《应用密码学》

课程教学大纲

一、 课程基本信息

课程类型	总学时为学时数	☑理论课（含上机、实验学时）			
	总学时为周数	□实习 □课程设计 □毕业设计			
课程编码	7242211	总学时	32 学时	学分	2 学分
课程名称	应用密码学				
课程英文名称	Applied Cryptography				
适用专业	信息安全				
先修课程	（7001631）C 程序设计、（7241101）信息安全数学基础				
开课部门	信息学院计算机系				

二、 课程性质与目标

本课程为信息安全专业的必修课。本课程为学生后续其它密码学专业课程的学习奠定理论基础，目的是让学生熟悉使学生学习和掌握古典密码体制、分组加密体制、流密码体制、消息认证码、公钥加密体制、数字签名体制和密码协议的基本概念、密码算法的设计，掌握现代密码学的设计技术和分析技术的基础知识，了解密码学的新进展，培养学生做出创新工作能力。

课程目标 1：学生应了解现代密码学的发展及其研究的主要内容、现代密码学的主要知识体系、基本理论

课程目标 2：学生应掌握各类典型的密码算法，了解各算法的发展状况及其安全状况

课程目标 3：学生应能掌握把密码思想融入到社会生活中思想

课程思政目标：本门课程在培养学生专业素质和思维能力的同时，通过将密码学技术和国家安全教育紧密结合，加深学生对国家安全，特别是网络空间安全的理论知识学习，使学生加深对信息安全专业的热爱，培养民族使命感和责任感。

三、 课程教学基本内容与要求

应用密码学课程共 32 学时，其中理论授课 32 学时。学时分配如表 1 所示。

表 1 学时分配表

总学时	讲授学时

32	32

1．课程重点

信息安全与密码学；数论；近世代数理论；分组密码；数据加密标准（DES）；AES 算法；序列密码；线性反馈移位寄存器；Hash 函数；Hash 算法；消息认证；公钥密码体制；RSA 公钥密码；椭圆曲线公钥密码；数字签名的实现方案；密码协议；零知识证明；安全多方计算；密钥管理；密钥生命周期；密钥分发技术；密钥协商技术

2．课程难点

数论；近世代数理论；香农理论；复杂度理论；数据加密标准（DES）；线性反馈移位寄存器；非线性序列；Hash 函数的攻击；RSA 公钥密码；椭圆曲线公钥密码；数字签名的实现方案；零知识证明；安全多方计算；密钥生命周期；密钥分发技术；秘密共享技术；量子密码学

3. 课堂教学（32 学时）

表 2 各知识单元教学内容、考核要求和学时分配

第一知识单元　密码学概论					
学时分配		2 学时	教学方式	课堂讲授，ppt 电子课件，板书	
教学内容				重点	难点
1	信息安全与密码学			√	
2	密码学发展史				
3	密码学基础				
考核要点	密码体制模型和原则；密码学的分类和体制；信息安全目标				
第二知识单元　传统密码体制					
学时分配		2 学时	教学方式	课堂讲授，ppt 电子课件，代码阅读及演示，板书	
教学内容				重点	难点
1	置换密码				
2	代换密码				

3	传统密码分析				
考核要点	置换密码和代换密码的原理；各种传统密码算法的原理；密码算法设计的基本思想				
第三知识单元　密码学基础					
学时分配	4 学时	教学方式	课堂讲授，ppt 电子课件，板书		
教学内容				重点	难点
1	数论			√	√
2	近世代数			√	√
3	香农理论				√
4	复杂度理论				√
考核要点	数论；近世代数；香农理论；复杂度理论				
第四知识单元　分组密码					
学时分配	6 学时	教学方式	课堂讲授，ppt 电子课件，代码阅读及演示，板书		
教学内容				重点	难点
1	分组密码概述			√	
2	数据加密标准（DES）			√	√
3	AES 算法			√	√
4	典型分组密码				
5	分组密码的工作模式				
考核要点	分组密码的设计思路；DES 算法的实现；分组密码的工作模式；加密标准 AES 和 SMS4				
第五知识单元　序列密码					

学时分配		2 学时	教学方式	课堂讲授，ppt 电子课件，板书	
教学内容				重点	难点
1	序列密码简介			√	
2	线性反馈移位寄存器			√	√
3	非线性序列				
4	典型序列密码算法				
考核要点	序列密码的原理； RC4 的实现；移位寄存器技术的流密码算法；移位寄存器序列；m 序列				
第六知识单元 Hash 函数和消息认证					
学时分配		4 学时	教学方式	课堂讲授，ppt 电子课件，板书	
教学内容				重点	难点
1	Hash 函数			√	
2	Hash 算法			√	
3	消息认证				
4	Hash 函数的攻击				√
考核要点	典型 hash 算法和 MAC 算法；杂凑函数和消息认证码的概念；MD5；CBC-MAC；HMAC				
第七知识单元 公钥密码体制					
学时分配		4 学时	教学方式	课堂讲授，ppt 电子课件，板书	
教学内容				重点	难点
1	公钥密码体制概述			√	

2	RSA 公钥密码	√	√
3	ElGamal 公钥密码		
4	椭圆曲线公钥密码	√	√
5	其它公钥密码		
考核要点	公钥密码体制的思想；典型的公钥加密算法 RSA；公钥密码体制的基本概念；单向陷门函数的概念；ElGamal 算法；椭圆曲线密码		
第八知识单元　数字签名技术			
学时分配	2 学时	教学方式	课堂讲授，ppt 电子课件，板书
教学内容		重点	难点
1	数字签名概述	√	
2	数字签名的实现方案	√	√
3	特殊数字签名		
考核要点	数字签名体制的基本概念、安全属性；属性典型的数字签名方案；数字签名的实现方案		
第九知识单元　密码协议			
学时分配	2 学时	教学方式	课堂讲授，ppt 电子课件，板书
教学内容		重点	难点
1	密码协议概述	√	
2	零知识证明		√
3	比特承诺		
4	不经意传送协议		

5	安全多方计算				√
考核要点	协议及密码协议；零知识证明协议；安全多方计算				
第十知识单元　密钥管理					
学时分配	2 学时	教学方式	课堂讲授，ppt 电子课件，板书		
教学内容				重点	难点
1	密钥管理概述			√	
2	密钥生命周期			√	√
3	密钥分发技术			√	
4	密钥协商技术			√	
5	密钥托管技术				
6	秘密共享技术				√
考核要点	密钥管理的各个环节及基本概念；典型密钥分配方案及密钥协商方案				
第十一知识单元　密码学新进展					
学时分配	2 学时	教学方式	课堂讲授，ppt 电子课件，板书		
教学内容				重点	难点
1	量子密码学				√
2	混沌密码学				
3	DNA 密码				
考核要点	量子密码；混沌密码；DNA 密码				

四、　课程学时分配

教学内容	讲授	实验	上机	课内学时小计	课外学时
1.密码学概论	√			2	
2.传统密码体制	√			2	
3.密码学基础	√			4	
4. 分组密码	√			6	
5. 序列密码	√			2	
6. Hash 函数和消息认证	√			4	
7. 公钥密码体制	√			4	
8. 数字签名技术	√			2	
9. 密码协议	√			2	
10. 密钥管理	√			2	
11. 密码学新进展	√			2	
合　　计				32	

五、 教学设计与教学组织

本课程所涉及到的概念较多，重点是理解各类密码技术在实际生产生活中发挥的作用，并通过对现有密码原型的分析培养密码学的思维方式，建立密码学框架体系。

鼓励学生组织学习小组，对相关课程模块进行短时间演示讲解，以此来激发学生的学习热情，在充分调动学习积极性的同时加深对密码学知识的理解和感悟。对于部分重要密码学技术手段，均采取相应的伪代码演示，使学生更为深入地了解密码技术的实现细节。通过丰富的实际案例加深学生对相关抽象理论和算法过程的理解。通过课后作业，使学生对课堂所学能够及时复习，对知识充分消化吸收。

此外，通过增强师生间、同学间的多种形式的讨论来提高课程的教学效果和教学质量。安排有课后答疑、课下讨论、网上讨论等环节，以多种方式帮助学生更好地掌握密码学思想，提高运用密码学技术解决实际问题的能力

课程教学方法及具体要求如下：

1. 课堂讲授

1）以能力培养为导向，注重理解应用密码学涉及到的各种密码学概念、理

论和方法。为保证教学质量，课堂讲授中应重点突出、点面结合，既要保证完成使广大学生接受应用密码学知识体系结构的教学目标，又要针对关键问题、重点内容作较为详尽、多引入实例的透彻讲解，使学生真正领会和掌握本课程的知识要点。

2）结合生产生活中的实际案例，使同学对密码学设计方法有更为直观、深刻的认识，对于某些密码学技术的重点或难点，通过伪代码讲解来增强学生的感性认识，使学生更好、更快地掌握。

3）多媒体课件、板书与代码演示结合的教学手段与多种教学方法兼施并用。教学方法则采取在教师讲授基本教学内容的过程中适当穿插引入个体针对性提问、集体提问、答疑等教学形式。

2. 讨论与自学

鼓励同学之间或同学与教师之间针对应用密码学课程的重点和难点内容展开讨论，以澄清知识要点、扩大知识面和培养独立思考能力及创新能力。对于部分重点和难点模块，鼓励学生以小组为单位进行短时间的演示和讲解。自学内容应以学生掌握相关知识结构基础上能比较方便地和理解为原则；对于有能力的同学，鼓励其多编写各种密码学相关算法程序，提高解决实际问题的能力，锻炼思维。

3. 课前预习和课后复习

建议学生课前预习相应教学内容；课后复习以课堂讲授内容为主线、完成相应作业，对于密码学中的关键应用查阅拓展资料以更为深入地理解。对于部分重要的密码算法鼓励同学进行相应的编程练习，提高实践能力。

六、 教材与参考资料

1.教材

《现代密码学教程》（第 1 版），谷利泽，郑世慧，北京邮电大学出版社，2009 年 8 月，9789563520190

2.参考资料

（1）《密码学导引》，冯登国，裴定一，北京科技大学出版社， 1999 年，9787030072955

（2）《信息安全与密码学》，除茂智，游林，清华大学出版社，2007 年，9787302139584

七、 课程考核要点与成绩评定标准

围绕每一个具体的课程目标，从相关支撑知识单元的角度设计不同的考核要点，如下表：

课程目标	知识单元	考核要点设计
目标 1	第一知识单元 密码学概论 第二知识单元 传统密码体制 第三知识单元 密码学基础 第四知识单元 分组密码 第五知识单元 序列密码 第六知识单元 Hash 函数和消息认证 第七知识单元 公钥密码体制 第八知识单元 数字签名技术	以填空题、单选题、计算题、综合题等方式考核。
目标 2	第四知识单元 分组密码 第五知识单元 序列密码 第六知识单元 Hash 函数和消息认证 第七知识单元 公钥密码体制 第八知识单元 数字签名技术 第九知识单元 密码协议 第十知识单元 密钥管理	以单选题、填空题、计算题、证明题等方式考核。
目标 3	第二知识单元 传统密码体制 第三知识单元 密码学基础 第六知识单元 Hash 函数和消息认证 第七知识单元 公钥密码体制 第八知识单元 数字签名技术 第九知识单元 密码协议 第十知识单元 密钥管理	以单选题、填空题、计算题、证明题等方式考核。

本课程成绩由平时成绩和期末成绩两部分组成，以百分制计算。平时成绩占 30%（其中出勤成绩占 10%，作业成绩占 20%），期末考试成绩占 70%。

八、 大纲制(修)订说明

无

大纲执笔人：王宝成

大纲审核人：曾凡锋

开课系主任：肖珂

开课学院教学副院长：宋威

制（修）订日期：2022 年 2 月