



电脑报

精品图书

百炼成钢

Practices makes perfect

曲靖 刘海平 石云 编著

不是学会的，是练会的

电脑安全 全能修炼

- | 修炼1 | 电脑密码破解与防护
- | 修炼2 | 攻击QQ/MSN方法与安全措施
- | 修炼3 | 针对邮箱（邮件）的攻击与防范
- | 修炼4 | 恶意网页攻防实战演练
- | 修炼5 | 病毒的攻击与防范
- | 修炼6 | 常见木马入侵入防范
- | 修炼7 | 电脑系统自身安全防护
- | 修炼8 | 电脑安全实例动画教程

四川出版集团 • 出版
四川电子音像出版中心

百练成钢

Practices makes perfect 曲靖 刘海平 石云 编著
不是学会的，是练会的

电脑安全 全能修炼

四川出版集团 • 出版
四川电子音像出版中心

内容提要

本书内容丰富,语言简洁明了,采用图文并茂、动画教学的实例 Step by step 方式进行讲解。全书共分为 8 章,详细讲解了个人电脑密码破解与防范、聊天软件的攻击与防范、邮箱的攻击与安全防范、网页浏览的攻击与防范、病毒的攻击与防范、木马的攻击与防范、系统自身的安全防护以及相关软件的安全防护等内容。

本书通过实例+动画教学的训练方式,带领读者完成相关个人电脑的安全与防护的实战演练,真正做到理论与实践相结合。本书广泛适合于对计算机及网络知识有所了解、喜欢网络安全、对入侵攻防技术感兴趣的读者。

版权所有 盗版必究

举报电话:四川省版权局: (028) 86636481

四川电子音像出版中心: (028) 86266762

书 名	百“练”成钢——电脑安全全能修炼
审校/责任编辑	马 黎 王 洁
CD 制 作 者	电脑报东方工作室
出版/发 行 者	四川电子音像出版中心
地 址	成都市盐道街 3 号
经 销	各地新华书店、软件连锁店
CD 生 产 者	东方光盘制造有限公司
文 本 印 刷 者	重庆升光电力印务有限公司
规 格 / 开 本	787 毫米×1092 毫米 16 开 14.75 印张 354 千字
版 次 / 印 次	2005 年 8 月第 1 版 2005 年 8 月第 1 次印刷
印 数	1—5000 册
版 本 号	ISBN 7-900397-74-4/TP·66
定 价	22.00 元 (1CD+配套手册)

修炼 1 个人电脑破解与防范

1.1 系统密码	2
1.1.1 CMOS 密码的设置与破解	2
1.1.2 Windows 98 登录密码设置与破解	6
1.1.3 Windows 98 共享目录密码的破解	7
1.1.4 Windows 2000 登录密码的破解	11
1.1.5 Windows XP 登录密码的破解	14
1.1.6 破解屏保密码	15
1.1.7 IE 内容审查密码的设置与破解	16
1.2 办公密码	18
1.2.1 Word 文档密码的设置与破解	18
1.2.2 Access 密码的设置与破解	21
1.2.3 Excel 密码的设置与破解	23
1.2.4 PowerPoint 密码的设置与破解	25
1.2.5 WPS 密码的设置与破解	28
1.2.6 PDF 文档密码的设置与破解	30
1.3 软件密码	33
1.3.1 WinZip 密码的设置与破解	33
1.3.2 WinRAR 密码的设置与破解	38
1.3.3 FlashFXP 密码破解	42
1.4 本章小结	44

修炼 2 聊天软件的攻击与防范

2.1 QQ 的攻击与防范	46
2.1.1 QQ 的 IP 探测与隐藏	46
2.1.2 QQ 密码在线破解与防范	51
2.1.3 QQ 炸弹的攻击与防范	54
2.1.4 QQ 黑软的攻击与防范	56
2.1.5 QQ 消息诈骗与防范方法	57
2.1.6 砍掉 QQ 的坏“尾巴”	58
2.1.7 加好友的万能方法	59
2.1.8 QQ 本地破解与防范方法	60
2.2 MSN 的攻击与防范	64
2.2.1 MSN 密码的窃取与防范	64

2.2.2 MSN 的“窃听”与防范	65
2.2.3 拒绝 MSN 自动登录	67

修炼 3 邮箱的攻击与防范

3.1 Web 邮箱的攻击与防范	70
3.1.1 Web 邮箱密码的破解与防范	70
3.1.2 E-mail 地址的窃取与防范	74
3.1.3 邮件炸弹的攻击与防范	80
3.1.4 虚假邮箱附件攻击与防范	83
3.1.5 HTML 邮件的攻击与防范	84
3.2 Foxmail 攻击与防范	85
3.2.1 Foxmail 密码的设置与破解	85
3.2.2 Foxmail 拒绝垃圾、病毒邮件大法	87
3.2.3 加密 Foxmail	90
3.3 Outlook Express 攻击与防范	90
3.3.1 Outlook Express 密码的设置与破解	90
3.3.2 Outlook Express 漏洞攻击	93
3.3.3 Outlook Express 垃圾、病毒邮件的防范	94

修炼 4 网页浏览的攻击与防范

4.1 恶意网页的攻击与防范	98
4.1.1 多种网页弹出窗口代码攻击	99
4.1.2 网页地震的攻击	103
4.1.3 超大图片炸弹的攻击	104
4.2 高级 Java 攻击	104
4.2.1 格式化硬盘炸弹的攻击	104
4.2.2 窗口炸弹的攻击	105
4.2.3 进入 Windows 之前弹出对话框	106
4.2.4 IE 死循环的攻击	107
4.2.5 强制设定 IE 主页的攻击	108
4.2.6 锁定注册码的攻击	109
4.2.7 锁定 IE 选项的攻击	111
4.2.8 在鼠标右键快捷菜单中加链接的攻击	112
4.2.9 修改 IE 标题栏的攻击	114
4.3 Java 攻击的防范	115

4.3.1 IE 被攻击后的修复	115
4.3.2 具体的防范措施	119
4.4 其他网页攻击与防范	121
4.4.1 个人网页的加密与破解	121
4.4.2 恶意共享的关闭	127

修炼 5 病毒的攻击与防范

5.1 常见病毒的攻击与清除	130
5.1.1 尼姆达病毒的攻击与清除	130
5.1.2 恶邮差病毒的攻击与清除	133
5.1.3 Word 宏病毒的攻击与清除	135
5.1.4 诺维格病毒的攻击与清除	136
5.1.5 欢乐时光病毒的攻击与清除	138
5.1.6 网络天空病毒的攻击与清除	139
5.1.7 恶鹰病毒的攻击与清除	141
5.2 系统漏洞病毒	142
5.2.1 冲击波病毒的攻击与清除	142
5.2.2 震荡波病毒的攻击与清除	144
5.3 即时通讯软件病毒	145
5.3.1 MSN 小尾巴病毒的攻击与清除	145
5.3.2 MSN 性感鸡病毒的攻击与清除	148

修炼 6 木马的攻击与防范

6.1 网页木马的攻击与防范	152
6.1.1 “3721” 网页木马的攻击	152
6.1.2 冰狐浪子超级网页木马的攻击	157
6.1.3 EXE2BMP 网页木马攻击	162
6.1.4 网页木马的防范	163
6.2 远程木马的攻击与防范	164
6.2.1 灰鸽子木马的攻击与防范	164
6.2.2 广外女生木马的攻击与防范	172
6.2.3 网络神偷的攻击与清除	175
6.2.4 黑洞木马的攻击与清除	178
6.2.5 DMRC 木马的攻击	183
6.2.6 冰河木马的攻击与清除	188

6.2.7	网络精灵 (NetSpy) 木马的攻击与清除	194
6.2.8	远程木马的防范	196
6.3	网络游戏的攻击与防范	197
6.3.1	传奇的木马攻击	198
6.3.2	奇迹 MU 的木马攻击	201
6.3.3	联众游戏的木马攻击与防范	203

修炼 7 系统自身的安全防范

7.1	账号安全设置	206
7.1.1	账号密码设置	206
7.1.2	本地安全策略设置	208
7.2	系统服务安全设置	210
7.2.1	设置服务项, 做好内部防御	211
7.2.2	修改注册表防御 DOS 攻击	211
7.2.3	禁止默认共享	212
7.2.4	提高 Cookies 安全级别	213
7.2.5	防止跨站攻击	214
7.3	系统权限设置	215
7.3.1	修改权限设置	215
7.3.2	重要文件加密	217

修炼 8 相关软件的安全与防护

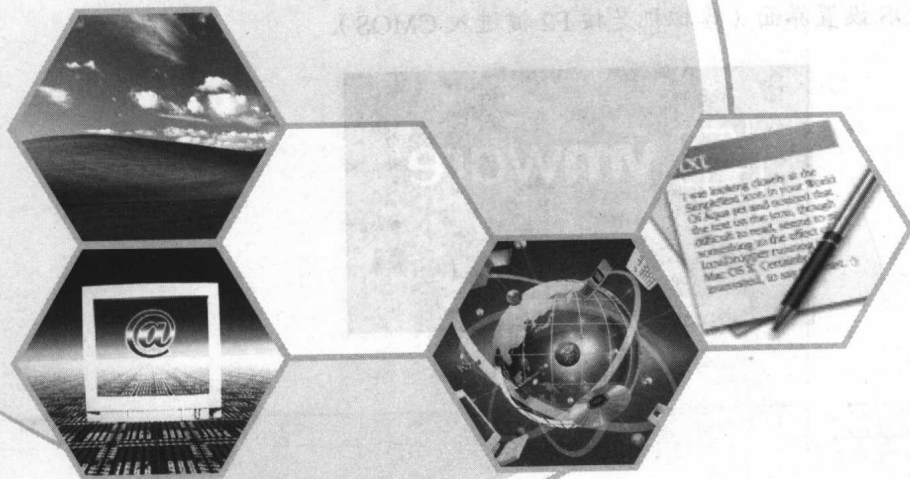
8.1	防火墙的选择与设置	220
8.1.1	天网个人防火墙 v2.73	220
8.1.2	江民黑客防火墙	225
8.2	杀毒软件的选择与设置	226
8.2.1	金山毒霸 6	227
8.2.2	江民杀毒软件 KV2005	228

『个人电脑破解与防范』

Chapter 1

本章能学到什么？

1. 系统密码的设置与破解，包括 CMOS 密码、登录密码、共享密码、屏幕保护程序密码等。
2. 办公密码的设置与破解，包括 Word、Access、Excel、PowerPoint、WPS、PDF 等办公软件密码。
3. 软件密码的设置与破解，包括 WinZip、WinRAR、FlashFXP 以及其他软件加密的方法。



修炼 1 个人电脑破解与防范

密码是我们在使用电脑过程中经常接触到的，它是保护电脑秘密和重要数据的安全之门，但是过多的密码又让朋友们非常头痛，万一遗失了密码，那就麻烦了。本章详细讲述了系统密码、办公密码、软件密码的设置与破解，让读者了解密码设置与破解的流程，学习如何防止黑客进行密码破解。

1.1 系统密码

计算机系统的常见密码包括 CMOS 密码、登录密码、共享密码、屏幕保护程序密码等，其中要数“屏幕保护程序密码”的设置和破解最容易，CMOS 密码最值得用户探究。

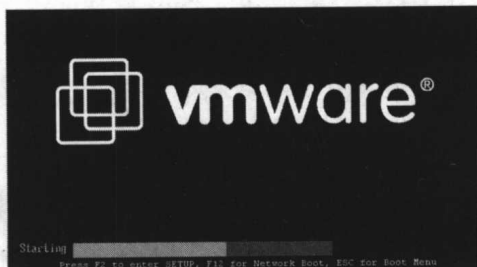
1.1.1 CMOS 密码的设置与破解

CMOS 是目前绝大多数电脑中都使用的一种用电池供电的存储器。它是确定系统的硬件配置、优化微机整体性能、进行系统维护的重要工具。它保存一些有关系统硬件设置等方面的信息，在关机以后，这些信息也继续存在（这一点与 RAM 完全不同）。开机时，电脑需要用这些信息来启动系统。如果不慎或发生意外而弄乱了 CMOS 中保留的信息，电脑系统将不能正常启动。

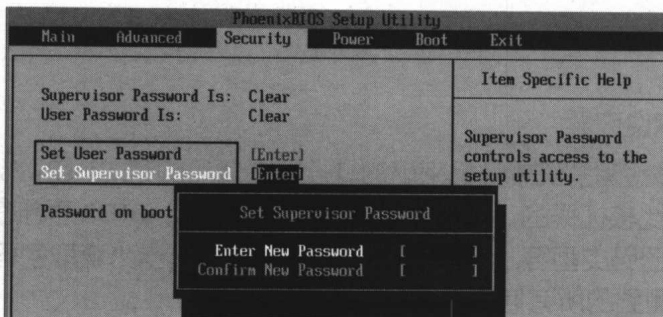
1. CMOS 密码的设置

CMOS 版本有多个，但密码设置方法基本相同，现以虚拟机上的 CMOS 版本为例，具体设置方法介绍如下：

步骤 1 开机后，当屏幕下方出现提示“Press DEL to enter SETUP”时，按下 Del 键，进入 CMOS 设置界面（虚拟机是按 F2 键进入 CMOS）。

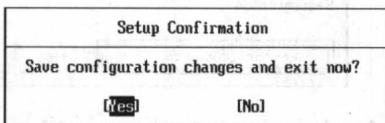


步骤 2 使用箭头键选择“Set Supervisor Password”（管理员密码）或“USER PASSWORD”（用户密码）后，按 Enter 键。



步骤 3 键入密码，按 Enter 键，再次键入密码，按 Enter 键。

步骤 4 设置完毕后选择“SAVE & EXIT SETUP”或按 F10 键，出现提示“SAVE to CMOS and EXIT (Y/N)?”，此时按下 Y 键，保存设置。



技巧与提示:

CMOS 密码分为两种，一种是 Setup 密码，另一种是 System 密码。在 CMOS 选项中“Advanced BIOS Features”(BIOS 功能设置)里，可以设置“Security Option”的选项为“Setup”或“System”，在多数情况下默认设置项为“System”，意指不但在进入 BIOS 设置时要求输入密码，而且进入操作系统时也要求输入密码；当设置为“Setup”时，意指开机时按 Del 键进入 CMOS 设置画面时要求输入密码，但进入操作系统时不要求输入密码。

我们可根据不同的目的进行设置，一般来讲，设置了 System 密码，那么安全性更高些，但如果此时忘记密码，其破解也就更复杂些，而设置了 Setup 密码则反之。

2. CMOS 密码的破解

对于用户设置的 Setup 与 System 两种密码，我们的破解方法是有所区别的。

(1) 破解 Setup 密码

如果计算机能正常引导，只是不能进入 BIOS 设置（即设置了 Setup 密码），那么我们有以下几种破解方法。

方法一：Debug 法

启动电脑进入纯 DOS 状态, 输入 Debug 命令后回车进入 Debug 程序, 然后输入以下命令:

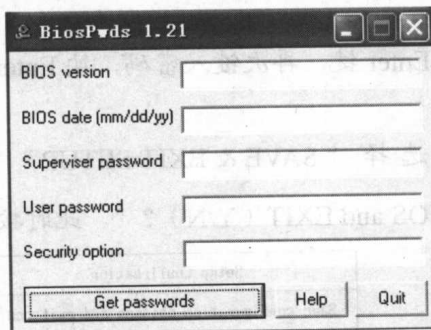
-o 70 11

-o 71 FF

-q

方法二: 软件破解

现在有很多检测系统或开机密码的软件, 最常见的有 BiosPwds、Cmospwd 等。其中 BiosPwds 是比较优秀的, 它可以检测出 BIOS 版本、BIOS 更新日期、管理员密码、CMOS 密码、密码类型等。在 BiosPwds 主界面中单击“获取密码”按钮即可显示出 BiosPwds 所检测到的所有信息。



下载地址: <http://down1.zol.com.cn/jiami/biospw12.zip>

技巧与提示:

由于软件破解密码是对 BIOS 编码过的密码进行逆向解码, 所以有时也许会发现程序的密码和真实的密码并不相同, 这属于正常现象。

方法三: DOS 下破解

这个方法直接在 MS-DOS 环境下便可完成, 在 MS-DOS 环境下输入“COPY CON CMOS.COM”后回车, 然后输入如下 10 个字符:

ALT+176 ALT+17 ALT+230 p ALT+176 ALT+20 ALT+230 q ALT+205 <空格>

然后按 F6 键, 再按回车保存, 这样以后只要运行 Cmos.com 文件即可清除 BIOS 密码。

(2) 破解 System 密码

如果设置了 System 密码, 我们就无法通过软件来解决密码遗忘的问题了。此时可以采用以下几种办法:

方法一: 通用密码

每个主板厂家都有主板的通用密码, 以便于提供技术支持之用。如果知道了该主板

的通用密码，那么无论是开机，还是进行 CMOS 设置都可以“穿墙而入”。

Award BIOS 通用密码：j256、LKWPETER、wantgirl、Ebbb、Syxz、aLLy、AWARD?SW、AWARD_SW、j262、HLT、SER、SKY_FOX、BIOSTAR、ALFAROME、lkwpeter、589721、awkard、h996、CONCAT、589589。

AWI BIOS 通用密码：AMI、BIOS、PASSWORD、HEWITT RAND、AMI_SW、LKWPETER、A.M.I.

注意：

各主板厂家出于某些原因，不同时期主板的通用密码会有所不同，因此这一招并不能通行天下，只有多尝试几次，是否有用就要看运气了。

方法二：CMOS 放电法

目前的主板大多数使用纽扣电池为 BIOS 供电，如果没有电，BIOS 里面的信息就会丢失，当再次通上电时，BIOS 就会回到未设置的原始状态，当然 BIOS 密码也就没有了。

我们先要打开电脑机箱，找到主板上银白色的纽扣电池，小心地将它取下，再把机箱尾部电源插头拔掉，用金属片短接电池底坐上的弹簧片，大概隔 30 秒后，再将电池装上。

此时 CMOS 将因断电而失去内部储存的信息，合上机箱后开机，系统就会提示“CMOS Checksum Error-DeFaults Loaded”，即提示你“CMOS 在检查时发现了错误，已经载入了系统的默认值”，BIOS 密码破解成功。

方法三：跳线短接

如果主板的 CMOS 芯片与电池整合在一起了，或者电池直接被焊在了主板上，那么就可以使用跳线短接这一招了。

打开机箱后在主板 CMOS 电池附近会看到一个跳线开关，在跳线旁边一般会标注有 RESET CMOS (重设 CMOS)、CLEAN CMOS (清除 CMOS)、CMOS CLOSE (CMOS 关闭) 或 CMOS RAM RESET (CMOS 内存重设) 等字样，用跳线帽短接，然后将它跳回就行了。

由于各个主板的跳线设置情况不太一样，所以在用这一招的时候，最好先查阅主板说明书。

技巧与提示：

在 CMOS 放电或者清除 CMOS 中的数据时，不要在系统开机的情况下进行，建议断开电脑电源。

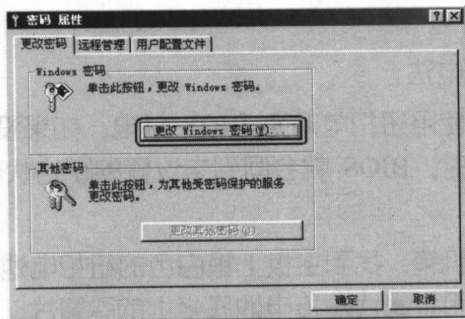
1.1.2 Windows 98 登录密码设置与破解

对于 Windows 9X 系列的操作系统而言, 它的密码安全较差, 启动时按 Esc 键即可跳过登录对话框, 利用其他方法也很容易破解 Windows 9X 系统的密码。

1. 创建 Windows 98 的系统登录密码

在安装完 Windows 98 系统后, 第一次进入操作系统时会弹出一个对话框, 要求输入密码, 如是这时没有输入密码, 而以后又想使用这个功能, 就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”。



步骤 2 单击“更改 Windows 密码”, 根据提示输入密码, 然后再输入新密码并进行确认。

2. 解除 Windows 98 密码

一般 Windows 用户的登录密码都记录在 *.pwl 密码文件里, 因此, 只要直接删除 Windows 目录下的 *.pwl 密码文件及 Profiles 子目录下的所有个人信息文件, 即可解除 Windows 98 密码。具体步骤如下:

步骤 1 重新启动计算机, 在进入 Windows 之前, 按 F8 键选择“Command prompt only”项进入 DOS 状态。

步骤 2 在 DOS 下进入 Windows 目录。一般为 C:\Windows。

步骤 3 在命令符下敲入“Dir *.pwl”命令, 这样在屏幕上将显示出所有用户的密码文件。

步骤 4 使用“Del *.pwl”命令删除所有密码文件。

步骤 5 重新启动计算机，进入 Windows 的登录窗口，选择某个用户名，然后任意输入密码就可以进入 Windows 系统了。

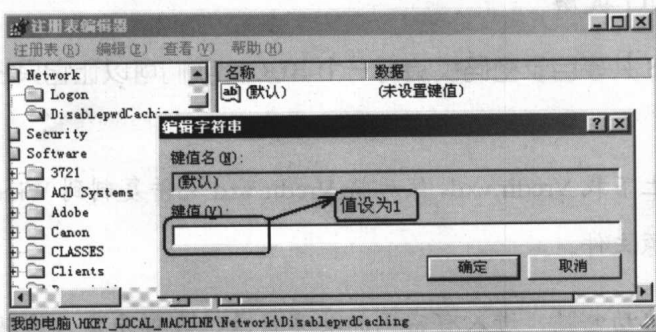
技巧与提示:

这里的用户名就是前面用 Dir 在 DOS 下查找到的文件名。虽然破解了密码，但我们没得到*.pwl 密码，怎么办呢？其实很简单，我们把*.pwl 文件复制到软盘，拿这张盘到其他系统上，安装并运行“PWL 密码查看器”即可。

3. 保护措施

既然 PWL 文件这么容易被击破，那么我们有什么办法能防范这种攻击呢？针对 PWL 密码高速缓存文件的特点，Windows 9X 的系统策略编辑器（System Policy Editor）可以用来禁止密码高速缓存，具体方法是把以下的 DWORD 类型注册表键值设置为 1。

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Network\DisablepwdCaching=1



1.1.3 Windows 98 共享目录密码的破解

在 Windows 98 系统中，有时我们为了能够实现某些资源的共享，往往会给其他用户设置一个共享目录，并给这个共享目录设置密码，这样其他用户就可以通过“网上邻居”实现对资源的访问。但是由于 Windows 98 密码的脆弱性，只要稍懂点密码知识的人都可以轻松取得你的密码。

1. 软件破解

利用工具——NetPass：它可以快速扫描网络中的主机 IP、主机名、MAC 地址，以及网络中主机所打开的端口。并且可以方便地将扫描结果存为 EXCEL 文件或文本文件。

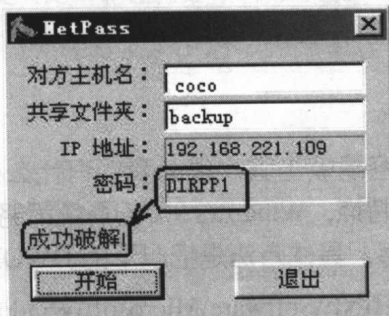
应用版本：NetPass 1.0

下载地址：ftp://61.186.252.131/download/2/19035_NetPass.rar

实例操作：

步骤 1 从上面的地址下载到共享密码破解软件 NetPass.exe，将文件解压缩后运行其主程序，在“对方主机名”后的文本框中输入需要破解共享口令的主机名，在“共享文件夹”中输入需要破解共享口令的文件夹。

步骤 2 单击“开始”按钮后，只需不到一秒钟的时间，就可以轻松地破解出对方的共享口令和 IP 地址。



2. 利用 BUG 破解

Windows 98 共享目录密码校验有一个 BUG，我们可以让它只校验密码的第一个字节。

步骤 1 从网上下载 Vredir.vxd，然后将 Vredir.vxd 文件复制到 Windows\System 目录并覆盖原文件。

步骤 2 重新启动电脑，进入有密码的共享目录，在弹出输入密码的提示框时不输入密码，按住回车键不放，直到进入此目录。如果弹出“密码不对”提示对话框，只要按住回车键不放，选择“确定”按钮，然后测试下一个密码。通常只要按住回车键不放很快就能进入 Windows。

技巧与提示：

只要从 <http://download.microsoft.com/download/win98se/update/11958/w98/en-us/273991sa.5.exe> 地址下载补丁程序进行安装即可解决此 BUG。

3. 查找法破解

利用查找法破解密码之前，首先要了解一下 Windows 98 共享密码对照表：

A=74=db=0c=e7=12=e8=95=2b

B =77 =d8 =0f =e4 =11 =eb =96 =28
 C =76 =d9 =0e =e5 =10 =ea =97 =29
 D =71 =de =09 =e2 =17 =ed =90 =2e
 E =70 =df =08 =e3 =16 =ec =91 =2f
 F =73 =dc =0b =e0 =15 =ef =92 =2c
 G =72 =dd =0a =e1 =14 =ee =93 =2d
 H =7d =d2 =05 =ee =1b =e1 =9c =22
 I =7c =d3 =04 =ef =1a =e0 =9d =23
 J =7f =d0 =07 =ec =19 =e3 =9e =20
 K =7e =d1 =06 =ed =18 =e2 =9f =21
 L =79 =d6 =01 =ea =1f =e5 =98 =26
 M =78 =d7 =00 =eb =1e =e4 =99 =27
 N =7b =d4 =03 =e8 =1d =e7 =9a =24
 O =7a =d5 =02 =e9 =1c =e6 =9b =25
 P =65 =ca =1d =f6 =03 =f9 =84 =3a
 Q =64 =cb =1c =f7 =02 =f8 =85 =3b
 R =67 =c8 =1f =f4 =01 =fb =86 =38
 S =66 =c9 =1e =f5 =00 =fa =87 =39
 T =61 =ce =19 =f2 =07 =fd =80 =3e
 U =60 =cf =18 =f3 =06 =fc =81 =3f
 V =63 =cc =1b =f0 =05 =ff =82 =3c
 W =62 =cd =1a =f1 =04 =fe =83 =3d
 X =6d =c2 =15 =fe =0b =f1 =8c =32
 Y =6c =c3 =14 =ff =0a =f0 =8d =33
 Z =6f =c0 =17 =fc =09 =f3 =8e =30
 space =15 =ba =6d =86 =73 =89 =f4 =4a
 1 =04 =ab =7c =97 =62 =98 =e5 =5b
 2 =07 =a8 =7f =94 =61 =9b =e6 =58
 3 =06 =a9 =7e =95 =60 =9a =e7 =59
 4 =01 =ae =79 =92 =67 =9d =e0 =5e
 5 =00 =af =78 =93 =66 =9c =e1 =5f
 6 =03 =ac =7b =90 =65 =9f =e2 =5c
 7 =02 =ad =7a =91 =64 =9e =e3 =5d

8=0d=a2=75=9e=6b=91=ec=52
 9=0c=a3=74=9f=6a=90=ed=53
 0=05=aa=7d=96=63=99=e4=5a
 ~ =4b=e4=33=d8=2d=d7=aa=14
 ` =55=fa=2d=c6=33=c9=b4=0a
 !=14=bb=6c=87=72=88=f5=4b
 @ =75=da=0d=e6=13=e9=94=2a
 # =16=b9=6e=85=70=8a=f7=49
 \$ =11=be=69=82=77=8d=f0=4e
 % =10=bf=68=83=76=8c=f1=4f
 ^ =6b=c4=13=f8=0d=f7=8a=34
 & =13=bc=6b=80=75=8f=f2=4c
 * =1f=b0=67=8c=79=83=fe=40
 (=1d=b2=65=8e=7b=81=fc=42
) =1c=b3=64=8f=7a=80=fd=43
 - =18=b7=60=8b=7e=84=f9=47
 _ =6a=c5=12=f9=0c=f6=8b=35
 + =1e=b1=66=8d=78=82=ff=41
 = =08=a7=70=9b=6e=94=e9=57
 [=6e=c1=16=fd=08=f2=8f=31
] =68=c7=10=fb=0e=f4=89=37
 { =4e=e1=36=dd=28=d2=af=11
 } =48=e7=30=db=2e=d4=a9=17
 ; =0e=a1=76=9d=68=92=ef=51
 : =0f=a0=77=9c=69=93=ee=50
 ' =12=bd=6a=81=74=8e=f3=4d
 " =17=b8=6f=84=71=8b=f6=48
 , =19=b6=61=8a=7f=85=f8=46
 < =09=a6=71=9a=6f=95=e8=56
 . =1b=b4=63=88=7d=87=fa=44
 > =0b=a4=73=98=6d=97=ea=54
 ? =0a=a5=72=99=6c=96=eb=55
 / =1a=b5=62=89=7c=86=fb=45