高等学校电子信息类“十三五”规划教材
应用型网络与信息安全工程技术人才培养系列教材

信息安全数学基础

（卓越工程师计划）

张金全　段新东　张仕斌　编著

西安电子科技大学出版社
http://www.xduph.com

高等学校电子信息类“十三五”规划教材
应用型网络与信息安全工程技术人才培养系列教材

信息安全数学基础

（卓越工程师计划）

张金全　段新东　张仕斌　编著

西安电子科技大学出版社

内 容 简 介

对称密码算法高级加密标准 AES 和公钥密码算法 RSA、DSA 以及 SM2、ECDSA 等在信息安全领域被广泛使用. 本书以帮助读者学习和理解这些密码算法为目标，以直接明了、浅显易懂的方式，介绍掌握这些算法所需具备的初等数论中同余和原根，近世代数中群、环、域的基础知识以及椭圆曲线的基础知识.

本书可作为高等学校信息安全本科生的教材，也可作为自学密码算法所基于的数学基础理论知识的人员的参考书.

图书在版编目(CIP)数据

信息安全数学基础/张金全，段新东，张仕斌编著. —西安：西安电子科技大学出版社，2015.12

高等学校电子信息类“十三五”规划教材

ISBN 978-7-5606-3924-6

Ⅰ. ① 信… Ⅱ. ① 张… ② 段… ③ 张… Ⅲ. ① 信息系统—安全技术—应用数学—高等学校—教材

Ⅳ. ① TP309 ② O29

中国版本图书馆 CIP 数据核字(2015)第 292072 号

策划编辑 李惠萍

责任编辑 王 瑛 李惠萍

出版发行 西安电子科技大学出版社(西安市太白南路 2 号)

电 话 (029)88242885 88201467 邮 编 710071

网 址 www.xduph.com 电子邮箱 xdupfxb001@163.com

经 销 新华书店

印刷单位 陕西天意印务有限责任公司

版 次 2015 年 12 月第 1 版 2015 年 12 月第 1 次印刷

开 本 787 毫米×960 毫米 1/16 印张 8.5

字 数 143 千字

印 数 1～3000 册

定 价 15.00 元

ISBN 978-7-5606-3924-6/TP

XDUP 4216001-1

序

进入21世纪以来，信息技术迅速改变着人们传统的生产和生活方式，社会的信息化已经成为当今世界发展不可逆转的趋势和潮流. 信息作为一种重要的战略资源，与物资、能源、人力一起已被视为现代社会生产力的主要因素. 目前，世界各国围绕着信息获取、利用和控制的国际竞争日趋激烈，网络与信息安全问题已成为一个世纪性、全球性的课题. 党的十八大报告明确指出，要“高度关注海洋、太空、网络空间安全”. 党的十八届三中全会决定设立国家安全委员会，成立中央网络安全和信息化领导小组，并把网络与信息安全列入了国家发展的最高战略方向之一. 这为包含网络空间安全在内的非传统安全领域问题的有效治理提供了重要的体制机制保障，是我国国家安全体制机制的一个重大创新性举措，彰显了我国政府治国理政的战略新思维和“大安全观”.

人才资源是确保我国网络与信息安全第一位的资源，信息安全人才培养是国家信息安全保障体系建设的基础和必备条件. 随着我国信息化和信息安全产业的快速发展，社会对信息安全人才的需求不断增加. 2015年6月11日，国务院学位委员会和教育部联合发出“学位[2015]11号”通知，决定在“工学”门类下增设“网络空间安全”一级学科，代码为“0839”，授予工学学位. 这是国家推进专业化教育，在信息安全领域掌握自主权、抢占先机的重要举措.

建国以来，我国高等工科院校一直是培养各类高级应用型专门人才的主力. 培养网络与信息安全高级应用型专门人才也是高等院校责无旁贷的责任. 目前，许多高等院校和科研院所已经开办了信息安全专业或开设了相关课程. 作为国家首批61所“卓越工程师教育培养计划”试点院校之一，成都信息工程大学以《国家中长期教育改革和发展规划纲要(2010—2020年)》、《国家中长期人才发展规划纲要(2010—2020年)》、《卓越工程师教育培养计划通用标准》为指导，

以专业建设和工程技术为主线，始终贯彻“面向工业界、面向未来、面向世界”的工程教育理念，按照“育人为本、崇尚应用”、“一切为了学生”的教学教育理念和“夯实基础、强化实践、注重创新、突出特色”的人才培养思路，遵循“行业指导、校企合作、分类实施、形式多样”的原则，实施了一系列教育教学改革. 令人欣喜的是，该校信息安全工程学院与西安电子科技大学出版社近期联合组织了一系列网络与信息安全专业教育教学改革的研讨活动，共同研讨培养应用型高级网络与信息安全工程技术人才的教育教学方法和课程体系，并在总结近年来该校信息安全专业实施“卓越工程师教育培养计划”教育教学改革成果和经验的基础上，组织编写了“应用型网络与信息安全工程技术人才培养系列教材”. 本套教材总结了该校信息安全专业教育教学改革成果和经验，相关课程有配套的课程过程化考核系统，是培养应用型网络与信息安全工程技术人才的一套比较完整、实用的教材，相信可以对我国高等院校网络与信息安全专业的建设起到很好的促进作用. 该套教材为中国电子教育学会高教分会推荐教材.

信息安全是相对的，信息安全领域的对抗永无止境. 国家对信息安全人才的需求是长期的、旺盛的. 衷心希望本套教材在培养我国合格的应用型网络与信息安全工程技术人才的过程中取得成功并不断完善，为我国信息安全事业做出自己的贡献.

高等学校电子信息类“十三五”规划教材
应用型网络与信息安全工程技术人才培养系列教材
名誉主编(中国密码学会常务理事)

何大可

二〇一五年十月

中国电子教育学会高教分会推荐

高等学校电子信息类“十三五”规划教材

应用型网络与信息安全工程技术人才培养系列教材

编审专家委员会名单

前　言

信息安全问题在当今社会愈显突出. 2015 年 6 月教育部已经决定在“工学”门类下增设“网络空间安全”一级学科. 数学是网络空间安全学科的重要理论基础之一，在信息安全人才培养中占有极其重要的位置.

近年来，对称密码算法高级加密标准 AES 和公钥密码算法 RSA、DSA、DH 等以及基于椭圆曲线公钥密码算法 SM2、ECDSA 等在信息安全领域被广泛使用. 本书以帮助读者学习和理解这些密码算法为目标，介绍掌握这些算法所需具备的初等数论、近世代数基础和椭圆曲线基础等知识.

本书具有以下特色：

(1) 根据作者多年的教学经验，将教学中发现的难点进行拆解，由浅入深、由易到难地介绍，并选取合适的例子进行说明，力求以直接明了、浅显易懂的方式介绍相关知识.

(2) 在每章节的例题中，为了读者更好地理解知识点本身，开始的例题比较简单，后面的例题则通过分拆密码算法，针对相应的知识点进行应用举例，同时说明了密码算法的原理.

(3) 为了激发读者的学习兴趣，本书加入了与内容相关的部分数学家的传记. 同时，书中编入了少量程序，也融入了作者多年的教学心得，希望这些内容可以帮助读者理解和掌握相关知识点.

本书由成都信息工程大学张金全博士主编，南阳理工学院段新东博士参与编写. 成都信息工程大学张仕斌教授为本书提供了大量素材，同时，张仕斌教授和哈尔滨师范大学刘焕平教授审阅了本书的结构，成都信息工程大学多位本科学生参与了编写和校对工作. 在编写过程中还得到了成都信息工程大学信息安全工程学院相关领导的大力支持，在此表示衷心的感谢.

感谢西安电子科技大学出版社李惠萍和王瑛编辑，她们对本书的出版付出了大量的劳动，王瑛编辑的敬业精神给我留下了非常深刻的印象.

编写过程中，编者除了参考文献中列出的国内外书籍外，还参考了Internet上的相关资料. 但由于部分网上资料来源不明确，无法把所有文献一一注明出处，在此致以诚挚的歉意.

本书获成都信息工程大学教改项目资助，以及四川省卓越工程师教育培养计划支持.

因编者水平有限，对于书中疏漏和不当之处，敬请读者批评指正. 恳请读者在发现问题的时候，不吝给我们发邮件(E-mail:zhjq@cuit.edu.cn)，谢谢!

编　者

2015年10月

目　录

第 1 章　整数的可除性

在中学我们已经学习过整除的部分知识，这里是对该部分知识的复习、加深和扩展，其中素数、最大公因数、带余除法和算术基本定理等知识在密码学中有广泛应用.

1.1　整　　除

本节介绍整除以及素数的定义和基本性质. 这些知识是数论的基础.

1. 整除

【定义 1.1.1】 设 $a, b\in\mathbf{Z}$(整数集合)，$b\neq 0$，如果存在 $q\in\mathbf{Z}$，使得 $a=bq$，则称 b 整除 a 或 a 可被 b 整除，记作 $b|a$，并称 a 是 b 的倍数，b 是 a 的因数(或约数、因子)；否则，称 b 不能整除 a 或 a 不能被 b 整除，记作 $b\nmid a$.

对于整除，应注意下述特殊情况：

① 0 是任何非零整数的倍数.

② ± 1 是任何整数的因数.

③ 任何非零整数是其自身的倍数，也是其自身的因数.

整数的整除具有以下基本性质：

① 设 $a, b\in\mathbf{Z}$，若 $b|a$，则 $b|-a$，$-b|-a$.

② 设 $a, b, c\in\mathbf{Z}$，若 $c|b$ 且 $b|a$，则 $c|a$.

证明　因为 $c|b$ 且 $b|a$，故存在 q_1 和 q_2，使得 $b=cq_1$ 且 $a=bq_2$，从而有 $a=cq_1q_2$，故 $c|a$.

③ 设 $a, b, c\in\mathbf{Z}$，若 $c|b$ 且 $c|a$，则 $c|a\pm b$.

证明　已知 $c|b$ 且 $c|a$，则存在整数 n 和 m，使得 $b=nc$ 且 $a=mc$，从而有

$$a\pm b=mc\pm nc=(m\pm n)c$$

又 $m\pm n$ 为整数，故 $c|a\pm b$.

④ 设 $a, b\in\mathbf{Z}$，且 p 为素数，若 $p|ab$，则 $p|a$ 或 $p|b$.

⑤ 设 $a, b, c \in \mathbf{Z}$，若 $c|b$ 且 $c|a$，则对任意整数 s、t，有 $c|sa \pm tb$.

证明 已知 $c|b$ 且 $c|a$，则存在整数 n 和 m，使得 $b=nc$ 且 $a=mc$. 于是，从 $sa \pm tb = msc \pm ntc = (ms \pm nt)c$ 即可看出 $c|sa \pm tb$.

性质⑤在后面会被多次使用. 该性质也可描述为：设 $a, b, c \in \mathbf{Z}$，若 $c|b$ 且 $c|a$，则 c 整除 a 和 b 的线性组合.

【例 1.1.1】 因为 $7|21$ 且 $7|98$，所以对任意整数 s、t，有 $7|21s+98t$.

2. 素数

在密码学中，素数是用得非常广泛的概念，例如公钥密码算法、数字签名算法以及一些密码协议中都有使用. 在对称密码算法高级加密标准(Advanced Encryption Standard，AES)中使用的不可约多项式，也可以看作是素数在一元多项式环上的推广.

【定义 1.1.2】 设 p 是大于 1 的整数，如果除了约数 1 和它本身外没有其它的约数，则称 p 为素数(或质数，取自英文单词 prime 的首字母). 若 m 是大于 1 的整数，且 m 不是素数，则称 m 为合数.

素数具有以下基本性质：

① 1 既不是素数也不是合数.

② 若 p 为素数，n 为正整数，当 $2 \leqslant p \leqslant \sqrt{n}$ 且 $p \nmid n$ 时，n 是素数.

【例 1.1.2】 n 为 37，因为 $6 \leqslant \sqrt{37}$，小于 6 的素数 p 有 2、3、5，用 p 去除 37，$p \nmid n$，故 37 为素数.

【例 1.1.3】 找出所有小于等于 50 的素数.

解 由性质②知，若一个数 n 是合数，则必有小于等于 $\sqrt{n}$ 的素因数，因为 $7 < \sqrt{50} < 8$，故依次划去 2 的倍数、3 的倍数、5 的倍数和 7 的倍数，剩下的数即为素数，见图 1.1.1.

	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~

图 1.1.1 用埃拉托色尼斯筛法求小于 50 的素数

上述方法是由古希腊数学家埃拉托色尼斯提出的，故称之为埃拉托色尼斯筛法.

【人物传记】埃拉托色尼斯(Eratosthenes，前 276—前 194)，出生于希腊属地埃及西部的 Cyrene，他在雅典的柏拉图学院学习了一段时间. 托勒密二世(Ptolemy Ⅱ)邀请埃拉托色尼斯到亚历山大教他的儿子，后来成为著名的亚历山大图书馆馆长. 他著有数学、地理、天文、历史、哲学和文学方面的书. 除了数学方面的工作，他还以古代编年史和地理测量闻名.

③ 素数有无穷多.

证明　用反证法. 假设只有有限个素数，它们是 q_1，…，q_k.

考虑 $m=q_1\cdots q_k+1$，因为素数个数有限且为 q_1，…，q_k，所以 m 必是合数，从而知必存在素数 q_i，使得 $q_i \mid m$. 由于 $m=q_1\cdots q_k+1$，故不可能整除，矛盾. 因此，假设是错误的，即素数必有无穷多个.

【定理 1.1.1】(素数个数定理)令 $\pi(x)$ 表示不超过 $x(x>0)$ 的素数的个数，则随着 x 的增大，$\pi(x)$ 和 $x/\ln x$ 的比值趋于 1，即

$$\lim_{x\to\infty}\frac{\pi(x)}{x/\ln x}=1$$

其中，$\ln x$ 是 x 的自然对数.

通过表 1.1.1 所示的对素数个数的统计，读者可以对素数的个数有个直观的了解.

表 1.1.1

x	$\pi(x)$	$x/\ln x$ 整数部分	$\pi(x)/(x/\ln x)$
1000	168	145	1.16
100 000	9592	8686	1.10
10 000 000	664 579	620 241	1.07
1 000 000 000	50 847 478	48 254 492	1.05

素数的性质当然不止这些，比如孪生素数猜想、哥德巴赫猜想、黎曼猜想等，感兴趣的读者可参阅相关书籍，这里只介绍了一些很基本的性质.

【人物传记】克里斯汀·哥德巴赫(Christian Goldbach，1690—1764)生于普鲁士哥尼斯堡(这个城市因七桥问题而在数学界很有名). 1725 年成为圣彼得堡皇家学院的数学教授. 1728 年到莫斯科成为沙皇彼得二世的老师. 1742 年任职于俄国外交部. 除了“每个大于 2 的偶数都能写为两个素数的和以及每个大于 5 的奇数能写为 3 个素数的和”的猜想外，在数学分析方面也做出了令

人瞩目的贡献.

【人物传记】中国数学家陈景润(1933—1996)取得了关于孪生素数和哥德巴赫猜想的重要结果. 1966 年发表《On the representation of a large even integer as the sum of a prime and the product of at most two primes》(《大偶数表为一个素数及一个不超过两个素数的乘积之和》,简称"1+2"),成为哥德巴赫猜想研究上的里程碑. 他所发表的成果也被称为陈氏定理.

【人物传记】美籍华裔数学家张益唐(1955—)于 1978 年进入北京大学数学科学学院攻读本科,1982 年读硕士,师从潘承彪,1985 年入读普渡大学,导师为莫宗坚. 2013 年由于在研究孪生素数猜想上取得了重大突破,于第六届世界华人数学家大会中荣获晨兴数学卓越成就奖,后来他还获得 Ostrowski 奖和 Rolf Schock 奖. 2014 年,美国数学学会更将崇高的柯尔数论奖授予张益唐. 同年 7 月 4 日,张益唐当选为中央研究院第 30 届数理科学组院士. 同年 9 月,张益唐获得了该年度的麦克阿瑟奖(俗称"天才"奖).

1.2 最大公因数

最大公因数是中学里面的知识. 在密码学中用得较多的是互素,这是最大公因数为 1 的情形. 在本门课程中,常用来求两个数的最大公因数的方法是欧几里德算法,也称辗转相除法.

1.2.1 带余除法

带余除法是关于整除性的一个重要结论.

【定理 1.2.1】 (带余除法)设 a、b 是两个给定的整数,$b>0$,则一定存在唯一的一对整数 q 与 r,满足

$$a=qb+r,\ 0\leqslant r<b$$

证明 先证存在性. 考虑一个整数序列

$$\cdots,\ -3b,\ -2b,\ -b,\ 0,\ b,\ 2b,\ 3b,\ \cdots$$

它们将实数轴分成长度为 b 的区间,而 a 必定落在其中的一个区间中,因此存在一个整数 q 使得 $qb\leqslant a<(q+1)b$.

令 $r=a-qb$,则有 $a=qb+r$,$0\leqslant r<b$.

再证唯一性. 如果分别有 q 与 r 及 q_1 与 r_1 满足

$$a=qb+r,\ 0\leqslant r<b$$

$$a=q_1b+r_1,\ 0\leqslant r_1<b$$

两式相减有 $b(q-q_1)=-(r-r_1)$，故 $b|r-r_1$.

由于 $0\leqslant r<b$，$0\leqslant r_1<b$，故 $-b<r-r_1<b$. 由 $b|r-r_1$ 知，$r=r_1$.

又因 $q_1b+r_1=qb+r$，故 $q=q_1$.

【定义 1.2.1】 在 $a=qb+r$，$0\leqslant r<b$ 中，称 q 为 a 被 b 除所得的不完全商，称 r 为 a 被 b 除所得的余数.

【定理 1.2.2】 设 a、b 是两个给定的整数，$b\neq 0$，则对任意整数 c，一定存在唯一的一对整数 q 与 r，满足

$$a=qb+r,\ c\leqslant r<|b|+c$$

这是带余除法的一般形式.

该定理的证明和定理 1.2.1 的相似.

【例 1.2.1】 设 $a=100$，$b=30$，由定理 1.2.2 知：

若 $c=10$，则 $10\leqslant r<40$，即 $100=3\times 30+10$；

若 $c=35$，则 $35\leqslant r<65$，即 $100=2\times 30+40$；

若 $c=-50$，则 $-50\leqslant r<-20$，即 $100=5\times 30+(-50)$.

【推论】 $b|a$ 的充要条件是 a 被 b 除所得的余数 $r=0$.

1.2.2　最大公因数

【定义 1.2.2】 设 a 和 b 是两个整数，若整数 d 是它们中每一个数的因数，则 d 称为 a 和 b 的公因数(或公约数). a 和 b 的公因数中最大的一个称为最大公因数，记为 (a, b). 也有的书将其记作 gcd(a, b)，即 greatest common divisor三个英文单词的首字母. 若$(a, b)=1$，则称 a 和 b 互素或互质.

进一步地，若整数 $a_1, a_2, \cdots, a_n$ 不全为零，那么 $a_1, a_2, \cdots, a_n$ 的公因数中最大的一个称为最大公因数，记作$(a_1, a_2, \cdots, a_n)$. 当$(a_1, a_2, \cdots, a_n)=1$ 时，称 $a_1, a_2, \cdots, a_n$ 互素或互质. 注意，这与 $a_1, a_2, \cdots, a_n$ 两两互素不同，$a_1, a_2, \cdots, a_n$ 两两互素要求$(a_i, a_j)=1$，$i\neq j$.

【例 1.2.2】 求最大公因数(168, 90).

解　这里采用短除法求解. 我们知道，一个整数要么是素数，要么有不超过$\sqrt{n}$的素因数. 要求 a 和 b 的最大公因数，可以依次用 2，3，5，…去试除 a 和 b，若都能整除，则找到公因数 p_1，然后用 2，3，5，…去试除 a/p_1 和 b/p_1. 重复这个过程，就可以找到 a 和 b 的所有公因数. 所有公因数的乘积即为 a 和 b 的最大公因数.

因为

$$\begin{array}{r|l} 2 & 168\ \ 90 \\ \hline 3 & 84\ \ 45 \\ \hline & 28\ \ 15 \end{array}$$

故 168 和 90 的最大公因数为$(168, 90)=2\times3=6$.

下面列出最大公因数的一些基本性质. 在掌握短除法的基础上,这些性质直观易懂,故证明从略.

① $(a, b)=(b, a)$.

② 设 a、b 为正整数,若 $b|a$,则$(a, b)=b$.

③ 设 $a_1, a_2, \cdots, a_n$ 是 n 个不全为零的整数,则

(i) $a_1, a_2, \cdots, a_n$ 与$|a_1|, |a_2|, \cdots, |a_n|$的公因数相同;

(ii) $(a_1, a_2, \cdots, a_n)=(|a_1|, |a_2|, \cdots, |a_n|)$.

④ 设 a、b 为正整数,则

$$(a, b)=(a, -b)=(-a, b)=(-a, -b)$$

⑤ 若 $b\neq0$,则$(0, b)=|b|$.

⑥ 设 $m>0$,则 $m(a_1, a_2)=(ma_1, ma_2)$.

⑦ 设 $a_1, a_2, \cdots, a_n$ 为整数,且 $a_1\neq0$,令$(a_1, a_2)=d_2$,$(d_2, a_3)=d_3$,$\cdots$,$(d_{n-1}, a_n)=d_n$,则$(a_1, a_2, \cdots, a_n)=d_n$.

【例 1.2.3】 计算最大公因数$(120, 150, 210, 35)$.

解 因为

$$(120, 150)=30, (30, 210)=30, (30, 35)=5$$

故

$$(120, 150, 210, 35)=5$$

或

$$\begin{aligned}(120, 150, 210, 35)&=((120, 150)\\&(210, 35))=(30,35)\ =5\end{aligned}$$

⑧ 设整数 a、b、c,若$(a, c)=1$,则$(ab, c)=(b, c)$.

⑨ 设整数 a、b、c,若 $a|bc$ 且$(a, b)=1$,则 $a|c$.

【例 1.2.4】 令 $a=5$,$b=3$,$c=10$,由于 $5|3\times10$ 且$(5, 3)=1$,故 $5|10$.