电脑报 总策划
http://www.yesky.com

电脑报技巧丛书

数据恢复与加密解密

系统文件、分区表、注册表恢复实战及加密解密技巧

张华　徐涛　张雁　编著

通过修复硬盘恢复数据

- ◆硬盘常见故障的处理方法
- ◆主引导记录损坏的恢复
- ◆分区表一般故障的恢复

数据文件丢失、损坏的恢复

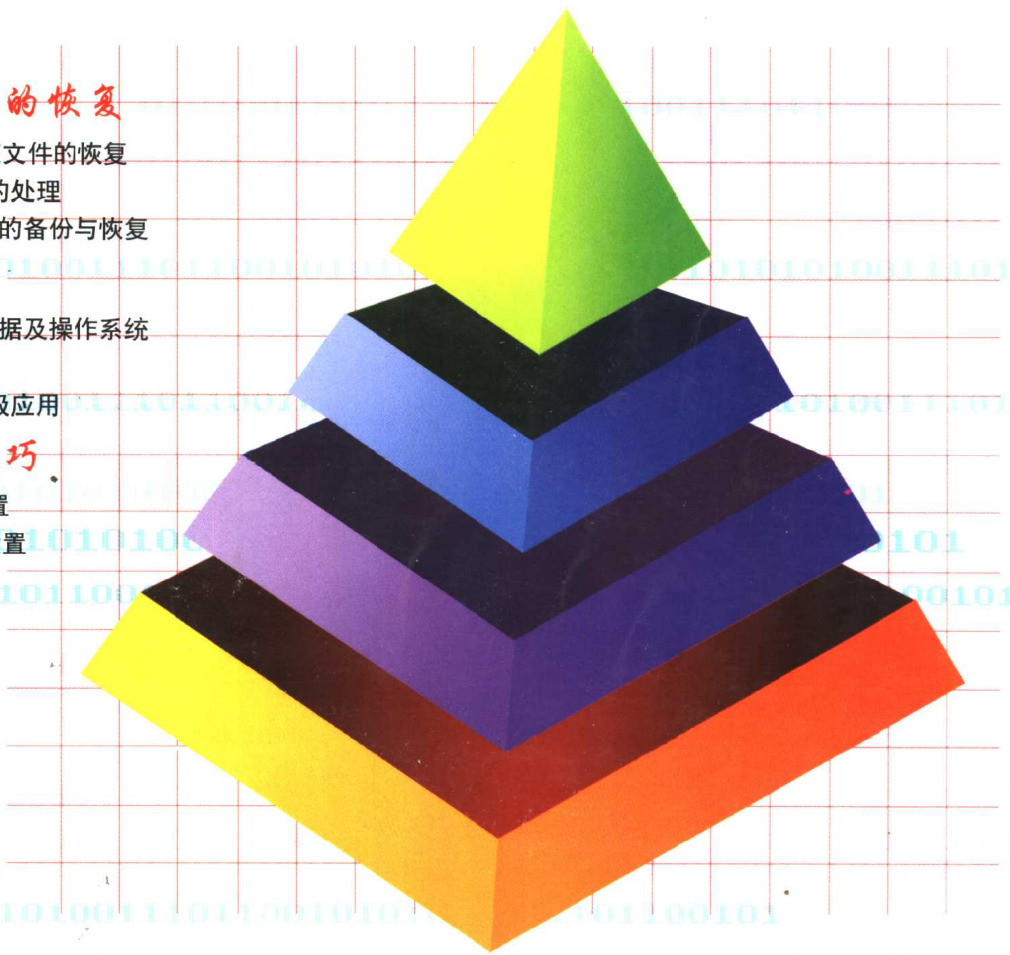
- ◆误删除、被修改、丢失系统文件的恢复
- ◆BIOS的备份与升级失败后的处理
- ◆OICQ、Foxmail等常用软件的备份与恢复

数据及系统备份技巧

- ◆用Ghost备份和恢复硬盘数据及操作系统
- ◆Backup Magic使用详解
- ◆Windows XP系统恢复的高级应用

数据的加密、解密技巧

- ◆对系统BIOS开机口令的设置
- ◆对重要数据文件进行加密设置



本手册随光盘赠送

光盘精彩内容

赠送Disk Genius正版软件
12款实用数据修复工具软件
硬盘分区表修复实例演示

金版电子出版公司出版

中科普传媒 China science media

数据恢复与加密解密

系统文件、分区表、注册表恢复实战及加密解密技巧

张华　徐涛　张雁　编著

本书配有光盘，需要的读者请到 http://210.34.51.1/tractate/index.asp
网页上申请，或到“网络与光盘检索实验室”联系。

金版电子出版公司出版

内容介绍:

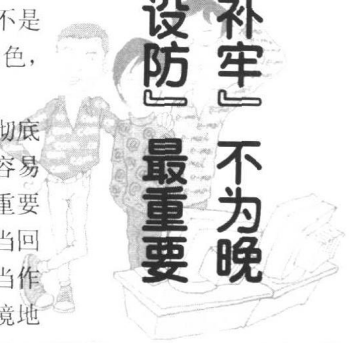
本手册主要讲解数据备份、恢复和数据加密解密等方面的内容。本手册从各种不同的用户角度出发，从问题本身着手，从数据恢复与加密解密技术基本知识，到一般数据文件丢失、损坏的拯救、硬盘系统的数据恢复、特殊文件丢失后的拯救、数据的备份、常用软件的备份与恢复、BIOS和注册表的备份与恢复，再到具体的数据加密技巧和数据安全防范措施等。全手册贯穿数据安全这一主题，并从数据拯救与数据加密两个层面对其进行具体阐述、剖析与实用操作的介绍，力图让读者在了解相关知识的基础上，全面掌握各种操作实践与技巧经验，轻松搞定数据安全!

光盘内容:

赠送Disk Genius正版软件
12款实用数据修复工具软件
硬盘分区表修复实例演示

书　　名：数据恢复与加密解密
编　　著：张　华　徐　涛　张　雁
策　　划：谢宁倡　李　林　余　飞
责任编辑：海　磊
封面设计：刘学敏
版式设计：冷　冰
程序开发：李璞一
出版发行：金版电子出版公司
CD生产者：北京中新联数码科技有限公司
印　　刷：重庆大学建大印刷厂
规　　格：787mm × 1092mm 1/16　　20印张　　450千字
版次/印次：2002年12月第1版　2002年12月第1次印刷
印　　数：1-5000册
版 本 号：ISBN 7-900131-32-6/G · 11
定　　价：20.00元(1CD+配套书)

前言 Preface



『亡羊补牢』不为晚 『提前设防』最重要

当今的世界已经是信息化无所不在的社会，大到国防科技、航空航天，小到办公信息处理，再到个人时尚甚至是家庭电器，各行各业、各个领域无不是计算机发挥潜能的地方，与此同时，计算机数据也扮演着越来越重要的角色，因此计算机数据的安全问题已经越来越受到人们的重视。

备份——这是解决数据丢失的最根本办法，也是最保险、最安全、最彻底有效的办法，甚至没有任何损失。然而在问题没有发生之前，人们总是很容易忽视它。对于很多单位，特别是一些小单位和个人用户来说，即便是很多重要数据信息存在潜在的危险，也并没有引起足够重视，甚至从来没有把备份当回事。有的即便知道备份的重要性，但半年、三个月才备份一次，只把备份当作闲暇无事时的额外休闲。如此种种的情况，当灾难来临之时，就会身临其境地体会到什么叫欲哭无泪、后悔莫及！

除了埋怨事前为什么如此无知而后悔外，面对已经丢失的数据，我们真的就束手无策了吗？其实，从理论上来说，除非数据载体（比如硬盘、软盘、光盘等）已经灰飞烟灭、被盗，或者已经不存在了，否则其数据都有部分甚至是全部被恢复、拯救的可能。据世界专业的数据恢复机构的统计资料表明，80%的数据丢失问题都能通过各种手段和拯救措施进行挽回。因此，在数据丢失以后，并不用彻底失望，我们还可以做的就是及时拯救，最大限度地拯救我们的数据，以挽回损失。

灾难的来临让我们能充分体会提前备份以及事后修复、拯救的重要性，然而对于我们的重要数据来说，是不是平安无事的时候，就万无一失了呢？机密文件、商业资料和其他重要信息，个人的隐私信息等等数据，如果被人盗走或者恶意利用所造成的损失，甚至比数据本身被丢失更严重，而且也是无法直接挽回损失！而现在的黑客入侵、恶意破坏与盗窃，以及因为大意而造成资料被偷窥等现象，已经是数据安全的另外一个大敌。面对如此种种的危机，如何进行防范？系统、数据的加密，无疑是最妥善的方法之一，这种方法提前对保存有重要信息数据的计算机系统进行设防，阻止非法用户擅自闯入；并对数据本身进行各种加密，使原始数据不被他人利用。如此牢牢把关，达到无懈可击的境界，可以让我们的重要信息和数据安然无恙、万无一失！

现在，你手上的正是一本教你如何在数据丢失之后对其进行修复、拯救，以及如何对重要数据进行加密保护措施等一系列实用操作的书。我们从各种不同的用户角度出发，从问题本身着手，从数据恢复与加密技术基本知识，到一般数据文件丢失、损坏的拯救、硬盘系统的数据恢复、特殊文件丢失损坏后的拯救、数据的备份、常用软件的备份与恢复、BIOS和注册表的备份与恢复，再到具体的数据加密技巧和数据安全防范措施等；全书贯穿数据安全这一主题，并从数据拯救与数据加密两个层面对其进行具体阐述、剖析与实用操作的介绍，力图让读者在了解相关知识的基础上，全面掌握各种操作实践与技巧经验，轻松搞定数据安全！

最后，我们想和读者说的是：对于重要数据，一定要及时做好备份；而万一当数据丢失而又没有备份的时候，“亡羊补牢”不为晚；当我们的重要数据不想被别人看到或者盗用的时候，“提前设防”最重要！

编者

2002年12月

目录

试读结束：需要全本请在线购买： www.ertongbook.com

目录

目录

目录

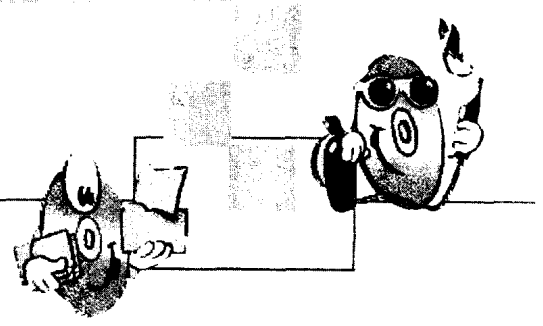
目录

目录

浅谈数据恢复和加解密技术

第一章

什么是数据恢复
哪些数据需要恢复
数据恢复一般采取的手段
数据恢复的一般过程与要点
什么是加密解密技术
哪些数据需要加解密
加解密采取的一般手段



试读结束：需要全本请在线购买： www.ertongbook.com

1.1 浅谈数据恢复

1.1.1 什么是数据恢复

当今的世界已经是信息化无所不在的社会，大到国防科技、航空航天，小到办公信息处理，再到个人时尚甚至是家庭电器，各行各业、各个领域无不是计算机发挥潜能的地方，如此同时，计算机数据也扮演着越来越重要的角色，因此计算机数据的安全问题已经越来越受到人们的重视。自然灾害、设备损坏、软硬件错误、误操作、黑客入侵、恶意破坏以及病毒袭击等等，都时时刻刻、无处不在地威胁着我们宝贵的计算机数据资源，而无论是大型单位还是个人用户，数据丢失所造成的损失是不可估量的，重则危及国家安全、造成巨额经济损失，轻则资料全无而做无用功!

从目前统计的资料来看，造成数据丢失或损坏的原因大致分为两种：软件故障和硬件故障。

软件故障的现象一般表现为无操作系统，读盘错误，文件找不到、打不开、乱码、报告无分区、无格式化等，具体包括：病毒感染、误格式化、误分区、误克隆、误操作、网络删除、0磁道损坏、硬盘逻辑锁、操作时断电等。

硬件故障一般表现为硬盘读写有误，常有一种“咔嚓咔嚓”的磁组撞击声或电机不转、通电后无任何声音、选头不对造成读写错误等现象，具体包括：磁盘划伤、磁组变形、芯片及其它原器件烧坏、硬盘寿命自然终结等。

综合以上各种故障，可以把它们分为五类，其所占数据丢失的比例分析如下（如下图所示）：

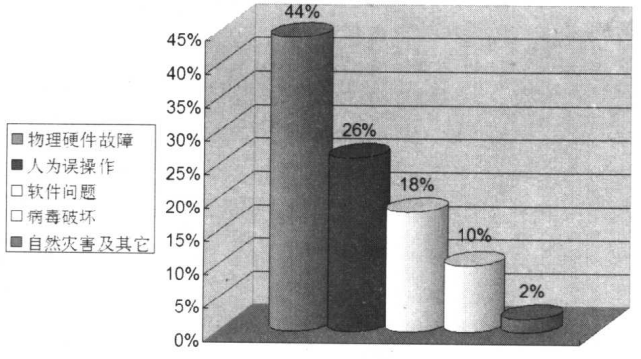


图1-1

(1)物理硬件故障（44%）：即以上提到的硬件故障及具体原因所造成的故障。

(2)人为误操作（26%）：误格式化、误分区、误克隆、误操作等属于操作不小心或恶意破坏。

(3)软件问题（18%）：由于操作系统或应用软件本身设计或编码存在漏洞或错误（BUG）所导致的数据丢失。

(4)病毒破坏（10%）：因为感染病毒而导致数据被改写、丢失，甚至是整个硬盘被破坏。

(5)自然灾害及其它（2%）：风雨雷电、洪水或其他不可抗拒的原因。

从以上的分析来看，造成数据丢失的原因确实很多，而且物理、人为误操作这样的故障，都有可能在我们周围的电脑上发生，概率相当大。

备份——这是解决数据丢失的最根本办法，也是最保险、最安全、最彻底有效的办法，只要备份及时得当，可将损失降到最小，甚至没有任何损失。然而在问题没有发生之前，人们总是很容易忽视它。对于很多单位，特别是一些小单位和个人用户来说，很多重要数据信息都存在潜在的危险，但是没有引起足够重视，甚至从来没有把备份当回事。有的即便知道备份的重要性，但半年、三个月才备份一次，只把备份当作闲暇无事时

的额外休闲。如此种种的情况，当灾难来临之时，就会身临其境地体会到什么叫欲哭无泪、后悔莫及！

除了埋怨事前为什么如此无知而后悔外，面对已经丢失的数据，我们真的就束手无策了吗？其实，从理论上来说，除非数据载体（比如硬盘、软盘、光盘等）已经灰飞烟灭、被盗、或者已经不存在了，否则其数据都有部分甚至是全部被恢复、拯救的可能。具世界专业的数据恢复机构的统计资料表明，80%的数据丢失问题都能通过各种手段和拯救措施进行挽回。因此，在数据丢失以后，并不用彻底失望，我们还可以做的就是及时拯救，最大限度地拯救我们的数据，以挽回损失。

而我们所说的数据拯救，也就是针对以上各种原因所导致的数据丢失问题，使用各种软、硬件工具与技术方法、措施对其进行恢复、把数据重新找回来，使宝贵的信息得以再用。

1.1.2 哪些数据需要恢复

概括地讲，所有个人的重要信息、数据资料与操作系统文件以及应用程序数据等，在丢失以后都需要拯救。当然，根据重要性来分，重要的数据资料和信息如果丢失以后，是最急切需要拯救的，而其他数据相对次要甚至没有必要。下面我们来具体分析讨论。

很多用户甚至在数据已经丢失的情况下还不知道真相，直至自己需要的时候，才发现已经找不到了，所以有必要明白哪些数据是比较容易遭受破坏以及相应的哪些数据需要拯救，以便在平时留意保护甚至是进行备份，且在数据丢失后进行恢复与拯救！

1.BIOS 数据文件

BIOS 是计算机能正常运行的基石，它是系统硬件与软件的输入 / 输出接口，可以说没有它，计算机就是废铁一堆。很多用户都认为 BIOS 是硬件，其实那只是它直接和硬件打交道而已，其本身也是软件和程序，是软件自然就需要有执行代码，而 BIOS 数据文件就是这样的代码。其实一般用户也很少接触这些，但随着能恶意破坏BIOS数据文件（软件破坏，而非硬件损坏）的CIH病毒的出现，以及越来越多的玩家对升级、刷新BIOS的热衷，导致BIOS数据文件经常受到破坏，而如果不及时恢复与拯救，我们的计算机将彻底瘫痪而无法运行。

2. 保存在 CMOS 中的 BIOS 配置数据

上面我们已经介绍了BIOS其实也是程序软件，只不过它和硬件直接打交道而比较“高级”而已。而BIOS程序运行也需要参数和配置信息，这些信息相当重要，它保存了计算机（也就是BIOS）各种硬件能正常运转的所有配置信息和其他高级信息（比如系统密码等），而这些信息都保存在CMOS（互补金属氧化物半导体，一种数据存储器件）中。CMOS中保存的数据如果丢失，会导致计算机运行不正常或无法运行。另外，早期的一些病毒专门感染CMOS，导致计算机无法运行甚至瘫痪。

3. 硬盘主引导纪录与分区表信息

硬盘分区的信息存在它的第一个扇区(即第一面第一道第一扇区)，这个第一扇区就是硬盘的硬盘主引导扇区。而硬盘主引导扇区又包括了主引导记录(MBR，446字节)和硬盘分区表（DPT，64字节）以及2字节的跳转信息。如果这些信息被破坏，系统（BIOS）就无法识别硬盘分区，系统也无法被引导，而磁盘分区上的数据就更无法访问了（即便他们没有破坏），因此，可以想象它的重要性了。

4. 操作系统的系统文件

操作系统运行所必需的系统文件也是很重要的，我们经常碰到因为这些文件被替换、覆盖或丢失而引起系统不稳定甚至崩溃的情况。

5. 操作系统的配置文件

绝大部分用户都使用Windows操作系统，而Windows能正常运行的配置文件“注册表”，它保存了操作系统本身以及其他应用软件的配置信息，如果它被破坏了，整个操作系统将无法正常运转。

6. 应用软件配置文件

如同 Windows 操作系统一样，应用软件得以正常运行也需要配置文件，且大部分应用程序的配置文件也同样保存在注册表中，但有些比较特别的软件并非这样，而是保存在某个文件中（比较常见的如 ini 文件，就是专门保存程序配置的文件）。

7. 个人重要数据与文档等

这也是最重要的数据了，一般为数据档案或者办公文档之类，比如常用的 Office 系列文档、WPS 文档等。

虽然我们谈的是数据拯救，但防患于未然，我们还是建议你平时多做备份，尤其是对那些重要数据来说，更是需要如此，而以上所列举的这些，则给我们平时的备份提供了很好的参考，知道到底哪些数据最为重要，哪些最需要备份。

备注：以上各种数据、文件的详细介绍与具体备份、拯救操作方法，将在后面章节逐一介绍和讲解。

1.1.3 数据恢复一般采取的手段

我们在 1.1.1 节讨论引起数据丢失的各种原因，除了出现严重的硬件故障时，需要专业的技术人员进行修复、拯救外，其他数据丢失问题，大部分都可以利用各种手段来进行修复和拯救。针对不同的数据丢失原因和各自的现象，有其自己的特定方法，需要视具体情况而定。下面我们总结出了数据拯救的一般方法：

1. 特定工具法

针对一些常见的数据丢失问题，或者比较普遍发生的，一般都有相应的工具软件进行专门特定的修复，只要获得这些工具软件，并进行正确的设置和操作，都能比较顺利地拯救出我们的数据。比如有专门修复被 CIH 病毒破坏的硬盘的工具；有专门拯救文件误删除的反删除软件；专门修复被破坏的硬盘主引导记录的工具等等。

2. 手工操作法

在我们了解了数据丢失的原因，以及相关的拯救措施的情况下，完全可以自己手动进行修复（当然，也需要配合一些常用工具软件）。虽然有些情况下，已经有一些特定的工具可以进行修复，但如果我们知道其拯救原理与操作，则可以更有针对性地进行操作，自由度更大，比如我们在修复被损坏的主引导记录时，虽然有一些工具软件可以做到，但为了更好地有针对性地操作，完全可以自己手工进行操作。而对于一些没有专门工具的操作来说，也必须是用手工方式了。

3. 替换法

有些数据丢失后，存在有备份或者可替换的文件，则可以用其进行替换。比如丢失的操作系统文件，可以利用手工方法或者工具软件来提取安装盘上的文件来进行替换，从而达到拯救的目的。在比如新的 Windows ME/XP 操作系统游自动备份当前状态的高级功能，而我们在出现数据丢失问题后，则可以里利用它相关的工具进行修复和拯救操作。

在实际操作中，一般来说是根据具体情况来定方法，而且有时候会综合利用各种方法来达到目的。

1.1.4 数据恢复的一般过程与要点

先冷静下来，并做好记录和准备工作：当你的数据丢失以后，千万不要手忙脚乱。这种情况全球每天要发生几十万例，惊惶失措以及病急乱投医会进一步地加剧数据的损失是不明智的。你立即需要做的是：详细记下丢失的经过和现象；记下设备的系统时间；回忆介质的相关数据（重要文件的路径、重要文件最后一次存盘的时间、硬盘分区情况及各分区的大小）；记下你试图恢复系统的每一步操作过程。如果你采用过任何启动盘，

请保留，可能在修复中我们很需要它。另外，如果文件有密码，也应在修复前提供。

“刻舟求剑”，丢失后的备份工作：是的，听起来让人感觉奇怪，数据已经丢失过了，现在才来备份，岂不是“刻舟求剑”吗？其实，对于那些需要进行大量操作的复杂拯救来说，有可能在拯救过程使数据丢失问题更加恶化而导致前功尽弃。所以对于那些重要数据的数据拯救操作来说，在条件允许的情况下，最好能用一个空硬盘完全备份待操作的硬盘数据（利用 Ghost 克隆软件，可以很容易做到这一点），这样可以做到万无一失。

对症下药，正确操作：回忆那些数据或文件丢失，作了哪些操作，从而分析数据丢失原因，然后再对症下药。对于大部分数据丢失现象，在你现在看到的这本书里，都有详细的介绍，并且包括具体的拯救措施和注意事项等，而你需要做的就是，首先仔细阅读这些，按照其介绍的方法正确操作。如果万一由于拯救操作的失误导致问题进一步恶化，我们就可以利用上一步提到的硬盘备份来挽回（因此我们强烈建议在数据拯救操作之前进行“刻舟求剑”，特别是那些重要数据的拯救）。

天外有天：对于大部分的数据丢失问题，都可以自己解决，而如果是很罕见、棘手的复杂问题，而且数据格外重要，那么也不要急，现在的计算机服务做的很好，在国内已经有很多专业的数据拯救服务机构，还有很多国际专业公司也在国内设立了分支代理机构，包括硬件损坏在内的各种数据丢失问题，80% 的都能成功拯救和恢复。所以即便是遇到一些棘手问题，也有理由相信我们的数据是有很大希望被拯救恢复成功的。

1.2 浅谈加密与解密

1.2.1 什么是加密解密技术

灾难的来临让我们能充分体会提前备份以及事后修复、拯救的重要性，然而对于我们的重要数据来说，是不是平安无事的时候，就万无一失了呢？机密文件、商业资料和其他重要信息，个人的隐私信息等等数据，如果被人盗走而恶意利用所造成的损失，甚至比数据本身丢失更严重，而且也是无法直接挽回损失！而现在的黑客入侵、恶意破坏与盗窃，以及因为大意而造成资料被偷窥等等现象，已经是数据安全的另外一个大敌。

面对如此种种的危机，如何进行防范？系统、数据的加密，无疑是最妥善的方法之一，这种方法提前对保存有重要信息数据的计算机系统进行设防，阻止非法用户擅自闯入；并对数据本身进行各种加密，使原始数据不被他人利用。如此牢牢把关，达到无懈可击的境界，可以让我们的重要信息和数据安然无恙、万无一失！

那么什么是密码技术呢？密码技术包括两个方面的内容：密码编码学和密码分析学，即通常所说的加密和解密。两个方面相互联系，一方面，二者在加强密码分析的安全性上相互促进；另一方面，在实施有效的攻击时也相互影响。可以说加密和解密是一对孪生兄弟，但同时又是矛和盾的关系。

通过隐写术的具体应用，密码的安全作用才会体现出来。隐写术通常又分为语言隐写术和技术隐写术两种。关于隐写术在古代的武侠小说中有较多的体现，比如用不可见的墨水进行书写。现代密码编码学的实质即是高级语言隐写术的灵活应用。

符号码（通过可见方式隐藏秘密的书写方法）和公开代码（通过不可见方式隐藏秘密的书写方法）是语言隐写术的两种具体应用形式。在网络的通信应用中，大多采用类似于符号码的密钥（密码钥匙）加密方式，即把需要隐写的传输报文按照以密钥为参变量的函数进行转换，生成相应的密码文件，完成从明文到密文的转变，达到安全传输的目的。换言之，报文的明文形式按照某个函数（某个加密法则）的变化规则进行转换，转换成密文形式，而这个函数的变量即是密钥。解密则是遵循相应法则，以相同的密钥为参数将密文还原成明文。

总之，为了把我们的宝贵数据与资源保护起来，不被让其他人盗取或利用而采用的一系列措施，都是保密行为，而其中主要以数据的加密 / 解密为措施和手段，辅之以其他方法，达到保护数据安全的目的。

1.2.2 哪些数据需要加解密

加密和解密是相对来说的，有加密自然就有解密。下面我们重点讨论一下哪些数据需要加密的问题。

如同我们在上面小节谈到的关于“哪些数据需要拯救”一样，作为需要加密/解密的数据来说，一个广泛意义上的原则就是，重要数据或者保存有重要数据的介质与载体，都是加密/解密的对象。比如，我们的一个文档很重要，这属于重要数据范畴，而此文件被保存在我们的某个目录文件夹下，而这个文件夹又保存在我们的某个驱动器盘上（C盘、D盘），而所有的驱动器盘都是硬盘中的，而硬盘是整个计算机硬件的一部分，计算机硬件被放在办公室或者机房内……

上面从“范围”的概念出发，列出了一个逻辑关系，我们大致就可以看出我们到底需要对那些数据或者媒质进行数据保护了。下面我们再来具体分析一下：

计算机系统：也就是我们的整个计算机硬件、软件系统。而BIOS是计算机系统中硬件与软件的接口，也是最低层、最“高级”的软件，而我们通过对其进行设置口令，即可以达到对计算机系统的加密保护。

存储系统：这里的存储系统，指的是所有计算机数据的存储载体，比如我们常见的硬盘、光盘、软盘、优盘等等。既然他们都是计算机数据存储的“仓库”，那么把这个仓库大门保护好，不就达到了数据安全保护目的了吗？

操作系统：可以说操作系统就是计算机系统“大管家”，也是计算机系统与操作者之间的“联络员”，它直接掌管着我们所用的软件、硬件资源，而我们的数据自然也在它的“管辖”之内，所以对操作系统的安全加密保护，在一定意义上来说也就是间接地对我们的数据进行保护。

驱动器盘、文件夹：任何数据都是要保存在某个驱动器盘的某个目录下（或者磁盘根目录），而他们就是我们宝贵数据的最后一道大门，能否把好这道门，对保护我们的数据起到至关重要的作用。

数据文件：对于具体的数据文件来说，就是保存我们数据的地方，其范畴很广，可以说，只要是计算机中的文件，都在这个范畴之类。而常见的一些重要数据文件格式，比如Office、WPS文档、电子邮件、网页、图片、其他特定格式文件等等，都是最常见的文件，大多数重要数据信息都是这些格式的文件。

1.2.3 加解密采取的一般手段

我们从上节中讨论的各种需要加密/解密的对象来看，都有其相应的手段，而一般来说，有如下的各种手段来对数据进行各种有效的保护手段：

系统设置法：这里的系统，可以理解为计算机的核心软件系统“BIOS”和“操作系统”。由于他们自身都带有相应的数据防范保护措施，所以我们只要通过一些密码与安全设置，即能达到对数据进行保护的效果。比如我们可以通过BIOS设置密码来保护整个计算机资源，而通过操作系统来达到软件保护。

硬件加密法：利用一些特殊的专业硬件设备，来对计算机局部或整体资源进行保护，属于硬件加密。比如，现在市面上流行的加密狗、加密棒等设备，可以很好的对数据进行保护和加密。另外，通过将机箱上锁、将硬盘进行特殊硬件设置等等特殊方法，也可以认为是硬件加密保护法。

软件加密法：很多方法都可以笼统地归纳为软件加密法，但这里特指的是，利用第三方软件对数据进行特殊的编码，让数据改变其原“貌”的方法或进行加壳。比如，我们的文档通过软件加密后，其内容和原来的已经完全不一样，必须在解密以后才能看到原始内容；我们通过对应用程序进行加壳方式的软件加密，则此应用程序在运行原来的代码程序之前，会运行保护程序，要求输入密码才能运行，这些都属于软件加密的方法。

手工改造法：在了解了一些系统、软件的运作机制后，我们可以通过一些特殊的技巧来对数据进行隐藏类的保护措施，这种手段一般不属于通用、公开的方法，只是一种小技巧，但有时也能达到很好的效果。比如我们在Windows下，通过对文件夹设置特殊的属性并设置一些文件，就能达到对文件夹进行隐藏的保护效果。

实时保护法：这种方法并不对具体的数据进行加密保护，而是根据指定的设置，禁止用户对各种资源、数据的访问，从而达到实时的保护效果。比如著名的Pc Security软件，对系统进行实时保护，一旦设置好并让它起作用后，就可对整个计算机资源进行保护。

在本书的后面章节中，将介绍通过上面各种手段来对数据进行加密/解密保护的方法。

1.3 数据拯救和加解密流程

下面，我们按照电脑的启动前后顺序，给出了数据拯救和加解密的一般流程图，供大家在日常操作中参考：

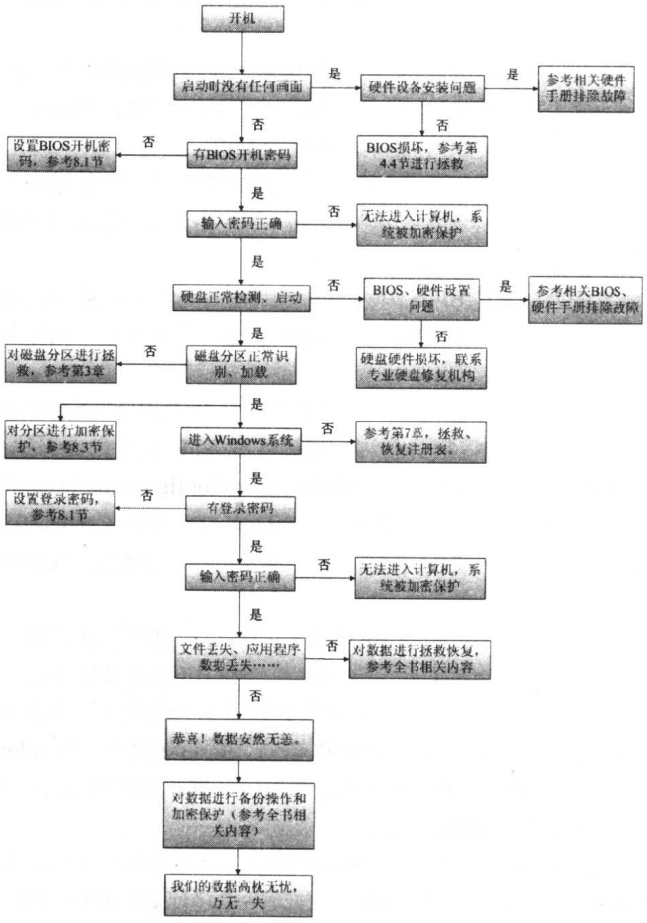


图1-2

从上图可以看出，电脑的启动过程中有一个非常完善的硬件自检机制。它在上电自检那短暂几秒钟里，就可以完成100多个检测步骤。所以，了解电脑启动的过程，对我们诊断电脑的故障是相当有帮助的。

步骤一： 当我们按下电源开关时，电源就开始向主板和其它设备供电，此时电压还不稳定，主板控制芯片组会向CPU发出一个Reset(重置)信号，让CPU初始化。当电源开始稳定供电后，芯片组便撤去Reset信号，CPU马上就从FFFF0H处开始执行指令，这个地址在系统BIOS的地址范围内，无论是Award BIOS还是AMI BIOS，放在这里的只是一条跳转指令，跳到系统BIOS中真正的启动代码处。

步骤二： 在这一步中，系统BIOS的启动代码首先要做的事情就是进行POST(Power On Self Test，加电自检)，POST的主要任务是检测系统中的一些关键设备是否存在和能否正常工作，如内存和显卡等。由于POST的检测过显卡初始化之前，因此如果在POST自检的过程中发现了一些致命错误，如没有找到内存或者内存有问题时(POST过程只检查64K常规内存)是无法在屏幕上显示出来的，这时系统POST可通过喇叭发声来报告

试读结束：需要全本请在线购买： www.ertongbook.com