《信息安全（Information security)》

教学大纲

制定时间：2024 年 4 月

一、课程基本信息

（一）适用专业：本科软件工程

（二）课程代码：3DX1197A

（三）学分/课内学时：2 学分/32 学时

（四）课程类别：专业教育

（五）课程性质：选修/理论课

（六）先修课程：《计算机网络》、《C 语言程序设计》、《操作系统》、《数据结构》等

（七）后续课程：《毕业设计》

二、课程教学目标

《信息安全》课程是软件工程专业的一门专业课程，内容涉及信息安全概述、信息收集技术、信息保密技术、信息认证技术、密钥管理技术、访问控制技术、数据库安全、木马及病毒、信息安全防御技术等。通过本课程的学习，学生应对信息安全领域有较全面的了解，同时掌握信息安全技术的基本原理和基本方法。使学生能了解信息安全在信息时代的重要性，培养学生的信息安全防护意识，增强信息系统安全保障能力。

通过本课程的学习，学生应对信息安全领域有较全面的了解，同时掌握信息安全技术的基本原理和基本方法。掌握信息收集技术、信息保密技术、信息认证技术、密钥管理技术、访问控制技术、数据库安全、网络安全技术等理论知识与相关的实践操作技能。同时，培养学生吃苦耐劳、爱岗敬业、团队协作的职业精神和诚实、守信、善于沟通与合作的良好品质，为发展职业能力奠定良好的基础。

（一）具体目标

目标 1：通过本课程的学习，使学生具备解决复杂软件工程问题的科学思维方法、工程设计方法，具备良好的软件工程素养。（对应毕业要求指标点 10.2）

目标 2：具有对复杂软件工程问题的解决实践所涉及的道德、版权、专利、知识产权、安全等进行恰当分析和评价的能力，并能准确理解界定责任和义务边界。（对应毕业要求指标点 10.2）

（二）课程目标与毕业要求的对应关系

毕业要求	毕业要求指标点	课程目标	教学单元	评价方式

1.能够应用数学、自然科学和工程科学的基本原理，识别、表达、并通过文献研究分析系统中的安全问题，以获得有效结论	10.2 能够具备一定的国际视野，能够了解和跟踪软件工程专业的最新发展趋势，具备一定的国际视野，能够通过（图书馆、数据库、网络等）多种资源渠道获取软件工程最新的发展趋势。	目标 1	信息安全概述、分组密码体制、序列密码体制、认证理论与技术、身份认证技术、密钥管理技术	纸笔考试
2.能够基于工程背景知识和技术标准，对计算机应用系统工程进行合理分析，评价系统及其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。	10.2 能够具备一定的国际视野，能够了解和跟踪软件工程专业的最新发展趋势，具备一定的国际视野，能够通过（图书馆、数据库、网络等）多种资源渠道获取软件工程最新的发展趋势。	目标 2	非对称密码体制、认证理论与技术、访问控制与防火墙、漏洞扫描与入侵检测	纸笔考试 平时作业

三、教学内容与方法

（一）教学内容及要求

序号	教学单元	教学内容	学习产出要求	推荐学时	推荐教学方式	支撑课程目标	备注
1	信息安全概述	信息的定义、性质和分类，信息安全的概念，信息安全威胁，信息安全的实现。	了解信息安全的相关概念；掌握信息安全的主要威胁与解决方案	2	讲授	目标 1	
2	密码学基础	密码学发展历史，古典密码中的基本运算，古典密码算法：移位密码、仿射密码、维吉尼亚密码和希尔密码	了解古典密码中的基本运算，掌握移位密码、仿射密码、维吉尼亚密码和希尔密码等古典密码算法及其安全性分析。	2	讲授	目标 1 目标 2	自主学习

序号	教学单元	教学内容	学习产出要求	推荐学时	推荐教学方式	支撑课程目标	备注
		等及其安全性分析。					
3	对称密码体制-分组密码体制	分组密码的定义、原理，典型分组密码体制DES、AES、SMS4，分组密码的工作模式。	了解分组密码的原理，掌握典型分组密码体制DES、AES、SMS4，掌握分组密码的工作模式。	2	讲授	目标1 目标2	自主学习
4	实验一：DES算法的部分实现	实现DES算法中S盒查找功能。	掌握S盒功能的实现原理。	2	讲授 实验	目标1 目标2	
5	对称密码体制-序列密码体制	序列密码的概念及模型，线性反馈移位寄存器，常用的序列密码算法。	掌握序列密码的概念及模型，熟悉线性反馈移位寄存器，掌握常用的序列密码算法。	2	讲授	目标1 目标2	自主学习
6	公钥密码体制	非对称密码的数学基础，非对称密码体制的原理、设计准则和分类等，典型的非对称密码体制，如RSA、ElGamal、ECC算法等，非对称密码算法的比较。	了解非对称密码的数学基础，理解 非对称密码体制的工作原理、设计准则和分类等，理解典型的非对称密码体制，如RSA、ElGamal、ECC算法等，了解非对称密码算法的比较。	2	讲授	目标1 目标2	自主学习
7	实验二：RSA算法的实现	使用小素数，实现RSA功能。	掌握RSA算法加密原理。	2	讲授 实验	目标1 目标2	
8	消息认证	消息认证的基本概念，散列算法的概念、结构	了解散列算法的概念、结构与发展现状，掌握典型的散列算法，如M	2	讲授	目标1 目标2	自主学习

序号	教学单元	教学内容	学习产出要求	推荐学时	推荐教学方式	支撑课程目标	备注
		与发展现状，典型的散列算法，如 MD5、SHA-1 等，散列函数的攻击现状，消息认证，数字签名的原理，典型的数字签名方案（如基于 RSA、ElGamal 和 DSA 的签名方案）。	D5、SHA-1 等，了解散列函数的攻击现状，理解消息认证，掌握数字签名的原理，了解典型的数字签名方案。				
9	身份认证与数字签名	认证模型及认证协议，身份认证技术，基于零知识证明的身份认证技术，Kerberos 及 X.509 身份认证技术。	了解认证模型及认证协议，掌握身份认证技术，掌握基于零知识证明的身份认证技术，理解 Kerberos 及 X.509 身份认证技术。	2	讲授	目标 1 目标 2	自 主学习
10	实验三：消息摘要算法 SHA-1 的实现	按照标准的要求，用程序实现 SHA-1 算法的填充部分。	掌握定长消息摘要计算算法。	2	讲授 实验	目标 1 目标 2	
11	密钥管理	密钥的结构与分类，密钥管理的周期，密钥托管，密钥协商与分配。	了解密钥的结构与分类，理解密钥管理的周期，掌握密钥托管，掌握密钥协商与分配。	2	讲授	目标 1 目标 2	自 主学习
12	实验四：PGP 软件的使用	掌握 PGP 加密软件的密钥生成及管理。	掌握密码软件的实际应用	2	讲授 实验	目标 1 目标 2	自 主学习

序号	教学单元	教学内容	学习产出要求	推荐学时	推荐教学方式	支撑课程目标	备注
13	网络攻击技术	常见系统漏洞，漏洞扫描技术,入侵检测技术，审计技术。	常见系统漏洞，漏洞扫描技术，入侵检测技术，审计技术。了解常见系统漏洞的原理；了解常见的入侵检测技术；掌握常用的扫描工具。	4	讲授	目标 1 目标 2	
14	实验五：HTTP 头分析及 cookie 欺骗	在 Windows 系统中搭建 IIS，并配置 ASP.NET 环境，cookie 工具使用。	掌握 IIS 设置及 web 系统部署及 cookie 欺骗方法。	2	讲授 实验	目标 2	自主学习
15	实验六：SQL 注入	SQL 注入漏洞的检测及查找方法。	掌握 SQL 注入点寻找方法。	2	讲授 实验	目标 2	自主学习

（二）教学方法

1.课堂讲授

（1）采用启发式教学，激发学生主动学习的兴趣，培养学生独立思考、分析问题和解决问题的能力，引导学生主动通过实践和自学获得自己想学到的知识。

（2）在教学内容上，系统讲授信息安全概述、古典密码、对称密码体制、非对称密码体制、HASH 函数和消息认证、数字签名、密钥管理访问控制、网络攻击技术等。

（3）在教学过程中采用多媒体教学与传统板书、教具教学相结合，提高课堂教学信息量，增强教学的直观性。

（4）理论教学与工程实践相结合，引导学生应用数学、自然科学和工程科学的基本原理，采用现代设计方法和手段，解决安全模型建立、加密算法选择领域面临的问题，培养学生解决网络安全问题的思维方法和实践能力。

2.实验教学

实验教学是密码学理课程中重要的实践环节，目的是培养学生运用实验方法研究解决网络安全领域数据保护的能力。课程必做实验 6 个，各实验按照实验指导书的要求学生独立完成，并提交实验报告。鼓励学生结合自己的兴趣进行自主实验。

四、考核及成绩评定

（一）考核内容及成绩构成

课程目标	考核内容	成绩评定方式	成绩占总评分比例	目标成绩占当次考核比例	学生当次考核平均得分	目标达成情况计算公式
目标 1：具备解决复杂软件工程问题的科学思维方法、工程设计方法，具备良好的软件工程素养。	信息安全基本概念和问题根源、信息安全模型、密码体制的分类、古典密码原理及典型算法、分组密码原理及典型算法、序列密码原理及典型算法、非对称密码原理及典型算法、消息摘要原理、身份认证原理。	纸笔考试	35%	100%	T1	$\frac{(\frac{T1}{100\%}\times 35\% + \frac{E1}{50\%}\times 10\% + \frac{A1}{50\%}\times 5\%)}{50}$
		实验	10%	50%	E1	
		平时作业	5%	50%	A1	
目标 2：具有对复杂软件工程问题的解决实践所涉及的道德、版权、专利、知识产权、安全等进行恰当分析和评价的能力，并能准确理解界定责任和义务边界。	访问控制、网络攻击技术	纸笔考试	35%	100%	T2	$\frac{(\frac{T2}{100\%}\times 35\% + \frac{E2}{50\%}\times 10\% + \frac{A2}{50\%}\times 5\%)}{50}$
		实验	10%	80%	E2	
		平时作业	5%	50%	A2	
总评成绩（100%）=实验（20%）+纸笔考试（70%）+平时作业（10%			100%	-	-	$\frac{学生总评平均分}{100}$

（二）平时考核成绩评定

1.平时作业：平时作业 2 次，支持目标 1、目标 2，共占总评分 10%，目标 1 占 5%、目标 2 占 5%。对应目标评分标准如下：

对应目标		目标 1：具备解决复杂软件工程问题的科学思维方法、工程设计方法，具备良好的软件工程素养	目标 2：具有对复杂软件工程问题的解决 实践所涉及的道德、版权、专利、知识产 权、安全等进行恰当分析和评价的能力， 并能准确理解界定责任和义务边界。
考查点		作业内容	成果显示、讲解
总评分占比		50%	50%
评分标准	**100%至90%**	对信息安全现状了解深入，对技术应用熟练；能够根据提出的问题，构建可行的解决方案，并具有个人独到的见解。	分析案例选择合理，密码技术应用原理分析透彻，语言描述准确通畅，符合规范。
	89.9%至80%	对信息安全现状了解深入，对技术应用相对熟练；能够根据提出的问题，构建基本可行的解决方案，并具有个人的见解。	分析案例选择合理，密码技术应用原理分析较为透彻，语言描述准确通畅，符合规范。
	79.9至70%	对信息安全现状基本了解，对技术应用水平一般；能够根据提出的问题，构建有一定参考价值的解决方案，但缺乏个人见解。	分析案例选择较为合理，密码技术应用原理分析较为透彻，语言描述准确通畅，符合规范。
	69.9%至60%	对信息安全现状了解甚少，对技术应用水平非常一般；对提出的问题，很难独立完成解决方案的构建；对相关安全问题缺乏个人见解。	分析案例选择较为合理，密码技术应用原理分析较为恰当，语言描述较为准确通畅，基本符合规范。
	59.9%至0	分析案例选择不恰当，密码技术应用原理分析错误，语言描述错误较多，多处不符合规范。	分析案例选择不恰当，密码技术应用原理分析错误，语言描述错误较多，多处不符合规范。

2.实验：实验 6 次，支持目标 1、目标 2，共占总评分 20%，目标 1 占 10%、目标 2 占 10%。对应目标评分标准如下：

对应目标		目标 1：具备解决复杂软件工程问题的科学思维方法、工程设计方法，具备良好的软件工程素养。	目标 2：具有对复杂软件工程问题的解决实践所涉及的道德、版权、专利、知识产权、安全等进行恰当分析和评价的能力，并能准确理解界定责任和义务边界。
考查点		实验内容	实验报告
总评分占比		50%	50%
评分标准	**100%至90%**	安全管理策略制定科学、严谨；熟练使用各类网络安全工具，能够准确分析网络安全中的相关漏洞及缺陷；能够提出可行的网络安全解决方案，效果良好。	有很强的总结实验和撰写报告的能力，实验报告内容完整、正确，有很好的分析与见解。文本表述清晰，书写工整，格式规范，专业术语用语准确。
	89.9%至80%	安全管理策略制定科学；熟练使用各类网络安全工具，能够准确分析网络安全 中的相关漏洞及缺陷；能够提出可行的 网络安全解决方案。	有较强的总结实验和撰写报告的能力，实验报告内容完整、正确，有较好的分析与见解。文本表述较为清晰，书写比较工整，格式规范。
	79.9至70%	安全管理策略制定较为完备；熟练使用主流网络安全工具，能够准确分析网络 安全中的相关漏洞及缺陷；能够提出可 行的网络安全解决方案。	有良好的总结实验和撰写报告的能力，实验报告内容较完整、正确，有自己的分析与见解。文本表述较为清晰，书写较为工整，格式较为规范。
	69.9%至60%	安全管理策略制定合理；能够使用主流的网络安全工具，能够分析网络安全中 的相关漏洞及缺陷；能够提出适当的网 络安全解决方案	有一定的总结实验和撰写报告的能力，实验报告内容基本完整、正确，没有分析或见解。文本表述基本清晰，书写基本工整，格式基本规范。
	59.9%至0	安全管理策略制定有待完善；能够使用一些网络安全工具，对网络安全中的相 关漏洞及缺陷有所了解；对网络安全解 决方案的制定缺乏完整性和可行性。	总结实验和撰写报告的能力差，实验报告内容不完整、错误多。文本表述不清晰，书写潦草、格式不规范。

五、参考学习资料

（一）推荐教材：熊平,朱天清. 信息安全原理及应用（第 3 版）. 北京：清华大学出版社，2016.

（二）参考资料：

贾铁军.网络安全技术及应用实践教程.北京：机械工业出版社，2016.张健,任洪娥,黄英来,郭继峰,李三平.信息安全原理与应用技术[M].清华大学出版社，2016.

（三）在线资源：《网络安全——应用技术与工程实践》https://www.icourse163.org/learn/BIT-1449611164?tid=1450076442

360 网络安全大学：https://university.360.cn/index.html

制订人：　李卫卫　　审核人：