网络空间安全学院

School of Cyberspace Security, BUPT

信息安全数学基础

—— 导　论

信数课题组

北京邮电大学网络空间安全学院

2024 年 9 月 8 日

目录

目录

国家战略前瞻

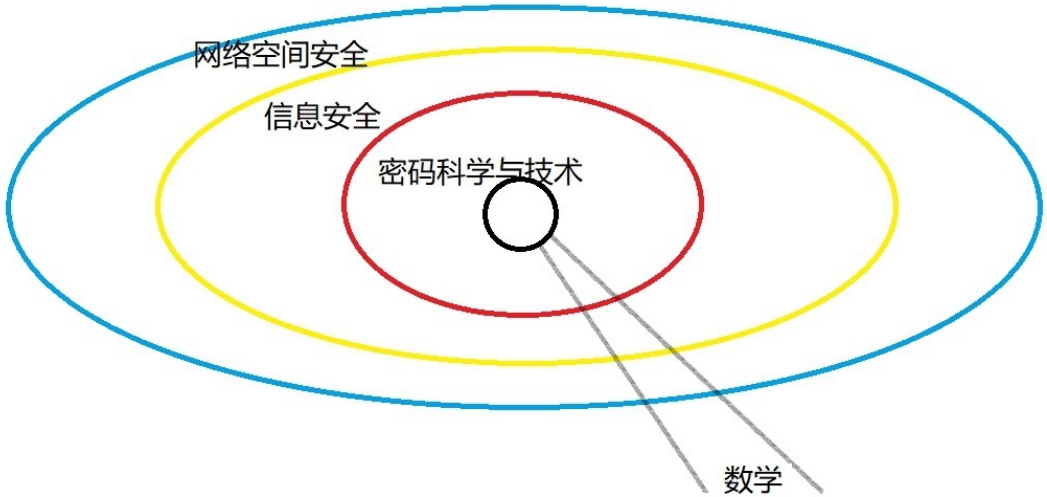
要全面贯彻网络强国战略，把数字技术广泛应用于政府管理服务，推动政府数字化、智能化运行，为推进国家治理体系和治理能力现代化提供有力支撑。

—— 习近平 2022 年 4 月 19 日在中央全面深化改革委员会第二十五次会议上的讲话

没有网络安全就没有国家安全，没有信息化就没有现代化。建设网络强国，要有自己的技术，有过硬的技术；……

—— 习近平 2014 年 2 月 27 日在中央网络安全和信息化领导小组第一次会议上的讲话

网络空间安全大类三大专业



专业关系示意图

注：通过密码技术（ **基于数学理论的变换** ）实现 **基本安全属性**。

基本安全属性

1. 机密性:

   保证信息被授权者使用而不泄露给未授权者；即让未授权者看不到信息或者看不懂信息。

基本安全属性

1. 机密性:

   保证信息被授权者使用而不泄露给未授权者；即让未授权者看不到信息或者看不懂信息。

2. 认　证：
   - 消息认证：包括消息源认证和消息完整性，前者保证消息来源未被冒充，后者保证消息未被篡改;
   - 身份认证：保证通信实体的真实性。

基本安全属性

1. 机密性:

   保证信息被授权者使用而不泄露给未授权者；即让未授权者看不到信息或者看不懂信息。

2. 认　证：
   - 消息认证：包括消息源认证和消息完整性，前者保证消息来源未被冒充，后者保证消息未被篡改;
   - 身份认证：保证通信实体的真实性。

3. 完整性：
   - 数据完整性：数据未被未授权篡改或损坏；
   - 系统完整性：系统未被非授权操控，即按既定的程序运行。

基本安全属性

1. 机密性:

   保证信息被授权者使用而不泄露给未授权者；即让未授权者看不到信息或者看不懂信息。

2. 认　证：
   - 消息认证：包括消息源认证和消息完整性，前者保证消息来源未被冒充，后者保证消息未被篡改;
   - 身份认证：保证通信实体的真实性。

3. 完整性：
   - 数据完整性：数据未被未授权篡改或损坏；
   - 系统完整性：系统未被非授权操控，即按既定的程序运行。

4. 不可否认性：

   无论发送方还是接收方都不能抵赖所进行的传输等行为。

数学理论基础

类别	涵盖内容	开课学期
先修课程	高等数学、线性代数、离散数学	第一、二学期
本门课程	数论、近世（抽象）代数、有限域	第三学期
其他课程	概率论与数理统计、数学建模、组合数学、复变函数、……	第三、四学期

注：详见各专业培养方案。

目录

课程目标

1. 掌握信息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信息安全等相关系统中。
2. 能够根据信息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。

目录

计划表——数论 (1)

知识模块	教学内容	学时
整数的可除性（1）	整除的概念，素数及其平凡判别，Eratosthenes 筛法、欧几里德除法、整数 b 进制表示	3
整数的可除性（2）	最大公因数，广义欧几里德除法，贝祖等式，最小公倍数，整数分解	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
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
同余方程（1）	同余方程的基本概念，一次同余方程，中国剩余定理，同余方程组	3

计划表——数论 (2)

知识模块	教学内容	学时
同余方程（2）	二次同余方程，平方剩余，勒让德符号，二次互反定律，雅可比符号，二次同余方程求解	3
同余方程（3）	高次同余方程的解数，素数模的高次同余方程，素数幂模的高次同余方程——幂指数提升	3
阶与原根	阶及其基本性质，原根的定义，原根存在的充要条件，指标与 n 次同余方程	3
素性检测	Fermat 素性检测、S-S 素性检测、M-R 素性检测、A-K-S 素性检测	3

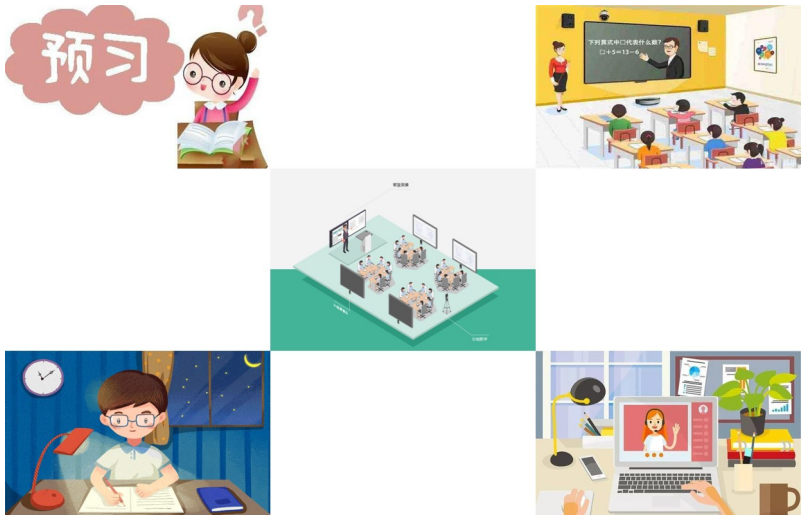
计划表——近世（抽象）代数及有限域

知识模块	教学内容	学时
群（1）	群的定义与性质，子群	3
群（2）	正规子群，商群，群同态与同构，群同态基本定理	3
群（3）	循环群，置换群	3
环（1）	环的定义，子环，理想和商环，环同态与同构，环同态基本定理	3
环（2）	多项式整环，多项式整除与不可约多项式，多项式欧几里德除法，多项式同余	3
域（1）	域与子域，分式域，素域，有限扩域，代数扩域，单扩域，分裂域	3
域（2）	Galois 基本定理，有限域	3

目录

学习要求

1. 课前预习，充分准备。
2. 课堂教学，认真听讲。
3. 研讨教学，积极探索。
4. 课后复习，消化巩固。
5. 线上自学，融汇贯通。



注：课程性质决定需要这样的学习方法 (成熟、会学习的表现)。

目录

教学资料

1. 课程教材

《信息安全数学基础》(第 2 版), 陈恭亮, 清华大学出版社, 2014 年 10 月.

2. 参考书目

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

《公钥密码学的数学基础》, 王小云、王明强等, 科学出版社, 2013 年 1 月.

《初等数论》（第三版）, 潘承洞、潘承彪, 北京大学出版社, 2019 年 5 月.

《算法数论》, 裴定一、祝跃飞, 科学出版社, 2015 年 9 月.

《近世代数基础》, 张禾瑞, 高等教育出版社, 2010 年 11 月.

《数论与密码》, 杨思熳, 华东师范大学出版社, 2010 年 9 月.

《数论与有限域》, 董丽华等, 机械工业出版社, 2010 年 10 月.

《代数学基础与有限域》, 林东岱, 高等教育出版社, 2006 年 7 月.

线上课程

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

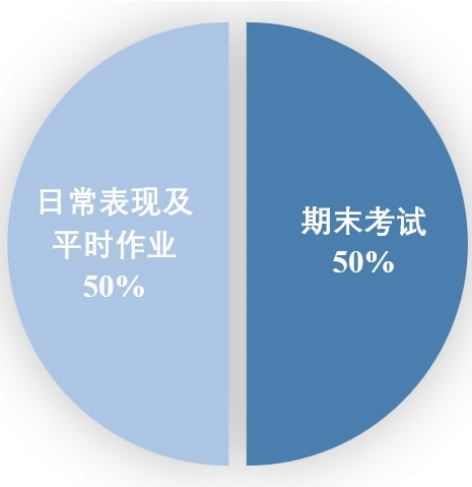
   开课学校：Massachusetts Institute of Technology

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

考核环节

考核环节主要包括日常表现、平时作业和期末考试。

1. 日常表现及平时作业
   包括出勤、课堂表现等，作业一般为每周一次，涵盖课程所有内容，根据是否按时提交、完成情况等进行综合评定。
2. 期末考试
   闭卷考试，题目涉及课程全部教学内容，按照卷面成绩进行评定。



交流与讨论

电子邮箱：

陈秀波：xb_chen@bupt.edu.cn

徐国胜：guoshengxu@bupt.edu.cn

金正平：zhpjin@bupt.edu.cn