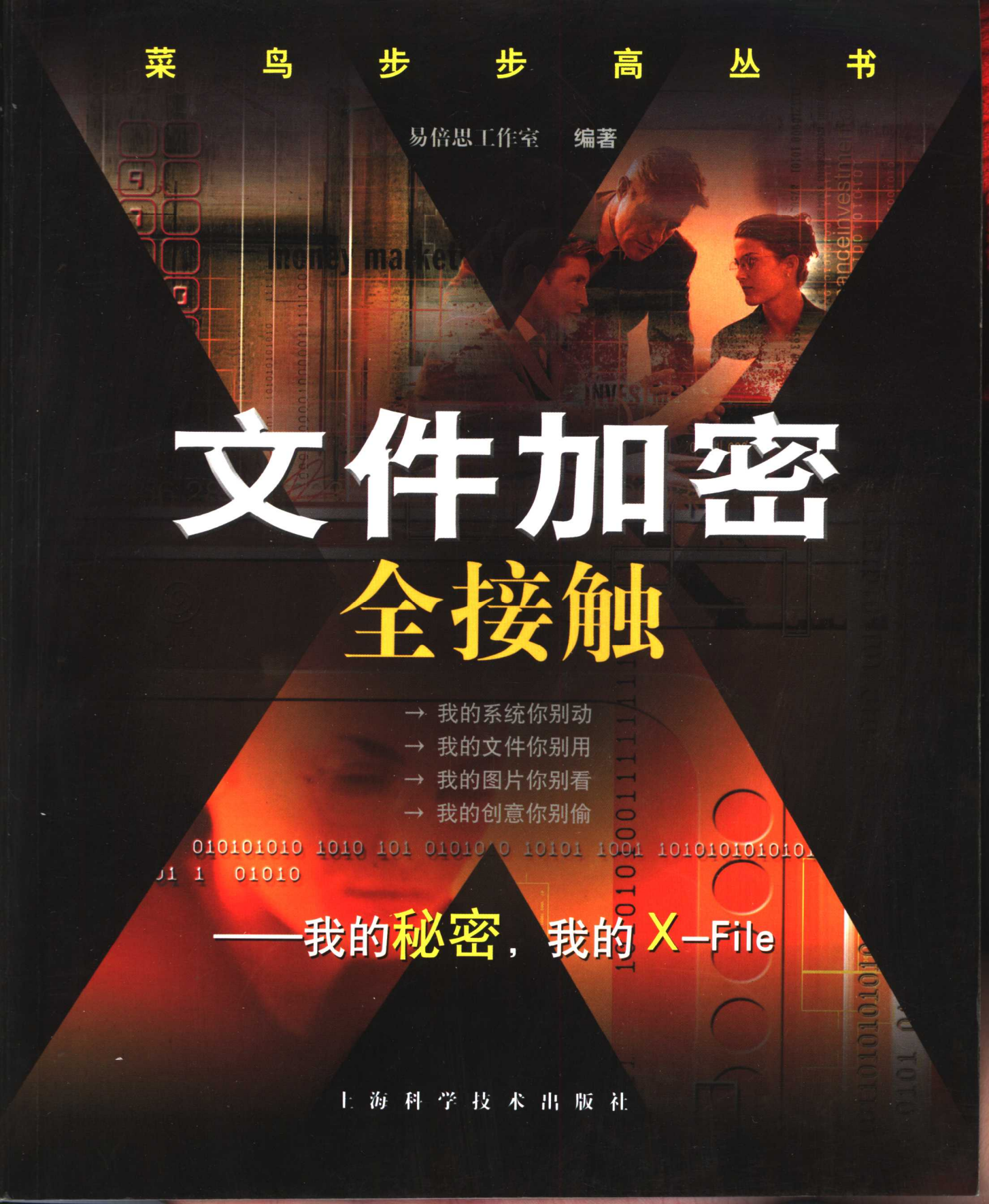
菜 鸟 步 步 高 丛 书

易倍思工作室 编著



文件加密全接触

→ 我的系统你别动
→ 我的文件你别用
→ 我的图片你别看
→ 我的创意你别偷

——我的秘密，我的X-File

上海科学技术出版社

《菜鸟步步高丛书》

文件加密全接触

易倍思工作室　编著

上海科学技术出版社

内 容 提 要

本书是《菜鸟步步高丛书》中的一册，全书以文件和系统的密码保护为主线，介绍了现在流行的加密技术，BIOS 和操作系统的加密方法，以及各种文件和应用程序的加密方法，最后介绍了密码被遗忘时的补救措施。全书循序渐进，步步深入，同时将读者在使用过程中容易忽略的细节问题和一些注意事项作了介绍，使读者可以更好地保护自己的隐私。

图书在版编目（CIP）数据

文件加密全接触 / 易倍思工作室编著. —上海：上海科学技术出版社，2003.11
（菜鸟步步高丛书）
ISBN 7-5323-7276-6

I. 文… II. 易… III. 电子计算机—密码—加密 IV. TP309.7

中国版本图书馆 CIP 数据核字（2003）第 087226 号

上海科学技术出版社出版、发行
（上海瑞金二路450号 邮政编码200020）
常熟市文化印刷有限公司印刷
新华书店上海发行所经销
开本 787×1092 1/16 印张 15.5 字数 350 000
2003年11月第1版 2003年11月第1次印刷
印数 1—5 200
ISBN 7-5323-7276-6/TP·312
定价：26.00元

实用电脑图书任你选

（元/册）

书　名	定价	光盘	书　名	定价	光盘
家庭电脑学校——基础篇	22		Phtoshop精彩创作实例	38	有
家庭电脑学校——办公篇	22		CorelDRAW精彩创作实例	40	有
家庭电脑学校——上网篇	22		Illustrator精彩创作实例	40	有
家庭电脑学校——工具篇	22		FreeHand精彩创作实例	40	有
家庭电脑学校——娱乐篇	22		DOS救命指令	12	
家庭电脑学校——影像篇	22		Windows快捷热键	12	
英汉计算机应用词典	25		Office快捷热键	12	
注册表实用手册	20		Excel函数实例	12	
Java2认证考试指南与试题解析	88	有	病毒防治便携手册	12	
电脑装机全接触	28		HTML实用标记	12	
系统安装全接触	30		Windows注册表	12	
电脑维护全接触	26		密码攻防秘笈	12	
硬件优化零距离	26		电脑救机手册	12	
个人服务器零距离	30		Flash动漫欣赏	15	
网路攻防零距离	28		五笔字型学习词典	25	有
Windows XP易学会（彩色）	18		跟我学五笔字型（第3版）	25	有
Word XP易学会（彩色）	18		五笔字型顺畅学习法（送字根表）	15	
Excel XP易学会（彩色）	18		五笔字型即查词典	10	
上网起步易学会（彩色）	18		DirectX9 3D图形程序设计	48	有
宽带上网易学会（彩色）	18		中文AutoCAD 2004基础教程	38	有
PowerPoint XP易学会（彩色）	18		热门网络游戏教你玩	20	
数码相机易学会（彩色）	18		手机铃声响叮当	10	
DV摄像易学会（彩色）	18		手机铃声哆来咪	14	

购书方法：

1. 直接到各地各大新华书店或去上海市瑞金二路448号（近打浦桥）上海科学技术出版社门市部购买。
2. 邮购请汇款到上海市瑞金二路450号（邮编200020），上海科学技术出版社邮购组，写清所需图书的书名、册数以及您的详细地址、邮编和电话，另外加收所购书款15%的挂号邮费（最低2元）。
3. 为了更好地服务于读者，欢迎来电咨询，电话：（021）64736055-2073，或访问上海科学技术出版社精品电脑图书频道：www.sstp.cn/computer.htm。

最新电脑图书推荐

“菜鸟步步高丛书”
《电脑装机全接触》
定价：28 元
如何挑选电脑配件与组装电脑

“菜鸟步步高丛书”
《系统安装全接触》
定价：30 元
如何分区与安装操作系统软件

“菜鸟步步高丛书”
《电脑维护全接触》
定价：26 元
如何对电脑进行维护和排除故障

“零距离丛书”
《硬件优化零距离》
定价：26 元
如何不花钱升级电脑的性能

“零距离丛书”
《个人服务器零距离》
定价：30 元
如何设立个人邮局和论坛服务器

“零距离丛书”
《网络攻防零距离》
定价：28 元
了解黑客攻击手段与防范措施

购书方法：

1. 直接到各地各大新华书店或去上海市瑞金二路 448 号（近打浦桥）上海科学技术出版社门市部购买。
2. 邮购请汇款到上海市瑞金二路 450 号（邮编 200020），上海科学技术出版社邮购组，写明所需图书的书名、册数以及您的详细地址、邮编和电话，另外加收所购书款 15%的挂号邮费。
3. 为了更好地服务于读者，欢迎来电咨询，电话：（021）64736055-2073，或访问上海科学技术出版社精品电脑图书频道：www.sstp.cn/computer.htm。

前　言

随着时代的进步，各行各业甚至个人的生活都与电脑密切相关，电脑作为一种现代化的高效工具，凭借其高速运算能力和海量储存能力，可以大大提高个人的工作效率。将个人资料以文件的形式保存在电脑中，将公司的会议记录储存在文件中，将设计好的程序保存在电脑中，将项目设计图纸以图片的形式储存在电脑内，这些机密的资料或数据都不想被第三者非法窥看，然而，越是机密的资料或数据，其“吸引力”就越大。

在什么情况下，电脑内的数据容易被盗用呢？事实上，只要使用电脑储存数据，无论是多人共用电脑、局域网环境、互联网环境，都有可能将自己电脑中的秘密大白于众人面前。对于没有任何保护措施的资料或数据，对非法盗用者来说，要得到它们简直是易如反掌，哪怕你的电脑是“个人电脑”，不连上任何网络，电脑内的数据依然不是安全的。

综上所述，为电脑内的资料以及数据加入保护措施势在必行，而目前最直接的数据保护措施就是加密，通过各种各样的加密技术，可以有效地防止数据被盗用。

本书正是基于电脑数据安全问题，有针对性地为读者介绍一系列的加密方法与操作，务求让每一位读者都掌握流行的加密保护技术。另外，对于一些基本的解密技术也有对应的介绍，以便供读者参照学习，提高应用水平。

本书的主要内容包括密码学与加密技术、BIOS 加密的方式、操作系统多用户的设置、增加操作系统安全性、锁定操作系统、加密/隐藏电脑中的驱动器、隐藏分区、利用系统加密隐藏文件、使用专业的加密软件加密文件、保护隐私图片的安全、办公文档的加密方法、使用 PGP 加密邮件以及密码管理技巧、密码破解恢复方式等，相信通过以上的内容，你的秘密就是你的 X-Files！

本书由易倍思工作室的马国平编写。由于时间仓促，编者的水平也有限，书中难免有疏忽和错误。我们热切地希望读者在使用本书的过程中提出宝贵意见并给予批评和指正。

读者在使用电脑中如遇到问题，可以登录 http://www.sstp.cn/computer.htm 网页中的“菜鸟学电脑论坛”，我们会尽力为您解答。

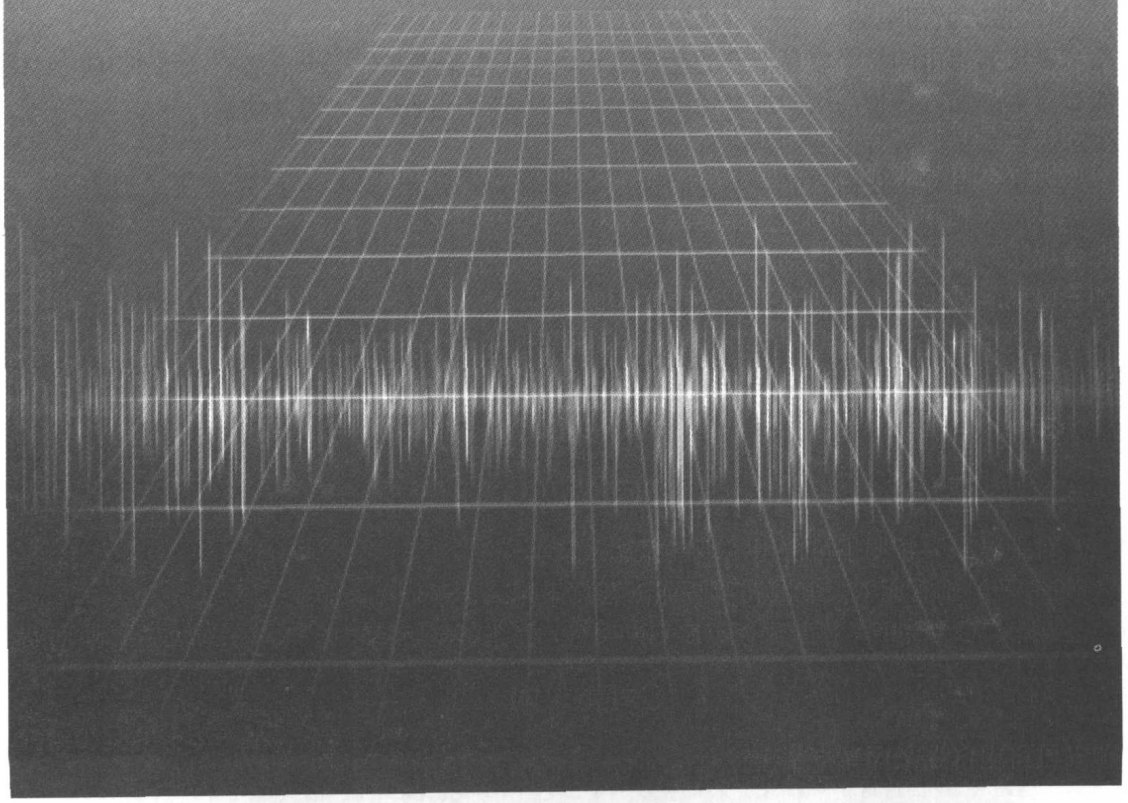
编者

2003 年 9 月

目 录

X-Files 第一季：密云不雨

初次接下加密任务的第一季，为了更好地开展加密工作，我们有必要先对加密来个理性认识。在第一个任务中可以了解到加密保护技术的基本概念、加密技术的现状等。完成了第一个任务后，我们就可以开始尝试对自己的电脑加入保密措施了，而第一道防线就是 BIOS 加密、操作系统加密等。接着，我们会假设第三者已通过了第一道防线，这时我们应该使用什么方法来防止数据泄密呢？在第三个任务中将会详细介绍亡羊补牢的方法。密云不雨，让我们进入加密的世界吧！



Mission 1 原来如此——了解加密保护技术

个人电脑作为一种现代化的数据处理/储存的工具，就好似银行中的保险柜一样，经常会存放一些非常重要的资料。现在，黑客和一些不怀好意的资料收集者经常躲在暗处，时刻准备偷窥别人的秘密，因此如何保护电脑中的数据安全就成为了一个不容忽视的问题。

为了保护电脑中的数据不被别人读取或窥视，从电脑诞生开始，就不断地出现各种加密保护技术，而本章将与读者一起探讨加密保护技术的现状，以及最常见的泄密途径。

通过本章，读者可以了解到：

- 常见的泄密途径
- 流行加密保护技术

1.1 泄密的途径

1. 多人共用电脑

多人共用电脑是最容易泄密的途径之一，由于电脑不是属于个人所有，每个用户都不能够对电脑加入各种高级的加密保护技术，数据安全形同虚设，而其他用户只要能够正常登录操作系统，所有重要的数据都会被一览无遗，此时，我们只能对重要的数据进行局部加密。

在多人共用电脑的情况下，如果使用的是 Windows 9X 操作系统，数据安全是最得不到保证的。虽然我们可以使用“用户”功能（如图 1-1 所示），在 Windows 9X 操作系统加入多用户设置，但由于操作系统本身的问题，其他用户仍然能够在不输入任何密码的情况下，在如图 1-2 所示的登录框中通过单击“取消”按钮进入操作系统，所以，数据安全根本得不到保障。

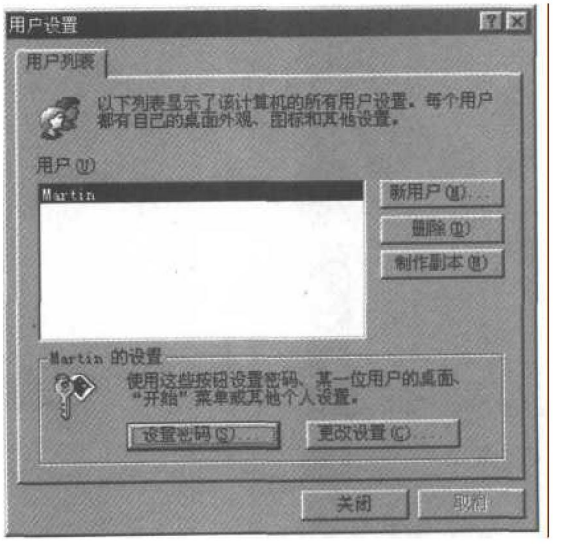


图 1-1

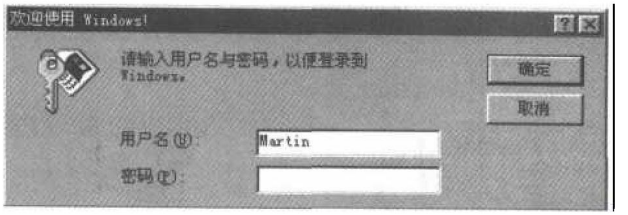


图 1-2

对于使用 Windows 2000/XP 的用户来说，通过多用户功能可以起到一定的保护措施，操作系统会为每一个用户设置不同的操作环境，而要进入该环境，必须输入正确的密码方可，否则用户就只能停留在登录窗口，如图 1-3 所示。

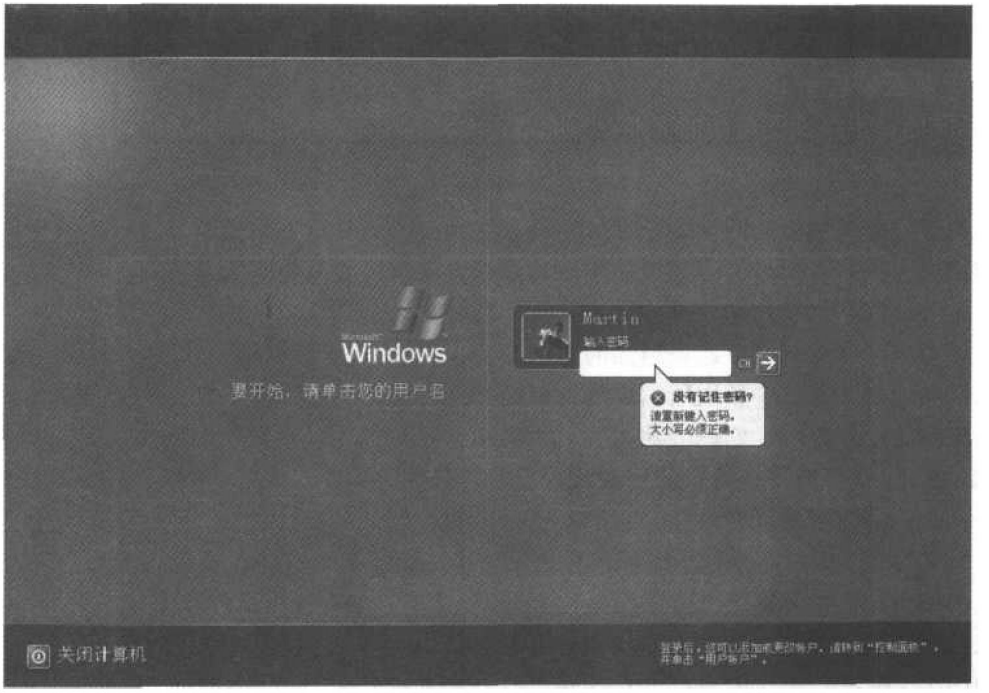


图 1-3

2. 局域网

局域网同样是一个容易泄密的途径，由于电脑在局域网中使用的时候，我们为了实现资源共享，都会将电脑中的某些文件夹设为“共享”，这样就无法避免自己电脑中数据或资料被别人读取或利用（如图 1-4 所示）。

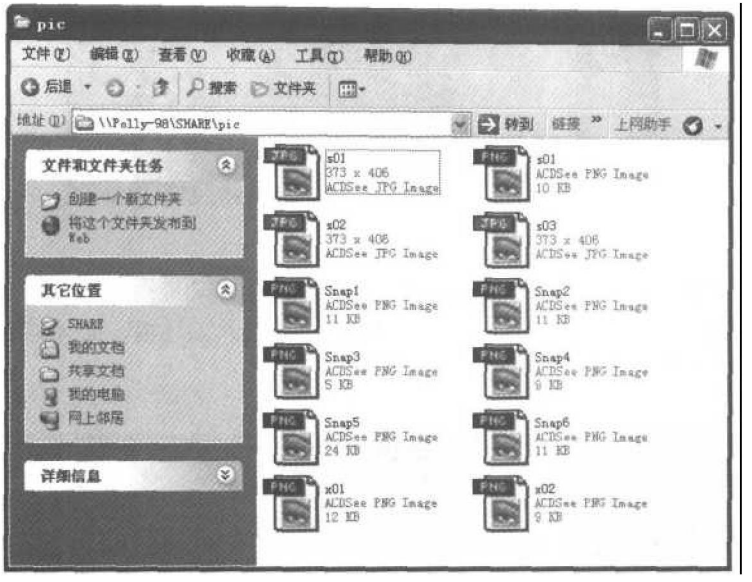


图 1-4

为了提高局域网的数据安全性，在设置文件夹的“共享”属性时，可以根据文件夹的内容来决定是否要通过密码才能访问。具体的方法可以参考后面的章节。

3. 互联网

随着互联网的普及，越来越多的电脑与互联网相连接，并从中获取所需的信息。而每当电脑连上互联网，它就会被无数只“眼睛”监视着，一旦发现有价值的资源或数据，有不良企图的监视者就有可能会开始入侵行动。

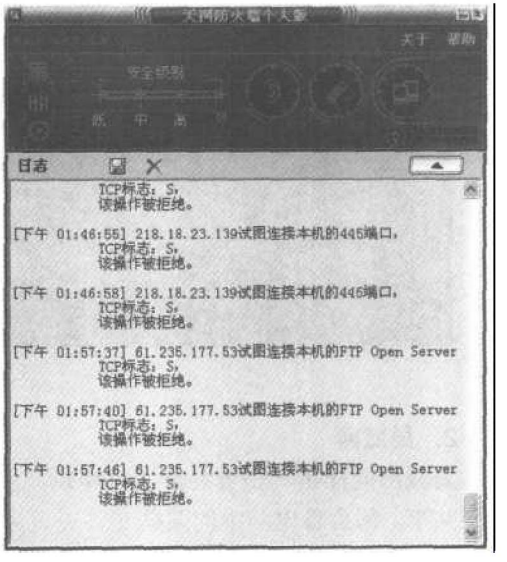


图 1-5

由此可见，电脑在连上互联网后，必须采取相应的措施来防止泄密，如安装防火墙（如图 1-5 所示）、不要随意打开互联网下载的文件等。

在这种泄密途径中，最危险的就是中了木马，一旦电脑被植入木马程序后，对方就可以远程控制你的电脑，所有重要的资料、数据甚至是银行帐号、密码等都可能泄漏给对方，损失无法估量。对于木马入侵这种情

况，我们可以使用专门的木马查杀软件来加强系统的安全性（如图 1-6 所示）。

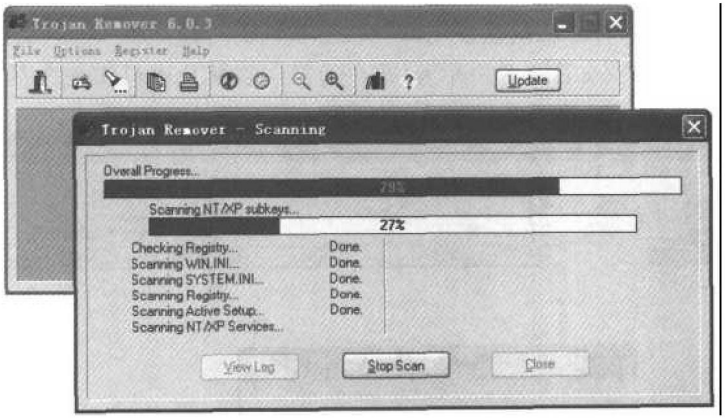


图 1-6

4．电子邮件

电子邮件现在日渐普及，用户可以用非常低廉的费用，将电子邮件发送到远方的亲友“手中”，而它的传送速度也是普通邮件无法相比的，但是，正因为电子邮件与网络挂钩，所以它的保密性就成为人们需要考虑的问题。就以最常用的邮件收发软件 Outlook Express 来说，系统默认进入 Outlook Express 无需输入密码，这样一来，其他用户就可以用你的电脑轻易打开你收过、发过的所有邮件（如图 1-7 所示）。

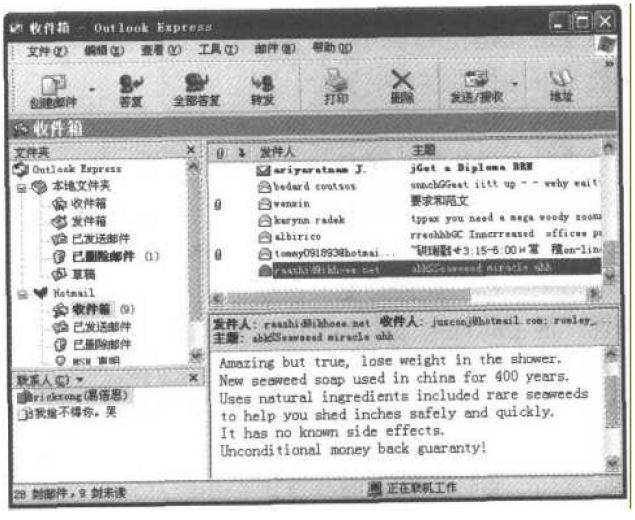


图 1-7

如果要减少电子邮件泄密的概率，我们可以使用以下两种方法：一种是直接在网页中开启邮件并在网上阅读，不要将邮件下载到本地电脑内（此种方法的工作效率不高，并且也不是完全保险）；另一种方法是在使用邮件收发软件的时候，加入密码访问功能，防止其他人随意阅读你的邮件（如图 1-8 所示），这种方法可以防止本机邮件内容被随意阅读。

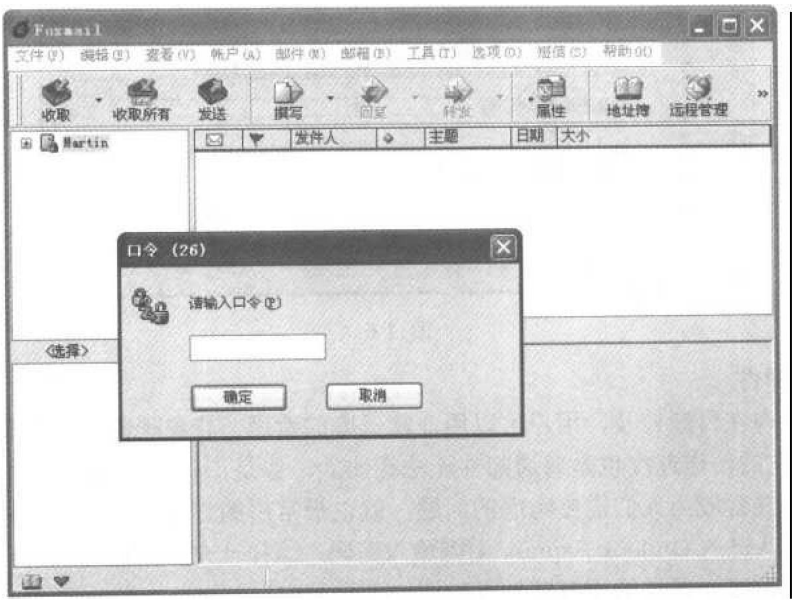


图 1-8

其实，最保险的方法应该是使用专门的加密软件，对邮件内容进行加密处理，这样，无论是阅读与传输都能更好地保证信息的安全。

5. 泄密的后果

电脑泄密到底会带来什么后果呢？这是一个看似很简单的问题，但实际上，泄密往往只是一个开始，因泄密而带来的一连串损失是无法预料的。例如，当电脑中的共享文件夹密码被破解后，入侵者就会通过此途径，使用种种手段，以获得电脑内的更多资料，只要是储存在电脑中的其他密码，都可能轻易地被窃取。

对于商业用户来说，泄密的危害比个人用户更大，例如，机密文件一旦被盗取，商机就从此失去；如果是设计图纸被泄漏，辛辛苦苦设计出来的效果就会被抄袭。以上只是针对个人用户和商业用户而言，如果泄密涉及到国家机密和军事等内容，其危害就更加无法估计了。

所以，为了确保信息的安全性，对重要信息进行加密处理是非常必要的，因为泄密所带来的损失可能没有谁能够负担得起。

1.2 初探信息加密技术

1.2.1 密码学概述

1. 什么是密码学

所谓密码学是一门研究加密与解密的学科，它以秘密通信为目的，研究信息通过何种秘密的变换后，使第三者无法获取源信息，避免机密信息被窃取。最初的变换技术可以追溯到古代希腊战争时传送军事指挥命令使用的卷筒阅读方法，而近代发明的“摩氏密码”则改为用不同长短的信号实现秘密通信。

密码学可分为两个分支，一个是研究并编制密码以保守通信秘密的，我们称为“编码学”；而另一个则是以破译密码获取通信情报为目的的“破译学”。密码学是在编码与破译的斗争中逐步发展起来的，并随着先进科学技术的应用，已成为一门综合性的尖端技术科学，与语言学、数学、电子学、声学、信息论、计算机科学等有着广泛而密切的联系。密码学的现实研究成果，特别是各国政府现用的密码编制及破译手段，都具有高度的机密性。

> **小知识**：作为在信息技术领域占主导地位的美国，一直对加密技术的出口进行限制，令别的国家不能采用较安全的先进加密技术，美联邦政府特别标明，密钥属于武器出口限制的范围，由此可见密码学和密钥算法的研究工作的艰巨性。

众所周知，计算机在网络中的公共信道通信是非常脆弱的，公共信道中的信息很容易被偷窃、复制或非法删除、更改等操作。随着网络的普及化，我们对信息的安全提出了更高的要求，而信息加密就是最有效的一种方法。

2. 密码学中的常用术语

在讲解信息加密技术的时候会遇到许多较为专业的术语，为了方便读者的理解，我们将几个常用的术语作简单的介绍。

明文：一般人够能看得懂的信息或文本，也就是源信息；

密文：通过变换技术（加密技术），由明文变换过来的、一般人看不懂的信息或文本；

加密：将明文变换成为密文的过程；

解密：将密文还原成为明文的过程；

密码体制：用于加密和解密的算法；

密钥：由使用密码体制的用户随机选取的、唯一能控制明文与密文之间变换的关键，它通常是一随机字符串。

3. 加密的表达式

既然加密是一种算法，那么我们就可以用一个表达式来表示加密的过程，一般来说，加密可以用以下表达式来表示：

$$C=E_K（M）$$

其中，C（Code）代表密文；E（Encrypt）代表变换过程；K（Key）代表密钥；而 M（Message）则是明文，其意思就是明文经过密钥产生变换，成为了密文。

对于解密，我们也可以用一个表达式来表示：

$$M=D_K（C）$$

其中，C 同样为密文，M 为明文，K 代表密钥，D（Decrypt）代表变解密过程，所以，我们必须获得密文与密钥，才能够恢复出明文。

从以上表达式可以看出，加密或解密变换是由一个密钥来控制的，如果获得密钥的话，加密或解密都很简单，而对于不知道密钥的第三者，要解出明文的话，就是一件相当困难的事情了。哪怕第三者得到了密文，他也必须先获得密钥，才能够变换出明文。

举一个相当简单的例子，假设明文是“Welcome to Shanghai”，我们将每一个英文字母对应的 ASCII 码值加 2，从而获得密文“Ygneqog vq Ujcpijck”。这样，对于不知道加密算法的第三者是很难确切恢复出明文的。

1.2.2 常用加密技术解析

1. 加密体制的分类

我们可以按照不同的加密体制以及不同的标准，将密码划分为不同的类别。

（1）按密钥来划分

对称加密系统：指加密与解密时使用的密钥是相同的，加密与解密者必须获得该密钥才能够进行相应的操作。

非对称加密系统：指加密与解密使用不同的密钥（公钥与私钥），即在加密的时候使用公钥，而解密则必须使用私钥。

（2）按应用技术或历史发展阶段来划分

手工密码：以手工方式完成加密作业，或者以简单器具辅助操作的密码，第一次世界大战前主要是这种作业形式。

机械密码：以机械密码机或电动密码机来完成加密和解密作业的密码，这种密码从第一次世界大战出现到第二次世界大战中得到普遍应用。

电子机内乱密码：通过电子电路，以严格的程序进行逻辑运算，以少量制乱元素生产