《密码学》教学大纲

课程编码：110895

课程名称：密码学

学时/学分：54/3

先修课程：《概率论》、《抽象代数》

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任意选修课。

2．课程任务：通过本课程的学习使学生了解密码学的一些基本概念，理解和掌握古典密码体制，分组密码体制、分钥密码体制、流密码、数字签名、密码协议的基本概念、基本理论、以及基本运算，领会密码体制设计与分析的基本思想与方法，理解密码产品的基本工作原理，以及培养学生在实践中解决问题的能力。

二、课程教学基本要求

通过本课程学习，让学生掌握密码学的基础理论中的基本概念、原理、方法的含义，较全面掌握应用密码学的基本密码协议和基本技术，并熟练掌握一些典型的密码学方案，能表达基本内容和基本道理，分析相关问题的区别与联系。

本课程理论学时 54 学时。

成绩考核形式：期终成绩（考查）（70%）＋期中成绩（20%）+平时成绩（平时测验、作业、课堂提问、课堂讨论等）（10％）。成绩评定采用百分制，60 分为及格。

三、课程教学内容

第一章　　密码学概论

1. 教学基本要求

理解密码学的基本概念及体系结构，包括密码体制的结构、安全性以及攻击类型。对密码学发展的历史及其应用前景有一定的了解。

2. 教学重点和难点

教学重点：密码体制的结构。

教学难点：密码体制的安全性和攻击类型。

3. 教学内容

（1）密码学的基本概念

（2）密码学的发展概况

第二章　　古典密码

1. 教学基本要求

掌握几种古典密码的概念、加解密算法及其破译方法。理解无条件安全的一次一密体制的设计方法和原理，了解其局限性。

2. 教学重点和难点

教学重点：古典密码的基本概念及分类。

教学难点：几种古典密码的加密算法及破译。

3. 教学内容

（1）代换密码

（2）置换密码

（3）古典密码的破译

（4）无条件安全的一次一密体制

第三章　　现代分组密码

1. 教学基本要求

掌握分组密码的基本原理，在对一些基本数学知识的理解下，熟练掌握数据加密标准 DES 和高级加密标准 AES 的加解密原理及其流程。掌握分组密码的 4 种基本工作方式。了解差分分析法和线性分析法。

2. 教学重点和难点

教学重点：数据加密标准 DES 和高级加密标准 AES 的加解密原理及其流程。

教学难点：差分分析法和线性分析法

3. 教学内容

（1）代换置换网络

（2）分组密码原理与设计准则

（3）数据加密标准 DES

（4）高级加密标准 AES

（5）分组密码的操作模式

（6）差分分析与线性分析

第四章　　流密码

1. 教学基本要求

理解流密码的原理，了解有限状态自动机，熟练掌握线性反馈移位寄存器

2. 教学重点和难点

教学重点：流密码的原理。

教学难点：线性反馈移位寄存器的工作原理及其在流密码设计中的应用。

3.教学内容

（1）流密码的原理

（2）有限状态自动机

（3）线性反馈移位寄存器

第五章　　公钥密码

1.教学基本要求

掌握公钥密码的数学基础知识，熟练掌握 RSA 公钥密码体制 EIGamal 公钥密码体制，理解其安全性和和易遭受的攻击方法，掌握 Diffie-Hellman 密钥协商方案

2.教学重点和难点

教学重点：RSA 公钥密码体制 EIGamal 公钥密码体制。

教学难点：Diffie-Hellman 密钥协商方案。

3.教学内容

（1）公钥密码体制简介

（2）公钥密码的数学基础知识

（3）RSA 公钥密码体制

（4）EIGamal 公钥密码体制

（5）Diffie-Hellman 密钥协商方案

第六章　　密钥管理

1.教学基本要求

对密钥的产生、存储、装入、分配、保护、丢失、销毁等内容有一定的理解。理解密钥分配、密钥传送、密钥协商、秘密共享、会议密钥广播与分发、密钥托管等概念及实现方法。

2.教学重点和难点

教学重点：密钥分配、密钥传送、密钥协商。

教学难点：会议密钥广播与分发、密钥托管的概念及实现方法。

3.教学内容

（1）密钥分配模式

（2）密钥传送

（3）密钥协商

（4）秘密共享

（5）会议密钥广播与分发

（6）密钥托管

第七章　　Hash 函数

1. 教学基本要求

理解 Hash 函数的概念、性质及应用。

2. 教学重点和难点

教学重点：hash 函数的用途。

教学难点：hash 函数的攻击方法。

3. 教学内容

（1）Hash 函数简介

（2）Hash 函数的安全性

（3）hash 函数的攻击方法

（4）hash 函数的用途

第八章　　数字签名

1. 教学基本要求

理解数字签名体制的概念,掌握 RSA、ElGamal 数字签名方案和数字签名标准 DSS，对其安全性有所了解,了解其他特殊数字签名方案及其应用。

2. 教学重点和难点

教学重点：RSA、ElGamal 数字签名方案。

教学难点：数字签名标准 DSS 及其安全性。

3. 教学内容

（1）数字签名体制

（2）RSA 数字签名方案

（3）EIGamal 签名方案

（4）Schnorr 数字签名方案

（5）数字签名标准 DSS

（6）椭圆曲线数字签名方案及其他特殊数字签名介绍

第九章　　身份识别

1. 教学基本要求

理解身份识别的概念，理解强、弱身份识别的分类及流程，掌握几个典型的身份识别协议，了解身份识别的安全性。

2. 教学重点和难点

教学重点：身份识别的概念。

教学难点：强、弱身份识别的分类及流程。

3.教学内容

（1）身份识别的概念

（2）弱身份识别

（3）强身份识别

（4）身份识别协议

（5）身份识别协议的安全

四、学时分配

章序	内容	课时	备注
一	密码学概论	2	
二	古典密码	2	
三	现代分组密码	12	
四	流密码	6	
五	公钥密码	10	
六	密钥管理	6	
七	Hash 函数	4	
八	数字签名	6	
九	身份识别	6	
合计		54	

五、主用教材及参考书

（一）主用教材：

《密码学教程》 主编：张福泰 出版社：武汉大学出版社 出版时间： 2006 年

（二）参考书：

1.《现代密码学》主编：陈鲁生 出版社：科学出版社 出版时间：2002 年。

2.《现代密码学理论与实践》 主编：Wenbo Mao 出版社：电子工业出版社 出版时间：2004 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：2003 年。

执笔：杜蛟

审定：皮磊 梁桂珍