公钥密码、数字签名、鉴别与认证等密码技术，解决信息系统中信息的安全与保密问题。	采用引导式和对比式教学方法，通过课堂讲解、课后实践、课堂练习、课后作业等手段。
课程目标 2：具备运用网络安全协议来增强网络通信安全保障的能力。	以启发式、研讨式教学方法为主，通过课堂讲解、案例分析、课堂练习、课堂互动、课堂研讨、文献阅读等诸多教学手段。
课程目标 3：具备网络攻击分析能力，并初步具备设计安全网络体系结构的能力。	采用案例教学法和类比教学法。

2. 学生成绩评定方法

本课程为考查课程。

课程成绩评定办法：课程成绩按百分制计分，由平时成绩和期末考查成绩综合评定。

期末总成绩=平时成绩*40%+期末课堂考试***60%**

其中平时成绩的评价内容如下表所示：

各部分的具体评价环节、关联课程目标、评价依据及方法和在总成绩中的占比，如表 7 所示。各考核内容的详细评分标准见表 8 所示。

表 7. 课程考核与成绩评定方法

成绩构成	考核项目	考核关联的课程目标	考核依据与方法	占总评成绩的比重
平时成绩	课程思政实践	1,2,3	通过课外文献查阅、课堂展示、课堂小组讨论、阅读报告等多种形式，考查学生对我国相关先进技术的了解情况以及核心价值观状况	5%
	课后作业	1,2,3	根据作业质量与正确率，给出批阅成绩（五分制），折算为百分制后，计算平均得分；至少 5 次作业；占比不超过 15%	15%
	实验	1,2,3	根据实验验收与报告质量，给出批阅成绩（五分制），折算为百分制后，计算平均得分；至少 5 次作业；占比不超过 15%	15%
	课堂互动	1,2,3	通过课堂提问、抢答等环节，根据回答质量与回答次数计分；占比不超过 5%	5%
期末考查	考查	1,2,3	课内测试成绩	60%
总评成绩		1,2,3	=平时成绩*40%+考试成绩*60%	100%

表 8. 考核内容详细评分标准

考核内容	评分标准			
	90-100	75-90	60-75	＜60
课程思政实践	报告条理清晰，文字流畅，字数≥4000，参考文献数量≥8 且相关性强；内容完整且材料丰富，体现强烈的使命感、责任心与民族自豪感	报告条理清楚，字数≥3000，参考文献数量≥5 且相关性较好；内容完整，材料不够丰富，能体现学生的使命感、责任心与民族自豪感	报告有一定条理，字数≥1000，参考文献数量≥2 且基本相关；内容基本完整但材料较少，能体现学生的使命感与民族自豪感	报告字数＜1000，参考文献数量＜2；内容少，或有抄袭现象，体现不出学生的使命感与民族自豪感
课后作业	非标作业：方案等设计合理，分析准确，能满足问题全部要求	非标讨论题：方案较合理，分析较正确，能基本满足问题全部要求	非标讨论题：方案基本合理，能满足问题大部分要求	非标讨论题：方案不够合理，只能满足问题少量要求
	标准题目：按照作业题目评分标准据实评价			
课堂参与	课堂练习、回答问题等据实评价；或参与回答次数在教学班前 15%	课堂练习、回答问题等据实评价；或参与回答次数在教学班前 50%	课堂练习、回答问题等据实评价；或参与回答次数在教学班前 85%	课堂练习、回答问题等据实评价；或参与回答次数在教学班后 15%
实验	非标作业：方案等设	非标作业：方案较合	非标作业：方案基本	非标作业：方案不够

	计合理，分析准确，能满足问题全部要求	理，分析较正确，能基本满足问题全部要求	合理，能满足问题大部分要求	合理，只能满足问题少量要求
期末考查	按照试卷评分标准据实评价			

八、教学资源

表 9. 课程的基本教学资源

资源类型	资源
教 材	密码编码学与网络安全——原理与实践（第七版），王后珍译，电子工业出版社，2017
参考书籍或文献	（1）网络与信息安全，林伯纲，机械工业出版社出版，2004 （2）计算机网络安全教程，石志国等编著，清华大学出版社，2007 （3）计算机网络安全，姚永雷、马利，清华大学出版社，2011
教学文档	无

九、课程目标达成度的定量评价

在课程结束后，需要对每一个课程目标（含思政课程目标）进行达成度的定量评价，用以实现课程的持续改进。

课程目标达成度的定量评价算法：

1、 使用教学活动（如课程思政实践、课后作业、课堂练习、单元测验、实验验收、演讲、课堂讨论、互动、阅读报告、大作业等等）成绩或期末考试部分题目得分率作为评价项目，来对某个课程目标进行达成度的定量评价；

2、 为保证考核的全面性和可靠性，要求对每一个课程目标的评价项目选择超过两种；

3、 根据施教情况，评价项目可以由教师自行扩展，权重比例可以由教师自行设计；

4、 对某一个课程目标有支撑的各评价项目权重之和为 1；

5、 使用所有学生（含不及格）的平均成绩计算。

本课程的课程目标达成度的定量评价算法建议如表 10 所示，教师可根据授课方式及考核内容适当调整：

表 10. 课程目标达成度定量评价方法

课程目标	课程目标达成度评价方式
课程目标 1：能够运用分组密码、公钥密码、数字签名、鉴别与认证等密码技术，解决信息系统中信息的安全与保密问题。	课程思政：0.05 课后作业：0.15 课堂讨论：0.05 实验：0.15 期末：0.6
课程目标 2：具备运用网络安全协议来增强网络通信安全保障的能力。	课程思政：0.05 课后作业：0.15 课堂讨论：0.05 实验：0.15

课程目标	课程目标达成度评价方式
	期末：0.6
课程目标 3：具备网络攻击分析能力，并初步具备设计安全网络体系结构的能力。	课程思政：0.05 课后作业：0.15 课堂讨论：0.05 实验：0.15 期末：0.6

十、说明

承担该课程的教师必须遵照本大纲安排授课计划、实施教学过程，完成学生各个阶段与各方面的学习成果考核与评价；在学期末，需对课程目标和课程支撑的毕业要求指标点进行达成度评价。

本课程大纲自 2021 年开始执行，生效之日原先版本均不再使用。

十一、编制与审核

表 11. 大纲编制与审核信息

工作内容	责任部门或机构	负责人	完成时间
编制	网络与信息安全课程组	张旻	2022.01.05
审核	网络与信息安全课程组	徐建	2022.01.15
审定	计算机学院教学工作委员会	袁友伟	2022.03.10