起步丛书

电脑锁密解密六日通

罗长天
主编

光明日报出版社

电脑锁密解密六日通

主　编　罗长天

副主编　肖春来

编　委　蓝　天　文　禹

伟　时　平　山

赫　然　田　力

光明日报出版社

（京）新登字101号

图书在版编目（CIP）数据

电脑锁密、解密六日通/罗长天编著．-北京：光明日报出版社，1994.7
（起步丛书）
ISBN 7-80091-525-5

Ⅰ．电… Ⅱ．罗… Ⅲ．电子计算机-密码术 Ⅳ．TP309

中国版本图书馆CIP数据核字（94）第07747号

JS463/06

光明日报出版社出版发行
（北京永安路106号）
邮政编码：100050
电话：3017788-225
新华书店北京发行所经销
北京市平谷玉福印刷厂印刷

787×1092 32开 印张7.75 字数 170千字
1994年7月第1版 1994年7月第1次印刷
印数：1-12，000册
ISBN 7-80091-525-5/TP·3

定价：6.80元

导 读

第一章是概说，让您先有一个初步印象。

第二章告诉您如何把入侵者挡在大门之外。

第三章告诉您如何使硬闯进门来的不速之客什么也找不见。

第四章告诉您如何使入侵者即便找到了一些什么也无法看懂。

第五章告诉您当入侵者企图破密时，如何使一切都自动毁掉，使秘密永不暴露。

以后几章是一些专题。

当然，每一章中都不乏“以子之矛，攻子之盾”的内容：锁法与解法同“章”操戈！读罢本书您会发现，这种较量兴味无穷。

编 者

1994 年 6 月

目　录

此为试读,需要完整PDF请访问: www.ertongbook.com

第一章　概说：电脑中最神秘的一个领域

一、在电脑中把秘密藏起来

电脑不仅已深入到社会生活的方方面面，而且也开始走入千家万户，正在逐渐成为我们每一个人的亲密伴侣。

机关的、公司的、个人的，各种文件、数据、资料，都可以敲到电脑里存上，调用起来真是方便！

但是，你能调用，别人也能调用。这样，电脑岂不成了没锁的抽屉，没门的资料库？机关里的政府机密，公司里的商业秘密，与个人相关的小秘密，岂不暴露无遗？特别是，在网络状态下，多台电脑，多个终端，秘密被窃了也无法知晓，这可怎么得了？

另外，电脑中的文件、数据、资料还可能被别人篡改甚至删除，使多年的心血毁之一瞬！

如此等等，不能不防！因此，电脑锁密技术应运而生。

不过，在电脑中锁密与一般的常规保密相比，有很大的区别，也更加不容易，需要一些特殊的技巧。这是因为，所要保护或封闭的不是一般的资源而是信息资源，其脆弱性更加明显。一般的资源具有独占性，即一旦被人占有其他人就不能再占有，或者说其使用只是一次性的。而信息资源则不同，它可以同时被许多人占有并利用，也就是说，具有共享性。因此，既要防止信息在传输过程中被截取，又要防止在存储中被窃取和

复制，还要防止被篡改或删除。

对电脑中所存储的信息的保护，涉及到许多方面，本书只讨论对电脑或电脑系统的人为攻击或威胁的预防。

总之，本书就是要讨论怎样在电脑中把秘密藏起来，使外人进不去，调不出来，偷不走，看不懂，改不了，也破坏不了（除非他把电脑或磁盘毁了）。

能办到吗？咱们一起试试看！

二、设置无形屏障的基本思路

实现电脑锁密，大致可有如下基本途径：封门、隐藏、密码和自毁。

所谓封门就是控制访问，即控制出入，是指设法挡住局外人或入侵者接触电脑中所藏秘密的各种手段。最常用的方法是设置口令，不晓得口令者便进不来。也可以设法把键盘锁住，使其无法输入任何指令，或者把硬盘锁住仿佛没有硬盘一样。在网络系统中，更多地是设置访问权限，对不同用户规定可访问的范围及读、写、改、删的权限。

隐藏，就是让人看不见，可以通过对子目录或文件名作手脚等办法，使信息本身以有化无，或以多化少；也可以通过对信息存放的空间搞名堂，如空间幻化，以东示西等等。总之，就是要让入侵者如入无物（有用物）之境。

密码技术的基本想法就是，伪装信息，把明文变成密文，使局外人无法理解信息的真正含义。只有掌握密钥的人，才能将密文还原为明文。需要强调的是，密码体制是可以公开的，而密钥却是最关键的，这好比保险柜与保险柜的钥匙。

自毁，就是巧设机关，当秘密有被入侵者发现的危险时，

信息发生自动"引爆"，留给入侵者的将是杂乱无章的一团或一片空白。当然我们自己也同样遭受损失，因为我们也什么都没了。

三、电脑破密与当代软件牛仔

有一些企业，特别是国外的一些公司，往往通过加密的软件黑箱来控制另一家使用其技术的企业或公司。为了摆脱这种控制，软件解密技术应运而生。

软件生产者，为了保护其经济利益，都想方设法对其磁盘进行加密，以防止被任意拷贝，这又给使用者带来了许多不便，由之产生磁盘解密技术的需要。当然，磁盘解密技术的发展，更可能是由盗版者而推动的。盗制一种软件显然比开发的投入要小得多。

更有甚者，在国外产生了一批软件牛仔，亦称"电脑朋克"，在电脑世界里横冲直撞。在电子游戏厅里，他们只敲几下键盘，得分便升到第一。他们使用别人的信用卡，假冒某大公司的账号到国外旅行，到处窃取资料，制造数据炸弹以致于电脑病毒。无缝不钻的电脑黑客并非什么绿林好汉，不过是一些所谓电子偷视者(Peeping Toms)、非法入侵者和窃贼。但其危害极大，对其切不可掉以轻心。当然，本书并不想提醒我们那些无忧无虑的朋友"锁上他们的门"(lock their doors)，而是想指导他们如何在门上安锁及设置各种路障。

在小说中，我们常看到，在古老的羊皮纸上画着某荒岛上的藏宝图，因年代久远，某些参照物已不复存在，遂成为难解之谜。是的，人类历史上确实存在许多已不可解之谜。但是，从理论上来讲，电脑的所有锁密技术都是可解的。

俗语说，“道高一尺，魔高一丈”。电脑的锁密与解密技术在相生相克中，正在共同向前飞速发展。

此为试读，需要完整PDF请访问：www.ertongbook.com

第二章　控制访问

控制访问是电脑锁密的重要手段，通过它，可以使局外人无法接触被保护的领域。在专用电脑的情况下，甚至可以将局外人挡在"大门"之外，以致于无法输入任何指令。

一、口令的妙用

口令(Password)，从阿里巴巴的开门咒语到军事要塞的哨兵口令，在人类社会中由来已久。口令应用于电脑系统，一般亦称为"通行字"，属于所谓身份鉴别问题。

1. 口令的生成

一般说来，口令可由两种方法生成：一种是由用户自己选择，一种是由电脑随机生成。

由用户自己选择口令的优点是容易牢记，不易忘掉，一般不必专门写下来留存。其缺点是很容易被人猜出来，因为人们在选择口令时，往往带有很强的私人色彩，如：

①用户的姓名或孩子的姓名；

②城市名、街道名、住址；

③生日、房间号、社会保险号、电话号码、汽车号码；

④倒过来拼写的有意义的字。

这些，都是入侵者将会优先猜测的目标。

用英文设计口令，国外的经验说明，一个好的口令，至少要有六个字母长，并且不是基于个人信息，中间应有非字母的字符(特别是控制字符)，如 4 score，my —— name，sistem(sic)

等，便是很难被破译的了，当然并非完全不可能。更好的一些口令，如 dg 7m33ex，Luxzrum，几乎是不可能破译的。但是，第一个几乎不可能被记住，以致于你需要把它写下来留存，这便不是一个好口令。可以选两个不相干的词，中间用数字或控制符连接起来。

如果采用汉字作为口令，则安全度大为提高，这是因为汉字多，口令字空间特别大的缘故。仅常用汉字便达 3500 多个，标准汉字约 7000 个，如果再适当结合阿拉伯数字、控制符号，以致于英文，是很难被解破的。不过，你可千万别忘了一条首要原则：自己能记得住！

用口令生成器来为用户指定口令，优点是随机性好，猜起来很困难，几乎不能被破译，缺点是不易记忆。口令生成器分为随机字生成器与随机数字生成器两种。为了有助于记忆，随机字生成器所生成的口令，是可以按照正常发言规则发言但没有任何意义的字符串，如 scramboo、fligmath 等。对于数码口令字，可采用分组联想记忆法。例如 902538，分为 3 组，“90”，你可以联想到亚运在中国举行，“25”，你可以联想到燕子与青蛙数数“两五一十”的笑话，至于“38”，去联想妇女节岂不很妙？

2. 口令的交换

在网络系统中，当对话的双方须进行彼此身份鉴别而交换口令时，存在着被冒充者套取口令的危险，一般利用单向函数予以防护。

设有 A、B 双方，口令各为 a、b，并均为对方所掌握或保存。双方约定一个单向函数 f。

当 A 对 B 进行身份鉴别时，首先向 B 发送一个随机数 X_1，B 收到后，利用单向函数 f 求得

$y_1=f(b,x_1)$

B 将 y_1 发送给 A。单向函数的作用在这里可保证，即使被局外人窃取了 y_1 与 x_1 的数值，也无法恢复出 b 来。注意，这时在 A 手中存有 b，而 x_1 是 A 发出的，所以 A 可计算 $f(b,x_1)$ 将之与 y_1(B 发过来的)相比较，如果相等，则知道对方确为 B，否则定是非法冒充者。

B 对 A 进行身份鉴别时，与以上步骤相同，即向 A 发出随机数 x_2，当收到返回值 y_2 时，比较是否与 $f(a,x_2)$ 相等。

二、口令设置实例

1. 在 DOS 系统设置口令功能

在电脑中常见的 DOS 系统没有口令检验功能下面我们用汇编语言给出一个简易口令设置程序。

源程序如下：

```
CODE    SEGMENT
        ORG     100H
        ASSUME  CS:CODE,DS:CODE,
                ES:CODE,SS:CODE
BGN:    JMP     START
MUS     DB      OAH,ODH,'Password:','$'
MUS2    DB      OAH,ODH,'Incorrect
                    password','$'
MUS3    DB      'hello'(读者可自己设定此口令值)
BUFFER  DB      6   DUP(O)
START:  MOV     DX,OFFSET   MUS
        MOV     AH,9
```

```
        INT     21H
        MOV     BX,07H
        MOV     DI,OFFSET  BUFFER
L2:     MOV     AH,07H
        INT     21H
        DEC     BX
        JZ      LO
        CMP     AL,ODH
        JZ      L1
        MOV     BYTE PTR[DI],AL
        INC     DI
        JMP     L2
L1:     MOV     SI,OFFSET  BUFFER
        MOV     DI,OFFSET  MUS3
        MOV     CX,5
        REPZ    CMPSB
        JZ      EXIT
LO:     MOV     DX,OFFSET  MUS2
        MOV     AH,9
        INT     21H
        JMP     START
EXIT:   INT     20H
CODE    ENDS
        END     BGN
```

此程序适用于采用 MS-DOS 操作系统的所有电脑，是一种可有效阻止普通非授权用户使用硬盘的简易方法。装载有本程

序的电脑起动后要求用户回答口令，并且不响应键盘中断CTRL-BREAK，直到回答准确后方可进入。

2. BIOS SETUP 中的口令功能

将 BIOS SET UP seruice system 的主菜单移至 Advancd CMOS set up 功能项上回车，计算机上会显示此功能下的所有设置子项，其中有一个 PASSWORD 的设置子项，此设置子项有三个设置值：disabled 、set up、allows，通过 PgDn 和 PgUp 键可以改变它的设置值。

现在按 PgDn 或 PgUp 键将 PASSWORD 的设置值设置为 set up 状态，这样我们便启动了 PASSWORD 的设置服务功能，然后按 Esc 键便可回到主菜单利用 Change PASSWORD 功能来设置口令了。

启动了 PASSWORD 的设置服务功能回到主菜单后，将菜单亮条移到 Change PASSWORD 功能项回车后，会出现如下情况：

(1)初次设置口令

Please insert PASSWORD:(光标)

此时，用户便可输入口令密码(计算机上看不见)，口令密码可以是任意 ASCII 字符，最长为 11 位。

(2)更换旧口令

Please insert CURRENT PASSWORD:(光标)

这时，用户必须正确输入旧口令，才能有权进入(1)中的状态，设置新的口令。因此，保证了系统口令只能被最初设置口令的人(知道旧口令的人)更改。

值得注意的是，上述口令的设置均属于盲操作(口令不能显示出来)，设置者必须正确按键输入并牢记。

(3)口令的启用

口令设置或修改完了以后，此时口令还不能生效，若使口令生效，必须进行以下操作。

①将主菜单亮条移到 Advanced CMOS SET UP 功能项回车，进入其设置界面，然后将亮条移到 PASSWORD 设置子项，按 PgDn 或 PgUp 键将其设置值改为 Allows 后返回主菜单。

②将所有新增设置存入 CMOS。将 Advanced CMOS SET UP 中的 PASSWORD 的设置值确定为 Allows 后，等于启用了新设置的口令，但到此为止所有操作的结果并没有得到有效的储存。为此，在离开 BIOS SET UP service system 主菜单时，必须选用 Write to cmos at Quit 项，以使新的 BIOS 的设置生效。

3. UNIX 系统的口令操作

UNIX 操作系统是一个通用的，交互式多用户、多任务分时系统。由于其结构紧凑，功能强，效率高，使用方便和可移植性好等优点，自 70 年初问世以来，受到了计算机界的众多青睐。在众多计算机厂商的产品中，从大型机、中型机、小型机到微型机许多都是采用 UNIX 操作系统。特别是近年来高档微机 386，486 的出现，普通的单用户操作系统已不能充分发挥这些机器的功能。UNIX 则以其卓著的性能在这个领域崭露头角。

在操作时，您必须以超级用户身份登录系统后，才能给一般用户注册开户，您才能够停止系统运行，为关机做准备。

要以超级用户的身份登录，您必须知道超级用户的口令

此为试读，需要完整PDF请访问：www.ertongbook.com