密码学及信息安全基础

陈小松 编著

清华大学出版社

密码学及信息安全基础

陈小松 编著

清华大学出版社
北京

内 容 简 介

全书共5章和2个附录，包含数论和代数基础知识、经典密码、对称密码、公钥密码、数字签名等信息安全知识的内容，还包括课内实验以及实验参考程序（包含用Java、MATLAB、Maple实现部分密码系统等）. 内容安排循序渐进，由浅入深，重点突出，读者在学习每一部分密码学内容之前，就刚好学完了所需的基础知识，便于读者学习. 本书可作为高等院校计算机、信息安全、网络、软件、通信等相关专业本科生以及低年级研究生的教材，也可作为与密码学及信息安全相关的工程技术人员学习的读本.

图书在版编目(CIP)数据

密码学及信息安全基础/陈小松编著. —北京：清华大学出版社，2018
ISBN 978-7-302-51100-7

Ⅰ. ①密… Ⅱ. ①陈… Ⅲ. ①密码学－高等学校－教材②信息安全－安全技术－高等学校－教材 Ⅳ. ①TN918.1②TP309

中国版本图书馆CIP数据核字(2018)第195624号

责任编辑：刘　颖
封面设计：傅瑞学
责任校对：赵丽敏
责任印制：丛怀宇

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦A座　　邮　　编：100084
社 总 机：010-62770175　　邮　　购：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 装 者：三河市国英印务有限公司
经　　销：全国新华书店
开　　本：170mm×240mm　　**印　张**：12　　**字　　数**：215千字
版　　次：2018年9月第1版　　**印　　次**：2018年9月第1次印刷
定　　价：38.00元

产品编号：081084-01

序 PREFACE

随着信息网络的发展，互联网对信息的保密和安全的要求越来越高，信息安全建设不仅关系到个人、单位利益，更重要的是关系到国家的安全和发展.很多与计算机相关的专业开设了密码学及信息安全的课程，但是所采用的大部分教材将密码学与数学内容分开，且大多只介绍数学结论，学生很难掌握密码学的思想和算法.本教材按照所需的数学基础知识结构编排，将密码学的内容融入数论和代数中，学生在学习密码学的每一部分内容之前，刚好学完了所需的基础知识.内容编排循序渐进，由浅入深，重点突出，尽可能讲清楚内容的方法和原理，以所需知识和思想方法先做铺垫，使学生更加容易理解，能够学得轻松，记得清楚.

本教材重点介绍密码学的基本思想和基本方法，包含数论和代数基础知识、经典密码、对称密码、公钥密码、数字签名等其他信息安全知识的内容，考虑到很多学校密码学和信息安全课程还包括课内实验，在第5章之后附加了课内实验内容，安排这些实验是为加深学生对算法或操作的理解和认识，也可以提高学生的应用能力和编程解决实际问题的能力.维吉尼亚密码作为经典密码的代表，第1章学完可以开始；RSA公钥作为基于大整数分解密码系统的代表，第2章第2节学完可以开始；Gamal公钥作为基于离散对数密码系统的代表，第2章学完可以开始；流密码密钥生成程序设计第4章学完可以开始；序列码生成程序设计作为认证码的一个应用，第5章第1节讲完可以开始；Windows 7自带防火墙的配置第5章第5节讲完可以开始.又考虑到不同专业学生掌握的编程语言不同，所以附加了用Java、MATLAB、Maple实现部分密码系统的实验参考程序.之所以选择这3种语言是因为：其一，Java是计算机专业最基本的编程语言；其二，MATLAB是理工科学生使用较多的编程语言；其三，Maple是实现一些算法简单高效

的编程语言，特别适合研究型读者使用. 教师可以根据教学实际情况选取. 很多学校密码学和信息安全课程(包括实践环节)为64学时或更少学时，为了适应这种情况，在保证教材内容完整和推导严谨的同时，结合各学校教学的实际情况，将某些内容设置为选讲内容，用星号标注. 在教学时可以跳过这些内容. 但是对于研究型读者来说，搞清楚这些内容，有助于理解后面的内容. 本教材各章节配备了适量习题，还配备了教学课件，需要教学课件的读者可向作者索取. 本教材可能会有需要改进的地方，若读者发现其中的问题，请通过邮箱与作者联系，以便在再版时加以完善.

作者

2018年6月

目录 CONTENTS

第1章

整除性、同余与经典密码

1.1 整数的整除性

1.1.1 整除的概念

本书中，用 $\mathbf{N}=\{0,1,2,3,\cdots\}$ 表示自然数的集合，$\mathbf{Z}^+=\{1,2,3,\cdots\}$ 表示正整数的集合，$\mathbf{Z}=\{\cdots,-2,-1,0,1,2,\cdots\}$ 表示全体整数的集合.

两个整数相加、相减、相乘的结果仍然是整数，但是两个整数相除却不一定是整数.

定义 1.1 设 $a,b\in\mathbf{Z},b\neq0$，若 $\frac{a}{b}\in\mathbf{Z}$，则说 b **整除** a，记作 $b|a$，也说 b 是 a 的**因数**或 a 是 b 的**倍数**；若 $\frac{a}{b}\notin\mathbf{Z}$，则说 b 不能整除 a.

为了使表达简洁，用 $\forall$ 表示“对于一切”，用 $\Rightarrow$ 表示“蕴含”，$\Leftrightarrow$ 表示“当且仅当”.

定理 1.1 $b|a\Leftrightarrow$存在 $q\in\mathbf{Z}$，使得 $a=bq(b\neq0)$.

证 若 $b|a,\frac{a}{b}=q\in\mathbf{Z}$，即 $a=bq(b\neq0)$；反过来，若 $a=bq(b\neq0)$，两边同除以 b，则得 $\frac{a}{b}=q\in\mathbf{Z}$.

当 $q\neq\pm1,\pm a$ 时，则说 b 是 a 的真因数.

整除有以下基本性质.

定理 1.2 (1) $c|b,b|a\Rightarrow c|a$.

(2) $d|a,d|b\Rightarrow\forall\ p,q\in\mathbf{Z},d|(pa+qb)$.

(3) $b|a,a\neq0\Rightarrow|b|\leqslant|a|$.

(4) $b|a,c\neq0\Leftrightarrow cb|ca$.

证 (1) $c|b,b|a\Rightarrow b=cs,a=bt\Rightarrow a=(cs)t=c(st)\Rightarrow c|a$.

(2) $a=ds, b=dt, pa+qb=dps+dqt=d(ps+qt)\Rightarrow d\mid(pa+qb)$.

(3) $a=bc\Rightarrow|a|=|b||c|, a\neq0\Rightarrow|a|\neq0$. 又 $|c|\geqslant1\Rightarrow|b|\leqslant|a|$.

(4) $a=bs\Rightarrow ca=cbs\Rightarrow cb\mid ca$.

例 1.1 k 个连续整数的乘积能被 $k!$ 整除.

证 考查 $n(n-1)\cdots(n-k+1)$.

(1) 若 $(n-k+1)>0$,则

$$C_n^k=\frac{n(n-1)\cdots(n-k+1)}{k!}\in\mathbf{Z}\Rightarrow k!\mid n(n-1)\cdots(n-k+1).$$

(2) 若 $n(n-1)\cdots(n-k+1)=0$,则 $k!\mid 0$.

(3) 若 $n<0$,则 $-n=n'>0$. 令 $n=-n'$,则 $n(n-1)\cdots(n-k+1)=(-n')(-n'-1)\cdots(-n'-k+1)=(-1)^k n'(n'+1)\cdots(n'+k-1)$,归结为第一种情况.

因此,$k!\mid n'(n'+1)\cdots(n'+k-1)$,所以,$k!\mid(-1)^k n'(n'+1)\cdots(n'+k-1)$,即 $k!\mid n(n-1)\cdots(n-k+1)$.

例 1.2 证明 对于任何正整数 n,$6\mid n(n+1)(2n+1)$.

证
$$\begin{aligned}n(n+1)(2n+1)&=n(n+1)(n-1+n+2)\\&=(n-1)n(n+1)+n(n+1)(n+2),\end{aligned}$$

由例 1.1,

$$3!\mid(n-1)n(n+1),\quad 3!\mid n(n+1)(n+2),$$

因此,$6\mid n(n+1)(2n+1)$.

定理 1.3(带余除法) 设 $a,b\in\mathbf{Z}, b>0$,则存在唯一的 q,r,使得

$$a=bq+r,\quad 0\leqslant r<b.$$

证 作数列$\cdots,-2b,-b,0,b,2b,\cdots$,则 a 必落在某一区间且只能落在一个区间,即存在 q,使

$qb\leqslant a<(q+1)b\Rightarrow 0\leqslant a-qb<b$. 令 $r=a-qb$,则有 $a=qb+r, 0\leqslant r<b$. 由于只能在一个区间,所以 q 唯一,从而 r 唯一.

1.1.2 最大公因数

定义 1.2 设 $a,b\in\mathbf{Z}$,a,b 不全为 0,如果 $d\mid a$ 且 $d\mid b$,则称 d 为 a 和 b 的公因数. 而把 a 和 b 的所有公因数中最大的称为 a 和 b 的**最大公因数**,记为 (a,b) 或 $\gcd(a,b)$.

最大公因数的概念可以推广到多个,即 n 个不全为 0 的整数 $a_1,a_2,\cdots,a_n$ 的所有公因数中最大的称为 $a_1,a_2,\cdots,a_n$ 的最大公因数,记为 $(a_1,a_2,\cdots,a_n)$,或

$\gcd(a_1,a_2,\cdots,a_n)$.

定理 1.4 $(a,b)=(|a|,|b|)$.

证 $d|a,d|b \Leftrightarrow d||a|,d||b|$,即 a,b 的公因数集与 $|a|,|b|$ 的公因数集合相同,因此最大的也就相同.

定理 1.4 表明,求两个整数的最大公因数归结为求两个正整数的最大公因数,故求 a 的公因数时,若 a 是负数,则可以去掉 a 的负号.

定理 1.5 如果 $a=bq+c$,则 $(a,b)=(b,c)$.

证 若 $d|a,d|b\Rightarrow d|b,d|(a-bq)$,即 $d|c$;反过来,若 $d|b,d|c\Rightarrow d|b,d|(bq+c)$,即 $d|a$. 这表明 a,b 的公因数集与 b,c 的公因数集合相同,最大的也就相同.

例 1.3 $c|(a+b)$,则 $(a,c)=(b,c)$.

证 $a+b=cs\Rightarrow a=cs-b$,由定理 1.4、定理 1.5,$(a,c)=(b,c)$.

求两个正整数的最大公因数的方法称为**辗转相除法**,又称为**欧几里得除法**.

定理 1.6 设 $a,b\in\mathbf{Z}^+$,反复用带余除法,即用每次的余数为除数去除上一次的除数,直到余数为 0,可得

$$\begin{aligned}
&a=bq_1+r_1, \quad 0<r_1<b,\\
&b=r_1q_2+r_2, \quad 0<r_2<r_1,\\
&r_1=r_2q_3+r_3, \quad 0<r_3<r_2,\\
&\vdots\\
&r_{n-2}=r_{n-1}q_n+r_n, \quad 0<r_n<r_{n-1},\\
&r_{n-1}=r_nq_{n+1}+r_{n+1}, \quad r_{n+1}=0.
\end{aligned}$$

最后一个不为 0 的余数 r_n 就是 a 和 b 的最大公因数.

证 由定理 1.5

$$(a,b)=(b,r_1)=(r_1,r_2)=\cdots=(r_{n-1},r_n)=(r_n,r_{n+1})=(r_n,0)=r_n.$$

例 1.4 求(525,231).

解 将 525 和 231 辗转相除,得

$$\begin{aligned}
&525=2\times231+63,\\
&231=3\times63+42,\\
&63=1\times42+21,\\
&42=2\times21+0.
\end{aligned}$$

这个过程可以按如下竖式计算出来:

2	525	231	3
	462	189	
1	63	42	2
	42	42	
	21	0	

所以(525,231)=21.

定理 1.7 a,b 的公因数集与(a,b)的因数集合相同.

证 设 d 是 a,b 的公因数,即 $d|a,d|b$,则由辗转相除法的过程,得 $d|r_n=(a,b)$,即 a,b 的公因数是(a,b)的因数;反过来,设 d 是(a,b)的因数,则 $d|(a,b)$.而$(a,b)|a,(a,b)|b$,于是 $d|a,d|b$,即(a,b)的因数是 a,b 的公因数.

推论 1.1 $\forall k\in\mathbf{Z},(a,b)=(a,b+ka)$.

证 $(a,b)|a,(a,b)|b$,由定理 1.5⇒$(a,b)|(b+ka)$,从而$(a,b)|(a,b+ka)$;令 $d=(a,b+ka)$,则 $d|a,d|ka+b\Rightarrow d|(b+ka)-ka$,即 $d|b\Rightarrow d|(a,b)$.

将推论 1.1 用于例 1.4,有$(525,231)=(525+(-2)\cdot 231,231)=(63,231)=(63,(-4)\cdot 63+231)=(63,21)=21$.

《九章算术》中的**更相减损术**,相当于 $a>b>0,k=-1$ 的情况下的推论 1.1.

* **引理 1.1** 设 $a,b\in\mathbf{Z},q_i$ 由辗转相除法得到,则

$Q_ka-P_kb=(-1)^{k-1}r_k$,这里

$$P_0=1,\quad P_1=q_1,\quad P_k=q_kP_{k-1}+P_{k-2},$$
$$Q_0=0,\quad Q_1=1,\quad Q_k=q_kQ_{k-1}+Q_{k-2},\quad k=2,3,\cdots,n.$$

证 对 k 用数学归纳法.当 $k=1$ 时,$Q_1a-P_1b=a-q_1b=r_1$,结论成立;

当 $k=2$ 时,$Q_2a-P_2b=a(q_2Q_1+Q_0)-(q_2P_1+P_0)b=-r_2$.

假定对于小于 k 结论成立,则

$$\begin{aligned}Q_ka-P_kb&=(q_kQ_{k-1}+Q_{k-2})a-(q_kP_{k-1}+P_{k-2})b\\&=q_k(Q_{k-1}a-P_{k-1}b)+Q_{k-2}a-P_{k-2}b\\&=q_k(-1)^{k-2}r_{k-1}+(-1)^{k-3}r_{k-2}=(-1)^{k-2}(q_kr_{k-1}-r_{k-2})\\&=(-1)^{k-2}(q_kr_{k-1}-(r_{k-1}q_k+r_k))\\&=(-1)^{k-2}(-r_k)=(-1)^{k-1}r_k,\end{aligned}$$

即结论对于 k 成立.

定理 1.8 $ax+by=(a,b),a>0,b>0$ 的一个解为

$$x_0=(-1)^{n-1}Q_n,\quad y_0=(-1)^nP_n.$$

证 在引理 1.1 中取 $k=n$,即得.

推论 1.2 设 a,b 不全为 0,$a,b\in\mathbf{Z}$,则存在 $x,y\in\mathbf{Z}$,使$(a,b)=xa+yb$.

证 不妨设 $a\neq 0$.若 x,y 满足 $|a|x+by=(a,b)$,当 $a<0$ 时,$-x,y$ 满足 $ax+by=(a,b)$.

定义 1.3 如果整数 a 与整数 b 的最大公因数为 1,则称 a 与 b **互素**,记为 $(a,b)=1$.

互素的概念可以推广到多个，即若 n 个整数 $a_1,a_2,\cdots,a_n$ 的最大公因数为1，则称 $a_1,a_2,\cdots,a_n$ 互素，记为 $(a_1,a_2,\cdots,a_n)=1$.

如果 $a_1,a_2,\cdots,a_n$ 中任意两个都互素，则称 $a_1,a_2,\cdots,a_n$ **两两互素**.

例如 2,3,6 互素，2,3 互素，但 2,6 不互素，所以 2,3,6 不是两两互素.

推论 1.3 $(a,b)=1 \Leftrightarrow$ 存在 $s,t\in\mathbf{Z}$，使得 $sa+tb=1$.

证 "⇒"$(a,b)=1$，由推论 1.2 直接得出；

"⇐"若有 $s,t\in\mathbf{Z}$，使 $sa+tb=1$，若 $d|a,d|b$，则 $d|(sa+tb)=1$，即 $(a,b)=1$.

定理 1.9 设 $a,b\in\mathbf{Z},a,b$ 不全为 0，则 $\forall m\in\mathbf{Z}^+$，有 $(ma,mb)=m(a,b)$.

证 将辗转相除法的等式乘以 m，有

$$
\begin{aligned}
&am=bmq_1+r_1m, \quad 0<r_1m<bm,\\
&bm=r_1mq_2+r_2m, \quad 0<r_2m<r_1m,\\
&r_1m=r_2mq_3+r_3m, \quad 0<r_3m<r_2m,\\
&\quad\vdots\\
&r_{n-2}m=r_{n-1}mq_n+r_nm, \quad 0<r_nm<r_{n-1}m,\\
&r_{n-1}m=r_nmq_{n+1}+r_{n+1}m, \quad r_{n+1}m=0,
\end{aligned}
$$

所以 $(am,bm)=r_nm=(a,b)m$.

定理 1.10 $a,b,c\in\mathbf{Z},b,c$ 不全为 0，且 $(a,c)=1$，则 $(ab,c)=(b,c)$.

证 $(a,c)=1$，故存在 $s,t\in\mathbf{Z}$，使得 $sa+tc=1$，两边乘以 b，得 $s(ab)+tbc=b$. 若 $d|ab,d|c$，则 $d|b$. 反之，若 $d|b,d|c$，则 $d|ab$，故 ab,c 与 b,c 有相同的公因数，由有限数集的最大数唯一，得 $(ab,c)=(b,c)$.

推论 1.4 若 $(a,c)=1,(b,c)=1$，则 $(ab,c)=1$.

推论 1.5 若 $c|ab,(a,c)=1$，则 $c|b$.

证 $c|ab,|c|=(c,ab)=(c,b)$，由定理 1.10，得 $c|b$.

定义 1.4 设 $a|m,b|m$，则说 m 是 a,b 的一个公倍数，最小的正公倍数称为**最小公倍数**，记作 $[a,b]$ 或 $\mathrm{lcm}(a,b)$.

定理 1.11 设 $a,b\in\mathbf{Z}^+$，则 $[a,b]=\dfrac{ab}{(a,b)}$.

证 设 $a|m,b|m\Rightarrow m=ak=bs$. 令 $a=(a,b)a_1,b=(a,b)b_1$，则

$$
m=(a,b)a_1k=(a,b)b_1s\Rightarrow a_1k=b_1s, \quad (a_1,b_1)=\left(\frac{a}{(a,b)},\frac{b}{(a,b)}\right)=1,
$$

$$
b_1|k,\text{即 } k=b_1t\Rightarrow m=(a,b)a_1b_1t=\frac{ab}{(a,b)}t,
$$

$t=1$ 时最小，即 $[a,b]=\dfrac{ab}{(a,b)}$.

例如，$a=18=2\times3^2$，$b=12=2^2\times3$，$(a,b)=6$，$[a,b]=\dfrac{ab}{(a,b)}=\dfrac{18\times12}{(18,12)}=36$.

习题 1.1

1. 对任意整数 n，证明 $30\mid n^5-n$.

2. 求$(39,63)$.

3. 设 $a_nx^n+a_{n-1}x^{n-1}+\cdots+a_0$ 是一个整系数多项式，则它的有理根 $\dfrac{p}{q}$ 一定满足 $p\mid a_0$，$q\mid a_n$，从而证明$\sqrt{2}$不是有理数.

1.2 不定方程

1.2.1 二元一次不定方程

公元5世纪《张丘建算经》里，有一道百鸡问题：

鸡翁一，值钱五，

鸡母一，值钱三，

鸡雏三，值钱一，

百钱买百鸡，

问鸡翁、鸡母、鸡雏各几何？

设买公鸡 x 只，买母鸡 y 只，买小鸡 z 只，那么

$$\begin{cases}x+y+z=100, & (1\text{-}1)\\ 5x+3y+z/3=100. & (1\text{-}2)\end{cases}$$

(1−2)×3−(1−1)，得 $14x+8y=200$，即

$$7x+4y=100.$$

设 a,b,c 是整数，

$$ax+by=c \tag{1-3}$$

称为二元一次不定方程. 适合方程(1-3)的整数 x,y 称为该不定方程解.

并不是所有二元一次方程都有解，例如方程 $4x+12y=15$ 无解，因为对任意整数 x,y，$4x+12y$ 永远是偶数.

定理 1.12 设 $ab\neq0$，则 $ax+by=c$ 有解$\Leftrightarrow(a,b)\mid c$.

证 “⇒”若方程(1-3)有解 x,y，即 $ax+by=c$，则$(a,b)\mid a$，$(a,b)\mid b$，因此