《信息安全数学基础》课程教学大纲

一、课程基本信息

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **课程名称** | 中文：信息安全数学基础 | | | **课程编号** | 3182121300 |
| 英文：Mathematic Foundations of Information Security | | |
| **学分/学时** | 3/48 | **必修（**√**）/ 选修（）** | | **开课学期** | 3 |
| **课程类别** | 数学与自然科学课程 | | **适用专业** | 网络空间安全 | |
| **先修课程** | 高等数学、线性代数、离散数学 | | | | |
| **授课教师** | 陈秀波、徐国胜 | | | | |

二、课程目标

本课程是网络空间安全专业的一门基础课，通过本基础理论课程的学习，使学生了解信息安全数学的基本概念、主要方法及应用，培养学生的数学思维训练与解决实际问题的能力，并为学习相关课程及进一步扩大数学知识面，打下必要的基础。具体目标为：

**课程目标1：**掌握网络空间安全领域的，编码与密码的数学基础知识，能够将信息安全数学基础中的基本概念、基本理论和基本方法应用到网络空间安全等相关系统中。（**毕业要求指标点1.1**）

**课程目标2：**能够根据网络空间安全领域中复杂工程问题的需求描述，运用信息安全数学基础的基本原理、方法进行综合分析，建立解决问题的抽象模型。（**毕业要求指标点2.2**）

三、课程目标与支撑的毕业要求指标点

本课程的知识点支撑网络空间安全专业毕业要求中的2个指标点：1.1和2.2。如下表所示，本课程的2个课程教学目标，分别对应工程教育专业认证标准规定的毕业要求中的2个指标点。

|  |  |  |  |
| --- | --- | --- | --- |
| **毕业要求指标点** | **课程目标** | **达成途径** | **评价依据** |
| 1.1 掌握解决网络空间安全领域复杂工程问题所需的数学与物理科学基础知识，领会重要数学、物理思想方法 | **课程目标1：**掌握网络空间安全领域的，编码与密码的数学基础知识，能够将信息安全数学基础中的基本概念、基本理论和基本方法应用到网络空间安全等相关系统中； | 通过课堂讲授等方式使学生掌握数论与近世代数的基本概念、基本原理和计算方法，进而掌握编码与密码的专业知识，通过课后作业巩固课堂知识；在期中考试和期末考试试卷中考察对于基本概念和基本原理的理解掌握和计算求解能力； | 考核内容约占总成绩的50%，包括作业、期中考试和期末考试； |
| 2.2 根据网络空间安全领域复杂工程问题的需求描述，运用数学、自然科学和工程科学原理及方法进行分析表达，建立解决问题的抽象模型。 | **课程目标2：**能够根据网络空间安全领域中复杂工程问题的需求描述，运用信息安全数学基础的基本原理、方法进行综合分析，建立解决问题的抽象模型。 | 对于网络空间安全领域相关的复杂技术与工程问题，设计相应抽象数学模型，通过课后作业进行强化训练，让学生自主进行研究与设计方案，让学生自主进行复杂工程问题的调研、寻找解决方案并进行分析；通过课后作业进行强化训练，通过考试中的综合应用类题目考查学生分析问题和解决问题的能力。 | 考核内容约占总成绩的50%，包括作业、期中考试和期末考试。 |

四、课程落实立德树人的举措

以《高等学校课程思政建设指导纲要》（教高〔2020〕3号）为依据，科学设计课程思政教学体系，将思政教育融入课程中的适当章节，主要包括：

**1、厚植爱国主义情怀**

讲授中国剩余定理时，不仅要讲授知识，而且要强调中国剩余定理是举世闻名的定理，它在解一次同余式组的问题上，不但时间遥遥领先，而且在理论和方法上也有光辉而独特的成就，在近代数学中有着重大的影响和作用，进而激发学生们的爱国主义情怀。

**2、培养坚定理想信念**

在教授素数个数的证明时，提及在数论中历经数十年甚至几百年长期未能解决、费劲九牛二虎之力才解决的数学猜想特别的多。这样，通过在传递知识的同时，将其背后艰辛探索的精神，潜移默化地传递给学生，可以培养学生们不畏艰险的坚定的理想信念和科学态度。

**3、增长广博知识见识**

在科学技术迅猛发展、知识日新月异的时代，要不断更新知识，特别是学科的理论前沿成果。例如，在讲授RSA密码相关数学基础知识时，不仅要提及目前比较常用的现代密码理论，更要给出量子信息中的量子密码、量子算法与量子计算机的最新理论与实验进展，增长学生们的知识见识。

**4、培养牢固守法意识**

在讲授欧拉定理等知识时，提出它是设计密码算法用来保证信息的安全性的重要基础，同时提出信息的安全管理也至关重要，进而融合《中华人民共和国网络空间安全法》，进行网络安全法律法规的教育普及，教育学生们知法，懂法，守法。

五、教学内容及学时安排

参见附表1。

六、教学方法

1、课堂教学：本课教学以教师课堂讲授为主，授课过程应能灵活运用板书和多媒体教学、加强师生互动、注重启发式教学、根据教学内容适时引入密码学中的案例。

2. 研讨教学：根据具体教学内容以及同学学习情况，适当开展研讨活动。由教师提供扩展学习资料、提出研讨问题，同学自主探索，在此基础上展开以小组为单位的研讨式教学。

3. 线上教学及自学：在教学过程中积极利用线上教学资源，实行包括翻转课堂、混合式教学在内的线上线下高度融合的教学模式，提高同学们的自学能力。

七、考核方式

本课程的考核环节主要包括平时作业、期中考试和期末考试，其中平时成绩占总成绩的25%，期中考试成绩占总成绩的25%，期末考试成绩占总成绩的50%。成绩评定采用百分制和综合成绩评定方式，即总成绩=课堂成绩（期末考试50%+期中成绩25%+课后作业25%）（注：课程教学组可根据实际情况，对每部分总评比例进行调整，但各教学班应保持一致）。

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 指标点  编号 | 课程目标编号 | 考核方式 | | | 总贡  献度 |
| 平时（贡献度50%） | | 期末  (贡献度50%） |
| 作业 | 期中 |
| **课程目标1** | 1.1 | 15 | 10 | 25 | 50 |
| **课程目标2** | 2.2 | 10 | 15 | 25 | 50 |
| 合计 | | 25 | 25 | 50 | 100 |

考核标准参见下表。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 考核  环节 | 所占  分值 | 考核内容 | 对应课程目标 | 评价细则 |
| 课后作业 | 25% | 50%为基础知识题，考核学生对基本概念和主要原理的理解、计算、掌握的能力，和掌握。 | 课程目标1 | 平时作业一般为10次左右，涵盖课程所有内容，按照是否按时提交、完成情况等进行综合评定。每次作业评分参考标准为（按照10分计算）：按时完成作业并提交，且正确率达到60%，计6分；在此基础上，作业正确率满足70%、80%、90%和100%分别为7分、8分、9分、10分，有创新解题思路或解决方案的可另加1-2分，但每次作业得分不超过10分。  作业得分6分及以上达成作业所支撑的课程目标1和2，说明学生具有理解计算信息安全数学基础课程的基本概念和基本原理、能够运用所学知识研究、分析和解决网络空间安全实际问题的能力。 |
| 50%为计算求解、证明题，考核学生考核学生对网络空间安全实际问题，设计相应的抽象数学模型，给出解决方案的能力。 | 课程目标2 |
| 期中考试 | 25% | 通过简答题、计算题、判断题与填空题考核学生对信息安全数学基础知识的理解和掌握。 | 课程目标1 | 评分参考标准参见试卷参考答案。（按照100分计算）  期中考试得分60分及以上达成期中考试所支撑的课程目标1和2，说明学生理解和基本掌握了数论与近世代数的主要概念和原理，能够对网络空间安全领域的复杂工程问题进行数学建模，计算求解。 |
| 通过分析、计算类题目，考核对网络空间安全领域实际工程问题的分析、数学模型设计和解决。提升对信息安全数学基础与领域复杂工程问题的抽象建模，计算与解决能力。 | 课程目标2 |
| 期末考试 | 50% | 填空、简答、分析、计算类题目，考核通过信息安全数学基础课程的学习，掌握编码与密码领域的专业基础知识和基本概念。 | 课程目标1 | 闭卷考试，题目涉及课程全部教学内容，并通过综合应用题考察学生分析解决复杂网络问题的能力。  评分参考标准参见试卷参考答案。（按照100分计算）  期末考试得分60分及以上达成期末考试所支撑的课程目标1和2，说明学生理解和掌握了信息安全数学基础课程的基本概念和主要原理，能够对网络空间安全领域的实际工程问题进行分析、计算、数学建模并提出解决方案的能力。 |
| 简答、分析、综合类题目部分计算题目，考核信息安全数学基础课程的基础知识进行网络空间安全领域相关问题的理解、计算和解决。 | 课程目标2 |

八、课程资源

课程教材：

《信息安全数学基础》（第二版）, 陈恭亮编著, 清华大学出版社, 2014年5月

参考书目：

（1）《信息安全数学基础》, 罗守山、徐国胜编著, 北京邮电大学出版社, 2018年8月

（2）《公钥密码学的数学基础》，王小云、王明强、孟宪萌编著，科学出版社，ISBN：9787030351364，2013年1月

（3）《数论与密码》, 杨思熳编著, 华东师范大学出版社, 2010年9月

（4）《数论与有限域》, 董丽华等编著, 机械工业出版社, 2010年10月

（5）《信息安全数学基础》, 覃中平、张焕国等编著, 清华大学出版社, 2006年8月

（6）《初等数论》（第二版）, 潘承洞、潘承彪编著, 北京大学出版社, 2003年

（7）《近世代数》, 杨子胥编著, 高等教育出版社, 2000年5月

参考课程：

（1）课程名：Number Theory

开课学校：University of York

课程链接：https://www.york.ac.uk/maths/research/number-theory/

（2）课程名：Modern Algebra

开课学校：Massachusetts Institute of Technology

课程链接：https://ocw.mit.edu/courses/mathematics/18-703-modern-algebra-spring-2013/

**执笔人:** 徐国胜

**审核人：**陈秀波

**时间：**2021年5月25日

表1 《信息安全数学基础》教学内容、学时分配及对毕业要求的支撑

| 序号 | 知识模块 | 教学内容 | 学时  分配 | 教学目标与要求 | 对课程目标的支撑 | 对毕业要求（指标点）的支撑 | 学生任务 | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 作业要求 | 自学要求 | 讨 论 |
| 1 | 整数的可除性（1） | 整数的概念，欧几里得除法，最大公因数，广义欧几里得除法，贝祖等式。 | 3 | 熟练运用厄拉托塞师 (Eratosthenes) 筛法，筛选出一定范围内的所有素数。运用广义欧几里得除法及贝祖等式。运用素数的平凡判别方法，判别任意一个奇数是否是素数。 | 支撑课程目标1  支撑课程目标2 | 支撑指标点1.1  支撑指标点2.2 | 完成涵盖欧几里得除法，Eratosthenes筛法，整数的*b*-进制表示，最大公因数，广义欧几里得除法知识点的书面作业。  P48 T(6), (11), (17), (18), (32), (33) | 最大公因数求解的计算机编程实现 | 贝祖等式的证明。 |
| 2 | 整数的可除性（2） | 最大公因数的进一步性质，整除的进一步性质，最小公倍数，素数的算术基本定理，素数定理。 | 3 | 熟练运用最大公因数的性质，计算出多个整数的最大公因数。运用最小公倍数与最大公因数的关系，计算最小公倍数。运用算术基本定理及标准分解式，计算出任意两个整数或者多个整数的最大公因数与最小公倍数。 | 支撑课程目标1  支撑课程目标2 | 支撑指标点1.1  支撑指标点2.2 | 完成涵盖整除的进一步性质，即三个关于互素与素数的定理，最小公倍数与最大公因数的关系式，算术基本定理，标准分解式的重要应用的书面作业。  P48 T(6), (11), (17), (18), (32), (33) | 整数分解定理。形式为的整数及其最大公因数。 | 素数定理的证明。 |
| 3 | 同余（1） | 同余的概念及基本性质，剩余，剩余类及完全剩余系。 | 3 | 熟练运用同余的概念与两个等价定义，判断出两个整数在模*m*下是否同余。同余的性质，掌握同余的一些具体应用。运用定义，给出模*m*的几种完全剩余系。 | 支撑课程目标1  支撑课程目标2 | 支撑指标点1.1  支撑指标点2.2 | 完成涵盖同余、剩余类的概念及性质，完全剩余系的概念与给出模*m*的几种完全剩余系，同余的七个重要性质的书面作业。  P88 T(1), (5), (6), (17) | 多个模的完全剩余系的证明。 | 模运算与同余在古典密码算法中的应用。 |
| 4 | 同余（2） | 简化剩余系，欧拉函数，欧拉定理，费马小定理，Wilson定理，模重复平方计算法。 | 3 | 欧拉函数的定义与性质，计算出任意整数的欧拉函数的函数值。运用欧拉定理，费马小定理，Wilson定理等，进行相关的计算优化运算。运用模重复平方计算法，对大整数模*m*和大整数*n*，计算出数值。 | 支撑课程目标1  支撑课程目标2 | 支撑指标点1.1  支撑指标点2.2 | 完成涵盖简化剩余系及相关性质，欧拉定理，费马小定理，Wilson定理的证明与应用，模重复平方计算法的算法过程与应用知识点的书面作业。  P89 T(16), (19), (23), (24) | 两个模的简化剩余系定理。 | 利用欧拉函数的性质，进行原根的构造。 |
| 5 | 同余式（1） | 同余式的基本概念，一次同余式，中国剩余定理的证明，中国剩余定理的算法优化应用 | 3 | 对一次同余式进行求解。熟练运用中国剩余定理求同余式组的解。运用中国剩余定理对一些复杂的运算进行优化。 | 支撑课程目标1  支撑课程目标2 | 支撑指标点1.1  支撑指标点2.2 | 完成涵盖一次同余式求解过程的证明并能对具体一次同余式进行求解，中国剩余定理之构造证明，并能对具体的同余式组进行求解，欧拉定理，模重复平方计算法，中国剩余定理，它们对复杂运算进行的算法优化的书面作业。  P121 T(1), (3), (7), (17) | 一次同余式求解的公式方法。中国剩余定理之递归证明。 | 一般同余式求解的基本思路与过程。 |
| 6 | 同余式（2） | 高次同余式的解数，高次同余式的提升，高次同余式的具体应用，素数模的同余式。 | 3 | 求解模为素数幂的同余式，利用高次同余式的提升进行具体应用。运用素数模的同余式的简化定理、解数估计定理，求模为素数的高次同余式的解。 | 支撑课程目标1  支撑课程目标2 | 支撑指标点1.1  支撑指标点2.2 | 完成涵盖高次同余式的求解转换为同余式组求解的等价证明；素数模的同余式的简化，素数模的同余式的解数估计；模为素数的高次同余式的求解方法  等知识点的书面作业。  P123 T(16), (18), (23), (24) | 素数模的同余式的因式分解。 | 运用费马小定理的推论，简化求解模为素数的高次同余式。 |
| 7 | 二次同余式与平方剩余（1） | 一般二次同余式，模为奇素数的平方剩余与平方非剩余，勒让得符号，二次互反律（上）。 | 3 | 运用平方剩余定义，计算出模*m*的平方剩余与平方非剩余。运用勒让得符号的定义与性质，计算出勒让得符号的数值。判断模为奇素数的二次同余式是否有解。熟练运用二次互反律。 | 支撑课程目标1  支撑课程目标2 | 支撑指标点1.1  支撑指标点2.2 | 完成涵盖勒让得符号的性质与熟练运算；平方剩余、欧拉判别法、勒让得符号、二次同余式是否有解，这四者之间的关系；运用二次互反律，计算勒让得符号的数值等知识点的书面作业。  P163 T(1), (2), (9), (13), (20) | 高斯引理的证明。 | 整数2是否为模*p*平方剩余的判断的证明。 |
| 8 | 二次同余式与平方剩余（2） | 二次互反律（下），雅可比符号，模平方根 | 3 | 运用二次互反律定理，判断二次同余式是否有解。运用雅可比符号的性质进行计算。运用模为奇素数*p*的求解定理与模为合数*m*的求解定理，求解出模为任意整数的二次同余式。 | 支撑课程目标1  支撑课程目标2 | 支撑指标点1.1  支撑指标点2.2 | 完成涵盖模奇素数*p*二次同余式的求解定理证明，并会运用定理进行一般二次同余式的求解；同余式有解必要条件的证明与具体运用等知识点的书面作业。  P164 T(22), (26) , (35), (37) | 素数的平方表示的求解。 | 二次互反律定理的证明。 |
| 9 | 原根与指标（1） | 指数及其基本性质，原根的定义，原根的构造方法。 | 3 | 运用指数与原根的定义，求任意一个模整数（较小的整数）的指数与原根。运用原根的方法，表示出简化剩余系。运用寻找原根的方法定理，求出模素数*p*的所有原根。 | 支撑课程目标1  支撑课程目标2 | 支撑指标点1.1  支撑指标点2.2 | 完成涵盖指数与原根的基本概念与基本性质的深刻理解；运用定义，掌握指数与原根的计算方法；理解寻找原根的定理的证明过程，并求出模素数*p*的所有原根等知识点的书面作业。  P196 T(1), (3), (7), (11), (13), (16) | 模*m*的简化剩余系指数。模奇素数*p*的原根的存在性证明方法。 | 利用原根的构造方法定理，求出模素数*p*的所有原根。 |
| 10 | 原根与指标（2），  素性检验 | 原根存在的充要条件，素性检测方法：包括伪素数，Euler伪素数，强伪素数。 | 3 | 运用原根存在的充要条件，判断是否存在并会求出原根。运用伪素数Fermat素性检验方法，对一个奇数进行检测。运用Solovay-Stassen素性检验方法，对一个奇数进行检测。熟练运用Miller-Rabin素性检验方法，对一个奇数进行检测。 | 支撑课程目标1  支撑课程目标2 | 支撑指标点1.1  支撑指标点2.2 | 完成涵盖原根存在的充要条件定理、相关定理的证明与理解；伪素数的3种定义，基*b*的伪素数，Euler伪素数，强伪素数，它们的联系与区别；三种素性检验方法，伪素数Fermat素性检验方法，Solovay-Stassen素性检验方法，Miller-Rabin素性检验方法，证明过程与具体应用等知识点的书面作业。  P211 T(1), (5), (9), (14), (17), (19) | 指标及*n*次同余式。平方因子的判别。 | 存在无穷多个对于基2的强伪素数。 |
| 11 | 群（1） | 群，子群，子群的生成 | 3 | 运用群的定义，验证某些具有结合法的集合是否成为一个群。熟练运用子群与子群的充要条件，验证某些具有结合法的集合的子集是否成为一个子群。循环群的表示。 | 支撑课程目标1  支撑课程目标2 | 支撑指标点1.1  支撑指标点2.2 | 完成涵盖掌握群的定义，能够证明具有结合法的集合是否成为一个群。熟知群的一些重要例题；子群定义与子群的充要条件。熟知子群的一些重要例题；掌握验证某些具有结合法的集合或者子集是否成为一个群或者子群的方法等知识点的书面作业。  P253 T(1), (2), (4), (9) | 一般群及非空子集的子群的生成。 | 群的第二种定义：方程在一个具有结合法的集合中有解。 |
| 12 | 群（2） | 正规子群，商群，同态与同构 | 3 | 运用Lagrange定理，求一个有限群的子群。运用正规子群、商群的概念，验证或者证明某个群为正规子群、商群。能够对具体应用的实例，熟练运用同态定理。理解同态分解定理的内容。 | 支撑课程目标1  支撑课程目标2 | 支撑指标点1.1  支撑指标点2.2 | 完成涵盖正规子群、商群的概念理解与基本性质；理解与运用同态定理；理解同态分解定理的内容等知识点的书面作业。  P253 T(3), (5), (10), (12) | Lagrange定理及相关定理的证明过程。 | 同态分解定理的进一步性质。 |
| 13 | 群的结构 | 循环群，置换群 | 3 | 运用循环群的性质，解决有关循环群及循环子群的问题。熟练运用对换对置换的表示。熟练表示出3元与4元对称群，及求出其所有的循环子群。 | 支撑课程目标1  支撑课程目标2 | 支撑指标点1.1  支撑指标点2.2 | 完成涵盖循环群的性质及相关定理的理解与熟练运用；对称群及其所有的子群的熟练表示等知识点的书面作业。  P266 T(1), (2), (4), (8), (10) | 由生成元的阶讨论有限群的生成元构造的相关引理。 | 有限生成交换群理论。 |
| 14 | 环与理想 | 环的定义与性质，同态，特征及素域，分数域，理想和商环，素理想 | 3 | 运用环的定义，判断一个具有两种结合法的集合是否为环。运用环的性质及相关定义，对一个环进行判别：是否是有零因子与单位元，是否为整环或域。熟练运用理想的定义与充要条件，对一个子环是否为理想进行判别。 | 支撑课程目标1  支撑课程目标2 | 支撑指标点1.1  支撑指标点2.2 | 完成涵盖判断一个具有两种结合法的集合是否为环；对一个环进行判别是否有零因子与单位元，是否为整环或域；理想的定义与充要条件等知识点的书面作业。  P285 T(1), (4), (6), (8), (12), (15) | 主理想相关定理的证明。 | 素理想及相关定理的证明。 |
| 15 | 多项式环 | 多项式整环，多项式整除与不可约多项式，多项式同余，本原多项式 | 3 | 熟练计算出F2[x]中的4次以下的不可约多项式与可约多项式。运用多项式的欧几里得除法，计算出多项式的最大公因数。运用多项式的性质，计算出或证明出本原多项式。 | 支撑课程目标1  支撑课程目标2 | 支撑指标点1.1  支撑指标点2.2 | 完成涵盖整环*R*上多项式构成整环的证明及理解；熟练运用多项式的性质，计算出或证明出本原多项式等知识点的书面作业。  P307 T(1), (2), (5), (8), (9), (11) | 不可约多项式相关定理的证明。 | 多项式理想、多项式结式与判别式。 |
| 16 | 域和Galois理论  域的结构 | 域，域的结构，有限域的具体构造 | 3 | 运用扩域的定义，判断出扩域。熟练运用本原元或生成元的定义，计算出生成元，并给出生成元的数目。运用有限域的构造方法，构造素域*Fp*上的*d*次代数扩张。 | 支撑课程目标1  支撑课程目标2 | 支撑指标点1.1  支撑指标点2.2 | 完成涵盖扩域，有限维扩域或无限维扩域的定义及相关性质；本原元或生成元的定义，生成元的数目；基于有限域的构造方法，构造素域*Fp*上的*d*次代数扩张等知识点的书面作业。  P325 T(1)，P338T(1), (2), (3), (12) | Galois基本定理相关内容。 | 域的子域的生成及相关定理。 |