PT SPT 高等院校选用教材 理工类

计算机密码应用基础

四川大学数学学院 组编
朱文余 孙琦 编著

科学出版社

计算机密码应用基础

高等院校选用教材

计算机密码应用基础

四川大学数学学院 组编

朱文余　孙　琦 编著

科学出版社

2000

内 容 简 介

本书是在四川大学密码学公共选修课所用的讲义基础上编写而形成的. 内容涉及密码学中几大“核心”领域，包括分组密码、香农理论、序列密码、公钥密码以及他们的应用，其中还涉及必要的数学知识.

本书可供高等院校计算机系、无线电系、数学系等专业用作密码学教材或参考书，也可供从事计算机科学、通信理论、密码学等工作的科技人员参考.

图书在版编目（CIP）数据

计算机密码应用基础/朱文余，孙琦编著. -北京：科学出版社，2000.8

（高等院校选用教材）

ISBN 7-03-008436-5

Ⅰ.计… Ⅱ.①朱… ②孙… Ⅲ.电子计算机-密码-高等学校-教材 Ⅳ.TP309.7

中国版本图书馆 CIP 数据核字（2000）第 06013 号

JS426/01

科学出版社 出版

北京东黄城根北街 16 号

邮政编码：100717

新蕾印刷厂印刷

科学出版社发行 各地新华书店经销

*

2000 年 8 月第 一 版 开本：787×960 1/16

2000 年 8 月第一次印刷 印张：13

印数：1—3 500 字数：231 000

定价：16.00 元

（如有印装质量问题，我社负责调换〈新欣〉）

前　言

密码学是一门古老的科学，大概自人类社会出现战争时便产生了密码，以后逐渐形成一门独立的学科．在密码学形成和发展的历程中，科学技术的发展和战争的刺激起了积极的推动作用．电子计算机一出现便被用于密码破译．电子计算机对密码学的发展产生了巨大的影响和推动．除了计算机通信的数据传输需要保密之外，计算机的操作系统和数据库的安全保密也很重要，由此产生了计算机密码学．

密码学的研究方式由过去的单纯秘密进行转向公开和秘密两条战线同时进行．自古以来，密码主要用于军事、政治、外交等要害部门，因而密码学的研究本身也是秘密地进行的．密码学的知识和经验主要由军事、政治、外交等保密机关掌握，不便公开发表，这是过去密码学的书籍一向很少的原因．然而由于微电子学、计算机科学的发展，使得计算机和通信网络的应用进入了人们的日常生活和工作领域；出现了电子转账、电子邮政、办公室自动化等必须确保数据安全的系统，使得民间和商业界对数据安全保密的需要大大增加，于是在民间产生了一批不从属于保密机关的密码学者，他们可以毫无顾忌地发表文章，互相竞争，公开地进行密码学研究．事实证明，正是这种公开地研究和秘密地研究相结合的局面促成了今天密码学的空前繁荣．

当前，信息安全已成为国家和民族的头等大事．因为，没有信息安全，就没有完全意义上的国家安全．90 年代进入了互联网时代，每个用户都可以连接遍布世界每个角落的上网计算机，满足人们交往、学习、消费、娱乐等各种社会需要．因此，现代的信息安全除了涉及到国家安全外，也涉及个人权益、企业生存和金融风险防范等．可以说，信息安全与国家、与单位、与个人都息息相关．信息安全的核心是密码技术和管理．因此，当前在大学开设密码学的基础课程是非常必要的．四川大学从 1997 年秋季开始，每学期开设密码基础课（每周 3 学时），作为一门公共选修课，本书是在为开设这门课所编写的讲义基础上形成的．全书共七章，现将各章主要内容，扼要介绍如下：

第一章介绍密码学的基本概念以及一些简单密码体制与它的破译．

第二章介绍了分组密码及其应用．

第三章包含密码学的香农方法以及完全保密体制的概念及论证．

第四章涉及近代密码体制中序列密码和移位寄存器，以及简单的非线性

序列.

第五章讲述了 RSA 公钥密码体制、素性测试和因子分解的数论背景以及有关 RSA 的一些安全性讨论，最后讨论了 RSA 在有限域 F_p 上多项式上的推广.

第六章讨论了其它一些公钥密码体制，包括离散对数公钥密码体制、概率公钥体制、椭圆曲线公钥体制、圆锥曲线公钥体制以及双密钥公钥密码体制.

第七章介绍了数字签名，包括利用公钥体制和私钥体制获得数字签名，还介绍了数字签名标准 DSS.

本书较难的内容用“*”号标志，在教学时可以删去. 书后所列参考文献，是我们在编写本书时参考较多的书和文章. 限于编者水平，不当之处，望读者批评指正. 最后，感谢龚奇敏研究员和我校数学学院张明志教授对本书提出了许多宝贵意见；98 级数论博士生罗家贵、任德斌参加了本书的校对工作，在此一并致谢.

目　录

第一章　简单密码体制及分析

§1.1　密码学的基本概念

密码学以研究秘密通信为目的，研究对传输信息采取何种秘密的变换，以防止第三者对信息的截取．密码学包含两个相互对立的分支，密码编制学和密码分析学．前者是研究把信息(明文)变换成为没有密钥不能解密或很难解密的密文的方法；后者是研究分析破译密码的方法．它们彼此目的相反，相互对立，但在发展中又相互促进．

在密码学中，需要变换的原消息称为明文消息．明文经过变换成为另一种隐蔽的形式，称为密文消息．完成变换的过程称作加密，其逆过程(即由密文恢复出明文的过程)称作解密．对明文进行加密时所采用的一组规则称作加密算法．对密文进行解密时所采用的一组规则称作解密算法．加密和解密操作通常在密钥的控制下进行，并有加密密钥和解密密钥之分．因为数据以密文的形式存储在计算机文件中，或在数据通信网络中传输，因此即使数据被未授权者非法窃取，或因系统故障和操作人员误操作而造成数据泄露，未授权者也不能理解它的真正含义，从而达到数据保密的目的．同样，未授权者也不能伪造合理的密文，因而不能篡改数据，从而达到确保数据真实性的目的．

一个密码系统，通常简称为密码体制，由五个部分组成：

(1)明文空间 M，它是全体明文的集合．

(2)密文空间 C，它是全体密文的集合．

(3)密钥空间 K，它是全体密钥的集合．其中每一个密钥 K 均由加密密钥 K_e 和解密密钥 K_d 组成，即 $K=(K_e,K_d)$．

(4)加密算法 E，它是一族由 M 到 C 的加密变换，对于每一个具体的 K_e，则 E 便确定出一个具体的加密函数 f，f 把 M 加密成密文 C，$C=f(M,K_e)$．

(5)解密算法 D，它是一族由 C 到 M 的解密变换，对于每一个确定的 K_d，则 D 便确定出一个具体的解密函数 f^{-1}，使得 $M=f^{-1}(C,K_d)$．

对于每一确定的密钥 $K=(K_e,K_d)$，$C=E(M,K_e)$，$M=D(C,K_d)=D(E(M,K_e),K_d)$．或记为 $C=e_{K_e}(M)$，$M=d_{K_d}(C)$．

如果一个密码体制的 $K_e=K_d$，或由其中一个很容易推出另一个，则称为单钥密码体制或对称密码体制或传统密码体制．否则，称为双密钥密码体制或非对称密码体制．进而，如果在计算上 K_d 不能由 K_e 推出，这样将 K_e 公开也不

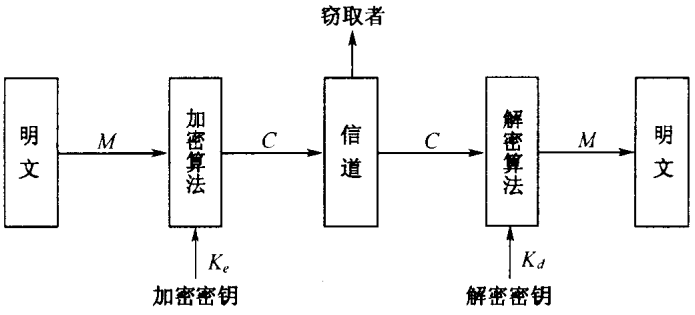

图 1-1

会损害K_d的安全,于是便可以将 K_e公开.这种密码体制称为公钥密码体制.

根据对明文的划分与密钥的使用方法不同可将密码体制分为分组密码和序列密码体制.

设 M 为明文,分组密码将 M 划分为一系列明文块$M_1, M_2, \cdots, M_n$,通常每块包含若干字符,并且对每一块 M_i 都用同一个密钥K_e 进行加密,即 $C=(C_1, C_2, \cdots, C_n)$.其中

$$C_i = E(M_i, K_e), \quad i = 1,2,\cdots,n.$$

而序列密码将 M 划分为一系列的字符或位 $m_1, m_2, \cdots, m_n$,并且对于这每一个 m_i 用密钥序列$K_e=(K_{e_1}, K_{e_2}, \cdots, K_{e_n})$的第 i 个分量K_{e_i}来加密,即 $C=(C_1, C_2, \cdots, C_n)$,其中

$$C_i = E(m_i, K_{e_i}), \quad i = 1,2,\cdots,n.$$

分组密码一次加密一个明文块,而序列密码一次加密一个字符或一个位.两种密码在计算机系统中都有广泛应用.

如果能够根据密文确定出明文或密钥,或者能够根据明文-密文对确定出密钥,则我们说这个密码是可破译的.否则,我们说这个密码是不可破译的.

密码分析者攻击密码的方法主要有以下三种.

(1)穷举攻击.所谓穷举攻击就是指密码分析者用试遍所有密钥的方法来破译密码.穷举攻击所花费的时间等于尝试次数乘以一次解密(加密)所需的时间.显然可以通过增大密钥量或加大解密(加密)算法的复杂性来对抗穷举攻击.当密钥量增大时,尝试的次数必然增大.当解密(加密)算法的复杂性增大时,完成一次解密(加密)所需的时间增大.从而使穷举攻击在实际上不能实现.

(2)统计分析攻击.所谓统计分析攻击是指密码分析者通过分析密文和明文的统计规律来破译密码.统计分析攻击在历史上为破译密码作出过极大的贡献.许多古典密码都可以通过分析密文字母和字母组的频率而破译.对抗统

计分析攻击的方法是设法使明文的统计特性不带入密文.这样,密文不带有明文的痕迹,从而使统计分析攻击成为不可能.

(3)数学分析攻击.所谓数学分析攻击是指密码分析者针对加密算法的数学依据通过数学求解的方法来破译密码.为了对抗这种数学分析攻击,应选用具有坚实数学基础和足够复杂的加密算法.

此外,根据密码分析者可利用的数据来分类,可将破译密码的类型分为以下三种:

(1)仅知密文攻击.所谓仅知密文攻击是指密码分析者仅根据截获的密文来破译密码.

(2)已知明文攻击.所谓已知明文攻击是指密码分析者根据已经知道的某些明文-密文对来破译密码.例如,密码分析者可能知道从用户终端送到计算机的密文数据以一个标准词"Login"开头.又例如,加密成密文的计算机程序特别容易受到这种攻击.这是因为诸如"begin"、"end"、"if"、"then"、"else"等词有规律地在密文中出现,密码分析者可以合理地猜测它们.近代密码学认为,一个密码仅当它能够经得起已知明文攻击时才是可取的.

(3)选择明文攻击.所谓选择明文攻击是指密码分析者能够选择明文并获得相应的密文.这是对密码分析者最有利的情况.计算机文件系统和数据库特别容易受到这种攻击,因为用户可随意选择明文,并得到相应的密文文件和密文数据库.

密码编制学的任务是寻求生成高强度密码的有效算法,满足对消息进行加密或认证的要求.密码分析学的任务是破译密码或伪造认证密码,窃取机密信息或进行诈骗破坏活动.对一个保密系统采取截获密文进行分析的方法进行进攻,称为被动进攻;非法入侵者采用删除、更改、添加、重放、伪造等手段向系统注入假消息的进攻是主动进攻.进攻与反进攻、破译与反破译是密码学中永无止境的矛与盾的竞技.

一个密码,如果无论密码分析者截获了多少密文和用什么方法进行攻击都不能被攻破,则称为是绝对不可破译的.绝对不可破译的密码在理论上是存在的.但是,如果能够利用足够的资源,那么任何实际的密码都是可破译的.因此,对我们更有实际意义的是在计算上不可破译的密码.如果一个密码不能被密码分析者根据可利用的资源所破译,则称为在计算上是不可破译的.

§1.2 一些简单密码体制与它的破译

先通过一些实例介绍加密和脱密是如何进行的,以增加感性认识.

密码学的基本任务是,使通常称为 A 和 B 的两个人在不安全的信道上进

行通信，而他们的敌人不能理解他们正在通信的内容. 比如，这个信道可能是电话线或计算机网. A 打算发送给 B 的消息，我们称为“明文”，它能够是英文文本，数字数据或任何其它东西——它的构造是完全任意的. A 用预先确定的密钥加密明文，同时在信道上发送产生的密文，在信道上通过截听而能看到密文的敌人不能确定明文是什么，但知道加密密钥的 B 能解密密文从而重构明文.

A 和 B 利用一个特定的密码体制将使用下列协议，首先他们选择一个随机密钥 $k \in K$，当他们在同一个地方能够完成这件事的同时，不能让他们的敌人观测到，或另一种方法，当他们在不同的地方而能进入一个安全信道来完成. 然后假设 A 在不安全信道上打算发送给 B 报文，我们假设这个报文是下列串 $M = m_1\ m_2 \cdots\ m_n$，对每一个 m_i 通过预先确定的密钥 k 和加密规则 e_k 来加密，这里 A 计算 $c_i = e_k(m_i)$，$1 \leqslant i \leqslant n$，同时结果的密文串为 $C = c_1\ c_2 \cdots\ c_n$. C 在信道上发送，当 B 接收到 C 后，他使用解密规则 d_k 来解密，获得原来的明文 M.

很明显，每一个加密规则 e_k 必定是一个单射函数(一对一)，否则无法完成解密.

例如：如果 $c = e_k(x_1) = e_k(x_2)$. 这里 $x_1 \neq x_2$，B 无法知道 C 将解密成 x_1 还是 x_2，注意，如果 $M = C$，它要求每一个加密函数是一个置换，即如果明文和密文集是相同的，那么每一个加密函数刚好重排(置换)明文集的元素.

1.2.1 置换密码

把明文中的字母重新排列，字母本身不变，但其位置改变了，这样编成的密码称为置换密码.

最简单的置换密码是把明文顺序倒过来，然后截成固定长度的字母组作密文.

例 1.1 明文为 this cryptosystem is not secure. 密文为 e r u c、e s t o、n s i m、e t s y、s o t p、y r c s、i h t.

另一种置换密码是把明文按某一顺序排成一个矩阵，然后按某一顺序选出矩阵中的字母以形成密文，最后截成固定长度的字母组.

例 1.2 明文为 this cryptosystem is not secure.

排成矩阵：

t h i s c r
y p t o s y
s t e m i s
n o t s e c

ure

选出顺序:按列

密文:tysnu hptor itete soms csie rysc.

由此可以看出,改变矩阵的大小和选出顺序可以得到不同形式的密码.

置换密码比较简单,它经不起已知明文攻击,但是,把它与其它密码相结合,可以得到十分有效的密码.

1.2.2 单表代替密码

在介绍单表代替密码体制之前,介绍一点必备的数论知识是必要的.

在正整数里,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且非素数的整数称为合数.

定义 1.1 任给两个整数 a、b,其中 $b\neq 0$,如果存在一个整数 q 使得等式 $a=bq$ 成立,我们就说 b 整除 a,记作 $b\mid a$,此时我们把 b 叫做 a 的因数,把 a 叫做 b 的倍数.如果不存在整数 q 使 $a=bq$ 成立,我们就说 b 不整除 a,记作 $b\nmid a$.

定理 1.1 设 a,b 是两个整数,其中 $b>0$,则存在两个唯一的整数 q 及 r,使得

$$a = bq + r, \quad 0 \leqslant r < b \tag{1}$$

成立.

证明 作整数羊列

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

则 a 必在上述序列的某两项之间,即存在一个整数 q 使得

$$qb \leqslant a < (q+1)b$$

成立.令 $a-qb=r$,则(1)成立.

设 q_1, r_1 是满足(1)的另一对整数,因为

$$bq_1 + r_1 = bq + r,$$

于是

$$b(q - q_1) = r_1 - r,$$

故

$$b \mid q - q_1 \mid = \mid r_1 - r \mid. \qquad \square$$

由于 r 及 r_1 都是小于 b 的非负整数,所以上式右边是小于 b 的.如果 $q\neq q_1$,则上式左边大于或等于 b,这是不可能的.因此

$$q = q_1, r = r_1.$$

定义 1.2 设 $a_1,a_2,\cdots,a_n$ 是 n 个不全为零的整数. 若整数 d 是它们之中每一个的因数,那么 d 就叫做 $a_1,a_2,\cdots,a_n$ 的一个公因数. 这时,它们的公因数只有有限个. 整数 $a_1,a_2,\cdots,a_n$ 的公因数中最大的一个叫最大公因数,记作 $(a_1,a_2,\cdots,a_n)$ 或 $\gcd\{a_1,a_2,\cdots,a_n\}$. 若 $(a_1,a_2,\cdots,a_n)=1$,我们称 $a_1,a_2,\cdots,a_n$ 互素. 我们有下面的定理.

定理 1.2 设 a,b,c 是任意三个不全为零的整数,且 $a=bq+c$,其中 q 是整数,则

$$(a,b)=(b,c).$$

证明 因为 $(a,b)\mid a$, $(a,b)\mid b$,所以 $(a,b)\mid c$. 因而 $(a,b)\leqslant(b,c)$. 同理可得 $(b,c)\leqslant(a,b)$,于是得到

$$(a,b)=(b,c).$$ □

我们先讨论两个正整数的最大公因数的求法,即辗转相除法,并借此推出最大公因数的若干性质.

任给整数 $a>0,b>0$,由带余数的除法,有下列等式:

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

因为 $b>r_1>r_2>r_3>\cdots$,故经有限次带余除法后,总可以得到一个余数是零,即(2)中 $r_{n+1}=0$.

现在我们证明

定理 1.3 若任给整数 $a>0,b>0$,则 (a,b) 就是(2)式中最后一个不等于零的余数,即 $(a,b)=r_n$.

证明 由定理 2 即得

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

从(2)式中 $r_n=r_{n-2}-r_{n-1}q_n$, $r_{n-1}=r_{n-3}-r_{n-2}q_{n-1}$,得

$$\begin{aligned}
r_n&=r_{n-2}-(r_{n-3}-r_{n-2}q_{n-1})q_n\\
&=r_{n-2}(1+q_nq_{n-1})-r_{n-3}q_n.
\end{aligned}$$

再将 $r_{n-2}=r_{n-4}-r_{n-3}q_{n-2}$ 代入上式,如此继续下去,最后可得 $r_n=sa+tb$,其中 s,t 是两个整数. 于是有

定理 1.4 若任给整数 $a>0,b>0$,则存在两个整数 s,t 使得

$$(a,b)=sa+tb.$$

推论 a 和 b 的公因数是 (a,b) 的因数.

另外，显然有$(a_1,a_2,\cdots,a_n)=(|a_1|,|a_2|,\cdots,|a_n|)$.所以只需对正整数讨论它们的最大公因数.

定理 1.5 若 $a|bc,(a,b)=1$,则 $a|c$.

证明 若 $c\neq0$,由$(a,b)=1$知存在两个整数 s,t 使

$$sa+tb=1,$$

故

$$sac+tbc=c.$$

由 $a|bc$,知 $a|c$;若 $c=0$,结论显然成立. □

定理 1.6 若 p 是素数,a 是任一整数,则有 $p|a$ 或$(p,a)=1$.

证明 因为$(p,a)|p$,所以$(p,a)=1$或$(p,a)=p$,后者即 $p|a$. □

定理 1.7 若 p 是素数,$p|ab$,则 $p|a$ 或$p|b$.

证明略.

定理 1.8(整数的唯一分解定理) 任一大于 1 的整数能表成素数的乘积,即对于任一整数 $a>1$,有

$$a=p_1p_2\cdots p_n,p_1\leqslant p_2\leqslant\cdots\leqslant p_n,\tag{3}$$

其中 $p_1,p_2,\cdots,p_n$ 是素数.并且若

$$a=q_1q_2\cdots q_m,q_1\leqslant q_2\leqslant\cdots\leqslant q_m,\tag{4}$$

其中 $q_1,q_2,\cdots,q_m$ 是素数,则 $m=n,p_i=q_i\ (i=1,2,\cdots,n)$.

证明 首先我们用数学归纳法证明(3)式成立.当 $a=2$ 时,(3)式显然成立.假定对于一切小于 a 的正整数(3)式都成立.此时,若 a 是素数,则(3)式对 a 成立;若 a 是合数,则有两个正整数 b,c 满足条件

$$a=bc,1<b\leqslant c<a,$$

由归纳法假设,b 和c 分别能表成素数的乘积,故 a 能表成素数的乘积,即(3)式成立.

下面证明唯一性.若对于 a 同时有(3),(4)两式成立,则

$$p_1p_2\cdots p_n=q_1q_2\cdots q_m,\tag{5}$$

由定理 1.7 知有 p_k,q_j 使得 $p_1|q_j,q_1|p_k$,但 q_j,p_k 都是素数,所以

$$p_1=q_j,q_1=p_k.$$

又 $p_k\geqslant p_1,q_j\geqslant q_1$,故同时有 $q_1\geqslant p_1$ 和 $p_1\geqslant q_1$,因而 $p_1=q_1$,由(5)式得

$$p_2\cdots p_n=q_2\cdots q_m,$$

同理可得 $p_2=q_2,p_3=q_3$,依次类推,最后得

$$m=n,p_n=q_n.$$ □

唯一分解定理告诉我们,任一大于 1 的整数能够唯一地写成

$$a=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k},\alpha_i>0\quad(i=1,\cdots,k),\tag{6}$$

其中 $p_i<p_j$ $(i<j)$是素数.

(6)式叫做 a 的标准分解式.

定义 1.3 设 $a_1,a_2,\cdots,a_n$ 是 n 个整数,n 大于等于 2,若 m 是这 n 个数中每一个数的倍数,则 m 就叫做这 n 个数的一个公倍数.在 $a_1,a_2,\cdots,a_n$ 的一切公倍数中最小的正数叫做最小公倍数.记作$[a_1,a_2,\cdots,a_n]$或 $\operatorname{lcm}\{a_1,a_2,\cdots,a_n\}$.

因为乘积$|a_1|\cdot|a_2|\cdots|a_n|$就是 $a_1,a_2,\cdots,a_n$ 的一个公倍数,故最小公倍数是存在的.

由于任何正整数都不是零的倍数,故讨论整数的最小公倍数时,总假定这些整数都不是零.

和最大公因数一样,显然有$[a_1,a_2,\cdots,a_n]=[|a_1|,|a_2|,\cdots,|a_n|]$,所以只需对正整数讨论它们的最小公倍数.

定义 1.4 给定一个正整数 m,如果用 m 去除两个整数a 和b 所得的余数相同或$m|(a-b)$,即 $a-b=km$,其中 k 为整数,我们就称 a,b 对模m 同余,记作 $a\equiv b\pmod m$.如果余数不同,我们就称 a,b 对模m 不同余,记作 $a\not\equiv b\pmod m$.

由同余的定义出发,立即可得以下一些性质.

(1)$a\equiv a\pmod m$(反身性);

(2)若 $a\equiv b\pmod m$,则 $b\equiv a\pmod m$(对称性);

(3)若 $a\equiv b\pmod m$,$b\equiv c\pmod m$,则 $a\equiv c\pmod m$(递推性).

定理 1.9 如果 $a\equiv b\pmod m$,$\alpha\equiv\beta\pmod m$,则有

(1)$ax+\alpha y\equiv bx+\beta y\pmod m$,其中 x,y 为任给的整数;

(2)$a\alpha\equiv b\beta\pmod m$;

(3)$a^n\equiv b^n\pmod m$,其中 $n>0$;

(4)$f(a)\equiv f(b)\pmod m$,其中$f(x)$为任意给定的一个整系数多项式.

证明 (1)因为$m|(a-b)$,$m|(\alpha-\beta)$,故有

$$m\mid[x(a-b)+y(\alpha-\beta)]=(ax+\alpha y)-(bx+\beta y),$$

即
$$ax+\alpha y\equiv bx+\beta y\pmod m.$$

(2)由$m|[\alpha(a-b)+b(\alpha-\beta)]=a\alpha-b\beta$ 可得结论.

(3)由(2)可证.

(4)由(1)和(3)可证. □

现在,我们举几个例子来说明以上性质的应用.

例 1.3 一个整数 $n>0$ 被 9 整除的充分必要条件是 n 的各位数字(十进制)的和被 9 整除.这是因为,如果

$$n=a_0+10a_1+10^2a_2+\cdots+10^ka_k,$$

由 $10^i \equiv 1 \pmod 9$ $(i=1,\cdots,k)$和定理 9 的(4)便得

$$n \equiv a_0 + a_1 + \cdots + a_k \pmod 9.$$

例 1.4 证明 $641 \mid F_5 = 2^{2^5}+1$.

证明 因为$2^8 = 256$,

所以 $2^{16} = 65536 \equiv 154 \pmod{641}$,

$$2^{32} \equiv (154)^2 = 23716$$
$$\equiv 640 \equiv -1 \pmod{641},$$

所以 $641 \mid 2^{2^5}+1$.

下面构造一个密文字母表,然后用密文字母表中的字母或字母组来代替明文字母表的字母或字母组,各字母或字母组的相对位置不变,但其本身改变了,这样编成的密码称为单表代替密码.

设 $A=\{a_0,a_1,\cdots,a_{n-1}\}$为含 n 个字母的明文字母表,$B=\{b_0,b_1,\cdots,b_{n-1}\}$是含 n 个字母的密文字母表,定义一个由 A 到B 的一一映射.

$f:A\to B, f(a_i)=b_i$.

设明文 $M=(m_0,m_1,\cdots,m_{c-1})$,则相应的密文 $C=(f(m_0),f(m_1),\cdots,f(m_{c-1}))$,可见,单表代替密码的密钥就是映射 f 或密文字母表B.

下面介绍几种典型的单表代替密码:

(1)加法密码:$f(a_i)=a_j, j\equiv i+k(\mathrm{mod}n), 0<k<n$.

加法密码实际是每一字母向前推移 k 位,不同的 k 可得不同的密文,若令 26 个字母分别对应于整数 0~25,如下表 1-1 所示:

表 1-1

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
u	v	w	x	y	z														
20	21	22	23	24	25														

则加法密码变换实际是 $c\equiv m+k(\mathrm{mod}26)$.其中 $0<k<26$,m 是明文对应的数据,c 是与明文对应的密文数据,k 是加密用的参数,也称做为密钥.

例如,明文为 data security 对应于数据序列为

3 0 19 0 18 4 2 20 17 8 19 24

$k=5$ 时得密文序列

8 5 24 5 23 9 7 25 22 13 24 3

对应的密文为