中国海洋大学本科生课程大纲

课程名称	密码学 Cryptography	课程代码	075103201291
课程属性	专业知识	课时/学分	32 / 2
课程性质	选修	实践学时	
责任教师	张京良	课外学时	64 (32×2)

课程属性：公共基础/通识教育/学科基础/专业知识/工作技能，课程性质：必修、选修

一、 课程介绍

1. 课程描述：

密码学是一门交叉学科，它与数学、电子、通信、计算机等学科关系密切。《密码学》课程是数学科学学院面向数学与应用数学专业、信息与计算科学专业高年级本科生开设的一门专业选修课。《密码学》课程的内容主要包含三个模块：第一模块，密码学中的数学基础知识，主要内容包括近世代数相关知识、初等数论知识和计算复杂度理论；第二模块，密码学基础知识，主要内容有：流密码（序列密码）、分组密码、公钥密码、密钥管理、杂凑函数、数字签名、密码协议；第三模块，现代密码专题，包括 DNA 密码、混沌密码、量子密码、多变量密码、基于纠错码的密码、格密码、可视密码学、同态加密、广播加密、叛逆者追踪等。

2. 设计思路：

开设《密码学》课程的目的是：（1）使学生了解现代密码学的发展及其研究的主要内容，掌握现代密码学的主要知识体系、基本理论。（2）使学生了解现代密码学在现实生活中的运用情况，能够把密码思想融入到社会生活中，把密码工具应用到通信系统中，解决一些实际问题。（3）使学生了解到数学知识在其它学科的应用，提高学习数学的兴趣；通过学习，增强网络通信安全意识，加强信息风险防范能力。

《密码学》课程的内容主要包含密码学中的数学基础知识，主要内容包括近世代数相关知识、初等数论知识和计算复杂度理论；密码学基础知识，主要内容有：流密码（序列密码）、分组密码、公钥密码、密钥管理、杂凑函数、数字签名、密码协议；现代密码专题简介。

《密码学》的内容基本按照密码学的发展编排的，主要有两条主线：一是传统密码学知识，包括对称密码体制（流密码和分组密码）、公钥密码体制（包括 RSA，ElGamal，Rabin,NTRU,椭圆曲线等）、密钥管理、杂凑函数、数字签名、密码协议等；二是现代密码简介，包括 DNA 密码、混沌密码、量子密码、多变量密码、基于纠错码的密码、格密码、可视密码学、同态加密、广播加密、叛逆者追踪等。

3. 课程与其他课程的关系：

与其他课程的关系（先修、并行和后置课程）：

先修课程：离散数学；概率统计；计算方法；初等数论；近世代数；

并行课程：毕业论文；

后置课程：无。

二、课程目标

本课程目标是：一方面，使学生了解现代密码学的发展及其研究的主要内容，掌握现代密码学的主要知识体系、基本理论。另一方面使学生了解到数学知识在其它学科的应用，提高学习数学的兴趣；通过学习，增强网络通信安全意识，加强信息风险防范能力。

到课程结束时，学生应达到以下几方面要求：

（1）了解密码学基本知识。知道对称密码包括流密码或序列密码以及分组密码；了解常见的公钥密码方案，如 RSA，椭圆曲线密码体制等；知道保护密钥的重要手段——秘密共享；知道 hash 函数；了解密码学的应用如数字签名、身份认证、电子商务等。

（2）能力有所提高。通过本课程的学习，使学生将数学知识应用到其它学科的知

识应用能力得到提高。

（3）素质有所提升。通过学习，知道密码学就是在方案建立与破解的对立统一的基础上发展的，没有绝对安全的方案，对事物的认知素质有所裨益。

三、学习要求

要完成所有的课程任务，学生必须：

（1）按时上课,上课认真听讲，积极参与课堂讨论、随堂练习和测试。本课程将包含较多的随堂练习、讨论、小组作业展示等课堂活动，课堂表现和出勤率是成绩考核的组成部分。

（2）按时完成常规练习作业。这些作业要求学生按书面形式提交，只有按时提交作业，才能掌握课程所要求的内容。延期提交作业需要提前得到任课教师的许可。

（3）完成教师布置的一定量的阅读文献和背景资料、案例分析、理论探讨和算法软件应用等作业，其中大部分内容要求以小组合作形式完成。这些作业能加深对课程内容的理解、促进同学间的相互学习、并能引导对某些问题和理论的更深入探讨。

四、参考教材与主要参考书

1、选用教材：

《现代密码学》（第 3 版）， 杨波 编著，清华大学出版社，2015 年 2 月出版。

2、主要参考书：

[1] 应用密码学——协议、算法与 C 源程序，(美) Bruce Schneier 著，吴世忠, 祝世雄, 张文政等译，机械工业出版社，2000.

[2] 应用密码学手册，（加）Alfred J. Menezes 等著，胡磊 等译， 电子工业出版社，2005。

五、进度安排

序号	专题	主题	计划课时	主要内容概述
1	引言	密码学基本概念	1	信息安全面临的威胁；信息安全模型；密码学基本概念；几种古典密码
2	密码学中的数学基础知识	初等数论基础知识	3	素数；模运算；费马定理和欧拉定理；素性检验 欧几里得算法；中国剩余定理；离散对数；平方剩余
		近世代数基础知识	2	群；环；域；有限域
		计算复杂度理论	1	复杂度理论
3	流密码	m 序列	2	流密码简介；线性反馈移位寄存器；m 序列；非线性序列
4	分组密码	分组密码的设计	3	分组密码概述；DES 方案；IDEA 方案
5	公钥密码	公钥密码的设计	2	公钥密码简介；RSA 方案；背包密码体制；RABIN 密码体制；NTRU 密码
			4	椭圆曲线密码；基于双线性对的密码；无证书密码；基于身份的密码制
6	密钥管理	秘密分割与秘密共享	2	密钥分配；密钥交换；秘密分割；秘密共享
7	杂凑函数	杂凑函数的构造	2	MD5;SHA
8	数字签名	签名方案	2	RSA 签名；ElG amal 签名；Schnorr 签名；代理签名；盲签名；门限签名；群签名；环签名；聚合签名；签密
9	密码协议	认证协议	2	零知识证明；安全多方计算；电子选举、电子拍卖、电子现金

10	现代密码学专题选讲	新的密码体制	6	DNA 密码；混沌密码；量子密码；多变量密码；基于纠错码的密码；格密码；可视密码学；同态加密；广播加密；叛逆者追踪等

六、成绩评定

1.考核方式：　C　：A.闭卷考试 B.开卷考试 C.论文 D.考查 E.其他

2.统考方式：b 提前。本课程主要面向四年级本科生开设，前 8 周上完，并考试。

3.课程综合评分方法：

出勤率、作业与平时讨论	50%
期末小论文	50%
总计	100%

附：论文、作业和平时表现评分标准

1）作业的评分标准

作业的评分标准	得分
1.严格按照作业要求并及时完成，基本概念清晰，解决问题的方案正确、合理，能提出不同的解决问题方案。	90-100 分
2.基本按照作业要求并及时完成，基本概念基本清晰，解决问题的方案基本正确、基本合理。	70-80 分
3.不能按照作业要求，未及时完成，基本概念不清晰，解决问题的方案基本不正确、基本不合理。	40-60 分
4.不能按照作业要求，未及时完成，基本概念不清晰，不能制定正确和合理解决问题的方案。	0-30 分

2）课堂讨论及平时表现评分标准

课堂讨论、平常表现评分标准	得分
1.资料的查阅、知识熟练运用，积极参与讨论、能阐明自己的观点和想法，能与其他同学合作、交流，共同解决问题。	90-100 分
2.基本做到资料的查阅、知识的运用，能参与讨论、能阐明自己的观点和想法，能与其他其他同学合作、交流，共同解决问题。	70-80 分
3.做到一些资料的查阅和知识的运用，参与讨论一般、不能阐明自己的观点和想法，与其他同学合作、交流，共同解决问题的能力态度一般。	40-60 分

4.不能做到资料的查阅和知识的运用，不积极参与讨论，不能与其他同学合作、交流，共同解决问题。	0-30 分

3）论文的评分标准

评价项目	评价标准	满分	评　　分				
			A	B	C	D	E
选题质量	选题符合专业培养目标，体现综合训练要求；题目具有适当难度，有一定的理论意义或实际意义	20	19-20	17-18	15-16	13-14	≤12
文献资料利用能力	能独立地利用多种方式查阅中外文献；能正确翻译外文资料；能正确有效地利用各种文献资料	20	19-20	17-18	15-16	13-14	≤12
论文（设计）质量	结构严谨，逻辑性强；语言文字表达准确、流畅；格式、图、表规范；有一定的学术水平或应用价值	40	35-40	30-35	25-30	20-25	≤20
创新能力	体现较强的创新意识；应用新理论、新方法，解决新问题；工作有独到见解或新突破	10	10	9	8	7	6
工作态度和工作量	工作认真主动；作风扎实严谨；工作量饱满；圆满完成了任务书所规定的各项任务	10	10	9	8	7	6
总分	100						

七、学术诚信

学习成果不能造假，如考试作弊、盗取他人学习成果、一份报告用于不同的课程等，均属造假行为。他人的想法、说法和意见如不注明出处按盗用论处。本课程如有发现上述不良行为，将按学校有关规定取消本课程的学习成绩。

八、大纲审核

教学院长：　　院学术委员会签章：