东北大学秦皇岛分校本科课程教学大纲

一、课程基本信息

<table>
<tr><td>开课单位</td><td colspan="3">悉尼智能科技学院</td><td>课程代码</td><td colspan="5">3030113080</td></tr>
<tr><td>中文名称</td><td colspan="8">信息安全基础</td></tr>
<tr><td>英文名称</td><td colspan="8">Information security Infrastructure</td></tr>
<tr><td>总学时</td><td>56</td><td rowspan="2">理论学时</td><td rowspan="2">32</td><td rowspan="2">实验学时</td><td rowspan="2">24</td><td rowspan="2">上机学时</td><td rowspan="2">0</td><td rowspan="2">设计学时</td><td rowspan="2">0</td><td rowspan="2">课外学时</td><td rowspan="2">0</td></tr>
<tr><td>学　分</td><td>3</td></tr>
<tr><td>课程类型</td><td colspan="8">☐理论课程　☑理论（含实验）课程　☐实践类课程</td></tr>
<tr><td>课程类别</td><td colspan="8">☐通识类　☐学科基础类　☑专业方向类　☐实践类</td></tr>
<tr><td>适用专业</td><td colspan="8">计算机科学与技术</td></tr>
<tr><td>先修课程</td><td colspan="8">计算机网络</td></tr>
<tr><td>建议开课学期</td><td colspan="8">☐1-1 ☐1-2 ☐2-1 ☐2-2 ☐3-1 ☑3-2
☐4-1 ☐4-2 ☐5-1 ☐5-2 ☐*（代表每学期都开设）</td></tr>
<tr><td>考核方式</td><td colspan="4">☐考试 ☑考查</td><td>成绩分制</td><td colspan="3">☑百分制 ☐五级制
☐二级制</td></tr>
<tr><td>使用教材</td><td colspan="8">1. 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 年.</td></tr>
<tr><td>参考书及教学资源</td><td colspan="8">1. Willliam Stallings 著，王后珍等译，《密码编码学与网络安全-原理与实践（第 8 版）》，电子工业出版社，2021 年.
2. 贾春福等，《信息安全数学基础》，机械工业出版社，2017 年.
3. 蒋建春等，《信息安全工程师教程》，清华大学出版社，2020 年.</td></tr>
<tr><td>其他说明</td><td colspan="8">无</td></tr>
</table>

二、课程简介

中文描述

信息安全在当今社会具有极端的重要性，它关乎个人隐私、企业利益、国家安全乃至全球稳定。随着信息技术的飞速发展，互联网、物联网、云计算、大数据等技术的广泛应用，信息已成为社会运行的重要基础资源，其价值日益凸显。因此，保护信息安全，防止信息被非法获取、篡改、泄露或滥用，已成为维护社会正常运行、促进经济发展的关键环节。

信息安全基础是计算机相关专业的专业选修课，其目的是使学生树立信息安全防范意识，掌握密码学、网络安全协议、系统安全等信息安全基本理论与应用技术，并在实际应用环境下能够运用所学相关技术和理论分析、判断和解决所遇到的信息安全问题。

课程知识内容主要包括网络安全形势分析与法律基础、网络安全模型、对称加密体制、公钥加密体制、随机数与流密码、消息认证、数字签名，密钥管理与分发、网络访问控制、无线安全网络、传输层安全、IP 安全、电子邮件安全、系统安全等内容，旨在介绍密码学与网络安全的原理与应用，让学生理解信息安全本质与防范策略。本课程可为学生后继续深造和就业过程中学习信息安全问题分析与处理奠定理论与实践基础，提升学生认识、分析和解决信息安全问题的思辨能力及实践能力，巩固学生知行合一意识和创新实践精神。

课程内容按照“价值塑造、知识传授、能力培养”三位一体育人理念开展，在专业课程中注重融入价值观教育，课程内容在信息安全相关知识点注重课程思政元素发掘，为大学生塑造正确的网络安全价值观及在学生群体中强化爱国情怀。

English Description

Information security is extremely important in today's society, which is related to personal privacy, corporate interests, national security and even global stability. With the rapid development of information technology and the widespread application of technologies such as the Internet, the Internet of Things, cloud computing and big data, information has become an important part for social operation, and its value is increasingly prominent. Therefore, information security and preventing information from being illegally obtained, tampered with, leaked or abused has become a key link in maintaining the normal operation of society and promoting economic development.

Information Security is a elective course for computer-related majors. Its aim is to instill in students an awareness of information security prevention, equip them with fundamental theories and applied techniques in information security, such as cryptography, network security protocols, and system security, and to enable them to apply the relevant techniques and theories they have learned to solve information security problems they encounter in practical application environments.

The course includes network security situation analysis and legal basis, network security model, symmetric encryption and asymmetric encryption algorithm, random number and stream cipher, message authentication, digital signature, key management and distribution, network access control, wireless security, TLS, IPSec, email security, system security, etc. It aims to introduce the principles and applications of cryptography and network security, so that students can understand the essence and prevention strategies of information security.

The course content is based on the three-in-one educational philosophy of "value shaping, knowledge impartment, and ability cultivation". In this course, we focus on integrating values education, especially aim to shaping correct cybersecurity values for college students and strengthening patriotism among the student population.

三、课程目标

1、知识目标：

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、社会与国家的影响；

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；

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；

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；

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

2、能力目标：

2-1：掌握对称分组加密方法，能够利用 DES、AES 等加密算法进行数据加解密；

2-2：掌握公钥加密方法，能够利用 RSA 等加密算法进行数据加解密及数字签名；

2-3：掌握常用哈希函数安全需求，能够利用安全散列函数进行数据完整性校验；

2-4：掌握密钥分配，能够基于对称加密算法与公钥加密算法制定安全的密钥分配方案；

2-5：掌握 Web 流量安全方法，能够基于不同应用场景选择从 IP 层、传输层、应用层选择相应的防护方案；

2-6：掌握数据包抓取与分析方法，掌握协议分析方法；

2-7：掌握密码爆破、网络攻防等常见攻击原理，能够根据实际需求制定系统防护方案。

3、**德育/素养目标：**

3-1：展示本专业在新时代中国特色社会主义建设中的成就和当前要解决的重大课题；

3-2：具有良好的团队协作意识和能力、较强的表达能力和人际交往能力；

3-2：具备一定的科学思维、科学精神和科学素质，树立科学思想以及正确的世界观和方法论；

3-4：理解信息安全对于刻画工程实践问题的重要意义；

3-5：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；

3-6：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。

表 1 课程目标与毕业要求的对应关系

毕业要求	指标点	课程目标	关联性（H/M/L）
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、方法和手段，识别、表达、并通过文献研究分析复杂工程问题，以获得有效结论。	指标点 2-1：专业知识掌握扎实，了解中国和世界经济领域及其研究的最新动态和发展趋势；能够应用数学、自然科学和工程科学的基本原理、方法和手段，分析、识别、表达本专业相关的复杂工程问题；	2-1、2-2、2-3、2-4、2-5、2-6、2-7	H
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。	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；	1-1、1-2、1-3、1-4	M

6、工程与社会：能够基于本专业相关背景知识和相关法规标准进行合理分析，评价本专业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。	指标点 6-1：能够基于本专业相关背景知识进行合理分析，评价计算机相关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；	1-5、3-1、3-2、3-3、3-4、3-5、3-6	M

四、主要教学内容

（一）理论教学

第 1 章 网络安全形势与法律基础 （支撑课程目标 1-1、1-2、3-1、3-3、3-4、3-5、3-6）

【1】知识点：

(1) 网络安全形势；
(2) 网络安全相关法律基础；
(3) 网络安全防范措施。

【2】学习目标：

了解： 网络安全形势与相关法律基础。
理解： 信息安全对国家与个人的影响。
掌握： 信息安全基本概念。

【3】重点内容：

《网络安全法》、《中华人民共和国国家安全法》、《中华人民共和国刑法修正案（九）》。

【4】难点内容：

网络安全日常防范措施。

【5】思政案例：

在讲解“网络安全对国家安全的影响”内容中，通过震网病毒、棱镜门等事件，介绍网络安全对国家安全的影响，进一步介绍国内外科技水平的差异，以及国家为保障网络安全所采取的措施，强调网络安全对国家安全的影响，激发学生的爱国情怀。

第 2 章：对称密码 （支撑课程目标 1-2、1-3、1-4、1-5、2-1、3-1、3-2、3-3、3-4、3-6）

【1】知识点：

(1) 信息安全目标，OSI 安全体系结构，网络安全模型；
(2) 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；
(3) 对称分组密码，数据加密标准 DES，3DES，高级加密标准 AES；
(4) 分组密码工作模式；
(5) 随机数和伪随机数，流密码和 RC4。

【2】学习目标：

了解： 密码学的发展历史，密码系统的分类，经典密码学。
理解： OSI 安全体系结构，网络安全模型。
掌握： 信息安全目标，对称分组密码及其工作模式。随机数和伪随机数，流密码。

【3】重点内容：

信息安全目标，对称分组密码，分组密码工作模式，随机数和伪随机数，流密码。

【4】难点内容：

对称分组密码，分组密码工作模式。随机数和伪随机数，流密码。

【5】思政案例：

介绍国产哈希算法 SM4，SM4 是我国采用的一种分组密码标准，由国家密码管理局于 2012 年 3 月 21 日发布。相关标准为“GM/T 0002-2012《SM4 分组密码算法》。SM4 主要用于数据加密，

其算法公开，分组长度与密钥长度均为 128bit，加密算法与密钥扩展算法都采用 32 轮非线性迭代结构，S 盒为固定的 8 比特输入 8 比特输出。通过对比国内外分组算法标准与使用情况，让学生了解我国信息安全发展现状，激发学生的责任感、民族自豪感。

第三章：公钥密码（支撑课程目标 1-3、1-4、1-5、2-2、3-1、3-2、3-3、3-4、3-6）

【1】知识点：

(1) 公钥密码体制基本原理；
(2) RSA 等公钥密码算法；
(3) Diffie-Hellman 密钥交换；

【2】学习目标：

了解： 公钥密码发展历史。
理解： 公钥密码体制与对称密码体制区别。
掌握： RSA 等公钥密码算法，Diffie-Hellman 密钥交换。

【3】重点内容：

(1) 公钥密码体制与对称密码体制区别；
(2) RSA 等公钥密码算法；
(3) Diffie-Hellman 密钥交换。

【4】难点内容：

(1) RSA 等公钥密码算法；
(2) Diffie-Hellman 密钥交换；
(3) 公钥加密的数学原理。

【5】思政案例：

介绍国产公钥加密算法 SM2，SM2 是国家密码管理局于 2010 年 12 月 17 日发布的椭圆曲线公钥密码算法，SM2 算法和 RSA 算法都是公钥密码算法，SM2 算法是一种更先进安全的算法，在我们国家商用密码体系中被用来替换 RSA 算法。SM2 性能更优更安全：密码复杂度高、处理速度快、机器性能消耗更小。通过强调国密算法标准，引发学生对于科学探索及创新的热情。

第四章：数据完整性（支撑课程目标 1-3、1-4、1-5、2-3、3-1、3-2、3-3、3-4、3-6）

【1】知识点：

(1) 密码学哈希函数；
(2) 消息认证码。
(3) 数字签名。

【2】学习目标：

了解： 哈希函数原理应用。
理解： 消息认证原理及用途。
掌握： 掌握数字签名方案。

【3】重点内容：

(1) 哈希函数安全需求；
(2) 数字签名实现流程。

【4】难点内容：

(1) 哈希函数安全需求；
(2) 数字签名实现流程。

【5】思政案例：

详细介绍我国著名密码学家王小云院士，王小云院士密码理论及相关数学问题研究所取得巨大成就，她提出了密码哈希函数的碰撞攻击理论，即模差分比特分析法，破解了包括 MD5、SHA-1 在内的 5 个国际通用哈希函数算法；将比特分析法进一步应用于带密钥的密码算法包括消息认证码、对称加密算法、认证加密算法的分析，给出系列重要算法 HMAC-MD5、MD5-MAC、SIMON、Keccak-MAC 等重要分析结果；在高维格理论与格密码研究领域，给出了格最短向量求解的启发

式算法二重筛法以及带 Gap 格的反转定理等成果；设计了我国哈希函数标准 SM3，在金融、交通、国家电网等重要经济领域广泛使用,并于 2018 年 10 月正式成为 ISO/IEC 国际标准。通过内容的讲述，强化学生学习信息安全的积极性，激发学生的民族自豪感，持续创新的工匠精神和对计算机科学的探索精神。

第五章：互信（支撑课程目标 1-3、1-4、1-5、2-4、3-1、3-2、3-3、3-4、3-5、3-6）

【1】知识点：

(1) 基于对称加密的密钥分配；
(2) 基于非对称加密的密钥分配；
(3) 用户认证。

【2】学习目标：

了解： 公钥基础设施 PKI。
理解： 理解利用公钥密码分配对称密钥的技术问题。
掌握： 基于对称加密算法的密钥分配方案，公钥分配方案，用户认证方案。

【3】重点内容：

(1) Kerberos 协议；
(2) X.509 证书。

【4】难点内容：

(1) Kerberos 协议；
(2) X.509 证书。

【5】思政案例：

由用户认证引出信息安全的重要作用，进而抛出目前学生关注的本专业的时事特别是贸易战中 IT 行业作为核心产业迫切需要独立自主发展等关键问题，激发学生的民族责任感。要求学生培养权利意识、责任意识和纪律意识，坚持公正法治常驻心间。

第六章：网络与 Internet 安全（支撑课程目标 1-4、1-5、2-5、2-6、2-7、3-1、3-2、3-3、3-4、3-5、3-6）

【1】知识点：

(1) 网络访问控制原理与实现；
(2) 传输层安全；
(3) 电子邮件安全；
(4) IP 安全。

【2】学习目标：

了解： 无线网络安全，云安全所面临的威胁与对策。
理解： 传输层安全、电子邮件安全、IP 安全机制原理机制。
掌握： TLS，IPSec，不同场景安全策略的选择。

【3】重点内容：

(1) TLS，HTTPS、SSH；
(2) S/MIME；
(3) IPSec。

【4】难点内容：

(1) TLS，HTTPS、SSH；
(2) IPSec。

【5】思政案例：

介绍西北工业大学遭受美国国家安全局网络攻击事件，进而抛出目前学生关注的国家网络安全对抗过程中迫切需要独立自主发展等关键问题，激发学生的民族责任感。要求学生培养权利意识、责任意识和自强意识。

第七章：系统安全（支撑课程目标 1-4、1-5、2-5、3-1、3-2、3-3、3-4、3-5、3-6）

【1】知识点：

(1) 常见计算机病毒的特征及原理；

(2) 入侵检测原理；

(3) 防火墙的安全策略。

【2】学习目标：

了解： 了解计算机病毒的定义、特征，病毒程序的构成；知道病毒传播途径、类型等。

理解： 了解入侵检测原理与口令管理。

掌握： 防火墙的安全策略，网络安全体防护体系。

【3】重点内容：

网络安全整体防护体系。

【4】难点内容：

网络安全防护体系。

【5】思政案例：

引入计算机系统等级保护方案 2.0，进一步介绍等级保护的级别划分，让学生了解国家对信息系统保护所采取的措施，激发学生学习兴趣、责任感、创新精神。

（二）实验教学

信息安全强调理论与实践相结合，课程实验旨在通过常见网络攻击向学生介绍渗透测试与系统防御方法。实验教学的项目名称及学时分配相关信息如表 2 所示。

表 2 实验教学信息表

序号	实验项目名称	实验学时	每组人数	实验类型	实验性质
1	数据的机密性	2	3	必做	设计型
2	数据包抓取与协议分析	2	3	必做	设计型
3	情报收集	2	3	必做	综合型
4	网络攻击	16	3	必做	综合型
5	系统加固	2	3	必做	综合型

实验项目一：数据的机密性（支撑课程目标 1-3、1-5，2-1、2-2，3-1、3-2、3-3、3-4、3-5、3-6）

【1】实验内容：

自选程序设计语言，实现数据的加密与解密；利用第三方实验平台，实现利用不安全的加密算法进行数据修改操作，并通过查询资料对实验平台中的安全问题提出改进方案。

【2】实验目的：

掌握程序设计中加密算法的使用方法；理解弱与不安全加密算法可能带来的风险。

【3】教学要求：

要求学生利用自己熟悉的程序设计语言实现数据的加密与解密功能，基本掌握程序设计中数据加解密算法的选择与使用方法

【4】实验方式：

程序设计、实践操作。

【5】实验场地与设备：

综合楼 1108，部署有实验环境的计算机。

实验项目二：数据包抓取与协议分析（支撑教学目标 1-3、1-4、1-5，2-5、2-6，3-1、3-2、3-3、3-4、3-5、3-6）

【1】实验内容：

抓取 ping 命令数据包，并查看数据包负载；抓取 DNS 请求数据包，分析 DNS 请求流程；分析给定数据包，获取目标主机信息，如主机的 IP 地址、用户名和密码等敏感信息；分析数据包进行流量分析，并获得密码等敏感信息。

【2】实验目的：

掌握数据包抓取方法；掌握分解与分析数据包；理解常见协议报文格式。

【3】教学要求：

要求学生利用流量分析工具分析用户上网流量，基本掌握流量与协议分析方法。

【4】实验方式：

实践操作。

【5】实验场地与设备：

综合楼 1108，部署有实验环境的计算机。

实验项目三：情报收集（支撑课程目标 1-3、1-4、1-5，2-7，3-1、3-2、3-3、3-4、3-5、3-6）

【1】实验内容：

利用系统命令、互联网或特定工具收集靶机或特定主机基本信息；利用 Nmap 等工具，收集目标靶机端口、系统类型、系统应用版本信息；使用漏洞扫描工具，扫描靶机可疑漏洞。

【2】实验目的：

掌握情报收集基本方法，理解隐私保护重要性。

【3】教学要求：

要求学生学习和掌握信息收集方法并理解隐私保护重要性。

【4】实验方式：

实践操作。

【5】实验场地与设备：

综合楼 1108，部署有实验环境的计算机。

实验项目四：网络攻防（支撑教学目标 1-3、1-4、1-5，2-7，3-1、3-2、3-3、3-4、3-5、3-6）

【1】实验内容：

通过弱密码漏洞、文件上传漏洞、应用漏洞、缓冲区溢出漏洞、SQL 注入、DDoS 等常见网络攻击方式进行网络攻击；针对以上攻击制定防御方案。

【2】实验目的：

了解常用网络安全练习平台；掌握常见网络攻击类型；掌握网络安全防御策略。

【3】教学要求：

学会自主搭建实验平台，包括攻击机与靶机的部署与调试；了解常见网络攻击类型，并可对具体攻击方法提出相应防御措施。

【4】实验方式：

实践操作。

【5】实验场地与设备：

综合楼 1108，部署有实验环境的计算机。

实验项目五：系统加固（支撑教学目标 1-3、1-4、1-5，2-7，3-1、3-2、3-3、3-4、3-5、3-6）

【1】实验内容：

对 LAMP 架构实现 Web 服务器加固；对 Linux 操作系统实现系统加固。

【2】实验目的：

通过常见网络安全攻击方式，理解系统加固方法，掌握网络安全防御措施。

【3】教学要求：

并通过日志记录、访问控制等方式，实现系统安全性能提升。

【4】实验方式：

实践操作。

【5】实验场地与设备：

综合楼 1108，部署有实验环境的计算机。

五、教学安排与学时分配

学时分配如表 3 所示。

表 3 学时分配表

讲　　课　　内　　容		学时				
		讲课	实验	上机	设计	课外
第 1 章	网络安全形势与法律基础	2	0	0	0	0
第 2 章	对称密码	8	0	0	0	0
第 3 章	公钥密码	8	2	0	0	0
第 4 章	数据完整性	2	0	0	0	0
第 5 章	互信	4	0	0	0	0
第 6 章	网络与 Internet 安全	6	20	0	0	0
第 7 章	系统安全	2	2	0	0	0
小计		32	24	0	0	0
总计	56					

六、教学方法

1、实践能力传授：理论与行业、实际案例相结合；

2、多媒体教学：基于信息化设备的课堂教学；

3、PBL 教学（Problem-based learning）：问题驱动的分组学习与交流；

4、课程思政建设：知识讲授与德育相结合。

七、成绩评定

1、课程结合平时作业、课堂提问、课堂交流、课程实验和期末考试成绩综合评定成绩。

（1）平时成绩占 10%，主要包括课堂交流、作业、线上资料学习等综合评定。

（2）实验成绩占 20%，主要为上机实验练习、作业和测评。

（3）期末成绩占 70%，主要为试卷成绩（开卷测试）。

2、所缺实验、作业等超过应完成量 1/3 者，或缺课学时超过计划学时 1/3 者，或实验考核成绩不合格者，取消该课程考核资格。

八、评价及持续改进

1、教学大纲

考核周期：4 年，修订周期：4 年。

改进措施：课程负责人组织课程团队所有教师讨论后提出改进意见，经教研室主任审核后由教学院长批准。

2、成绩评定考核

考核周期：1 学年，评价依据：学生最终成绩综合分析。

改进措施：根据学生最终成绩的分布，进行相应的内容调整和优化，并改进教学方法。

撰写：　于七龙

审核：　韩鹏

批准：　史闻博

日期：　2023.07.05