高等学校教材

# 计算机密码学

## 通信中的保密与安全

卢开澄

清华大学出版社

# 计 算 机 密 码 学

——通信中的保密与安全——

卢开澄　编著

方世昌　审校



清华大学出版社

## 内 容 简 介

计算机密码学是计算机科学的新分支，也是一门边缘学科，它研究信息的保密与安全问题。本书前两章是数学准备。中心部分除了介绍传统密码系统，数据加密标准外，着重讨论了公钥密码系统，流码系统。最后一章介绍了计算机网络通信的保密、安全及软件保护等问题。本书除供计算机专业师生作教材外，还可供应用数学及计算机科学工作者参考。

# 计 算 机 密 码 学

——通信中的保密与安全——

卢开澄 编著

方世昌 审校

☆

清华大学出版社出版

北京 清华园

北京昌平环球科技印刷厂印刷

新华书店总店科技发行所发行

☆

开本：850×1168 1/32 印张：7.5 字数：192 千字

1990年3月第1版 1990年3月第1次印刷

印数：0001-8000

ISBN 7-302-00607-5/TP·213

定价：1.80 元

# 前　言

随着计算机科学的蓬勃发展，我们这个社会已进入信息时代。特别是数据库技术和计算机网络的广泛应用，使数据通信有了广阔的前景，也开辟了计算机应用新的疆域。

许多事实说明，信息本身就是时间，就是财富，就是生命。所以，保护信息的安全，更确切地说，计算机通信的保密与安全问题自然地提到日程上来，成为计算机科学的新课题。对信息加密是达到上述目的的有效措施。这便是密码学研究的重要内容。经过加密后的信息只有事先有通信协议的双方才有可能知晓，对于局外人却是一堆乱杂无章、莫名其妙的随机字符串。

密码学是一个新的领域，还非常年轻。密码的出现虽然可以追溯到远古时代，然而密码学成为一门学科，则是近几年的事。为了军事和外交的需要，为了国家的安全和现代化建设的需要，我们必须研究自己的密码系统。

密码学隶属计算机科学，也可算是应用数学，更确切地说，它是两者之间的边缘学科。数学无疑是其重要的工具，涉及到组合论、算法复杂性理论、概率统计等方面。数论和信息论更是近代密码学研究所必不可少的，故在第一、二两章介绍必要的概念。

# 目　录

# 第一章 数 论

数论是一个相当古老的数学分支，它和近代密码学的发展有着密切的联系，它在密码学中的应用是近若干年来的一大成就。下面介绍后面讨论时所必需的基础理论。

## §1 整数的表示法

可能是由于人的手有10个指头，所以十进制是最方便的一种整数表示法。例如1987实际上就是

$$1\cdot10^3+9\cdot10^2+8\cdot10+7$$

然而在电子计算机中，则常用以 2 为基，即所谓二进制数。严格地说，其它一些正整数也可以作为基。

**定理 1** 设 $m$ 是大于 1 的正整数，则每一个正整数 $n$ 可唯一地表示为

$$n=c_km^k+c_{k-1}m^{k-1}+\cdots+c_1m+c_0 \qquad (1)$$

其中 $c_j$ 是整数，满足 $0\leqslant c_j<m$，且 $c_k\neq0$，这里 $j=0,1,2,\cdots,k$。

**证明**：用 $\lfloor x\rfloor$ 表示不大于 $x$ 的最大整数。设 $n_0=n$，令 $n_1=\lfloor n_0/m\rfloor$，则

$$n_0=n_1m+c_0$$

其中 $c_0$ 是用 $m$ 除 $n_0$ 的余数。同样可得

$$n_1=n_2m+c_1$$

$c_1$ 为以 $m$ 除 $n_1$ 的余数。依次类推，可得

$$c_0,c_1,c_2,\cdots,c_k$$

一般地，令

$$\begin{cases} n_j = \left[\dfrac{n_{j-1}}{m}\right], & j = 1,2,\cdots,k \\ n_0 = n \end{cases}$$

则有

$$\begin{cases} n_{j-1} = n_j m + c_{j-1}, j = 1,2,\cdots,k+1 \\ n_0 = n \end{cases}$$

其中 $n_{k+1} = 0$。于是有

$$n = n_1 m + c_0$$

$$n_1 = n_2 m + c_1$$

……

$$n_{k-1} = n_k m + c_{k-1}$$

$$n_k = n_{k+1} m + c_k = c_k$$

由 $n = n_1 m + c_0$ 及 $n_1 = n_2 m + c_1$

可得 $n = (n_2 m + c_1)m + c_0 = n_2 m^2 + c_1 m + c_0$

同样，由于 $n_2 = n_3 m + c_2$

所以 $n = (n_3 m + c_2)m^2 + c_1 m + c_0$

$$= n_3 m^3 + c_2 m^2 + c_1 m + c_0$$

$$= \cdots\cdots$$

$$= c_k m^k + c_{k-1} m^{k-1} + \cdots + c_2 m^2 + c_1 m + c_0$$

其中 $0 \leqslant c_j < m, j = 0,1,2,\cdots,k$

下面证明表示法（1）是唯一的。

如若不然，设

$$n = c_k m^k + c_{k-1} m^{k-1} + \cdots + c_1 m + c_0$$

$$n = d_l m^l + d_{l-1} m^{l-1} + \cdots + d_1 m + d_0$$

由 $c_k m^k + \cdots + c_1 m + c_0 = d_l m^l + \cdots + d_1 m + d_0$

可得 $(c_k m^k + \cdots + c_1 m) - (d_l m^l + \cdots + d_1 m) = d_0 - c_0$

由于 $m$ 整除左边，所以也应有

$$m \mid (d_0 - c_0)$$

而$0 \leqslant d_0 < m$, $0 \leqslant c_0 < m$, 所以必定有 $d_0 = c_0$, 从而上式变为

$$(c_k m^{k-1} + \cdots + c_2 m) - (d_l m^{l-1} + \cdots + d_2 m) = d_1 - c_1$$

由此又可得 $m \mid (d_1 - c_1)$, 即 $d_1 = c_1$

依次类推, 可知

$$k = l, d_i = c_i, i = 0, 1, 2, \cdots, k$$

所以, $n$ 以 $m$ 为基的表示法是唯一的。 ■

表达式（1）可表示为 $(c_k c_{k-1} \cdots c_1 c_0)_m$

列如 $n = 389$, $m = 5$

$n_0 = n = 389$, $n_1 = \lfloor 389/5 \rfloor = 77$, 余数 $c_0 = 4$

$n_2 = \lfloor n_1/5 \rfloor = \lfloor 77/5 \rfloor = 15$, 余数 $c_1 = 2$

$n_3 = \lfloor n_2/5 \rfloor = \lfloor 15/5 \rfloor = 3$, 余数 $c_2 = 0$

$n_4 = \lfloor n_3/5 \rfloor = \lfloor 3/5 \rfloor = 0$, 余数 $c_3 = 3$

即 $389 = 3 \cdot 5^3 + 2 \cdot 5 + 4$, 或 $389 = (3\ 0\ 2\ 4)_5$

同样的方法可将 $n = 389$ 表示为 2 进制数如下;

$n_0 = 389$

$n_1 = \lfloor n_0/2 \rfloor = \lfloor 389/2 \rfloor = 194$, $c_0 = 1$

$n_2 = \lfloor n_1/2 \rfloor = \lfloor 194/2 \rfloor = 97$, $c_1 = 0$

$n_3 = \lfloor n_2/2 \rfloor = \lfloor 97/2 \rfloor = 48$, $c_2 = 1$

$n_4 = \lfloor n_3/2 \rfloor = \lfloor 48/2 \rfloor = 24$, $c_3 = 0$

$n_5 = \lfloor n_4/2 \rfloor = \lfloor 24/2 \rfloor = 12$, $c_4 = 0$

$n_6 = \lfloor n_5/2 \rfloor = \lfloor 12/2 \rfloor = 6$, $c_5 = 0$

$n_7 = \lfloor n_6/2 \rfloor = \lfloor 6/2 \rfloor = 3$, $c_6 = 0$

$n_8 = \lfloor n_7/2 \rfloor = \lfloor 3/2 \rfloor = 1$, $c_7 = 1$

$n_9 = \lfloor n_8/2 \rfloor = \lfloor 1/2 \rfloor = 0$, $c_8 = 0$

故 $389 = 2^8 + 2^7 + 2^2 + 1$

或 $389 = (1\ 1\ 0\ 0\ 0\ 0\ 1\ 0\ 1)_2$

## §2 因数分解

整数 1 只能被 1 除尽。其他整数至少可被两个整数除尽，一

个是1，另一个是这个数本身。只能被1和该数自身除尽的数称为素数。

不是1且非素数的正整数称为合数。$a$除尽$b$表示为$a|b$。以后不特别说明英文字母$a$、$b$、$c$等都是表示正整数。若$a|b$，且$a|c$，就说$a$是$b$和$c$的公因子。若$a$是$b$和$c$的公因子，且$b$和$c$的每一个公因子都除尽$a$，则称$a$是$b$和$c$的最大公因子，用$gcd\{b,c\}$或$(b,c)$表示它，即

$$a=gcd\{b,c\}，或 a=(b,c)$$

例如，$12=gcd\{12,60\}$。

若$a|c$，则称$c$是$a$的倍数；若$a|c$，$b|c$，则称$c$是$a$和$b$的公倍数；如果$a$和$b$的公倍数$c$除尽$a$和$b$的任一个公倍数，则称$c$是$a$和$b$的最小公倍数，表示为

$$c=lcm\{a,b\}，或 c=[a,b]$$

例如，$60=lcm\{15,20,30\}$。

**定理1** 若$a=bq+r$，则

$$gcd\{a,b\}=\pm gcd\{b,r\}$$

**证明：** 设$d=(a,b)$，$d'=(b,r)$，则

$$d|(a-bq)，即 d|r$$

所以$d$是$b$和$r$的公因数，即$d|d'$。类似地，由$d'|(bq+r)$可得$d'|a$，所以$d'|d$。

由$d|d'$，可令$d'=hd$；同理由$d'|d$，可令$d=kd'$。即$d'=hkd'$，因此有

$$hk=1$$

$$h=k=\pm 1，\quad d=\pm d'$$ ■

**定理2** 每一双不全为零的整数，必有一个正的最大公因数。

**证明：** 不失一般性，设$a$和$b$是正整数，且$a>b$。令$a=bq+r$，$0\leqslant r<b$。由定理1，可得

$$(a,b)=(b,r)$$

又令 $b = rq_1 + r_1, 0 \leqslant r_1 < r$。那么

$$(a,b) = (b,r) = (r,r_1)$$

依此类推，直到出现余数为零为止。这样，存在某一整数 $k$，使得

$$r_{k-2} = r_{k-1}q_k + r_k, r_k \neq 0$$

$$r_{k-1} = r_k q_{k+1}$$

对于这个序列有

$$r_1 > r_2 > \cdots > r_k > 0$$

且

$$(a,b) = (b,r) = (r,r_1) = \cdots$$

$$= (r_{k-1},r_k) = r_k$$

所以 $r_k$ 是 $gcd\{a,b\}$。 ■

定理的证明过程提供了一个求 $gcd\{a,b\}$ 的具体步骤。

例 1：求 $gcd\{726,393\}$。

$$726 = 1 \times 393 + 333$$

$$393 = 1 \times 333 + 60$$

$$333 = 5 \times 60 + 33$$

$$60 = 1 \times 33 + 27$$

$$33 = 1 \times 27 + 6$$

$$27 = 4 \times 6 + 3$$

$$6 = 2 \times 3 + 0$$

所以，$d = gcd\{726,393\} = 3$。

**定理 3** 若 $d = gcd\{a,b\}$，则存在整数 $p$ 和 $q$，使得 $d = pa + qb$。

**证明**：由定理 2 的证明可得

$$r_k = -q_k r_{k-1} + r_{k-2}$$

$$r_{k-1} = -q_{k-1} r_{k-2} + r_{k-3}$$

$$\cdots\cdots$$

$$r_1 = -q_1 r + b$$

$$r = -qb + a$$

依次消去 $r_{k-1}, r_{k-2}, \cdots, r_1$，可得

$$d = r_k = pa + qb$$ ■

由上例 1 可知

$$\begin{aligned} 3 &= 27 - 4 \times 6 \\ &= 27 - 4 \times (33 - 27) \\ &= -4 \times 33 + 5 \times 27 \\ &= -4 \times 33 + 5 \times (60 - 33) \\ &= 5 \times 60 - 9 \times 33 \\ &= 5 \times 60 - 9 \times (333 - 5 \times 60) \\ &= -9 \times 333 + 50 \times 60 \\ &= -9 \times 333 + 50 \times (393 - 333) \\ &= 50 \times 393 - 59 \times 333 \\ &= 50 \times 393 - 59 \times (726 - 393) \\ &= -59 \times 726 + 109 \times 393 \end{aligned}$$

若 $gcd\{a,b\} = \pm 1$，则称 $a$ 和 $b$ 互素。1 和任意整数互素。

若 $a$ 和 $b$ 互素，则根据定理 3，存在整数 $p$ 和 $q$，便得

$$pa + qb = 1。$$

**定理 4** 若 $a|bc$，$gcd\{a,b\} = 1$，那么 $a|c$。

**证明**：若 $a$ 和 $b$ 互素，则将 $pa + qb = 1$ 的两端同乘以 $c$，得

$$pac + qbc = c$$

由假定，$a|bc$，所以 $a$ 除尽等式的左端，因此 $a|c$。

**推论** 若素数 $p$ 除尽 $a_1 a_2 \cdots a_n$，则必存在 $k$：$1 \leqslant k \leqslant n$，使得 $p|a_k$。

**证明**：若 $p$ 与 $a_1$ 互素，则 $p|a_2 \cdots a_n$；若 $p$ 也和 $a_2$ 互素，则 $p|a_3 \cdots a_n$；……。

若 $p$ 和 $a_1, a_2, \cdots, a_{n-1}$ 的每一个互素，则最后有 $p|a_n$。 ■

**定理 5** 每一个正合数，可表示为正素数的乘积，并且不考虑乘积的顺序时，表示法是唯一的。

**证明**：若 $c$ 是合数，则存在 $a$ 和 $b$，使得 $c = ab$；若 $a$ 和 $b$ 是合

数，可设$a=a_1a_2$，$b=b_1b_2$，从而$c=a_1a_2b_1b_2$；继续以上的步骤，直到不能再分解因子为止。这个过程可在有限步内完成，故有

$$c=p_1p_2\cdots p_n$$

若这个分解不是唯一的，设

$$c=q_1q_2\cdots q_m$$

那么 $p_1p_2\cdots p_n=q_1q_2\cdots q_m$。

素数 $p_1|q_1q_2\cdots q_m$，故存在 $q_i$，$p_1|q_i$，由于 $q_i$ 也是素数，因此 $p_1=q_i$。不妨设 $p_1=q_1$，由 $p_1\neq 0$可知

$$p_2p_3\cdots p_n=q_2q_3\cdots q_m$$

继续这个步骤，直到取尽所有的$p_i$为止。所以

$$n=m$$

由这个定理，若 $c$ 有素数因子 $p_1,p_2,\cdots,p_n$，那么

$$c=p_1^{a_1}p_2^{a_2}\cdots p_n^{a_n}$$

## §3 同余类

若 $m|a-b$，即 $a-b=km$，我们就说 $a$ 和 $b$ 模 $m$ 同余，记以

$$a\equiv b \mod m$$

$m$ 称为是这个同余式的模。

同余关系和通常意义的相等关系极为相似。

**定理 1** 模 $m$ 的同余关系满足

（1）自反的，即 $a\equiv a \mod m$；

（2）对称的，即若 $a\equiv b \mod m$，则

$$b\equiv a \mod m;$$

（3）传递的，即若 $a\equiv b \mod m$，$b\equiv c \mod m$，则

$$a\equiv c \mod m$$

证明从略。

**定理 2** 若 $a\equiv b \mod m$，$c\equiv d \mod m$，则

（1）$a\pm c\equiv b\pm d \mod m$

（2）$ac\equiv bd \mod m$。

**证明**：因 $a\equiv b \mod m$，$c\equiv d \mod m$，所以

$$a=km+b,\quad c=hm+d$$

$$a\pm c=(k\pm h)m+(b\pm d)$$

从而

$$a\pm c\equiv b\pm d \mod m$$

同理可证：$ac\equiv bd \mod m$。 ■

**定理 3** 若 $ac\equiv bc \mod m$，且 $c$ 和 $m$ 互素，则

$$a\equiv b \mod m。$$

**证明**：由 $ac\equiv bc \mod m$，可知

$$ac=km+bc$$

即

$$c(a-b)=km$$

由于 $c$ 和 $m$ 互素，因此 $c|k$。设 $k=hc$，则

$$c(a-b)=hcm$$

$$a-b=hm \text{ 或 } a\equiv b \mod m$$ ■

**定理 4** 若 $ac\equiv bc(\mod m)$，$d=(c,m)$，则

$$a\equiv b \mod m/d。$$

证明留作习题。

例：因 $42\equiv 7 \mod 5$，$(7,5)=1$，所以

$$6\equiv 1 \mod 5$$

## §4 线性同余式

若整数 $x_1$ 满足线性同余式

$$ax\equiv b \mod m$$

即

$$ax_1\equiv b \mod m$$

可证明模 $m$ 与 $x_1$ 同余的所有整数都满足这个线性同余式，即若 $x_2\equiv x_1 \mod m$，则

$$ax_2\equiv b \mod m$$

模 $m$ 和 $x_1$ 同余的整数构成同余式

$$ax\equiv b \mod m$$

的同余解。

例如：$2x \equiv 3 \mod 5$

$x \equiv 4 \mod 5$是这个线性同余式的解。

**定理 1** 同余式

$$ax \equiv b \mod m \qquad (1)$$

有解的充要条件是 $d|b$，其中 $d=(a,m)$。

令 $m'=m/d$。若 $x_0$ 是(1)的一个解，则(1)的所有解 $x$ 均满足

$$x \equiv x_0 \mod m'$$

**证明**：若 $x_0$是（1）的一个解，则

$$ax_0 - km = b$$

所以，$d=(a,m)$除尽 $b$，即 $d|b$。

反之，若 $d|b$，令 $b=b'd$，

$$a=a'd,\ m=m'd$$

则 $a'$ 和 $m'$ 互素，即存在整数 $p$ 和 $q$，使得

$$pa' + qm' = 1$$

从而

$$\begin{aligned} b &= bpa' + bqm' \\ &= b'dpa' + b'dqm' \\ &= pb'a + qb'm \end{aligned}$$

即$pb'$ 满足同余式（1）。

不难验证，若 $x_0$ 是（1）的解，则 $x_0+km'$ 也是（1）的解，其中 $k$ 是任一整数。因

$$\begin{aligned} a(x_0+km') &= ax_0 + akm' = ax_0 + a'dkm' \\ &= ax_0 + a'km \equiv ax_0 \equiv b \mod m \end{aligned}$$

同时，若 $x_0'$ 是（1）的任意一个解，可以证明

$$x_0' \equiv x_0 \mod m'$$

若 $ax_0 \equiv b \mod m$，$ax_0' \equiv b \mod m$，则

$$a(x_0 - x_0') \equiv 0 \mod m$$

根据定理 4，可知

$$x_0 \equiv x_0' \mod m/d$$

即

$$x_0 \equiv x_0' \mod m'$$

■

## §5 联立的同余式和中国剩余定理

**定理1** 下列两个同余式

$$x\equiv b_1 \bmod m_1, x\equiv b_2 \bmod m_2 \tag{1}$$

有一个共同解的充要条件是

$$b_1\equiv b_2 \bmod d, d=(m_1,m_2)$$

**证明**：设 $x_1$ 满足（1）的两个同余式，则

$$x_1=b_1+k_1m_1=b_2+k_2m_2$$

从而

$$k_2m_2\equiv b_1-b_2 \bmod m_1 \tag{2}$$

从§4定理1可知，（2）式中 $k_2$ 存在的充要条件是

$$(m_1,m_2)\mid(b_1-b_2)$$

对于 $n$ 个联立同余式同样有类似结果

**定理2** 对于联立同余式

$$x\equiv b_i \bmod m_i \quad i=1,2,\cdots,n$$

有一共同的解的充要条件是

$$(m_i,m_j)\mid(b_i-b_j), i\neq j, i,j=1,2,\cdots,n$$

证明从略。

**定理3** 若 $a\equiv b \bmod m_1$，$a\equiv b \bmod m_2,\cdots,a\equiv b \bmod m_k$ 则

$$a\equiv b \bmod [m_1,m_2,\cdots,m_k]$$

**证明**：因 $a\equiv b \bmod m_i, i=1,2,\cdots,k$，所以

$$m_i\mid(a-b),\ i=1,2,\cdots,k$$

$$[m_1,\ m_2,\cdots,m_k]\mid(a-b)$$

从而

$$a\equiv b \bmod [m_1,m_2,\cdots,m_k]$$ ■

**中国剩余定理** 设 $m_1,m_2,\cdots,m_k$ 是两两互素的正整数，则

$$x\equiv b_i \bmod m_i,\ i=1,2,\cdots,k \tag{3}$$

模 $[m_1,m_2,\cdots,m_k]$ 有唯一解。

**证明**：令 $M=m_1m_2\cdots m_k$

$$M_j=M/m_j=m_1m_2\cdots m_{j-1}m_{j+1}\cdots m_k$$