普通高等教育“十一五”国家级规划教材

密码学与信息安全技术

罗守山 陈 萍 邹永忠 刘 琳 编著

北京邮电大学出版社
www.buptpress.com

普通高等教育“十一五”国家级规划教材

密码学与信息安全技术

罗守山　陈　萍　邹永忠　刘　琳　编著

北京邮电大学出版社
·北京·

内容简介

本书是在作者多年的教学与科研实践的基础上编写的。本书系统地介绍了密码学与信息安全技术的基本原理和方法。本书的内容包括密码学与网络安全基础、现代密码学加密算法与协议、信息认证与身份识别、密钥管理、访问控制、网络攻击、防火墙和虚拟专用网等内容。

本书可作为计算机、通信、信息安全等专业的本科生教材，也可供从事相关专业的教学、科研人员和工程技术人员参考。

图书在版编目(CIP)数据

密码学与信息安全技术/罗守山等编著. —北京：北京邮电大学出版社，2009

ISBN 978-7-5635-1904-0

Ⅰ.密… Ⅱ.罗… Ⅲ.①密码—理论—高等学校—教材②信息系统—安全技术—高等学校—教材
Ⅳ.TN918.1 TP309

中国版本图书馆 CIP 数据核字(2009)第 050393 号

书　　名：密码学与信息安全技术
作　　者：罗守山　陈萍　邹永忠　刘琳
责任编辑：艾莉莎
出版发行：北京邮电大学出版社
社　　址：北京市海淀区西土城路 10 号(邮编：100876)
发 行 部：电话：010-62282185　传真：010-62283578
E-mail：publish@bupt.edu.cn
经　　销：各地新华书店
印　　刷：北京源海印刷有限责任公司
开　　本：787 mm×1 092 mm　1/16
印　　张：24.75
字　　数：629 千字
印　　数：1—5 000 册
版　　次：2009 年 4 月第 1 版　2009 年 4 月第 1 次印刷

ISBN 978-7-5635-1904-0　　定　价：39.00 元

前　言

随着计算机网络的发展，特别是 Internet 的发展，我们的学习、工作、生活方式都发生了变化。由于计算机系统的大量增加，人们越来越依赖这些系统，用它们来实现信息的存储与传输，同时也带来了新的需求，包括保证数据与资源不被泄露、保证数据与消息的真实性、保护系统不受攻击。密码学与信息安全技术能够满足这些需求。近年来，密码学与信息安全学科正在迅速发展与成熟，它们能够提供很多安全应用的解决方案。

本书介绍了密码学与信息安全技术的基本理论和基本方法。本书的结构安排如下。

第 1 章“密码学与网络安全基础”介绍了密码学的数学基础、信息论基础和计算复杂性基础，同时还介绍了密码学与信息安全技术的基础知识。

第 2 章“现代密码学加密算法与协议”介绍了重要的对称密码体制与非对称密码体制，同时还介绍了密码协议的知识，并将针对密码协议研究中的一个热点问题——安全多方计算协议——作比较详细的论述。

第 3 章“信息认证与身份识别”介绍了杂凑函数、数字签名和身份识别协议等内容。

第 4 章“密钥管理”介绍了密钥管理的相关知识，包括密钥分配协议、密钥的分散管理与托管等知识。

第 5 章“访问控制”介绍了访问控制的知识，包括访问控制矩阵、访问控制策略和一些经典的访问控制模型等内容。

第 6 章“网络攻击”介绍了计算机网络的主要漏洞、网络攻击的分类与实现、木马、计算机病毒和网络蠕虫等相关知识。

第 7 章“防火墙”介绍了防火墙的基本知识，包括防火墙的概念、技术及其结构等内容。

第 8 章“虚拟专用网”介绍了虚拟专用网的有关知识，包括虚拟专用网的概念和网络层虚拟专用网的相关知识等。

在一些章节的最后，还附有和密码学与信息安全技术相关的阅读内容，可供

读者了解相应的知识并增强学习的兴趣。

通过本书内容的学习，读者可以获得密码学与信息安全技术的基本知识。通过对本书习题的思考，读者可以获得相关技能的训练，为今后对我国信息与网络安全事业的发展作贡献打下坚实的基础。本书可作为计算机、通信、信息安全等专业的本科生教材，也可供从事相关专业的教学、科研人员和工程技术人员参考。

本书由北京邮电大学罗守山、陈萍、邹永忠和公安部第一研究所刘琳共同编写。在编写的过程中，得到了一些研究生的支持，贾晓芸、高海英、刘文、王小妹、蒲明松、刘红波、廖千才、邱梅、王文彬、马敏耀、肖倩、康威和袁军会等同学帮助整理了一部分文档，阅读了一部分初稿，并改正了不少错误，作者向他们表示感谢。

作　者

目　录

第 6 章　网络攻击

第 7 章　防火墙

第1章 密码学与网络安全基础

The fundamental problem of communication is that of reproducing at one point either exactly or approximately a message selected at another point. Frequently the messages have meaning; that is they refer to or are correlated according to some system with certain physical or conceptual entities. These semantic aspects of communication are irrelevant to the engineering problem.

—C. E. SHANNON,1948

通信的基本问题是:通信的一方选择一条信息,另一方能够将其精确地(或近似地)恢复出来。通常,这些信息是有含义的,它们与某些物理或概念的实体有关。通信的语义方面与工程问题不相关。

——香农,1948

信息安全已经成为一个全社会关注的问题。密码学与网络安全和国家的政治安全、经济安全、社会稳定以及人们的日常生活密切相关。从技术角度看,密码学与网络安全是一个涉及计算机科学、网络技术、通信技术、密码技术、应用数学、信息论等多知识、边缘性的综合学科,其重要性有目共睹。特别是随着全球信息基础设施的建立与形成,网络化、信息化已经成为现代社会的一个重要特征。应用密码技术,提供这些信息基础设施的安全保障机制是社会发展的需要。本章介绍密码学的数学基础、信息论基础、计算复杂性基础,同时还将介绍密码学与网络安全的一些基础知识。

1.1 密码学的数学基础

在现代密码学中需要使用许多的数学理论。例如,近世代数、数论、组合论、概率论及线性代数等,这些数学理论均为设计密码系统及协议不可或缺的工具。本节将对现代密码学中必要的数学基础作一重点整理。同时,也简单地介绍一些应用实例,一方面能够使读者了解所学的数学知识在密码学与网络安全中的应用,另一方面也可以将这些应用实例作为背景,帮助读者更好地理解这些抽象的数学知识。

1.1.1 近世代数基础

1. 群

【定义 1-1】 设 G 是非空集合,并在 G 内定义了一种代数运算"$\circ$",若满足下述公理:

(1) 运算封闭性成立，对任意 $a,b\in G$，恒有 $a\circ b\in G$；

(2) 结合律成立，对任意 $a,b\in G$，有 $(a\circ b)\circ c=a\circ(b\circ c)$；

(3) G 中有单位元 e 存在，对任意 $a\in G$，有 $a\circ e=e\circ a=a$；

(4) 对任意 $a\in G$，存在有 a 的逆元 $a^{-1}\in G$，使 $a\circ a^{-1}=a^{-1}\circ a=e$。

则称 G 构成一个群，记做 $(G,0)$。

上述定义中，G 的运算“$\circ$”指代一般意义下的运算，它可以是通常的乘法或加法。对乘法群而言，单位元常记为 1，a 的逆元记为 a^{-1}；对加法群而言，则单位元常记为 0，a 的逆元记为 $-a$。群中元素的个数，称为群的阶。若群中元素个数有限，称为有限群；否则，称为无限群。

上述定义的(3)和(4)可以换成一个条件：对于 G 的任何两个元 a，b 来说，方程 $ax=b$ 和 $ya=b$ 都在 G 中有解。

若群 $(G,0)$ 中，对任何 $a,b\in G$，有 $a\circ b=b\circ a$，则称 G 为交换群或 Abel 群。

【例 1-1】 整数集 $\mathbf{Z}$ 关于普通的加法运算“+”，形成一个 Abel 群，其中单位元是 0，任一整数 a 的逆元是 $-a$。

【例 1-2】 剩余类集 $\mathbf{Z}_n$ 关于模 n 加法运算形成一个阶为 n 的 Abel 群，称为整数模 n 的加群。$\mathbf{Z}_n$ 关于模 n 的乘法运算不是一个群，因为不是所有的元素都有乘法逆。

仅对剩余类加法运算作一个解释。

对任意 $[a],[b],[c]\in\mathbf{Z}_n$，

(1) $([a]+[b])+[c]=[a+b+c]=[a]+([b]+[c])$；

(2) $[0]+[a]=[a]+[0]=[a]$；

(3) $[a]+[n-a]=[n-a]+[a]=[n]=[0]$。

由此可知，$[0]$ 是单位元，$[n-a]$ 是 $[a]$ 的逆元。

【定义 1-2】 设 H 是 G 的一个非空子集，如果 H 本身在群 G 的运算“$\circ$”之下构成一个群，就说 H 是 G 的一个子群。如果 H 是 G 的一个子群，且 $H\neq G$，则称 H 是 G 的一个真子群。

【例 1-3】 $(\mathbf{Z},+)$ 是 $(\mathbf{R},+)$ 的真子群，$(\mathbf{R},+)$ 是 $(\mathbf{C},+)$ 的真子群。这里，“+”表示普通的加法运算，$\mathbf{Z}$ 表示全体整数集，$\mathbf{R}$ 表示全体实数集，$\mathbf{C}$ 表示全体复数集。

【定义 1-3】 设 G 是一个群，如果 G 中有一个元素 a 使得对每一个 $b\in G$ 都存在一个整数 i，使得 $b=a^i$，则称 G 是一个循环群，a 称为 G 的一个生成元。

【定义 1-4】 设 G 是一个群，$a\in G$，a 的阶定义为使得 $a^t=1$ 的最小正整数 t（假定这样的正整数存在的话）。如果这样的正整数 t 不存在，那么 a 的阶定义为 ∞。

易知，如果 G 是一个群，$a\in G$，则 $\{a^k\mid k\in\mathbf{Z}\}$ 形成 G 的一个循环子群，称做由 a 生成的子群，记为 $\langle a\rangle$。如果 a 的阶为 t，则 $|\langle a\rangle|=t$。

关于群有下列重要的基本定理。

【定理 1-1】 在一个群 G 里存在一个并且只存在一个元 e，能使 $ea=ae=a$，对于 G 的任意元 a 都成立。

【定理 1-2】 对于群 G 的每一个元 a 来说，在 G 里存在一个而且只存在一个元 a^{-1}，能使 $aa^{-1}=a^{-1}a=e$。

关于有限群有下列重要的基本定理。

【定理 1-3】 (Lagrange 定理)设 G 是一个有限群，H 是 G 的一个子群，则 $|H|\,\big|\,|G|$（表示 $|H|$ 是 $|G|$ 的因子），因此，如果 $a\in G$，则 a 的阶整除 $|G|$。

关于循环群有以下基本性质：

(1) 循环群的子群也是循环群。如果 G 是一个阶为 n 的循环群，那么对 n 的每一个正因子 d，G 恰好包含一个阶为 d 的子群。

(2) 设 G 是一个群，如果 $a\in G$ 的阶为 t，则 a^k 的阶是 $t/\gcd(t,k)$。

2. 环

【定义 1-5】 一个环$(R,+,\times)$是由两个满足下列条件的 R 上的二元运算“+”(称为加法)和“×”(称为乘法)构成，并且满足以下条件：

(1) $(R,+)$是一个 Abel 群，单位元用 0 表示；

(2) 运算“×”是可结合的，即对所有的 $a,b,c\in R$，有 $a\times(b\times c)=(a\times b)\times c$；

(3) 乘法对加法的分配律，即对所有的 $a,b,c\in R$，有 $a\times(b+c)=(a\times b)+(a\times c)$和$(b+c)\times a=(b\times a)+(c\times a)$。

一般而言，对于乘法运算，一个环未必有单位元、逆元。

【例 1-4】 $R=\{$所有偶数$\}$，R 对于普通加法和乘法来说显然形成一个环。但对于乘法运算，R 没有单位元。

如果一个环$(R,+,\times)$还满足条件：对所有的 $a,b\in R$，有 $a\times b=b\times a$，则称环$(R,+,\times)$为交换环。

【例 1-5】 整数集 $\mathbf{Z}$ 关于通常的加法和乘法运算形成一个交换环。

【例 1-6】 剩余类集 $\mathbf{Z}_n$ 关于模 n 加法和乘法形成一个交换环。

【例 1-7】 设 $F[x]$表示数域 F 上的所有一元多项式组成的集合，则 $F[x]$关于多项式的加法与乘法构成一个环。

【定义 1-6】 设 R 是一个环，$a,b\in R$，且 $a\neq0,b\neq0$，但 $a\times b=0$，则称 a,b 为零因子，称含有零因子的环为有零因子环。

有零因子环中消去律不一定成立，如$(\mathbf{Z}_6,+,\times)$中运算$[2]\times[1]=[2]\times[4]$，但$[1]\neq[4]$。

关于环有以下重要的性质。

(1) 在一个交换环里，对于任何正整数 n 以及环的任意两个元 a,b 来说，都有 $a^nb^n=(ab)^n$。

(2) 在一个没有零因子的环里两个消去律成立：$a\neq0,ab=ac\Rightarrow b=c$；$a\neq0,ba=ca\Rightarrow b=c$。反过来，在一个环里如果有一个消去律成立，那么这个环没有零因子。

【定义 1-7】 一个环 R 叫做一个整环，假如：

(1) 乘法适合交换律：$ab=ba$；

(2) R 有单位元 1：$1a=a1=a$；

(3) R 没有零因子：$ab=0\Rightarrow a=0$ 或 $b=0$。

这里，a,b 可以是 R 的任意元。

3. 域

【定义 1-8】 F 是至少含有两个元素的集合，对 F 定义两种运算“+”和“×”，并且满足以下 3 个条件的代数系统称为域，记为$<F,+,\times>$，可简记为 F。

(1) F 的元素关于运算“+”构成 Abel 群，设其单位元为 0。

(2) $F\backslash\{0\}$关于运算“×”构成 Abel 群。

(3) 对于 $\forall a,b,c\in F$，分配律成立，即：

$$(a+b)\times c=a\times c+b\times c$$
$$c\times(a+b)=c\times a+c\times b$$

在域上不仅可以进行加、减、乘法运算，还可以实现除法运算(逆)，因此域是一个非常完备的代数系统，其应用比环的应用更为广泛。

【定义 1-9】 设 F 是一个域，如果对任何 $m\geqslant 1$，$1+1+\cdots+1\neq 0$(m 个 1 相加)，则称 F 的特征为 0，否则，F 的特征是使得 $\sum_{i=1}^{m}1=0$ 的最小正整数 m。

【例 1-8】 整数环 **Z** 不是一个域，因为只有 1 和 −1 有乘法逆。然而，有理数集 **Q**、实数集 **R** 和复数集 **C** 在通常的加法和乘法运算下形成特征为 0 的域。

【定理 1-4】 $\mathbf{Z}_n$ 是一个域，当且仅当 n 是素数。如果 n 是素数，则 $\mathbf{Z}_n$ 的特征是 n。

关于域的特征有以下重要事实：如果一个域的特征不是 0，则它的特征必是素数。

【定义 1-10】 设 E 是一个域，F 是 E 的一个子集，如果 F 关于 E 的运算本身形成一个域，则称 F 为 E 的子域，也称 E 为 F 的扩域。

根据域所包含的元素是否有限，将域分为无限域和有限域；包含有限个元素的域称为有限域，否则称为无限域。域 F 中的元素个数也称为有限域 F 的阶。

在大多数的计算机工程领域中(包括密码学)，有限域是一个重要的理论基础。有限域常以数学家 Galois 的名字命名，称做 Galois 域，并以 GF(q)表示，其中 q 表示有限域的阶。

关于有限域有以下的重要结果。

(1) (有限域的存在性和唯一性)如果 F 是一个有限域，那么 F 包含素数幂个元素，即存在素数 p 和整数 $m\geqslant 1$，使得 $|F|=p^m$；反之，对每一个素数幂 p^m，(在同构的意义下)存在唯一的一个阶为 p^m 的有限域，将这个域记为 F_{p^m} 或 GF(p^m)。

(2) (有限域的子域)设 F_q 是一个阶为 $q=p^m$ 的有限域，p 是素数，则 F_q 的每个子域有阶 p^n，且 $n|m$；反之，如果 $n|m$，则 F_q 恰有的一个阶为 p^n 的子域，而且 $a\in F_q$ 是 F_{p^n} 的一个元素，当且仅当 $a^{p^n}=a$。

(3) $F_q^*=F_q\backslash\{0\}$ 关于乘法形成一个阶为 $q-1$ 的循环群。因此，对所有的 $a\in F_q$，有 $a^q=a$。这个群称为 F_q 的乘法群，乘法群 F_q^* 的生成元称为 F_q 的本原元，共有 $\varphi(q-1)$ 个本原元〔函数 $\varphi(x)$ 成为欧拉函数，表示小于 x，并且与 x 互素的数的个数〕。

(4) 设 F_q(其中 $q=p^m$)是一个有限域，p 是一个素数，$m\geqslant 1$，则 F_q 的特征为 p，而且对所有的 $a,b\in F_q$ 和 $t\geqslant 0$，有 $(a+b)^{p^t}=a^{p^t}+b^{p^t}$。

当 p 为素数时，任何整数 $a\in\mathbf{Z}_p^*$，必存在一乘法逆元 $a^{-1}\in\mathbf{Z}_p^*$，使得 $aa^{-1}=1 \bmod p$。故在模 p 的同余运算中，$\mathbf{Z}_p$ 为一有限域，通常以 GF(p)表示。已经证明，一有限域 GF(q)，其 q 必为 p 或 p^m(p 为素数)，$m>1$。在此介绍 GF(p^m)的运算方式。

令 $a\in$GF(p^m)，则 a 可表示成下列阶数为 $m-1$ 或更小的多项式：

$$a=a_{m-1}x^{m-1}+a_{m-2}x^{m-2}+\cdots+a_1x+a_0$$

式中，系数 a_i 为模 p 的余数。每一元素 a 均为模 $f(x)$ 的余多项式，$f(x)$ 为一阶数为 m 系数为模 p 的整数的不可约多项式。

(1) GF(p^m)的加法

令 $a,b\in$GF(p^m)，且 $a=a_{m-1}x^{m-1}+a_{m-2}x^{m-2}+\cdots+a_1x+a_0$，$b=b_{m-1}x^{m-1}+b_{m-2}x^{m-2}+\cdots+b_1x+b_0$，则 $c=a+b=c_{m-1}x^{m-1}+c_{m-2}x^{m-2}+\cdots+c_1x+c_0$，其中 $c_i=a_i+b_i \bmod p$，$0\leqslant i\leqslant m-1$。

【例 1-9】 在 GF(3^3)中，若 $a=2x^2+x+2$，$b=2x^2+2x+2$，则 $c=a+b=x^2+1$。

(2) GF(p^m)的乘法

若 $a,b\in GF(p^m)$，a 与 b 的乘积与一般多项式的乘积相同。其差别为，若其积的阶数等于或比 m 大时，以不可约多项式 $f(x)$ 除之。故若 $d=ab$，则 d 可表示为 $d=\sum_{i=0}^{m-1}(a_ib_{m-1-i})x^i \bmod f(x)$。

【例 1-10】 如【例 1-9】中设 $f(x)=x^3+2x+1$，$d=ab=(2x^2+x+2)(2x^2+2x+2)$。

(1) 先求 $ab=x^4+x^2+1$。

(2) 再除以 $f(x)=x^3+2x+1$，得 $d=2x^2+2x+1$。

4. 多项式环

系数在整数环 **Z**、有理数域 **Q**、实数域 **R** 或复数域 **C** 上的一元多项式的全体形成一个环。类似可以定义系数属于一般域 F 上的多项式。

【定义 1-11】 多项式

$$f(x)=a_0+a_1x+\cdots+a_nx^n,a_i\in F,i=0,1,2,\cdots,n$$

如果 $a_n\neq 0$，就说 $f(x)$是域 F 上的 n 次多项式，记做 $\deg f=n$，并称 a_n 为 $f(x)$的首项系数。当 $f(x)$的所有系数都是 0 时，就说 $f(x)$是零多项式，仍用 0 表示，约定 $\deg(0)=-\infty$。

设 $f(x)=\sum_{i=0}^{n}a_ix^i$，$g(x)=\sum_{i=0}^{m}b_ix^i\in F[x]$，如果 $m=n$，且 $a_i=b_i$，$i=0,1,2,\cdots,n$，则称 $f(x)$与 $g(x)$相等，记做 $f(x)=g(x)$。

F 上全体多项式的集合记做 $F[x]$。下面定义 $F[x]$中的加法和乘法运算。

设 $f(x)=\sum_{i=0}^{n}a_ix^i$，$g(x)=\sum_{i=0}^{m}b_ix^i\in F[x]$，令 $M=\max(n,m)$。当 $n<m$ 时，约定 $a_{n+1}=a_{n+2}=\cdots=a_m=0$。当 $n>m$ 时，约定 $b_{m+1}=b_{m+2}=\cdots=b_n=0$。此时，$f(x)$和 $g(x)$可分别写成

$$f(x)=\sum_{i=0}^{M}a_ix^i,g(x)=\sum_{i=0}^{M}b_ix^i$$

定义加法运算：$f(x)+g(x)=\sum_{i=0}^{M}(a_i+b_i)x^i$，显然 $f(x)+g(x)\in F(x)$。再令

$$a_{n+1}=a_{n+2}=\cdots=a_{n+m}=0,b_{m+1}=b_{m+2}=\cdots=b_{n+m}=0$$

此时，$f(x)$和 $g(x)$可分别写成

$$f(x)=\sum_{i=0}^{m+n}a_ix^i,g(x)=\sum_{i=0}^{m+n}b_ix^i$$

定义乘法运算：$f(x)\cdot g(x)=\sum_{i=0}^{m+n}\left(\sum_{j=0}^{i}a_jb_{i-j}\right)x^i$，显然 $f(x)\cdot g(x)\in F(x)$。

容易验证($F[x]$，+，·)是一个交换环，通常称之为多项式环。

【例 1-11】 设二元域上多项式为 $f(x)=x^3+x+1$，$g(x)=x^2+x\in Z_2[x]$，则

$$f(x)+g(x)=x^3+x^2+1,f(x)\cdot g(x)=x^5+x^4+x^3+x$$

多项式环 $F[x]$与整数环 **Z** 非常类似，有许多共同的特性。

对应于整数环 **Z** 中的素数的概念，多项式环 $F[x]$中引入了不可约多项式的概念，它的作用类似于素数的作用。

【定义 1-12】 一个多项式 $p(x)\in F[x]$称为 F 上的不可约多项式，是指 $\deg p\geqslant 1$，而 $p(x)$在 F 上仅平凡分解，即如果有一个分解 $p(x)=f(x)g(x)$，其中 $f(x),g(x)\in F[x]$，则 $\deg f=0$ 或 $\deg g=0$。

因此，除了一个常数倍数外，$p(x)$的因式只有自身和 1。

【定理 1-5】 （带余除法）设 $f(x),g(x)\in F[x],g(x)\neq 0$，则 $F[x]$中存在唯一的一对多项式 $q(x)$和 $r(x)$，使得 $f(x)=q(x)g(x)+r(x),\deg[r(x)]<\deg[g(x)]$。多项式 $q(x)$称做商式，$r(x)$称做余式，通常记 $r(x)=f(x)\bmod g(x)$。当 $r(x)=0$ 时，就说 $g(x)$整除 $f(x)$，并称 $g(x)$是 $f(x)$的因式，或 $f(x)$是 $g(x)$的倍式，记为 $g(x)\mid f(x)$。当 $r(x)\neq 0$ 时，就说$g(x)$不整除 $f(x)$，记为 $g(x)\nmid f(x)$。

【例 1-12】 设 $f(x)=x^6+x^5+x^3+x^2+x+1,g(x)=x^4+x^3+1\in Z_2[x]$，则 $f(x)=x^2g(x)+x^3+x+1$，因此 $f(x)\bmod g(x)=x^3+x+1$。

类似于整数环的情形，可在 $F[x]$中定义最高公因式的概念。如果 $h(x)\in F[x]$是 $f(x)$的因式，又是 $g(x)$的因式，则称 $h(x)$是 $f(x)$和 $g(x)$的公因式。将 $f(x)$和 $g(x)$的公因式中次数最高的而且首项系数为 1 的公因式 $d(x)$叫做 $f(x)$和 $g(x)$的最高公因式，记为 $\gcd[f(x),g(x)]$。约定 $\gcd(0,0)=0$。

当 $\gcd[f(x),g(x)]=1$ 时，就说 $f(x)$和 $g(x)$互素。像整数环中一样，求两个不全为零的多项式的最高公因式也有相应的 Euclidean 算法。类型地，在 $F[x]$中也有相应的唯一因式分解定理。

【定理 1-6】 $F[x]$中任一正次数的多项式可分解为 $F[x]$中有限个首项系数为 1 的不可约多项式与 F 中常数之积；并且这些不可约多项式是唯一决定的（如果不计它们在乘积中的次序）。

【定义 1-13】 设 $f(x),g(x),m(x)\in F[x],m(x)\neq 0$，如果 $m(x)\mid[f(x)-g(x)]$，则称 $f(x)$和 $g(x)$模 $m(x)$同余，记做 $f(x)\equiv g(x)\bmod m(x)$。

多项式的同余式和整数中的同余式有着类似的性质。“模 $m(x)$同余”是 $F[x]$中的一个等价关系。按此关系将 $F[x]$分类，$f(x)$的同余类是 $F[x]$中所有与 $f(x)$模 $m(x)$同余的多项式所构成的集合。与整数中情形不同的是，模 $m(x)$同余类的类数不必是有限的。

用 $F[x]/m(x)$表示 $F[x]$中次数小于 $n=\deg m(x)$的全体多项式的集合，也就是模$m(x)$的等价类之集。$F[x]/m(x)$在模 $m(x)$的加法和乘法下形成一个交换环，称为多项式剩余类环。进一步，如果 $m(x)$是 F 上不可约多项式，则模 $m(x)$的同余类中还可以作除法，从而形成一个域。这是代数学中构作域的基本手法。

【定理 1-7】 如果 $m(x)\in F(x)$在 F 上不可约，则 $F[x]/m(x)$是一个域。

由【定理 1-7】可知，如果取 $F=\mathbf{Z}_p$（p 为素数），$m(x)$是一个 n 次不可约多项式，则$F[x]/m(x)$是一个阶为 p^n 的有限域。这表明，可用不可约多项式来构造密码学中常用的有限域。那么不可约多项式是否存在呢？人们已经证明，对任意的有限域 F 和任意的正整数 n，$F[x]$中一定存在 n 次不可约多项式，不仅如此，人们还给出了不可约多项式的精确计数公式。

1.1.2 数论基础

数论是研究整数性质的一个数学分支，它在密码学与网络安全领域中有着很多重要的应用。

1. 素数与互素数

整数集合中，除了加法和乘法之外还可以做减法运算，但是一般不能做除法，由此引出初等数论中第一个基本概念：数的整除性。

【定义 1-14】 设 a 和 b 是整数，$b\neq 0$，如果存在整数 c 使得 $a=bc$，则称 b 整除 a，表示成 $b|a$，并称 b 是 a 的因子，而 a 为 b 的倍数。如果不存在上述的整数 c，则称 b 不整除 a，表示成 $b\nmid a$。

由整除的定义，立即导出整除的如下基本性质：

(1) $b|b$；

(2) 如果 $b|a$，$a|c$，则 $b|c$；

(3) 如果 $b|a$，$b|c$，则对任意整数 x，y，有 $b|(ax+cy)$；

(4) 如果 $b|a$，$a|b$，则 $b=\pm a$。

【定理 1-8】 设 a 和 b 是整数，$b>0$，则存在整数 q，r，使得

$$a=bq+r,\text{其中 } 0\leqslant r<b$$

并且整数 q，r 由上述条件唯一决定。以上方法称为带余除法，或欧几里德除法。式中，整数 q 称为 a 被 b 除的商，数 r 称为 a 被 b 除得的余数。

【定义 1-15】 设 $a,b,\cdots,c$ 是有限个不全为零的整数，满足下面两个条件，整数 d 称为它们的最大公约数，记做 $(a,b,\cdots,c)$ 或 $\gcd(a,b,\cdots,c)$：

(1) d 是 $a,b,\cdots,c$ 的公共约数，即 $d|a,d|b,\cdots,d|c$；

(2) d 是 $a,b,\cdots,c$ 的所有公约数中最大的，即如果整数 d_1 也是 $a,b,\cdots,c$ 的公约数，则 $d_1\leqslant d$。

任意整数 $a,b,\cdots,c$ 必然有公约数(如 ± 1)。如果它们不全为零，则易知它们的公约数只有有限多个，所以它们的最大公约数必然存在并且是唯一的。此外，最大公约数一定是正整数。

如果 $(a,b,\cdots,c)=1$，则称 $a,b,\cdots,c$ 是互素的。如果 $a,b,\cdots,c$ 中任意两个是互素的，则称两两互素。

【定理 1-9】 设 a,b,c 为 3 个正整数，且 $a=bq+c$，其中 q 为整数，则 $(a,b)=(b,c)$。

对于正整数 a,b，利用【定理 1-9】及带余除法，可以求出 a,b 的最大公约数 (a,b)，该方法称为辗转相除法。具体方法如下：

令 $r_0=b,r_1=a,b\leqslant a$；

用 r_1 除 r_0：$r_0=r_1q_1+r_2,0\leqslant r_2<r_1$；

用 r_2 除 r_1：$r_1=r_2q_2+r_3,0\leqslant r_3<r_2$；

$\vdots$

用 r_{m-1} 除 r_{m-2}：$r_{m-2}=r_{m-1}q_{m-1}+r_m,0\leqslant r_m<r_{m-1}$；

用 r_m 除 r_{m-1}：$r_{m-1}=r_mq_m$。

注意到：$r_0>r_1>\cdots>r_{m-1}>\cdots\geqslant 0$。

从而上述的带余除法有限步后余数必为零。另外，

$$(a,b)=(r_0,r_1)=(r_1,r_2)=\cdots=(r_{m-1},r_m)=(r_m,0)=r_m$$

欧几里德辗转相除法不仅可以求出 (a,b)，还可以求出方程 $sa+tb=(a,b)$ 的一组整数解。具体做法如下：

由算法的倒数第 2 行，得到 $(a,b)=r_m=r_{m-2}-r_{m-1}q_{m-1}$，这就将 (a,b) 表示成 r_{m-2}，r_{m-1} 的整系数线性组合，再用算法的倒数第 3 行 $r_{m-1}=r_{m-3}-r_{m-2}q_{m-2}+r_m$ 代入上式，消去 r_{m-1}，得