瀚文工作室　编著

电脑行家一点通丛书

加密与破解行家一点通

机械工业出版社
CHINA MACHINE PRESS

电脑行家一点通丛书

加密与破解行家一点通

瀚文工作室　编著

机械工业出版社

信息技术的迅速发展，给人们带来巨大便利的同时，也带来了巨大的安全隐患。邮箱密码、QQ 密码、重要的文档资料都存储在计算机上，如何有效的保证这些数据的安全，困扰着每一位电脑用户。但这些问题又具有一些专业性，对于普通的网络用户，往往是望尘莫及，甚至是无能为力。

本书为适应广大普通读者的需求，从实用的角度出发，力求为读者奉献一本简单易懂，实用性强的专题图书，可以让读者自己也能安全地对计算机进行多层次全方位的加密，在忘记密码的时候，选择合适的方法、适当的工具恢复密码，找回机密的数据。

图书在版编目（CIP）数据

加密与破解行家一点通/瀚文工作室编著.—北京：机械工业出版社，2003.4
（电脑行家一点通丛书）
ISBN 7-111-11862-6

Ⅰ.加… Ⅱ.瀚… Ⅲ.电子计算机—安全技术—基本知识 Ⅳ.TP309.7

中国版本图书馆 CIP 数据核字（2003）第 019033 号

机械工业出版社（北京市百万庄大街 22 号 邮政编码 100037）
策　　划：胡毓坚
责任编辑：孙　业
责任印制：付方敏

北京中加印刷有限公司印刷 · 新华书店北京发行所发行

2003 年 4 月第 1 版 · 第 1 次印刷
787mm×1092mm 1/16 · 11.5 印张 · 282 千字
0001—5000 册
定价：18.00 元

丛 书 序

当 CPU 的运算速度与网络的传输速度竞相加快时，我们需要学会更聪明地使用电脑，更快捷地解决问题。随着电脑的普及，很多人从对电脑一无所知到成为电脑的初级用户甚至玩家，很多人可能觉得电脑操作很简单，即使不学习也完全可以应付日常的工作了。其实，在电脑操作的过程中还有很多经验技巧可以总结。

每个人在使用了一段时间的电脑之后，都会从各种渠道了解到一些电脑操作技巧，有些是自己无意间发现的，有些是从朋友口中听说的，还有的是从杂志或网络上了解的。无论是从哪里了解到的技巧知识，都是很多人经过很长时间的使用得出的经验，当然也都能使我们的操作提高效率。但是，这些知识技巧都很零散，有的时候，也会由于很长时间用不到而忘记，等到用的时候又不知从何找起。那么，有没有一本书能把这些好的技巧收集起来，并进行分类，能够放在手边，随时可以翻阅查找呢？

就这样，“电脑行家一点通丛书”诞生了。

本系列丛书主要有以下特点：

1．主题专一

本丛书将当前最时尚的计算机及网络应用依据其自身特点分成 Windows XP、加密与破解、光盘刻录、宽带网、网络下载、网络聊天等专题。同时还将最实用的计算机技能（电脑快捷操作、系统安装、网络设置）纳入进来。本丛书中的每一册只讲解单一主题，因此可以较全面地涉及与本专题有关的知识和技巧。

2．易读易上手

本丛书完全采用步骤式的讲解方法，图文结合紧密，没有长篇累牍的理论，只有按部就班的实例操作，强调应用技能的快速掌握，绝对简单易读，易于上手。“电脑行家一点通丛书”所讲解的内容均是在电脑操作过程中常遇到的问题，也是最能提高电脑操作效率的方法，是广大电脑用户最需要学习的知识和技巧。在内容结构的安排上，分类明确，每一节为一个知识点（即一个技巧），每个知识点的内容相对独立，无论是全书通览还是单独阅读都不会影响对知识的理解和掌握。

3．篇幅短小

由于现代人的工作和生活节奏越来越快，尤其是广大的电脑用户，几乎已经没有时间再去“啃”那些又厚又枯燥的教程，而是需要迅速地补充知识，这也是编写本丛书所遵循的原则。由于本丛书的内容完全可能成为读者日常的必备速查手册或案头书，所以力求篇幅短小，以便于快速阅读，迅速掌握。

能够迅速提高电脑应用的水平，像高手一样解决棘手的问题，一直是广大电脑用户所期望的。“电脑行家一点通丛书” 将为您晋级高手行列提供一条崭新的捷径。

编 者

前　言

有些时候，一些重要的文件不想被人看见；一些商业机密不想被人知道；甚至自己的电脑设置也不想让人窥视，应该怎么办呢？这就需要对电脑系统或文件进行加密。本书的内容就是告诉读者如何防止“别有用心”的人“窥视”自己的电脑，以及如何防止“蓄意破坏”的人“侵入”电脑。

还有些时候，比如使用共享软件，通常会有使用日期或次数的限制，或者每次启动时都出现注册画面，厂家的目的是希望用户试用了这些软件之后，愿意付钱购买，但这些共享软件通常内容很庞杂，往往在我们还来不及对所有功能全盘了解之前，使用期限已经结束。对于消费者来说，在对这个软件还不够了解时就购买，确实有点强人所难。

除了使用软件的诸多限制之外，广告泛滥也是个恼人的问题，每每打开E-mail信箱，经常会看到满篇的广告邮件，而且有些广告重复发送，这样，删除这些垃圾邮件就会浪费很多宝贵的时间。有时打开ICQ与朋友聊天，闪烁的横幅广告令人心烦，或者突然莫名其妙地出现一则广告，一下子扰乱了好心情，可见网络上的广告真是无孔不入。

但这些问题都没有黑客恐怖，黑客会通过网络恣意入侵和操纵别人的电脑，但被操纵的人却浑然不觉。在网络时代，我们虽然每天体验着网络带来的无限便利，同时又要经受E-mail信箱和ICQ被无数信息灌爆、密码被盗用、信件被偷看，甚至电脑文件被窃取、硬盘被格式化的危险。就在最近，美国还有至少四个州的大学校园网络被黑客入侵，犯罪分子试图借此“捕猎”信用卡的帐号和密码。

那么以上这些问题到底该如何解决呢？本书就针对以上问题，为读者讲解全套的解决方案，帮助读者扫除网络世界的种种阻碍和危险。

由于编写者水平有限，加之编写时间匆忙，在选材和内容上恐有不当之处，恳请读者给予批评指正。

编　者

目　录

第1章

加密与解密基础知识

本章将为读者介绍一些加密与解密的基础知识，这些内容会有助于更好地理解加密与解密的过程，能为读者系统地学习加密与破解的知识。当然，对理论内容不感兴趣的读者也可以略过这一章，并不影响对全书内容的理解。

Chapter 1

1.1 加密技术原理

1.1.1 密码学概述

密码学以研究秘密通信为目的，即研究对传输信息采取何种秘密的变换以防止第三者对信息的窃取。

保密有载体保密和通信保密两种。密码学主要研究通信保密，而且仅限于数据通信保密。

不安全的密码技术比没有还要坏，因为它给人们以安全的假象。

由于传输中的公共信道和存储的计算机系统非常脆弱，容易受到被动攻击（从传输信道上截取或从存储载体上偷窃、拷贝信息）和主动攻击（对在传输过程中或在存储载体上的信息进行非法的删除、更改、插入等操作）。对于这两种攻击，密码技术是一种有效的办法。事实证明，这是最经济可行的办法。它在一种潜在不安全的环境中保证通信的安全。

近代密码学并不是传统密码学的旧话重提，它有新的特点。快速计算机和现代数学方法的广泛应用一方面为密码技术提供了新的工具和概念，另一方面也给破译者以有力武器。

密码加密算法的对立面就是密码分析，也就是密码的破译技术研究。加密与破译是一对矛盾，是相辅相成的，了解破译对研究加密是非常必要的。

1.1.2 密码的基本概念

密码就是一组含有参数 k 的变换 E。设已知信息 m，通过变换 E 得到密文 c，即

$c=E_k(m)$

这个过程称之为加密，参数 k 称为密钥。

不是所有含参数 k 的变换都可以作为密码，它要求计算 $E_k(m)$ 不困难；而且若第三者不掌握密钥 k，即使截获了密文 c，他也无法从 c 恢复信息 m。

从密文 c 恢复明文 m 的过程称之为解密。解密算法 D 是加密算法 E 的逆运算，解密算法也是含参数 k 的变换。

传统密码加密的密钥 k 和解密的密钥 k 是相同的，所以也叫对称密码。通信双方用的密钥 k 是通过秘密方式由双方私下约定产生的，只能由通信双方秘密掌握。

1.1.3 加密技术简介

在计算机上实现的数据加密，其加密或解密变换是由密钥控制实现的。密钥（Keyword）是用户按照一种密码体制随机选取，它通常是一随机字符串，是控制明文和密文变换的惟一参数。

1．加密体制及比较

根据密钥类型不同将现代密码技术分为两类：一类是对称加密（秘密钥匙加密）系统，另一类是公开密钥加密（非对称加密）系统。

对称钥匙加密系统是加密和解密均采用同一把秘密钥匙，而且通信双方都必须获得这把钥匙，并保持钥匙的秘密。

对称密码系统的安全性依赖于以下两个因素：

（1）加密算法必须是足够强的，仅仅基于密文本身去解密信息在实践上是不可能的；

（2）加密方法的安全性依赖于密钥的秘密性，而不是算法的秘密性。

因此，我们没有必要确保算法的秘密性，而需要保证密钥的秘密性。对称加密系统的算法实现速度极快，从 AES 候选算法的测试结果看，软件实现的速度都达到了每秒数兆或数十兆比特。对称密码系统的这些特点使其有着广泛的应用。因为算法不需要保密，所以制造商可以开发出低成本的芯片以实现数据加密。这些芯片有着广泛的应用，适合于大规模生产。

对称加密系统最大的问题是密钥的分发和管理非常复杂、代价高昂。比如对于具有 n 个用户的网络，需要 $n(n-1)/2$ 个密钥，在用户群不是很大的情况下，对称加密系统是有效的。但是对于大型网络，当用户群很大，分布很广时，密钥的分配和保存就成了大问题。对称加密算法另一个缺点是不能实现数字签名。公开密钥加密系统采用的加密钥匙（公钥）和解密钥匙（私钥）是不同的。由于加密钥匙是公开的，密钥的分配和管理就很简单，比如对于具有 n 个用户的网络，仅需要 2n 个密钥。公开密钥加密系统还能够很容易地实现数字签名，因此，最适合于电子商务应用需要。在实际应用中，公开密钥加密系统并没有完全取代对称密钥加密系统，这是因为公开密钥加密系统是基于尖端的数学难题，计算非常复杂，它的安全性更高，但它实现速度却远赶不上对称密钥加密系统。在实际应用中可利用二者的各自优点，采用对称加密系统加密文件，采用公开密钥加密系统加密“加密文件”的密钥（会话密钥），这就是混合加密系统，它较好地解决了运算速度问题和密钥分配管理问题。因此，公钥密码体制通常被用来加密关键性的、核心的机密数据，而对称密码体制通常被用来加密大量的数据。

2．对称密码加密系统

对称加密系统最著名的是美国数据加密标准 DES、AES（高级加密标准）和欧洲数据加密标准 IDEA。1977 年美国国家标准局正式公布实施了美国的数据加密标准 DES，公开它的加密算法，并批准用于非机密单位和商业上的保密通信。随后 DES 成为全世界使用最广泛的加密标准。加密与解密的密钥和流程是完全相同的，区别仅仅是加密与解密使用的子密钥序列的施加顺序刚好相反。

3．公钥密码加密系统

自公钥加密问世以来，学者们提出了许多种公钥加密方法，它们的安全性都是基于复杂的数学难题。根据所基于的数学难题来分类，有以下三类系统目前被认为是安全和有效的：大整数因子分解系统(具有代表性的有 RSA)、椭圆曲线离散对数系统（ECC）和离散对数系统（具有代表性的有 DSA)。

当前最著名、应用最广泛的公钥系统 RSA 是由 Rivet、Shamir、Adelman 提出的（简称为 RSA 系统），它的安全性是基于大整数因子分解的困难性，而大整数因子分解问题是数学上的著名难题，至今没有有效的方法予以解决，因此可以确保 RSA 算法的安全性。RSA 系统是公钥系统的最具有典型意义的方法，大多数使用公钥密码进行加密和数字签名的产品和标准使用的都是 RSA 算法。

1.1.4 密码研究现状

随着 Internet 的商务应用的增长，对安全的和受信任的信息基础设施的需要也在不断

的增长。没有一个安全的和受信任的基础设施，公司或者个人就不会愿意把他们的私有业务和个人信息放到网上来。安全的、受信任的应用平台应提供以下功能：

- 保护文件不被盗窃、不被非法获取；
- 保护通信不被截获；
- 保证安全的商务交易；
- 保证一个文件或者是信息的内容没有被修改（完整性）；
- 提供安全合理的身份认证；
- 产生有法律意义的签名（数字签名）。

加密技术是保证信息安全的一个必不可少的手段。所谓加密是使用数学过程来组织数据，使得除了合法的接收者，任何其他人要想恢复原先的“明文”，即使不是不可能的，也是非常困难的。这样实现的一个加密就可以使一些重要数据存储在一台不太安全的计算机上，或者可以在一个不太安全的网络上传送。只有持有正确密钥的一方才能够获得“明文”。

1．加密技术的核心就是密码技术

早期人们重视密码是为了军事、政治、外交的信息保密。密码一度成为官方专有的技术，民间不允许使用。随着计算机网络的社会普及应用，特别是 Internet 网的全球普及，人们看到了密码对解决信息安全所要求的保密性、完整性、可用性、可控性和不可否认性都具有有效的能力。社会应用密码成为公众的广泛要求。虽然，在政策法规方面世界各国还没有统一的认识和处理的办法，人们对管理的办法还有许多争论，但是，在进入信息社会后，社会公众也需要密码已经成为基本的共识。

政府、军队对密码的研究一直特别关注，据透露，在美国情报部门工作的高素质的密码专家就有万人之多。20 世纪 70 年代以来，在民间从事密码研究、开发、生产的机构和人员也大大增加。各个从事信息产业的公司，高等院校的学者学生，从研究数学应用的角度或从研究计算机安全的角度参加到信息安全研究、开发、产业的队伍中来。美国是这方面工作走在世界前列的国家，欧洲各国、加拿大、澳大利亚、日本等国也有很多机构和学者从事这方面工作。就是在韩国，据了解全国从事密码研究的科技工作者也有 2000 多人。

2．密码学现状

DES 的研究，以及以 RSA 为代表的公开密钥密码算法的研究推动了密码技术的深化研究和社会应用，成为相当长时间国际社会上应用的密码算法的主流算法。

从 DES 一推向市场，学术界就有不同的看法。开始，以 Whitfield Diffie and Martin Hellman 为代表的一些专家提出怀疑，DES 是否是美国情报机构已经拥有了破译能力的背景下推向社会的，在有关听证会议上，有关当局断然否认。其后，Diffie 和 Hellman 又提出 DES 标准设计使用 56-bit 密钥不安全。他们认为可以构做一部授索密钥的机器，到 1994 年花费 100 美元代价就可以得到一个密钥。1993 年 Michael Wiener 设计了这样特殊目的的机器，它要使用 57600 个授索芯片，花费 100 万美元在 3.5 小时就可以攻破 DES。近年来学者们对穷授密码算法的能力进行了研究分析。表 1-1 汇总了他们的结论。

表 1-1

经费预算/美元	工　具	攻破 40 bit 密钥的时间	攻破 56 bit 密钥的时间	对抗相应能力对手推荐的密钥长度/bit 1996-2018
400	FPGA - 1 chip	5 小时	38 年	50～65
30000000	CrayT3D1024 nodes	10 分钟	15 个月	-
10000	FPGA - 25 chips	12 分钟	18 个月	55～70
300000	FPGA - 750 chips ASIC - 15000 chips	24 秒 18 秒	19 天 3 小时	60～75
10000000	FPGA - 25000 chips ASIC - 500000 chips	7 秒 005 秒	13 小时 6 分钟	70～85
300000000	ASIC - 15000000 chips	002 秒	12 秒	75～90

由于 DES 公布使用的时间已经 20 年，人们在研究中发现了它的一些弱点，特别是 56 bit 的密钥长度，面对现代计算机的能力，已经不能对抗可能的攻击。1997 年 1 月 28 日，美国的 RSA 数据安全公司在 RSA 安全年会上公布了一项“秘密密钥挑战”(Secret-Key Challenge)竞赛，分别悬赏 1000 美元、5000 美元、10000 美元用于攻破不同密钥长度的 RC5 密码算法，同时还悬赏 10000 美元破密钥长度为 56 bit 的 DES 算法。RSA 发起这场挑战赛是为了调查 Internet 上分布式计算的能力，并测试不同密钥长度的 RC5 算法和密钥长度为 56 bit 的 DES 算法的相对强度，也隐含了想把 RC5 分组密码算法推为新的加密标准的打算。

到目前为止，40 bit 和 48 bit 的 RC5 算法已被攻破，美国克罗拉多州的程序员 Rocke Verser 从 1997 年 3 月 13 日起，用了 96 天的时间，在 Internet 上数万名志愿者的协同工作下，于 6 月 17 日成功地找到了 DES 的密钥，获得了 RSA 公司颁发的$10000 的奖金。

Rocke Verser 的成功，凝聚着一大批志愿参加者的工作和努力。目前，攻击 DES 的最有效的办法是密钥穷举攻击，Verser 设计了一个密钥穷举攻击程序，用以穷举所有可能的 DES 密钥，直至找到正确的那一个密钥，这个计算机程序可以从 Internet 上分发和下载。他把这项计划命名为 DESCHALL，这项计划开始时只有几百人参与，最终吸引了数万名志愿者参加。每有一名新的志愿者加入，DESCHALL 小组就为其分配一部分密钥空间让其测试，这样，正确的密钥最终会在某一名志愿者的计算机中出现。参与 DESCHALL 计划的 Internet 志愿者使用了企业、高校和政府的大量的计算资源，其中有计算能力强大的小型机、工作站，更不乏普通的 PC 机，参与的志愿者或计算机的具体数字尚未有精确的统计，但根据 IP 地址统计至少有 78156 个。

DES 的全部密钥穷举量为 72057584037927936，DESCHALL 计划完成时，搜索的密钥量为 17731502968143872，占全部密钥穷举量的 24.6%，平均每天最多搜索 601296394518528 个，每秒最多搜索 7000000000 个，其中最后 24 小时搜索了 559085783089152 个，占全部穷举量的 0.7%，假若一开始就以这个速度搜索，则 DESCHALL 计划只需 32 天即可完成。根据基于 IP 地址的统计，每天最多有 1400 台志愿计算机工作。

在 RSA 挑战赛公布之后的第 140 天、DESCHALL 计划实施的第 96 天，即 6 月 17 日的晚 10 点 39 分，幸运降临到了盐湖城 iNetZ 公司的职员 Michael Sanders 身上，当 Sanders 在他那台主频为奔腾 90Hz、16M 内存的 PC 机上成功地解出了 DES 的明文——“The

unknown message is: Strong cryptography makes the world a safer place" 时，他知道他终于找到了正确的密钥 (85 58 89 1a b0 c8 51 b6)。根据 Verser 的诺言，他将和 Verser 按 40/60 的比例共同分享 10000 美元的奖金。

DES 被攻破的消息公布之后，舆论界顿时哗然，开发密码产品的厂商认为这将为迫使美国政府放松密码产品的出口限制推波助澜，因为依靠 Internet 的分布式计算能力，公众已经可以轻而易举地攻破 DES。在如此短的时间内 DES 被攻破的消息让那些使用 DES 进行保密通信的机构、公司和个人从心里打了一个寒颤。Verser 认为政府应该慎重考虑现有的密码政策，Internet 上数万名志愿者使用普通 PC 机的协同工作就可以攻破 DES，因而 DES 已经不能抵抗任何一个有决心的对手的攻击了，已经不再安全了。英国剑桥的资金和技术决策主任 David Weisman 认为，DES 的破解应使人们认识到随着计算能力增长，必须相应增加算法的密钥长度。Scott Schnell，RSA 公司的副总裁认为 DESCHALL 计划十分成功，" DES 广泛地被用于加密敏感电子信息，有着非常深远的影响，因为 DES 被破可能是密码分析史上最有意义的里程碑事件"。

3. 分组密码现状

在对称算法中，最常用的和最受关注的算法是分组加密算法。据报道，国际上公开的密码算法已不下 100 多种，但是知名度最高，应用最广泛的只有少数几种。

国际上公布的著名的分组密码如表 1-2 所示。

表 1-2

名　称	研 制 国	明文分组	密钥长度/bit	迭代次数/bt	软件实现速度 Mbit/s	年　代
LUCIFER	美国	128	128	8		1970
DES	美国	64	56	16	16.9	1976
3-DES	Diffie-Hellmen	64	168	48		1977
2k3DES	Tuchmann	64	112	48		1978
FEAL-4	日本	64	64	4		1987
FEAL-8	日本	64	64	8		1988
FEALN	日本	64	64	32		1991
Khufu	Merkle	64	512	8s, s>1	43.6	1990
Khafre	Merkle	64	64t, t>0	8s, s>1		1990
LOKI	澳	64	64	16		1990
REDOC-II	美国	80	80	10		1990
LDEA	欧	64	128	8	9.75	1990
SAFER	Massey	64	64、128	6、10	13.8～17.0	1993
	Massey Knudsen	64	40、64、128	8、10		1995
Blowfish	Sohneier	64	32～448	16	36.5	1993
RC5	Rirest	64	8s, s<256	12	14.4～29.1	1994
SHARK	Rijmen Daemen 等	64	128	6	9.85	1996
SQUARE	Daemen Knudsen	128	128	8	36.6	1997
MISTY	Matsui	64	128	8～12		1997

从上表可以看出分组密码算法研究中的一些趋势。

（1）分组有扩大的趋势。从美国政府在 IBM 呈报的作为 DES 的基础的 LUCIFER 算法的 128 bit，为适应当时的技术条件和信到水平被降到 64 bit 的基础上，又有扩大到 128 bit 的动向，这是因为当前计算机的处理能力有很大的增强和信道质量有了很大的提高。

（2）密钥长度有增长的趋势。这是人们普遍认识到面对当今计算机的能力密钥的变化量少了肯定不能应对穷举攻击。为了保证较长期的安全性，密钥变量在设计时就需要留有余地。

（3）迭代轮次有减少的趋势。这是人们为了在保证安全强度的前提下，追求算法的实现速度，以便适应多媒体和高速信道对实时加密的需要。从给出的几个测试的结果看，软件实现的速度都达到了每秒数兆到数十兆比特。

4．非对称加密算法现状

目前国际上流行的公钥密码主要有两类，一类建立在大整数因子分解问题基础之上，其中最典型的是 RSA 公钥密码；另一类是基于离散对数问题，其中影响最大的是椭圆曲线公钥密码。由于大整数因子分解的能力日益增强，对 RSA 公钥密码的安全带来了威胁，512 bit 安全模长的 RSA 体制已经被攻破，768 bit 安全模长也指日可破。学者建议使用 1024 bit 安全模长，要保证 20 年的安全就要选择 1280 bit 安全模长，增大模长带来了实现上的难度。椭圆曲线公钥密码在国际上受到越来越多的重视，RSA 等一些公司声称已开发出符合 IEEE P1363 标准的椭圆曲线公钥密码。

1.1.5 信息加密技术

信息加密的目的是保护网内的数据、文件、口令和控制信息，保护网上传输的数据。网络加密常用的方法有链路加密、端点加密和节点加密三种。链路加密的目的是保护网络节点之间的链路信息安全；端-端加密的目的是对源端用户到目的端用户的数据提供保护；节点加密的目的是对源节点到目的节点之间的传输链路提供保护。用户可根据网络情况酌情选择上述加密方式。

信息加密过程是由形形色色的加密算法来具体实施，它以很小的代价提供很大的安全保护感。在多数情况下，信息加密是保证信息机密性的惟一方法。据不完全统计，到目前为止，已经公开发表的各种加密算法多达数百种。如果按照收发双方密钥是否相同来分类，可以将这些加密算法分为常规密码算法和公钥密码算法。

在常规密码中，收信方和发信方使用相同的密钥，即加密密钥和解密密钥是相同或等价的。比较著名的常规密码算法有：美国的 DES 及其各种变形，比如 Triple DES、GDES、New DES 和 DES 的前身 Lucifer；欧洲的 IDEA；日本的 FEAL－N、LOKI－91、Skipjack、RC4、RC5 以及以代换密码和转轮密码为代表的古典密码等。在众多的常规密码中影响最大的是 DES 密码。

常规密码的优点是有很强的保密强度，且经受住时间的检验和攻击，但其密钥必须通过安全的途径传送。因此，其密钥管理成为系统安全的重要因素。 在公钥密码中，收信方和发信方使用的密钥互不相同，而且几乎不可能从加密密钥推导出解密密钥。比较著名的公钥密码算法有：RSA、背包密码、McEliece 密码、Diffe-Hellman、Rabin、Ong-Fiat-Shamir、零知识证明的算法、椭圆曲线、ElGamal 算法等等。最有影响的公钥密码算法是 RSA，它能抵抗到目前为止已知的所有密码攻击。

公钥密码的优点是可以适应网络的开放性要求，且密钥管理问题也较为简单，尤其可方便地实现数字签名和验证。但其算法复杂，加密数据的速率较低。尽管如此，随着现代电子技术和密码技术的发展，公钥密码算法将是一种很有前途的网络安全加密体制。

当然在实际应用中人们通常将常规密码和公钥密码结合在一起使用，比如：利用 DES 或者 IDEA 来加密信息，而采用 RSA 来传递会话密钥。如果按照每次加密所处理的比特来分类，可以将加密算法分为序列密码和分组密码。前者每次只加密一个比特而后者则先将信息序列分组，每次处理一个组。

密码技术是网络安全最有效的技术之一。一个加密网络，不但可以防止非授权用户的搭线窃听和入网，而且也是对付恶意软件的有效方法之一。

1.2 破解密码的方式

密码破解方法很多，这里简单介绍几个。

1．穷举法

穷举法对于纯数字密码有很好的破解效果，但是包含字母的密码不适合这种方式。穷举法的原理是逐一尝试数字密码的所有排列组合，效率最低，而且很不可靠。穷举法破解密码的原理如图 1-1 所示。

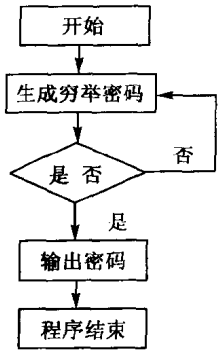

图 1-1 穷举法破解密码

2．黑客字典法

由于一些用户通常采用某些英文单词或姓名的缩写作为密码，所以就先建立一个包含巨量英语词汇和短语、短句的可能的密码词汇字典，然后使用破解软件去一一尝试，不断循环往复，直到试出正确的密码，这种破解密码方法的效率远高于穷举法，因此大多数密码破解软件都支持这种破解方法。黑客字典法破解密码流程如图 1-2 所示。

3．猜测法

猜测法依靠的是经验和对目标用户的熟悉程度，很多人的密码就是姓名汉语拼音的编写或生日的简单组合，这时猜测法拥有最高的效率。猜测法破解密码的流程和黑客字典法比较类似，这里就不再累赘。

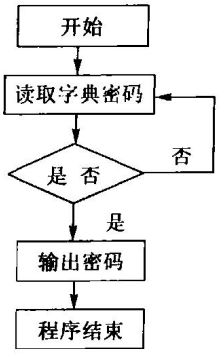

图 1-2 黑客字典法破解密码

4. 网络监听

网络监听工具是一种监视网络的状态。数据流动情况以及网络上传输的信息的管理工具，将网络接口设置在监听模式，可以截获网上传输的信息。当登录网络主机并取得超级用户权限后，若要登录其他主机，使用网络监听可以有效地截获其上传输的数据，是网上黑客使用最多的方法。网络监听只能连接物理上属于同一网段的主机。网络监听常常被用来获取用户的口令（如图 1-3 所示）。

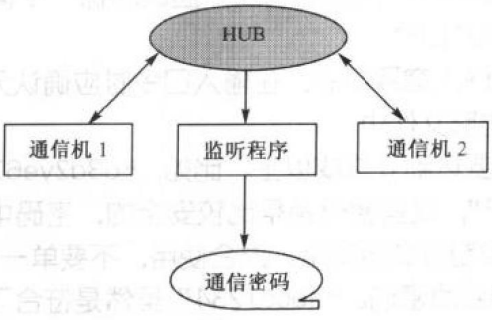

图 1-3 使用网络监听的方法获得密码

1.3 从密码心理学看如何保护自己的密码

1.3.1 密码心理学

很多黑客的入门是从破解口令开始的，本节要讲述的不是他们如何去破解口令，而是关于用户在设置口令时的心理学问题。如果下述的一些情况正好与读者的口令设置大同小异，那么请马上更改它，因为这说明读者的口令属于“危险”口令，被破解的可能性很大。

首先要说明的是许多 ROOT 没有采用口令保护的方法，当他的口令设置完之后，检测程序会自动提示，口令的不安全性，直到 ROOT 改成了没有规则的口令。所以对这些口令用口令心理学来分析是白费工夫了。我们主要是针对一些普通的用户。

当设定口令时一般的人都会用自己熟悉的单词，这样能使他们便于记忆。没办法，人天生就懒惰！那么哪些单词是人们容易记住的呢？是不是没有规律呢？