《现代密码学》教学大纲

课程名称：现代密码学

英文名称：Modern Cryptography

课程编号：0602003120

课程性质：专业必修课

先修要求：高等数学、离散数学、概率论、信息安全的数学基础、信息论与编码、计算机网络

适用专业：信息安全专业及相关专业

任课老师：方贤进、葛斌、王丽、赵宝

一、教学目标

通过本课程的理论教学及实验训练，使学生具备以下知识和能力：

目标 1：掌握密码学与信息安全的关系、信息安全的目标（5 要素）；掌握现代密码学的研究内容与体系结构；掌握保密系统的模型及安全性、认证系统的模型及安全性。

目标 2：掌握古典密码体制中的两种方法：置换密码与代换密码；掌握古典密码分析方法，能使用“拟重合指数法”对“多表代换加密”实行“唯密文攻击”。

目标 3：掌握 DES 加密算法、AES 加密算法，能够在实际的应用系统或安全系统中实现。

目标 4：掌握序列密码的算法 A5、RC6，具备在通讯系统的设计中实现的能力。

目标 5：掌握 hash 函数 MD5、SHA-1 算法，具备在实际应用中消息认证、实体认证系统实现的能力。

目标 6：掌握公钥密码体制模型、RSA 算法、ECC 算法、基于 RSA 和 ECC 的数字签名机制；能够在实际应用中利用公钥密码算法及签名机制实现加解密、数字签名、公钥基础设施平台的能力。

二、课程教学目标与毕业要求的对应关系

教学目标	毕业要求	支撑强度
目标 1	1.2 具有扎实的专业基础理论，包括信息论与编码、密码学原理、信息安全数学基础、计算机网络技术等，能够用其解决信息安全相关领域的复杂工程问题；	H
	1.3 培养学生掌握扎实的信息安全理论知识和核心知识，了解学科的知	M

	识组织结构、学科形态、典型方法、核心概念等；	
	3.5 能基于信息安全专业相关背景知识分析和评价解决方案对社会、经济、法律、安全、健康等因素的影响。	M
目标 2	3.1 具有工程实习、工程设计及社会实践经历，能根据用户要求确定设计目标；	H
	1.2 具有扎实的专业基础理论，包括信息论与编码、密码学原理、信息安全数学基础、计算机网络技术等，能够用其解决信息安全相关领域的复杂工程问题；	H
	3.2 能够设计满足信息获取、传输、处理或使用等需求的系统，并能够在设计环节中体现创新意识；	L
目标 3	3.4 熟悉信息安全专业相关技术标准、知识产权、产业政策和法规，并能在其现实约束条件下，通过技术经济评价对设计方案进行可行性研究；	M
	2.1 能够应用信息安全的基本原理，研究分析信息安全领域复杂工程问题；	H
	1.2 具有扎实的专业基础理论，包括信息论与编码、密码学原理、信息安全数学基础、计算机网络技术等，能够用其解决信息安全相关领域的复杂工程问题；	H
目标 4	4.3 能够基于信息安全专业理论，选择合适的研究路线、设计可行的实验方案；	M
	2.1 能够应用信息安全的基本原理，研究分析信息安全领域复杂工程问题；	H
	1.2 具有扎实的专业基础理论，包括信息论与编码、密码学原理、信息安全数学基础、计算机网络技术等，能够用其解决信息安全相关领域的复杂工程问题；	H
目标 5	2.1 能够应用信息安全的基本原理，研究分析信息安全领域复杂工程问题；	M
	1.2 具有扎实的专业基础理论，包括信息论与编码、密码学原理、信息安全数学基础、计算机网络技术等，能够用其解决信息安全相关领域的复杂工程问题；	H
	4.5 能正确采集、整理实验和模拟数据，对实验及模拟结果进行关联、建模、分析处理，获取合理有效的结论。	M
目标 6	4.5 能正确采集、整理实验和模拟数据，对实验及模拟结果进行关联、建模、分析处理，获取合理有效的结论。	H
	4.3 能够基于信息安全专业理论，选择合适的研究路线、设计可行的实验方案；	H
	3.4 熟悉信息安全专业相关技术标准、知识产权、产业政策和法规，并	L

	能在其现实约束条件下，通过技术经济评价对设计方案进行可行性研究；	

备注：H-高度支撑；M-中度支撑；L-一般支撑。

三、课程教学主要内容

课程导入内容

第 1 章 密码学概论（支撑教学目标 1）

1.1 信息安全与密码学

1.2 密码学发展史

第 2 章 密码学基础 (支撑教学目标 1)

2.1 密码学分类

2.2 保密系统模型

2.3 认证系统模型

第 3 章 古典密码体制 (支撑教学目标 2)

3.1 置换密码

3.2 代换密码

3.3 古典密码体制分析

第 4 章 分组密码(支撑教学目标 3)

4.1 分组密码的定义

4.2 分组密码的发展史

4.3 DES 算法

4.4 AES 算法

4.5 分组密码算法的运行模式

第 5 章 序列密码(支撑教学目标 4)

5.1 序列密码简介

5.2 线性反馈移位寄存器

5.3 m 序列及其生成算法

5.4 m 序列密码的破译

5.5 A5 算法

第 6 章 HASH 函数与消息认证码(支撑教学目标 5)

6.1 hash 函数的定义

6.2 hash 函数的通用结构

6.3 MD5 算法及其它 hash 函数

6.4 消息认证

6.5 生日攻击

第 7 章 公钥密码体制(支撑教学目标 6)

7.1 公钥密码体制的基本概念

7.2 RSA 算法

7.3 椭圆曲线加密算法

第 8 章 数字签名技术(支撑教学目标 6)

8.1 数字签名简介

8.2 基于 RSA 数字签名

8.3 基于 ECC 数字签名

第 10 章 密钥管理(支撑教学目标 6)

10.1 密钥管理的简介

10.2 密钥的生命周期

10.3 公钥证书

10.4 密钥分配

10.5 密钥协商

10.6 密钥托管

10.7 密钥分割

实验课程内容 (支撑教学目标 1、2、3、6)

设计性实验一：多表代换 Vigenere 加解密算法及密钥破解算法的实现

验证性实验二：AES 加密、解密算法的实现

验证性实验三：利用 RSA 算法实现加解密、数字签名

设计性实验四：椭圆曲线加密算法的设计与实现

四、建议教学进度

章节内容	学时数
导入内容	1
第 1 章 密码学概论	2
第 2 章 密码学基础	2
第 3 章 古典密码体制	4
第 4 章 分组密码	6
第 5 章 序列密码	4
第 6 章 HASH 函数与消息认证码	5

第 7 章 公钥密码体制	8
第 8 章 数字签名技术	4
第 10 章密钥管理	4
现代密码学实验	8
总学时	48

五、教学方法

1．阐述基本原理，理论联系实际，培养学生实际动手能力、创新能力；

2．课堂讲授注意采用启发式教学，激励学生思考；利用多媒体课件等教学手段，强化讲课效果；

3．建立了专门的《现代密码学》课程建设网站，其中不仅有教学课件、课程介绍、课堂教学大纲、教案设计，还有四个实验任务书和指导书，以强化信息安全专业的学生实际动手能力、设计能力、创新能力的培养。

4．专门的课程建设网站为 http://star.aust.edu.cn/~xjfang/crypto/

5．由于《现代密码学》主要是讲解算法、模型及协议，比较抽象，因此课程组开发了一些辅助教学软件（见课程建设网站），用以提高教学效果。

6．下一步拟在专门的课程建设网站中开发《现代密码学》课程教学的师生互动、答疑模块。

六、考核方式

闭卷笔试，课程作业、实验成绩、课堂表现、考勤。

七、成绩评定方法

期末笔试成绩占 80%，平时成绩占 20%（根据课程作业、实验成绩、课堂表现、考勤等）。

八、主要参考书籍

1．谷利泽，郑世慧，杨义先. 现代密码学教程. 北京邮电大学出版社，2015.3（教材）。

2．B. Schneier. Applied cryptograghy second edition: protocols, algorithms, and source code in C. NewYork: John Wiley & Sons, 1996. 中译本：吴世忠，祝世雄，张文政译。

3．马春光. 现代密码学教程，哈尔滨工程大学自编讲义。

大纲编写者：方贤进，xjfang@aust.edu.cn， http://star.aust.edu.cn/~xjfang/crypto/