掌握66种密码攻击 获取 防范方法 就拥有了电脑的一切

黑客

密码终极攻防战

Win2000 WinXP Linux管理员密码手到擒来

揭露传奇 奇迹等游戏账号密码简单截取方法

自由查看QQ2003 MSN 聊天室密码

突破VIP会员限制观看在线电影

动网 雷傲 VBB论坛管理员密码如何获取

光盘加密破解指南 光盘解密有高招

大众网络报 POPUNET WEEK

网络安全警站配套手册

网络安全驿站配套手册

密码终极攻防战

PASSWORD ATTACK&KEEP AWAY

Win2000、WinXP、Linux管理员密码手到擒来

揭露传奇、奇迹等游戏账号密码简单截取

自由查看QQ2003、MSN、聊天室密码

动网、雷傲、VBB论坛管理员密码如何获取

突破VIP会员限制观看在线电影

光盘加密破解指南，光盘解密有高招

内容简介

密码在如今的生活中日趋重要，每个人在使用电脑的时候会有多个密码以供使用。但是你是否想过密码的来源？是否知道什么样的密码才是安全的密码？是否遇到过密码被他人强取豪夺？常言说知己知彼，百战不殆，我们有必要知道自己的密码是如何落入他人之手，才能正确地防护自己的密码。本手册就为你深入浅出地介绍了密码的由来，系统、软件、网络等多方位的密码攻防实例，让你能轻松掌握各种密码知识，最终真正保障自己密码的安全。

注：本手册只探讨密码技术，不得利用本手册介绍的知识去进行恶意攻击，违者将受到法律制裁。

光盘运行环境

CPU 主频	PII 500 以上
分辨率	800×600 像素以上
内存	32M 以上
显存	8M 以上
光驱	8 倍速以上
操作系统	Win9x/Me/NT/2000/XP

密码终极攻防战

策　　划：乔康毅

责任编辑：杨　波　曾庆强　王　洁　乔康毅

装帧设计：聂　培　朱　艳

光盘设计：冯　伟

非卖品　本手册随光盘赠送　光盘售价：12 元

目录

Password Attack&Keep away

第一章 密码基础知识

第二章 密码攻防战场

目 录

Password Attack&Keep away

第三章 加密解密精粹

第一章 密码基础知识

第一节 密码学

一、明灯指路——初识密码

密码这个东东大家再熟悉不过了，每天登录 Win2000、WinXP，上 BBS 灌水都要输入它。大家一定也听说了不少关于加密解密的传奇故事，是不是感觉密码学这个东西始终戴着一层神秘的面纱？今天我们撩起它的头巾。本文不涉及任何具体技术，只是希望给大家一个感性的认识，为后面的具体介绍扫清障碍。下面就让我们来了解一下吧。

记得古埃及人曾经用过一种加密技术：把窄窄的布条螺旋形裹在一根木棒上。布条间相互贴齐，不让里面的木棒露出来，然后用笔沿着木棒的方向竖着写要传递的消息。写完后把木条解下来，上面的文字就是一段密文(加密后产生的信息)。如果小阿要送信给小艾(小张小李的叫法好像不太合适了^_^)，就照上面的方法做为好。小艾拿到布条以后，取出一根木棒，粗细和小阿的那条一样。像前面说的那样，也把布条缠到自己的木棒上，就可以竖着读小阿的信了。这几乎就是最早的密码学。我国宋朝的时候也曾经有人在五言律诗里藏密文。最简单的例子就是藏头诗。不知道大家是否记得小时候看过的《一休》？有一次，一休被抓了，强盗要老和尚送钱去赎。一休牛得很，写了一首诗回来：不慎落入强人手，必死无疑甚忧愁。送来黄金可救命，钱到即可获自由。乍看是让家里快送钱的，可是你把每句话第一个字连起来看看呢！

1. 密码的分类

第一种就是——古埃及人用的办法。什么名字？(当然不能叫棍子。学术上的东西，怎能那么土)密码学家称之为“错乱”，即按照规定的图形和线路，改变明文字母或数码等的位置使之成为密文。下面的这种处理也可以看成简单的“错乱”：把英文的 26 个字母按照下面的对应规则配对：

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v

每个字母对应自己后面第四个字母，最后的 w,x,y,z 又各自对应 a,b,c,d。其实也就是通常所说的循环右移四位。这样一句“I love you”经过简单的加密处理，就变成了“e hkra ukq”。著名的凯撒密码就和上面的方法类似，只不过它是把字母左移若干位对应。

第二种叫“代替”——用一个或多个代替表将明文字母或数码等代替为密文。比如我们用“asdf”代替字母“k”，用“sedg”代替字母“y”。乍一看，好像变得复杂了很多。但是有一个好处，可以增加常用字母的隐蔽性。小说《福尔摩斯》有一个很有名的案例，就是关于破译密码的。英语里“e”这个字母出现频率最高。如果按上面第一种加密表格里的对应，就是字母“a”出现得最多。这样别人看见密文，很容易就推断出加密的规

则。有了“代替加密”,情况就不同了,一个字母变成了好几个。如果我不告诉你一个字母最后是变成了三个字母还是五个字母,你就慢慢统计去吧。

第三种是“密本”——用预先编定的字母或数字密码组,代替一定的词组单词等变明文为密文,莫尔斯电码就是一个好例子。再比如用“Houston”代替“I”,用“has”代替“love”,再用“YaoMing”代替“you”。这样,我们的“I love you”就变成了“Houston has YaoMing”。加密就是这么简单!

最后一种叫“加乱”——用有限元素组成的一串序列作为乱数,按规定的算法,同明文序列相结合变成密文。 如果大家以后有机会接触软件加密的历史,就会知道有一种加密方法叫“花指令”,就是在汇编代码里插入一系列无用的指令,干扰 cracker 阅读程序。这种方法 80~90 年代用得比较多,现在好像没什么人用了。

说完了加密方法的分类,再来说说解密。是不是所有的密码都可以破解的呢?从理论上说,只要你知道了密文,知道了加密规则,用穷举法就一定能搞定原来的密码。后面我们会举一些例子告诉你穷举法实际上是受条件限制的。现在肯定有人要问,除了穷举法就没有别的方法了吗? 我知道了密文,还不能逆推上去吗?问得好! 这就是加密的关键所在。加密绝不仅仅局限于加减乘除这些可逆的四则运算,有的加密算法是不可逆的,比如取余数。7 除以 3 余 1,10 除以 3 也余 1。即使我告诉你密文是 1,我们的算法是除以 3 取余数,你如何知道原文是 7 还是 10 呢? 当然,真正的加密不可能这么简单。我这里只是举一个例子说明,数学处理并不总是可逆的。

如果你看完了前面的部分,自觉对加密解密有了点想法,或者想知道一点更加细节的东西,就看下去吧。

2. 密码加密原理

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)o 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。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=Ek(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 Ek(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,所以也可叫对称密码。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。

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

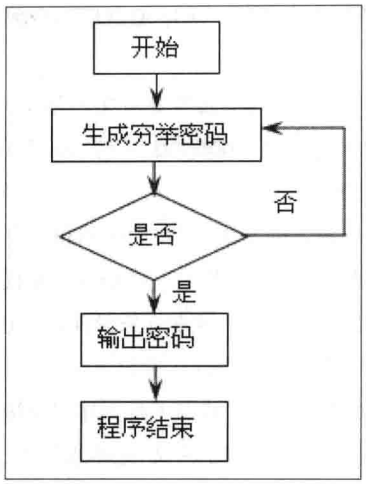

图 1-1

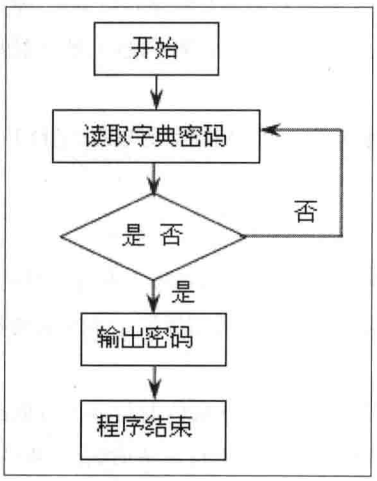

图 1-2

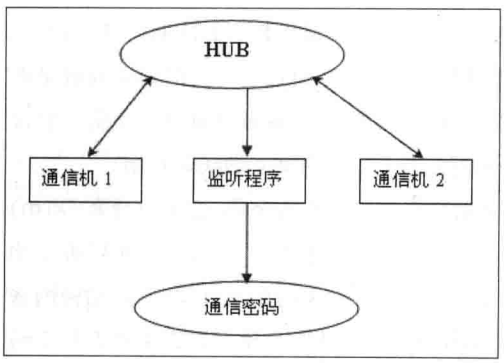

图 1-3

种密码体制随机选取的，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。

3. 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。

(2)骇客字典法

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。骇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，这种猜测法拥有最高的效率。猜测法破解密码的流程和骇客字典法比较类似，这里就不再赘述。

(4)网络监听

网络监听工具是一种监视网络状态的手段。数据流动情况以及网络上传输的信息的管理工具，将网络接口设置为监听模式，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，是网上骇客使用最多的方法。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)。

4. 你使用的密码安全吗

很多骇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 R00T 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功夫了。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?

专家曾做过一个心理试验,从大学中抽出一百名学生,然后要他们写下两个单词,并告诉他们这个单词是用于电脑的口令非常重要,且将来的使用率也很高。要求他们尽量慎重考虑。下面我们来分析一下测试结果:

(1)用自己名字的中文拼音者最多 37 人。这就告诉我们口令破解字典应针对中国的国情,使用一些中文姓名拼音的字典。如:wanghai,zhan,shengin 等。

(2)用常用的英文单词有 23 人。其中许多人都用了很有特定意义的单词,hello,good,happy,anything 等。

(3)用计算机中经常出现的单词的有 18 人。这些单词中还有操作系统的命令,system,COmmand,copy,harddiSk 等。

(4)用自己的出生日期 7 人。其中年月日各不相同,但其中有 3 人用了中国常用的日期表示方法,如:970203,199703,050498 等。

上述测试中两个单词相同的有 27 人,接近相同的有 33 人,虽然还有一些人用的没给他们归类,但还是有规律的。希望上面的心理测试能给读者带来一些启示,今后再设置密码的时候千万不要图一时的省事,给别人留下攻击的漏洞。

5. 如何设定安全的密码

经过了以上的分析,是不是开始觉得有些"胆战心惊"?请读者不要紧张,下面我们就来介绍怎样设置安全的用户口令。

(1)为防止眼明手快的人窃取口令,在输入口令时应确认无人在身边,而且不要将口令写下来或者将口令存于电脑文件中。

(2)密码的长度至少要达到 8 位或以上。比如,"d3d2ye6723"、"my007K00L2me" 或者"$73gtye5&FG72oPP",这些密码都是比较安全的,密码中必须包括大小写字母、数字、特殊的符号,如果有控制符会更安全。混合使用,不要单一地使用其中的某一个.

(3)避免使用容易猜到的密码。"abcd1234"虽然是符合了前面的要求,但是骇客很容易猜到。千万不要自作聪明地把什么"1"映射为叫",骇客先生们早替你想到了。像"you"映射到"U","bee"映射到"600"等都在其中。

(4)养成定期更新密码的习惯。任何安全的密码都经不住时间和骇客们的考验。只有符合安全要求的密码,力求每 3 个月更新一次,才能避免被骇客盯梢。

(5)狡兔三窟 ISP 密码、E-mail 号密码、BBS、个人主页或者 QQ 的密码应该避免重复。万一某个地方的密码发生泄漏(不是因为密码被猜到,而是其他原因的泄密),可以保证不至于全军覆灭。

第二节 常见的加密算法

一、华山论剑——加密算大比拼

谈起密码算法，有的人会觉得陌生，但提起 PGP，很多朋友都很熟悉，它是一个工具软件，能向认证中心注册后就可以用它对文件进行加密、解密和数字签名。密码算法的目的是为了保护信息的保密性、完整性和安全性，简单地说就是信息的防伪造与防穷取。

密码算法可以看作是一个复杂的函数变换，A=XY，Key，A 代表密文，即加密后得到的字符序列，Y 代表明文即待加密的字符列，Key 表示密钥，是秘密选定的一个字符序列。密码学的一个原则是：一切秘密寓于密钥中，算法可以公开。当加密完成后，可以将密文通过不安全渠道送给收信人，只有拥有解密密钥的收信人可以对密文进行解密即反变换得到明文，密钥的传递必须通过安全渠道。所以好的加密算法就是一件艺术品，颠扑不破的强壮性就是其魅力所在。在这个殿堂里，RSA、MD5、DES、DSA，以及被人们常用的 PGP 都在其中。下面是关于它们传奇的一点介绍，限于篇幅，我们只比较RSA、MD5 和 DES 这三个最重量级的加密算法。

1. RSA 加密算法

作为第一代集数据加密和数字签名于一身的算法，RSA 的强壮性已经基本被大家认可。从算法提出到现在已经二十多年了，无数的攻击者在这堵墙壁前折服，然后开始研究它。RSA 的安全性依赖于大数的因子分解，依赖于如何界定一个数是不是质数(这可是费马大定理要证的东西。)。所以从理论上，还没有人能证明破解 RSA 的难度和大数分解是等价的。也就是说，至今无法在理论上说明 RSA 的保密性究竟如何。

如果说实验上令人满意的结果可以弥补理论证明的不足，那么在具体加密操作过程中，RSA 还有不少不尽如人意的地方。首先，为了保证安全性，它需要很大的质数。产生质数的技术一直是一个瓶颈，找到一对好的密钥不容易。其次，运算代价太高，基本上都是大数运算，直接导致了运算速度慢。和下面提到的 DES 比起来，RSA 慢好几个数量级。最后，它的升级性比较差：随着现在计算机速度的突飞猛进，要保证安全性，通常要找更大的 p 和 q 做种子。而运算量是以级数倍增长的，每增大一点 p 和 q，运算开销都要增大很多，不利于品种改良。

(1)RSA 的安全性

RSA 的安全性依赖于大数分解，但是否等同于大数分解一直未能得到理论上的证明，因为没有证明破解 RSA 就一定需要作大数分解。假设存在一种无须分解大数的算法，那它肯定可以修改成为大数分解算法。目前，RSA 的一些变种算法已被证明等价于大数分解。不管怎样，分解 n 是最显然的攻击方法。现在，人们已能分解 140 多个十进制位的大素数。因此，模数 n 必须选大一些。因具体适用情况而定。

(2)RSA 的速度

由于进行的都是大数计算，使得 RSA 最快的情况也比 DES 慢上 100 倍，无论是软件还是硬件，速度一直

是RSA 的缺陷。一般来说只用于少量数据加密。

(3)RSA 的选择密文攻击

RSA 在选择密文攻击面前很脆弱。一般攻击者是将某一信息作一下伪装(Blind),让拥有私钥的实体签署。然后,经过计算就可得到它所想要的信息。

前面已经提到。这个固有的问题来自公钥密码系统的最有用的特征,每个人都能使用公钥。但从算法上无法解决这一问题,主要措施有两条:一条是采用好的公钥协议,保证工作过程中实体不对其他实体任意产生的信息解密,不对自己一无所知的信息签名;另一条是决不对陌生人送来的随机文档签名,签名时首先使用 One-Way Hash Function 对文档作 HASH 处理,或同时使用不同的签名算法。

(4)RSA 的缺点

A. 产生密钥很麻烦,受到素数产生技术的限制, 因而难以做到一次一密。

B. 分组长度太大,为保证安全性,n 至少也要 600 bits 以上,使运算代价很高,尤其是速度较慢,较对称密码算法慢几个数量级;且随着大数分解技术的发展,这个长度还在增加,不利于数据格式的标准化。目前,SET(SecureElectronicTransaction)协议中要求 CA 采用 2048 比特长的密钥,其它实体使用 1024 比特的密钥。

尽管如此,RSA 算法仍然被广泛地使用着,一般多用于加密少量的数据。由于软件实现太慢,也有人提出用引入硬件的改良方案,比如使用 TMS320C5402 DSP 芯片提升加密解密速度。在这条道路上,研究者们已经投入了太多的精力,就算痛,现在也不是撒手的时候。

2. MD5 加密算法

如果你要问,最近流行什么快速黑论坛的办法,那无疑是 SQL 注入了。“忽如一夜黑风起,大家都来搞 SQL 注入”。为什么不下载数据库像以前一样挂个软件跑密码了?原因很简单:加密算法不可逆,除了傻傻地穷举,我们什么也作不了。在众多论坛中,动网是大名鼎鼎的一个。由于使用太广泛,它的每一个漏洞都成了骇客们追逐的目标。大家提到动网,也会带上一句:“它是用 MD5 加密的”。动网的密码和提示问题的答案就是经过 MD5 加密的。

MD5 也是 RSA 公司的荣誉出品之一。MD 加密系列历史悠久。玩骇客的人恐怕没有不知道 l0pht 这个 NT 口令破解工具的吧。NT 的用户密码就是用 MD4 加密的。安全性如何?即使有 l0pht 这么强的工具,穷举起来也让每个人头疼了。MD 系列所基于的计算概念是消息摘要散列。消息摘要散列是将变长消息转换到定长(大多数情况下,通常是 128 位)的结果。散列函数为每个不同消息给出不同的结果,因此对于消息散列也将产生唯一的值。首先调整要加密的信息的长度,使其长度恰好是 512 位的整数倍。产生散列也需要种子,MD5 中一般取四个种子,然后通过后面四轮非线性函数的杂化,产生一段散列。由于杂化的过程不可逆,MD5 的坚固性也得到了众多专家的首肯。

MD5 实际上是由 MD2、MD4 等慢慢演化而来的。和前面的版本相比,MD5 在安全性和速度上都有了提高,比如增加了一轮非线性函数杂化,近似优化每轮中的循环位移,使得杂化更快发生。MD5 作为消息摘要散列的代表作,一定会在加密界继续占据重要的一席。

3. DES 加密算法

由美国国家标准局推出的 DES(Data Encryption Standard)加密标准只是蓝色巨人 IBM 公司创造的故事之一,不过在密码学界,它就如传说一般,为人们津津乐道。它的应用也渗透到了各个领域。我曾经遗忘了自己信用卡的密码,去银行查询,被告之无法查到,只能重办一张。当时甚是疑惑,后来了解到,现在银行金融数据加密基本上都采用了不可逆的 DES 加密,当然无法查询密码。其实不单单是银行内部,POS、ATM、磁卡、IC 卡、加油站、高速公路收费站等领域也是 DES 大展身手的好地方。

和 RSA 公开密钥不同,DES 的密钥是秘密的。DES 的加密过程实际上是把 64 位的数据块按位重新组合若干次,组合过程中不断生成子密钥。而解密过程也是一样的,只是解密过程中逆着生成子密钥的顺序恢复数据。利用 DES 的通信过程很简单。通信双方都有一个共同的 Key。发信人在加密模式下用 Key 把数据加密成 64 位的密码形式,然后收信人再用相同的 Key 在解码模式下解密。为了提高安全性,通信双方可以定期修改新的 Key。

DES 算法的安全性极高,除了穷举搜索,目前还没有发现更好的手段。有人做过估测,如果一台计算机一秒钟可以检测一百万个密钥,则它搜索完整个密码空间的时间是近 2285 年。即便出现超高速计算机后,只要把 DES 密钥的长度再增长一点,这样搜索空间的大小就以级数倍增长,搞穷举搜索的人又要多等不少年了。

因为确定一种新的加密法是否真的安全是极为困难的,而且 DES 的惟一密码学缺点,就是密钥长度对比较短,所以人们并没有放弃使用 DES,而是想出了一个解决其长度问题的方法,即采用三重 DES。

从目前 DES 使用的情况看,这个算法完全达到了当年美国国家标准局提出的要求:"具有相当高的复杂性,使得破译的开销超过可能的获益,同时又要便于理解和掌握。"如果你是一个热衷于穷举破解的人,我劝你不要痴情于 DES,因为没准在你破出密码之前,管理员已经换了新的密码了,呵呵。

4. RSA 算法的实现

现代加密技术的核心就是算法。古典加密体制在现代计算机的高速运行下显得越来越脆弱。好的加密算法逐渐成了主角。RSA 作为最经典的算法之一,无疑是一个教学的好例子:它的算法简单,但是异常坚固。透过 RSA 这个窗口,你可以窥见现代加密技术的一点轮廓。

自从 RSA 诞生的第一天起,外界对它的猜疑就没有停止过。它的安全性至今未能得到理论上的证明,但是经过二十多年的风风雨雨,饱经攻击的它终于为人们接受了。其中原因只有一个:至今尚未被攻破。

它是世界上第一个既能用于数据加密也能用于数字签名的算法。作者是 Rivest、Shamir 与 Adleman 三人。算法名称就是他们的名字的缩写。理解和实现都很方便,它是基于一个非常简单的数论思想:"将两个素数乘起来是很容易的,但是分解该乘积是非常困难的"。下面是一个简单的例子。例子理解起来远胜于代数表达式。

(1)实战 RSA 原理

如果小张想给小李发送秘密信息,那么小张要用小李公布给大家的公钥加密信息,然后把密文发给小李。小李再用他的私钥解密这些密文,得到原始信息。

小李要做的事情就是先公布一个公钥。制造公钥的步骤如下：

第一步 选择任意两个质数，比如 p=11 和 q=7 这两个数。这两个数一定要保密。

第二步 计算 N=p×q=77。

第三步 再取一个数 r，r 和(p−1)×(q−1)互质，也就是说，r 和 60 没有公因数。例如，这里我们设 r=13。这个 r 是密钥。

(2)RSA 实现过程

这样，我们就得到了一个公共密钥——(r,N)，也就是(13,77)。小张把这个公钥告诉了小张。小张接下来要做的事情就是用这个公钥加密信息。

A. 给手上的信息 M 进行编码，把英文字母转换成数字。使用每个字符的 ASCII 码就是一个好办法。比如加密“love”这个单词，字母“l”，“o”，“v”，“e”的 ASCII 码分别是 76(01001100)，79(01001111)，86(01010110)和 69(01000101)，括号里是对应的二进制数。把这四个二进制数放在一起，编码结果就是 01001100010011110101011001000101。把这个数再还原成十进制的。如果把这一长串二进制数都还原，结果是 1280267845，数字太大了。为了方便以后的说明，我们假定要加密的内容只有“e”一个字母。于是得到的编码，也就是最后 M 的编码就是 69。

B. 对 M 的编码加密。假设最后加密结果是 Encode，则使用公式 Encode=M^r(modN)。预算的顺序是先求 M 的 r 次方，即 69^13。然后用这个大数除以 N，也就是 77，取其余数。如果你觉得数字太大，Windows 的附件里面提供了计算器。或许很多人都没有用过，好好研究一下，不要被普通计算界面迷惑了，觉得这个计算器很土。它还有一个科学计算的界面。我的系统是英文 XP，点 view(查看)，然后选 scientific(科学)，一个功能强大的科学计算器就展现在我们眼前了。它最让我满意的地方就是可以做大数运算。话归正题，最后我们得到的 Encode=27。注意，这个运算过程是不可逆的，就算知道结果，也算不出 M 的初值。

C. 把密文 Encode=27 发送给小李。小李收到密文后开始解密：先生成私钥。知道了 p 和 q，还有公钥 r，小李就可以生成私钥 r'了。在教材里有这么一个等式：r×r'=1 (mod (p−1)×(q−1))。意思就是找到一个数 r'，使得 r×r'除以(p−1)×(q−1)的余数是 1。在这个例子里，就是让 13r'除以 60 余 1。写个简单的穷举搜索程序或者使用 Euclides 算法可以算出 r'=37。不过就事论事，任何除以 60 余 1 的数肯定都是以 1 结尾的。而和尾数是 3 的数相乘(比如这里的 13)，得到的乘积尾数是 1 的只有 7。所以我们要找的 r'一定是以 7 结尾的。简单测试几次，测试次数不会超过 10 的，有兴趣的话可以想想看，为什么？永远不要让思维凝固，Hack 的快乐在于思考。

D. 现在要做的就是利用私钥解密信息。使用公式 M=Encode^r' (mod N)，我们得到 M=27^37 (mod 77)=69。如果你对大数运算感到恐惧的话，我们也可以动动脑筋玩点数学手段。27^37=(27^8)×(27^8)×(27^8)*(27^8)×(27^5)，或者你可以划分得更细。然后你对每项取余，比如 27^8 对 77 的余数是 15，27^5 对 77 的余数是 34。这样把所有的余数乘起来：15×15×15×15×34=1721250。这个数大于 77，再对 77 取一次余数，得到答案 69。用数学式表达就是 27^37(mod 77)=[27^8(mod77)×27^8(mod77)×27^8(mod77)×27^8(mod77)×27^5(mod77)] mod(77)。有数论基础的朋友可以自己证明一下。

E. 得到 69 以后，对照 ASCII 码表，就找到了字母“e”。这样解密完成！

从上面的步骤，你可以看出我们当初选定的 p 和 q 是多么的重要。一旦这两个数公诸于世，任何人都

能解读你的密文。从理论上说，要破解私钥，就要对 N 做因式分解，找出 p 和 q。本例中为了行文方便，p 和 q 取得都很小。实际应用中，它们都是很大的质数。取大数的目的就是为了对抗因式分解。在当今的数学领域里，大合数分解一直是一个热门而又没有彻底解决的话题。也正因为如此，RSA 依然在公钥密码体制中占据重要的一席。坚固就是硬道理，对密码来说就是这样！

5. 设计自设的算法

题目起的得炫，实际上例子很简单。这里的例子只是为了帮助大家了解什么是对称加密。至于不对称加密，也就是公开密钥的加密，后面介绍 RSA 的时候具体谈到了，这里不再赘述。

这里我们只做一个最简单的对称加密算法——XOR。假设我们要传输的数据已经编码完毕，明文是 00101101。我们的加密算法就是异或。密钥就用 10101010 吧。

00101101 XOR 10101010 = 10000111。这里的结果 10000111 就是我们的密文。

如果我们的朋友知道我们使用了异或算法，也知道我们的密钥 10101010，那么他们只要把密钥和密文再异或一次，就可以得到原来的明文，即：10000111 XOR 10101010 = 00101101

从上面的步骤我们可以看出，发信方和收信方的操作是一样的，都是把手上的信息和 10101010 异或，这就是对称操作。对称操作的安全性依赖于我们对密钥的保管。即使我们的算法被泄漏出去了，别人不知道我们的密钥也是白搭。

再举一个例子，还用位操作。如果你要发送的下面的一张表给你的 GF，你想说得话就是第三列里面的八个字母（如图 1–4）。

但是你又担心被别人看见，于是你和 GF 约定好加密算法——把奇数行循环左移两位。下面的表就是你加密后的杰作（如图 1–5）。

这张表恐怕不会再有人看出端倪来了吧。你的 GF 收到信，只要如法炮制，把把奇数行循环左移两位就又能看到原文了。怎么样？发挥你的想象力吧。加密的研究永远没有尽头，因为我们的我们的思想无极限。

S	D	I	K
A	E		I
Q	U	L	P
J	O	O	M
N	Y	V	G
B	Y	E	D
V	T		A
J	S	Y	W
T	R	O	X
E	Z	U	D

图 1–4

I	K	S	D
A	E		I
L	P	Q	U
J	O	O	M
V	G	N	Y
B	Y	E	D
	A	V	T
J	S	Y	W
O	X	T	R
E	Z	U	D

图 1–5

第二章 密码攻防战场

第一节 系统密码

一、Windows 98 登录密码设置与破解

对于 Win9x 系列的操作系统来讲（也包括 WinMe），它的密码安全较差，很容易破解。与其说是用于“系统安全”，还不如说成是用来“做秀”，这一点从下面 Win9x 密码轻松被破解就可以看出来。

1. 创建 Win98 的系统登录密码

在安装完 Win98 系列产品之后，第一次进入操作系统时都会有一个对话框，要求你输入密码，并且提示你如果不输入密码直接进入，那么下次这个对话框将不再出现。这时，你可以输入你的密码，用作登录 Windows。如是这时你没有输入密码，而以后你又想使用这个功能，那么只能从控制面板里进行更改了，具体步骤如下：

步骤 1 打开“控制面板”→“密码”（如图 2-1）；

步骤 2 单击“更改 Widows 密码”根据提示输入密码，然后再输入新密码并进行确认，这样下次你登录 Windows 时系统就会要求你输入密码了。

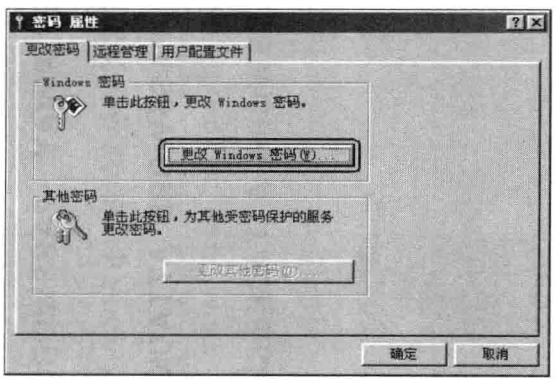

图 2-1

2. 解除 Win98 密码

一般 Windows 用户的登录密码都记录在 *.pwl 的密码文件里，因此，只要能破解 *.pwl 文件，就可以破解登录密码，加密后的 Win98 密码清单即 PWL 文件可以在系统的根目录下找到（通常是 C:\Windows）。这些文件按该系统上每个用户的初始定制文件命名。因此在驱动器 A 的软盘上执行如下命令可以获得大部分 PWL 文件：

```
copy c:\Windows\*.pwl a:\
```

提示：PWL 文件实际上只是一个用于访问以下网络资源的一个高速缓存的密码清单：

（1）由共享级安全机制保护的资源；

（2）编写用到密码高速缓存 API 的应用程序，例如 DUN(Dial_up NetWorking)；

（3）没有加入任何 NT 域的 WinNT 计算机；

（4）不是 Primary Network Logon 的 WinNT 的登录密码。

3. 破解 PWL 文件

破解 PWL 密码文件最快捷的方法是直接删出所有 Windows 下的 *.pwl 文件。一般来说 *.pwl 放在 Windows 所在的目录中。因此破解文件方法非常简单，具体步骤如下：

步骤 1 重新启动计算机，在进入 Windows 之间，按 F8 键通过“Command prompt only”项进入 DOS 状态。