化蝶丛书

# 金屋藏娇

## ——电脑加密技巧

陈益材　耿国续　编著



海洋出版社

# 金屋藏娇

## ——电脑加密技巧

陈益材　耿国俊　编著

海洋出版社

2004年·北京

**图书在版编目（CIP）数据**

金屋藏娇：电脑加密技巧/ 陈益材，耿国续编著.
北京：海洋出版社，2004.4
(网虫化蝶丛书)
ISBN 7-5027-5313-3

Ⅰ. 金… Ⅱ. ①陈… ②耿… 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(2004) 第 014551 号

**责任编辑：高朝君**
**责任印制：严国晋**
http://www.oceanpress.com.cn
**海洋出版社** 出版发行
(100081 北京市海淀区大慧寺路 8 号)
**北京玥实印刷有限公司印刷**
2004 年 4 月第 1 版 2004 年 4 月北京第 1 次印刷
开本：850mm ×1168mm 1/48 印张：5.5
字数：150 千字 印数：6 000 册
定价：12.00 元
**海洋版图书印、装错误可随时退换**

# 前 言

电脑技术和网络技术的发展，带来了人类历史上空前广泛的联合与沟通，但同时，个人数据、文档的隐密性也成为不可忽视的问题。尤其是办公室一族，公用电脑中重要的个人数据、文档的安全尤其令人担心，加密技术由此而生。

不懂！没关系，只要你具备电脑的基本操作能力，本书将一步一步地带你进入电脑加密的世界。

本书中有多处用到了 *Be Careful* 图标（小心，注意），这些地方往往是需要读者特别注意的地方，否则会带来时间、精力、甚至是金钱的损失，千万 *Be Careful*。

本书由陈益材、耿国续编写，同时参加写作的还有郑木兰、姜帆、李瑞奕、程冉、赵军轩、朱天祥、傅鹏等。由于作者水平有限，加之创作时间仓促，本书疏漏之处在所难免，欢迎各位读者与专家批评指正。如有更佳经验，或对《网虫化蝶》丛书有好的建议与意见，欢迎与我们联系，以便更好地服务于广大计算

机爱好者。

编著者

2004 年 4 月

编者信箱：chgwsry@hotmail.com

技术支持信箱：haiwangzi2002@163.com

# 目 次







# 第1章

## 加密技术的“秘密”

当今社会是一个互动的社会，网络技术越发达，人与人之间的联系越密切。不管是针对办公室的开放办公，还是针对小型局域网办公，关于个人文件的保护问题已经提到了一个全新的课题上。对于个人而言，在面对越来越开放的办公形式，如果你的计算机上有些个人隐私，该如何加强自我保护意识呢？就目前的计算机技术而言，只有加密才能保证个人电脑的相对安全。

下面我们就先了解一下加密知识的方方面面，希望能为那些对加密技术还不是很清楚的朋友提供一个了解的机会！

# 1.1 加密的意义

加密作为保障数据安全的一种方式，并不是现在才有的，它产生的历史相当久远，起源要追溯于公元前2000 年（几十个世纪了），虽然不是现在我们所讲的加密技术（甚至不叫加密），但作为一种加密的概念，确实很早就诞生了。从大的方面来说加密关系到国家的国防建设，从小的方面来说加密可以加强个人隐私权的保护。

## 1.1.1 加密有利于加强国防建设

早期加密技术主要应用于军事领域，如美国独立战争、美国内战和两次世界大战。最广为人知的编码机器是 German Enigma 机，在第二次世界大战中德国人利用它创建了加密信息。此后，由于 Alan Turing 和 Ultra 计划以及许多人的努力，终于对德国人的密码进行了破解。当初，计算机的研究就是为了破解德国人的密码，人们并没有想到计算机给今天带来的信息革命。当今社会，随着计算机的不断发展，运算能力的不断增强，过

去设置的密码都变得十分简单而易被破译了，于是人们又不断地研究出了新的数据加密方式来加强自己的计算机的安全性，如利用 ROSA 算法产生的私钥和公钥就是在这个基础上产生的。随着计算机网络的逐步发展，网络信息安全也变得日益重要了，于是加密术也被提上了日程，加密术的提高更加有利于人们对自己的隐私的保护。

### 1.1.2 加密有利于保护个人的隐私权

在当今网络社会中为了自己的安全，除了加密别无选择。一方面在互联网上进行 ftp 文件传输、E-mail 电子邮件商务往来等过程中存在许多不安全的因素，特别是对于一些大公司和一些机密文件在网络上传输。只要别人知道你的 ftp 地址，对应的 ftp 文件传输协议就会被别人匿名盗用，而且这种不安全性又是互联网存在基础——TCP/IP 协议所固有的，包括一些基于 TCP/IP 的服务；另一方面，互联网给众多的商家带来了无限的商机，互联网把全世界连在了一起，走向互联网就意味着走向了世界，这对于无数商家无疑是梦寐以求的好事，

特别是对于中小企业。但同时由于自身的条件限制，网络安全不可能有那些大公司做得好，于是网络安全又成了问题，为了解决这一对矛盾，为了能在安全的基础上打开这通向世界之门，我们只好选择数据加密和基于加密技术的数字签名。

加密在网络上的作用就是防止有用或私有化的信息在网络上被拦截和窃取。一个简单的例子就是密码的传输，计算机密码极为重要，许多安全防护体系是基于密码的，密码的泄露在某种意义上来讲意味着其安全体系的全面崩溃。

通过网络进行登录时，所键入的密码以明文的形式被传输到服务器，而网络上的窃听是一件极为容易的事情，所以很有可能黑客会窃取到用户的密码，如果用户是 Root 用户或 Administrator 用户，那后果将是极为严重的。

解决上述难题的方案就是加密，加密后的口令即使被黑客获得也是不可读的，加密后的标书没有收件人的私钥也就无法解开，因为标书已成为一大堆无任何实际意义的乱码。

在这里需要强调一点的就是，文件加密其实不只用于电子邮件或网络上的文件传输，其实也可用于静态的文件保护，如 PIP 软件就可以对磁盘、硬盘中的文件或文件夹进行加密，以防他人窃取其中的信息。

总之，无论是单位还是个人，在某种意义上来说，加密也成为当今网络社会进行文件或邮件安全传输的时代象征！

加密吧！对自己的文件加密，从某种意义上说就是为自己创造财富。

## 1.2 加密的分类

加密的分类还是比较多的，下面先从三个不同的角度来了解一下加密的分类及方法。

(1) 从专业的角度来分类

加密技术通常分为两大类：对称式和非对称式。

对称式加密就是加密和解密使用同一个密钥，通常称之为“Session Key”。这种加密技术目前被广泛采用，如美国政府所采用的 DES 加密标准就是一种典型的对称

式加密法，它的 Session Key 长度为 56bits。

非对称式加密就是加密和解密所使用的不是同一个密钥，通常有两个密钥，称为“公钥”和“私钥”，它们两个必须配对使用，否则不能打开加密文件。这里的公钥是指可以对外公布的，私钥则不能，只能由持有人一个人知道。它的优越性就在这里，因为对称式的加密方法如果是在网络上传输加密文件就很难把密钥告诉对方，不管用什么方法都有可能被别人窃听到。而非对称式的加密方法有两个密钥，且其中的“公钥”是可以公开的，也就不怕别人知道，收件人解密时只要用自己的私钥就可以，这样就很好地避免了密钥传输的安全性问题。

(2) 从操作角度来分类

将信息打乱成为不可读的格式，再将打乱的信息重新构造起来。加密的过程是将明码（可以阅读的信息，也就是普通的文本）转换成密码（看起来完全是任意的一序列位或字符）的过程。解密是上述过程的相反过程。多数系统使用的密码术都包括加密和解密两个方面，但是有时候也使用单方向的加密方法，但这种方法只限于

个人使用。

大多数现代加密算法要求在加密的过程中使用一个关键字作为一部分。有些算法是可逆的，在对信息加密和解密的时候使用同一个关键字。由于这个特征，这些算法被称为是对称的。因为任何知道关键字的人都能破译这种信息，因此这些对称算法的安全性完全依赖于关键字的安全性。因为对称型加密术已经使用了很长一段时间，因此它被称为传统加密术。DES（数字加密术标准）是对称加密术算法中使用最多的。

还有一些加密术根本就不依靠关键字，它是把普通的文本信息通过一定的方法转换成不能被破译的密码。这些方法称为单程函数，例如单程的随机函数，在保护数据系统方面有一些用途，但是它们通常不用于通讯安全方面。

(3) 从个人的加密操作手法来分类

上面所讲的可能专业性太强了一点，对于你来说可能看不懂，所以我们特别列出了这一类，本书所要介绍的就是这里面介绍的一些针对个人的实用的加密方法。常用的一些加密方法归类如下：