《信息安全》教学大纲

课程编码：112709
课程名称：信息安全
学时/学分：46/2
先修课程：
适用专业：信息与计算科学
开课教研室：信息与计算科学教研室

一、课程性质与任务

1．课程性质：本课程是信息与计算科学专业的专业基础课，是信息与计算科学专业信息方向学生的必修课。

2．课程任务：本课程针对信息与计算科学专业学生的发展需求，通过一系列数学基础理论、密码学相关知识和信息安全体系的学习，把数学的相关知识融入信息与计算机方面的应用当中，从而使学生保持浓厚的学习热情，加深对专业知识的认识、理解和掌握。课程内容涉及大量前沿科技动态，具有很强的实用性。

二、课程教学基本要求

《信息安全》是信息与计算科学专业中信息方向的核心课程，所以该方向的学生均需学习并掌握信息安全与密码学的相关技术理论和工具方法，这是深入理解和从事有关信息安全行业工作的基础。因此信息安全在信息与计算科学专业课程中占有不可替代的地位。

本课程的先修课程有《高等代数》、《离散数学》、《计算机文化基础》、《C 程序设计》等，学生应掌握线性代数、离散数学和程序设计等方面的基础知识。通过本课程的学习，使学生对密码学的原理、思想和算法都有一定的了解。同时，基于密码系统设计的基本方法和基本步骤，帮助学生理解密码学在信息安全中的地位，并引导了解密码学领域及信息安全领域的新进展、新方向。掌握本课程后，可以为以后的网络安全的分析、设计与开发奠定坚实的专业基础。

通过本课程的学习各种信息安全概念、传统密码算法、公钥密码体制、Hash 函数等多种密码学工具，培养学生的密码学素养与分析问题解决问题的能力，为学生今后从事各种实际工作打下坚实的基础。

成绩考核形式：末考成绩（闭卷考查）（70%）＋平时成绩（平时测验、作业、课堂提问、课堂讨论等）（30％）。成绩评定采用百分制，60 分为及格。

三、课程教学内容

第一章　　绪　论

1. 教学基本要求

让学生了解信息安全和密码学的概念与研究目标，从而对本课程的内容与应用范围有一个全面的理解。

2. 要求学生掌握的基本概念、理论、技能

通过本章教学使学生了解信息安全的目的、内容与基本模型，掌握信息安全的几种攻击类型；理解信息安全与密码学之间的关系；了解密码学的发展历程，能够区别不同的密码体制，并知道各种密码体制的主要特点；掌握密码学的基本术语与基本模型。

3. 教学重点和难点

教学重点是信息安全与密码学的基本模型，密码体制的分类与攻击类型。教学难点是理解密码学在信息安全系统中所处的位置，与不同密码体制的特点与区别。

4. 教学内容

第一节　　信息安全

1. 信息安全的目的
2. 信息安全中攻击的基本类别
3. 信息安全的基本模型
4. 信息安全研究的基本内容

第二节　　密码学

1. 密码学发展简史
2. 密码体制分类
3. 密码体制的攻击类型
4. 密码学的基本术语
5. 密码学的基本模型
6. 密码学与信息安全的关系

第二章　　信息安全初步

1. 教学基本要求

掌握信息安全主要任务的特点和实现手段。

2. 要求学生掌握的基本概念、理论、技能

通过本章学习，使学生理解每一个信息安全模块的任务和目标，对信息安全体系有一个正确的认识。掌握每一模块存在的必要性，并了解现实中有哪些具体的应用。

3. 教学重点和难点

教学重点是信息安全的主要需求与解决方案。教学难点是理解这些解决方案的有效性与实际中的应用。

4. 教学内容

第一节　　引言

第二节　　身份识别

1. 基于物理形式的身份识别技术
2. 基于密码技术的身份识别协议

第三节　　机密性保护

1. 机密性保护粒度
2. 机密性保护方法

第四节　　数据完整性保护

1. 完整性保护粒度
2. 完整性保护方法

第五节　　不可抵赖性

第六节　　访问控制

1. 访问控制粒度
2. 访问控制策略
3. 访问控制实现机制与方法

第三章　　信息安全技术

1. 教学基本要求

理解信息安全应用的几类主要技术，掌握这些技术的实现方式。

2. 要求学生掌握的基本概念、理论、技能

通过本章学习，使学生了解密码学的加密、数字签名、身份识别等技术，为后续章节的具体内容学习打下基础；理解整个信息安全体系的结构；掌握与通信技术相关的数据检测技术，理解完整性对于数据传输的意义；对数据存储工具的访问和数据恢复有一个初步的了解。

3. 教学重点和难点

教学重点是加密技术、数字签名、访问控制与身份识别技术。教学难点是对信息安全体系的理解。

4. 教学内容

第一节　　保护技术

1. 加密技术
2. 数字签名

3. 访问控制

4. 身份识别

5. 通信量填充与信息隐藏

6. 路由控制

7. 公证

8. 安全标记

第二节　检测技术

1. 数据完整性

2. 事件检测与安全审计

第三节　恢复技术

1. 运行状态恢复

2. 数据恢复

第四节　信息安全体系

1. 信息安全技术体系

2. 信息安全组织体系

3. 管理体系

第四章　传统密码学

1.教学基本要求

掌握传统密码学的基本要求，理解 DES 加密算法与 AES 加密算法的流程。

2.要求学生掌握的基本概念、理论、技能

通过本章学习，使学生了解传统的分组密码的运作模式与基本要求；掌握 DES 加密算法各个基本模块的特点与作用，DES 算法的加密流程、解密流程与基本的安全性分析；理解 AES 算法的数学基础，掌握整个 AES 算法的特点与加解密流程；区别 DES 与 AES 的安全性理论基础。

3.教学重点和难点

教学重点是 DES 算法与 AES 算法的加解密流程与算法特点。教学难点是对 DES 算法与 AES 算法安全性分析的理解。

4.教学内容

第一节　传统密码学的基本知识

1. 机密性要求

2. 完整性要求

第二节　DES 加密算法

1. 初始置换 IP

2. 圈函数

3. 密钥扩展

4. 脱密

5. DES 的安全性

第三节　三重 DES

第四节　AES

1. 数学基础

2. Rijndael 的状态、密钥和圈函数

3. 圈变换

4. 密钥扩展

5. 加/脱密流程图

第五章　公钥密码算法

1.教学基本要求

掌握 RSA 与 ElGamal 等密码算法的数学基础、加解密流程与安全性理论。

2.要求学生掌握的基本概念、理论、技能

通过本章学习，使学生了解公钥密码体制的特点与基本模块；了解 RSA 与 ElGamal 等密码算法的数学基础，掌握其加解密的步骤，与安全性所依赖的理论基础；掌握 Diffie-Hellman 算法的步骤，理解其运作机制。

3.教学重点和难点

教学重点是 RSA 与 ElGamal 等密码算法的加解密步骤与安全性分析。教学难点是对这些算法构造理念的理解。

4.教学内容

第一节　RSA 密码算法

1. 算法的描述

2.计算方面

3. 安全性方面

第二节　ElGamal 算法

1. ElGamal 算法描述

2. 离散对数问题与 EIGamal 密码体制的安全性

第三节　椭圆曲线密码体制

1. 有限域上的椭圆曲线

2. 椭圆曲线离散对数问题与安全性

第四节　Diffie-Hellman 算法

1. Diffie-Hellman 算法描述
2. Diffie-Hellman 算法举例

第五节　MH 背包公钥密码系统

1. 背包（Knapsack）问题
2. MH 背包公钥密码系统描述

第六章　Hash 函数

1.教学基本要求

了解 Hash 函数的构造方式，掌握 MD5 算法的流程与安全性分析。

2.要求学生掌握的基本概念、理论、技能

通过本章学习，使学生了解 Hash 函数主要的三种构造方式，与不同构造方式的特点；掌握 MD5 算法的流程与安全性分析；理解基于分组密码的 Hash 函数的特点与构造机制。

3.教学重点和难点

教学重点是 MD5 的实现步骤与安全性分析。教学难点是对 Hash 函数概念的整体把握。

4.教学内容

第一节　Hash 函数的性质

第二节　Hash 函数 MD5

1. MD5 算法描述
2. MD5 算法的安全性

第三节　Hash 函数 SHA-1

第四节　基于分组密码的 Hash 函数

1. 构造 Hash 函数的一般性原则
2. 基于分组密码算法构造 Hash 函数

四、学时分配

1.讲授内容及学时分配

章序	内容	课时	备注
一	绪论	7	
二	信息安全初步	5	
三	信息安全技术	3	
四	传统密码学	7	
五	公钥密码算法	14	
六	Hash 函数	8	

五、主用教材及参考书

（一）主用教材：

《信息安全与密码学》主编：徐茂智 出版社：清华大学出版社 出版时间：2007 年。

（二）参考书：

1. 《密码学导引》主编：裴定一 出版社：科学出版社 出版时间：1999 年。

2. 《应用密码学：协议、算法与 C 源程序》主编：Bruce Schneier 出版社：机械工业出版社 出版时间：2000 年。

3.《密码学原理与实践》主编：Douglas R. Stinson 出版社：电子工业出版社 出版时间：2009 年。

执笔：董乐

审定：皮磊 梁桂珍