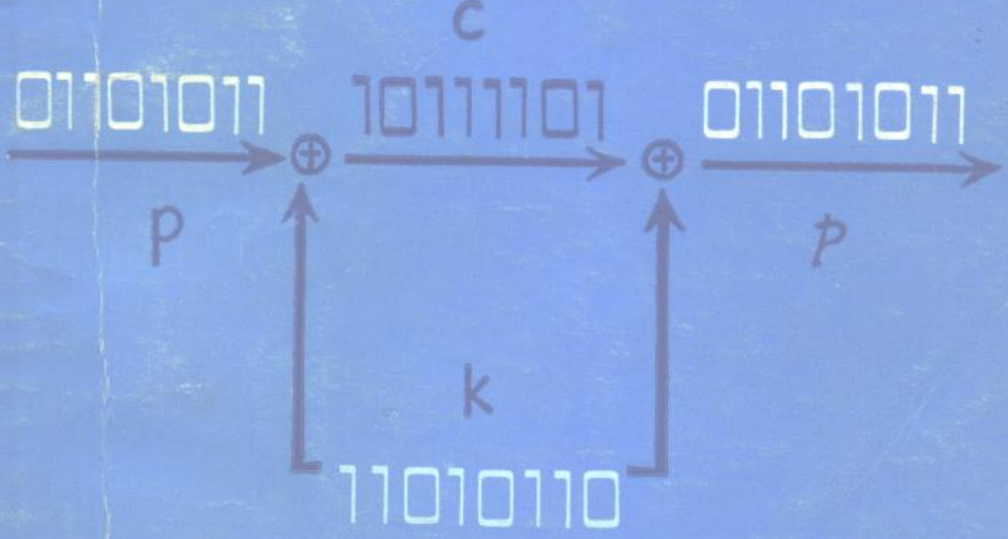
计算机安全保密入门



游之墨　鲍振东　李为镭　编著

计算机安全保密入门

游之垦　鲍振东　李为镭　编著

人民邮电出版社

内 容 提 要

目前，与计算机有关的犯罪活动在发达国家已经屡见不鲜。在我国，随着计算机应用的深入和普及，人们也很自然地要考虑如何才能安全可靠地贮存和处理数据，贮存在计算机里的数据如何才能不被破坏、窃取或非法修改的问题。

本书针对上述问题，分六个部分对计算机安全保密的主要技术和措施进行了介绍。第一部分概论，简单介绍了计算机安全保密的实际意义和研究的主要内容。第二、三部分分别介绍计算机硬件和操作系统所提供的安全保密措施。第四部分介绍密码学的主要内容，包括各种古典的和现代的密码技术。第五部分着重介绍数据库系统中所特有的安全保密问题及所采取的措施。最后一部分介绍了计算机安全保密的非技术性措施。

本书是计算机系统的管理人员、技术人员了解计算机安全保密问题的入门书，也可作为计算机专业的大专院校师生的学习参考书。

计算机安全保密入门

游之墨　鲍振东　李为镭　编著

责任编辑：王若珏

*

人民邮电出版社出版

北京东长安街27号

广 益 印 刷 厂 印 刷

新华书店北京发行所发行

各 地 新 华 书 店 经 售

*

开本：787×1092　1/32　1988年4月　第一版

印张：6 12/32　页数：102　1988年4月北京第一次印刷

字数：144 千字　印数：1— 8,000 册

ISBN7115-03535-0/TP

定价：1.40 元

前　言

在过去的十多年中，随着计算机技术的发展，数据处理技术有了长足的进步。超大规模数据库系统以及分布式计算机网路的建立，标志着现代数据处理的规模和速度都达到了前所未有的地步。现在，数据的贮存和处理都由计算机系统来承担，这一方面大大减少了书面文件的数量，简化了工作步骤，提高了工作效率和管理水平，另一方面也给数据的安全性和保密性带来了许多新的课题。虽然数据的安全和保密是一个早已存在的问题——数据的贮存、处理和保护历来有各种办法，窃取数据、破坏数据也历来有各种手段，但是自从利用计算机来处理数据以后，数据的安全和保密这一古老的问题又增添了许多全新的内容，例如，如何保护存放在计算机存储部件中的机密文件，如何保护计算机系统中的共享数据，如何解决计算机数据传送过程中的保密问题，等等。

现在，计算机已经由计算中心、实验室走向企业，走向家庭，走向社会的各个角落，成为社会运转的一个重要组成部分。一个计算机化的机构是一个高效率的机构，但是从数据安全保密的角度来讲，它又是一个不安全的、容易受到破坏的机构。现在，与计算机有关的犯罪活动在发达国家已经屡见不鲜。在我国，计算机应用的发展也很快，越来越多的机密数据都将由计算机系统来贮存和处理，于是，人们就会提出这样的疑问：计算机贮存和处理数据如何才能安全可靠？贮存在计算机里的数据如何才不会被破坏、不会被非法修改，或不会被他人非法窃取？

目　录

一、概　论

信息是自然界的一种基本特征，是组成现代社会的一个重要方面。人们利用各种各样的信息来认识世界，区分事物的共性和差异，并对自己的社会活动进行决策。目前，信息的生成、传递、接收和处理已经成为人类活动中的一项基本内容，它是现代科学技术、工农业生产、交通运输、经济管理、社会交往诸方面的基础。能否正确地利用信息和合理地保护信息，将直接或间接地影响到人们的生活，甚至人类社会的发展。

1．数据的处理问题

人们在生产实践、科学实验和社会活动中所遇到的信息处理问题是多种多样的，有些问题可以通过一定的数学表达式，利用常规的数学运算规则来进行计算或求解。例如，在经济生活中，几乎每个人都会碰到收支结算的问题；在工厂管理中，必然要对产品的成本进行核算，对生产情况进行统计，对供、产、销、利润分配等进行预算和结算；在工程设计、科学实验中存在着大量的数值计算。对于这一类数值计算问题，人们已经积累了比较丰富的经验，掌握了一些比较成熟的处理方法。近年来，由于计算技术的迅速发展，人们解决数值计算问题的能力更加提高了，无论是计算速度还是计算精度，都达到了令人赞叹的程度。

更为广泛的另一类问题是非数值计算问题。例如，在奕棋过程中，棋手对每一步棋进行判断，并作出决策的问题；医生

在为病人诊病的过程中，对病人的症状进行分析、判断，最终提出治疗方案的问题；对信息进行识别、检索、模拟和控制的问题，它们都不是利用数学公式来进行计算和求解的。利用电子计算机来处理非数值信息，一般称为数据处理，它是信息科学中的一项重要内容。在进行数据处理时，首先要考虑的是非数值信息的数字化问题，也就是如何将非数值信息转换成能够在计算机中贮存和处理的数字量。解决这个问题的方法很多，下面我们举几个例子。

例如，通信中常用的何勒内斯（Hollerith)码，就是把每个英文字母用两位十进制数来表示的，具体对应规则如下：

空格↔ 0 0
A ↔ 0 1
B ↔ 02
⋮ ⋮ ⋮
Z ↔ 26

这样，任何一串英文字母就可以用一串相应的十进制数字来表示。譬如，“Computer Security”（计算机安全保密）这一英文字组，根据何勒内斯对应规则

c↔03，o↔15，m↔13，…t↔20，y↔25，它可以用一串数字

03151316212005180019050321180920 25

来表示。

又如，在汉字的电报码中，每个汉字都可唯一地用一个四位十进制数来表示（具体的对应情况可参阅«标准电码本»)。对于任何一组电码本中存在的汉字或符号，都可以用一串相应的数字来表示。譬如，“计算机安全保密”这一组汉字，就可根据电码本，将其数字化为：

“606046152623134403560202137 8”

再如，对于一个平面图形（如图 1.1 所示），首先把它限制在平面直角坐标系中由折线O A B C O所围成的矩形区域内，并用平行于坐标轴且等距离的两组直线，把矩形区域O A B C O划分成很多正方形的小格。我们规定，如果一个正方形小格中含有该图形的点，那么这个小格的值为“1”，否则为“0”。所有这些小方格的值就组成了一个布尔矩阵。因此，图 1.1 中的平面图形就可以用一个布尔矩阵来表示：

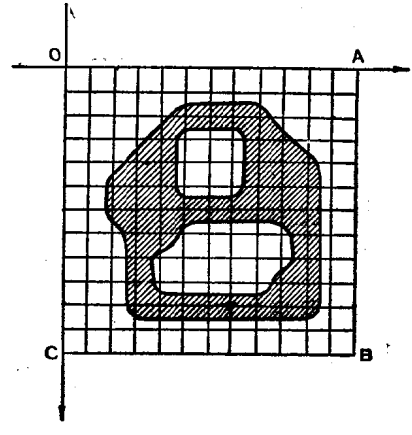


图 1.1　平面图形的矩形划分

$$\begin{bmatrix}
0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&1&1&1&1&1&0&0&0\\
0&0&0&1&1&1&1&1&1&1&0&0\\
0&0&1&1&1&0&0&1&1&1&1&0\\
0&1&1&1&1&0&0&1&1&1&1&0\\
0&1&1&1&1&1&1&1&1&1&1&0\\
0&1&1&1&1&1&1&1&1&1&1&0\\
0&0&1&1&1&0&0&0&0&1&1&0\\
0&0&1&1&0&0&0&0&0&1&1&1&0\\
0&0&1&1&1&1&1&1&1&1&1&0\\
0&0&1&1&1&1&1&1&1&1&1&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0
\end{bmatrix}$$

显然，我们把包含平面图形的矩形区域划分得越细，就越能精确地表示该图形，但是这样会使布尔矩阵的尺寸变得很大，增加了计算机处理时的困难。

非数值信息数字化的方法还有很多，例如：用 ASCII 代码表示字母和符号、用四角号码表示汉字以及连续曲线的离散化处理……等等。通过这些转换方式，我们就可以利用电子计算机来处理非数值信息了。

2. 数据的可靠性问题

我们要求数据在生成、传送、接收和存储的过程中，始终是正确可靠的。大量实践告诉我们，如果处理的数据不正确，常常会把事情搞糟。以日常的电报通信为例，一旦电码出现差错，往往就会改变发报人的原意，以致产生严重的后果。例如，某人发一个电报："母病乘火车速回"，其相应的电码为：

3018 4016 0042 3499 6508 6643 0932

假若在电码传送过程中出现错误，第十一位数字"4"变成了"7"，那么收到的电码变成

3018 4016 0072 3499 6508 6643 0932

这时，电码的译文为："母病亡火车速回"，对收报人来说，这显然是不堪设想的。同样，在计算机处理数据时，往往也会由于一个数据的差错，造成程序中断，或计算结果错误等严重后果。上述例子虽然十分荒诞，但它从某种意义上说明数据的可靠性是一个十分重要的问题，绝不可以忽视。

3．数据的保密性问题

与数据的可靠性同样重要的另一个问题是数据的保密性问题。

人们的社会实践告诉我们，某人或某个集团所提供或保存的信息往往不是全社会化的，也就是说，不必要让所有人（指无关的第三者）都知道。有时，为了某人或某个集团的利益，必须有意把有关信息的传播范围作适当的限制，使那些不该了解这些信息的人们无法知道，这就涉及到信息的保密问题。

例如，法律规定银行要保护用户存款的安全。因此，银行必须对每个用户的帐号、存款金额、支付情况、以及其它与用户有关的信息负责保密，防止第三者窃取存款或探得用户的收支情况。

又如，作战的双方在发布作战或调防命令时，必须对敌方保密，以便出其不意，攻其不备。第二次世界大战的“珍珠港事件”就是其中一例。1941 年 12 月 7 日，“珍珠港事件”爆发前夕，日本驻美国大使野村在美国大唱和平高调，使美国政府深信太平无事，可以高枕无忧。但是，日本政府却用密码向以“赤诚号”为首的特遣队发送了“秘密南进”的命令，并且用密码向野村大使发送了日本天皇给美国总统的“最后通谍”。

由于美国的情报人员几乎是在日本滥炸“珍珠港”的同时才破译出“最后通谍”，而且事前没有足够的防备，所以使珍珠港惨遭日军偷袭，损失巨大。

后来，当日军妄图在“中途岛”再战的时候，由于所使用的密码体制已被攻破，大量军事情报被破译，最后遭到毁灭性的打击。正如当时太平洋舰队总司令尼米兹所说：“中途岛作战

本质上是情报的胜利，企图突然袭击的日军反而遭到了突然袭击。”

再如，在竞争激烈的国际商业活动中，每个企业对商品信息、技术关键、经营策略等，在特定时间、地点和业务范围内也都有信息保密的要求，否则就会由于秘密的泄漏而造成损失。

由此可见，在信息的贮存和传递时，为了减小泄露机密的可能性，除了必要的法律保护条例之外，还必须有许多技术措施，尤其是利用计算机系统来处理、传递数据以后，各类技术措施就变得更为必要了。

4．与计算机有关的犯罪活动

近二十年来，在一些工业发达国家里，计算机的应用已经渗透到社会的各个方面，许多政府机构、民间企业都由计算机系统来贮存文件、管理日常事务、参与决策，这些机构都已经完全“计算机化”了。现在，贮存在计算机系统中的数据越来越多，其中有许多是非常机密的。而且，计算机系统变得越来越复杂，几乎没有一个人能够掌握系统工作的全部细节问题，因此管理和使用计算机系统需要各种专业技术人员。

这样的局面，既提高了整个社会运转的效率，又带来了许多新的问题。一些敌对分子和极端利己的不法之徒，搞了一系列的犯罪活动，我们把这类活动称为“与计算机有关的犯罪活动”。

虽然因为种种原因，与计算机有关的犯罪活动并没有得到如数的报导，但是从所披露的材料来看，这个问题已经成为工业发达国家的一个社会问题，日益受到社会各方面的重视。

与计算机有关的犯罪活动的形式和手法是多种多样的，一般来说可以分为两大类：一类犯罪活动是直接以破坏计算机系统为目标的，另一类犯罪活动是利用计算机系统作为犯罪工具的。

以破坏计算机系统为目标的犯罪活动包括纵火、爆炸、设置障碍（包括断电、断水）等，目的是直接破坏计算机系统或者阻止计算机系统的正常工作，采取这样的破坏行动往往是因为政治原因。例如，1980 年 3 月至 1981 年 3 月，荷兰菲利浦公司、美国霍尼威尔公司、美国国际商业机器公司等几家公司在法国的子公司相继遭到“3 月 27 -28 直接行动组织”等几个恐怖组织的袭击，这些组织炸毁或破坏了计算机系统，使系统无法工作。他们的理由是这些公司的计算机程序和数据是政府手中的武器，是为武装力量和反间谍组织服务的。类似的事件，在意大利也发生过多次。

利用计算机作为犯罪工具的非法活动是与计算机有关的犯罪活动的主要形式，参与这类犯罪活动的以管理、使用计算机系统的内部工作人员为主。这一类犯罪活动主要包括盗窃和贪污。

盗窃的方式很多，最一般的是盗窃计算机系统中的硬件和有关的器材。现在，这类盗窃在工业发达国家中已经比较少见，因为这些器件很难在非法市场上出售。比较大量的盗窃方式是盗取系统中有用的信息，包括计算机软件、计算机系统中的文件、输出数据等等，然后将它们出卖给有兴趣的个人或集团。例如，在 1964 年，美国得克萨斯仪器自动化计算机公司的一名程序员私自复制了属于该公司的四十九个计算机程序，企图以五百万美元的代价私自卖给公司的客户，险些使公司蒙受巨大损失。还有一种形式的盗窃是所谓“偷用计算机时间”，也

就是无偿使用不属于个人的计算机系统为个人的私利服务。例如，1980 年 8 月，在英国一家国际性保险公司的计算机系统中，程序员偶然发现了一些很奇怪的程序和文件，经过调查发现这是一名在该公司工作了十二年的计算机系统高级分析员为自己的亲属所编写的会计程序，他已经在系统中将这个程序运行过几十次了，最后公司解雇了这位高级职员。

贪污的手法就更多了，从增加或删除输入数据、修改文件中的数据、修改程序、隐瞒输出数据，直到在通信线路上窃取系统中的信息、窃取某个用户的口令、假冒系统的合法用户等等，最终达到非法获取金钱的目的。这种犯罪活动主要发生在银行的计算机系统中。例如，1978 年，美国洛杉矶市的“安全太平洋银行”的一名计算机系统分析员，利用他职务上的方便和对于银行的安全预防措施的了解，假冒银行办事员，通过计算机系统向他本人在纽约一家信托公司的帐户里汇入了一大笔钱，然后他又将这笔钱转汇到瑞士银行，购买了价值八百万美元的钻石。这一犯罪行为直到八天以后才被发觉。又如，美国洛杉矶市“威尔福格国家银行”的一名业务经理利用在计算机终端上开空头支票的办法，到 1981 年 1 月为止，两年内一共贪污了二千一百万美元，这是当时洛杉矶地方法院所受理的最大的一次银行盗窃案。

最后，为了使读者能够比较具体地了解利用计算机进行犯罪活动的可能性，我们举一个用“积少成多”的办法进行贪污的例子。

银行在用计算机管理用户存款业务时，经常要计算利息。这类计算由于受最小记帐单位的限制，往往要对计算结果进行四舍五入。对于一个不诚实的管理员来说，这是进行非法活动的好机会。假设银行的某个存户在一定时期内的存款次数为 n，

记帐的最小单位为“分”，那么，管理员只要在计算利息的程序中，插入一个累计舍去值的子程序，使舍去值累计超过1分时，就将该分值取出，并把它加到这个管理员的帐号内，当用户频繁存取时，管理员获得的非法存款金额，再加上利息，其总金额将是十分可观的。

下面，我们根据表1-1和表1-2，看看这个不诚实的管理员是如何贪污的。为了造表方便，我们假设存款次数n＝12，利率

表 1-1　　正常算法的记帐表

原存款额	本息合计值	记入款额	记帐误差	误差累计值
15.86	16.27236	16.27	0.00236	0.00236
221.75	227.51550	227.52	(0.00450)	(0.00214)
18.68	19.16568	19.17	(0.00432)	(0.00646)
564.44	579.11544	579.12	(0.00456)	(0.01102)
		*579.11		*(0.00102)
101.32	103.95432	103.95	0.00432	0.00330
77.11	79.11486	79.11	0.00486	0.00816
127.49	130.80474	130.80	0.00474	0.01290
		*130.81		*0.00290
789.03	809.54478	809.54	0.00478	0.00768
425.34	436.39884	436.40	(0.00116)	0.00652
247.10	253.52460	253.52	0.00460	0.01112
		*253.53		*0.00112
331.32	339.93432	339.93	0.00432	0.00544
111.34	114.23484	114.23	0.00484	0.01028
		*114.24		*0.00028
3030.78	3109.58028	3109.58		0.00028

表 1-2　　非正常算法的记帐表

原存款额	本息合计值	记入款额	记帐误差	补充值累计	舍去值累计
15.86	16.27236	16.27	0.00236	(0.00000)	0.00236
221.75	227.51550	227.52	(0.00450)	(0.00450)	0.00236
18.68	19.16568	19.17	(0.00432)	(0.00882)	0.00236
564.44	579.11544	579.12	(0.00456)	(0.01338)	0.00236
		*579.11		*(0.00338)	
101.32	103.95432	103.95	0.00432	(0.00338)	0.00668
77.11	79.11486	79.11	0.00486	(0.00338)	0.01154
					**0.00154
127.49	130.80474	130.80	0.00474	(0.00338)	0.00628
789.03	809.54478	809.54	0.00478	(0.00338)	0.01106
					**0.00106
425.34	436.39884	436.40	(0.00116)	(0.00454)	0.00106
247.10	253.52460	253.52	0.00460	(0.00454)	0.00566
331.32	339.93432	339.93	0.00432	(0.00454)	0.00998
111.34	114.23484	114.23	0.00484	(0.00454)	0.01482
					**0.00482
3030.78	3109.58028	3109.55		(0.00454)	0.00482

k＝2.6%，也就是说存入 100 元，到期时连本带息为 102.60 元。

表 1-1 是银行在进行正常处理时的记帐表。表中，记帐误差＝本息合计值－记入款额。当记帐误差值大于或等于零时，我们称之为“舍去值”，当记帐误差值小于零时，我们称之为“补充值”。在表中，“补充值”仍然写成正数，但加上括号，以区别于“舍去值”。当误差累计值超过 1 分时，就将此值减去 1 分，所得数据单独写在下一行，并在该数据前打上一个 * 号。