西门子 S7-200CN 解密教程

1. 需要热风枪一把，镊子一把，烙铁一把

2. 需要自制 24C 编程器一个，(DB9 头一个，4.7K 电阻两个(或贴片 472)，电阻等可以在废旧电器里找，现在贴片元件最多了。

3. 下载安装 PonyProg2000-CN 软件

4. 下载安装 WINHEX 软件

拆机机密请慎用，动手能力不强者或没有电子电路维修经验者慎用。

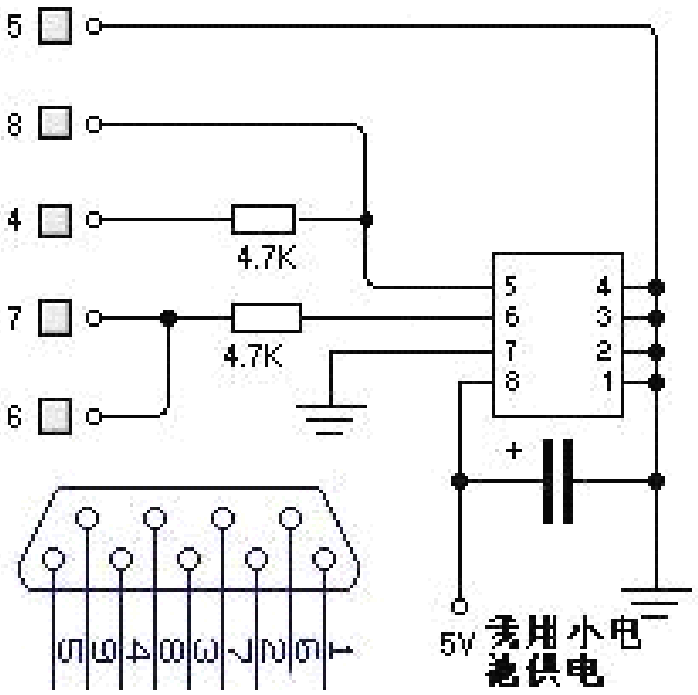
有问题交流联系我 QQ ：1300358487

一：拆机解密，经实践，已证实此方法可以破解迄今为止市面所售的所有西门子 S7-200PLC（进口，国产 CN 型）的密码，型号包括（212、214、216、222、22CN、224、224CN、224XP、224XP CN、226、226CN、226XM）轻松破解 3 级和 POU 密码。是迄今为止最为先进且真正实用的解密方法，直接读取 PLC 的 EEPROM 芯片获取密码。（注：目前市面上没有纯软件可解西门子 S7-200CN 新版，必须通过拆机来解密，如果说卖家说有不需拆机能解密者，请你三思而后行）.

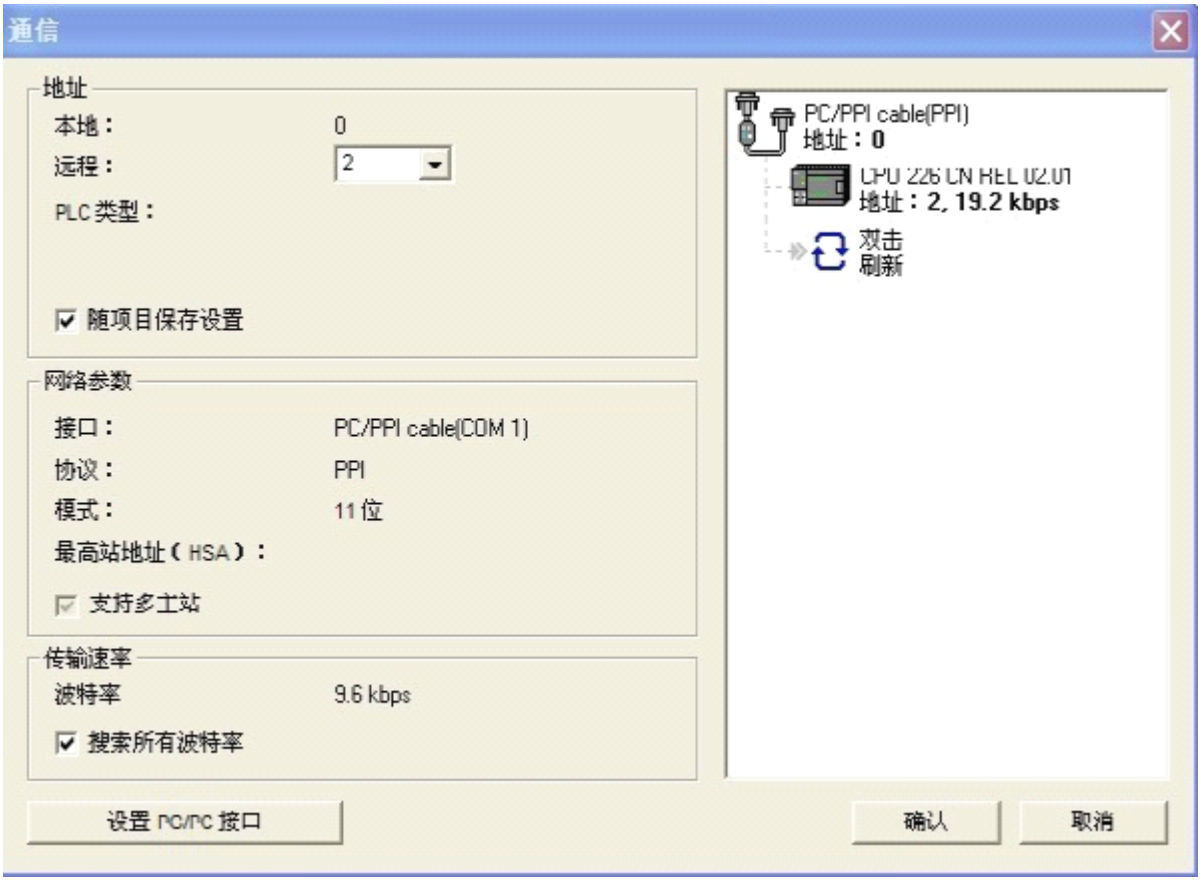
二：初次解密时有条件的最好能够先找一台 PLC 机实验或我们提供的一个有程序的

EEPROM 芯片 24C512 读取数据，按照下面的流程操作一次。不可莽撞行事，以免有不可预料的麻烦。下面你需要自备工具 2 件，第一件就是电烙铁或风枪一个最好是热风枪（如果没有可以买一个工业塑料焊枪小的那种），第二件就是镊子一把。

按下图制作一个 24C 的编程器



三：在拆机解密之前，请先用西门子 4.0 以上的编程软件“STEP 7-MicroWIN”或西门子 S7-200 内存读写工具，读取一下 PLC,第一确定 PLC 的加密等级，第二确定 PLC 的通讯波特率与 PLC 地址。

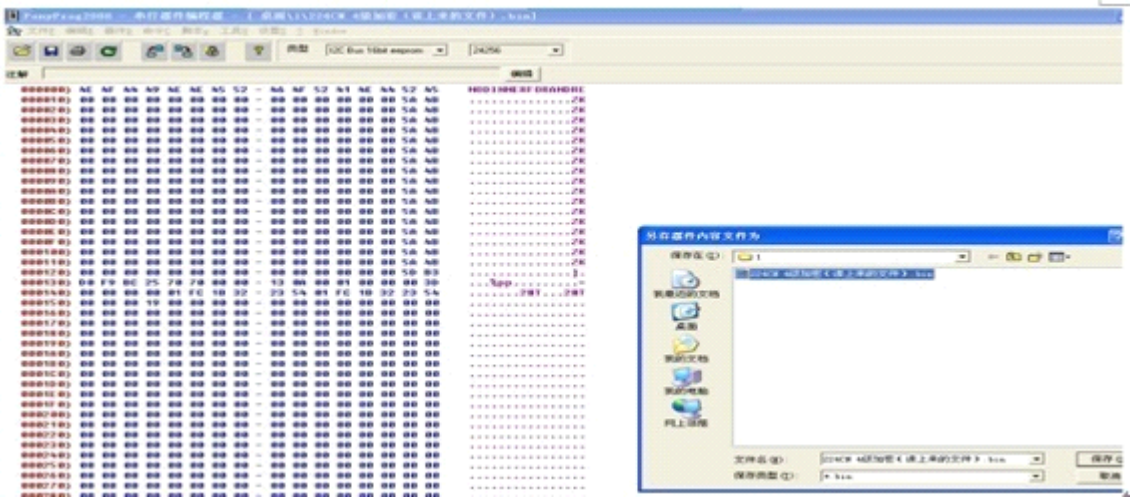


用“西门子 S7-200 内存读写工具”读出 PLC 的内存数据，（断电保持的数据等）

四：按照西门子的 PLC 的安装说明拆开上盖，拆下 CPU 板，找到 24CXX 芯片，用电烙铁或风枪拆下 EEPROM 芯片来。 注：CPU221CN CPU222 CN EEPROM 芯片是 24C64，CPU224 CN，CPU224XP CN EEPROM 芯片是 24C256，CPU226 CN，CPU226XP CN EEPROM 芯片是 24C512，其他型号的 PLC 可以不用拆机解密，解密软件网络上下载

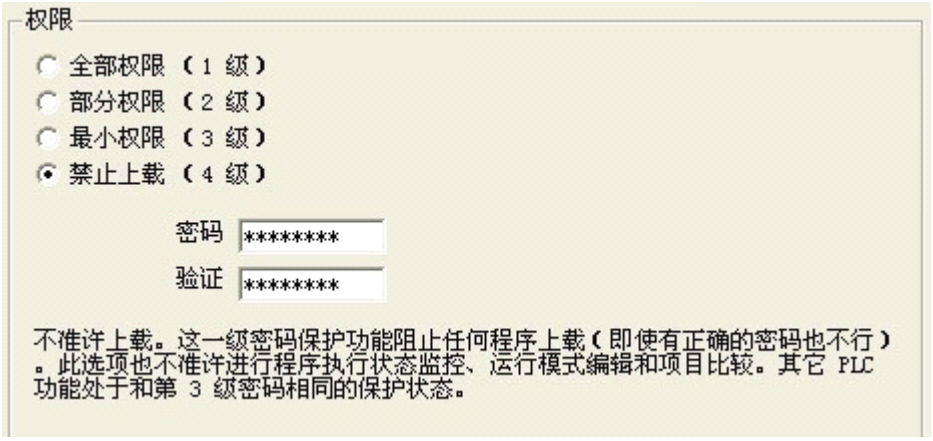
五：接下来下一步开始读 EEPROM 芯片，把芯片和编程器焊接 好后，先插 DB9 的数据线，5V 供电采用 USB，然后再插 USB 供电，打开软件 PonyProg2000-CN 设置一下通讯

端口后点击读取器件，保存。注意保存此文件将来用它可以恢复 PLC 至拆机前的状态。



六：**S7-200CN（新版 PLC）解密分 3 级解密与 4 级解密**：3 级密码破解比较简单，芯片读取完数据后保存为 BIN 文件后，你就可以直接运行此套软件包里的“S7－200 拆机解密软件”直接就可以显示密码了。然后把芯片焊回 CPU 板上就可以用密码上载程序了。

S7-200CN（新版 PLC）4 级解密是 CN 解密的关键技术，我们先看看**西门子官方说法：**

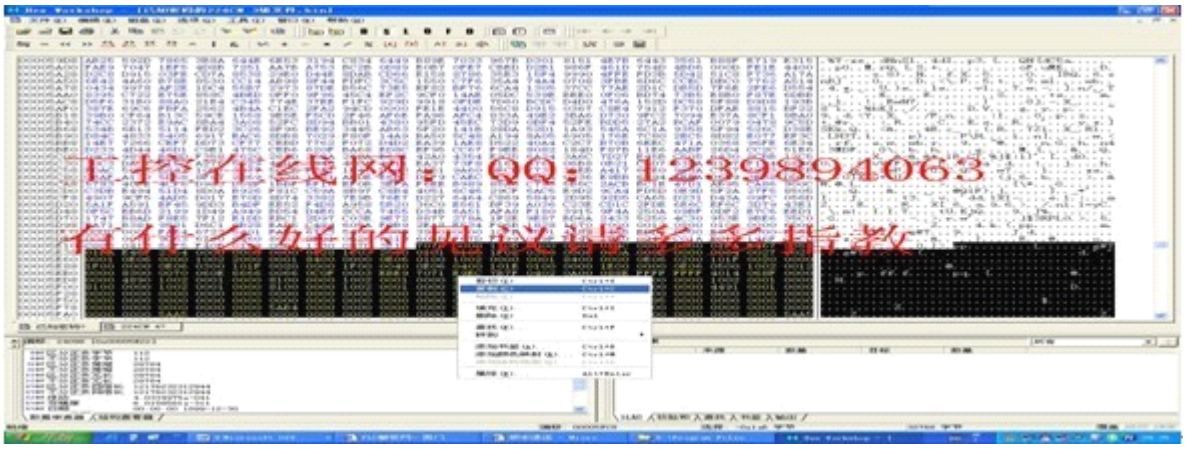


⑦：新版本的 S7-200plc 新增加了第 4 级保护，就是禁止读取和写入，无论你是否已知密码。都无法上传 PLC 中的程序。破解这种加密的 PLC 确实有一定的难度。**破解 4 级密码思路**是：**西门子的程序都是分为程序块、数据块和系统块的，密码就是在系统块里的，在 BIN 文件里是分别保存的。但是 4 级的你读取了密码也不能上载程序，所以要把 4 级修改成 3 级或更低级，但是如果你只修改密码保护级别，又牵扯到一个关于块的校验码的问题，校验错误同样不能上载程序或上载来是空白程序，并且 PLC 故障灯报错。我们能否用已知 3 级加密的整个系统块来替换未知的整个 4 级加密系统块，程序块、数据块不动。这样，我们就能够破解 S7-200CN plc 第 4 级的加密保护**。这就是最简便容易破解 4 级保护的方法。也是目前唯一的便捷解密之法。

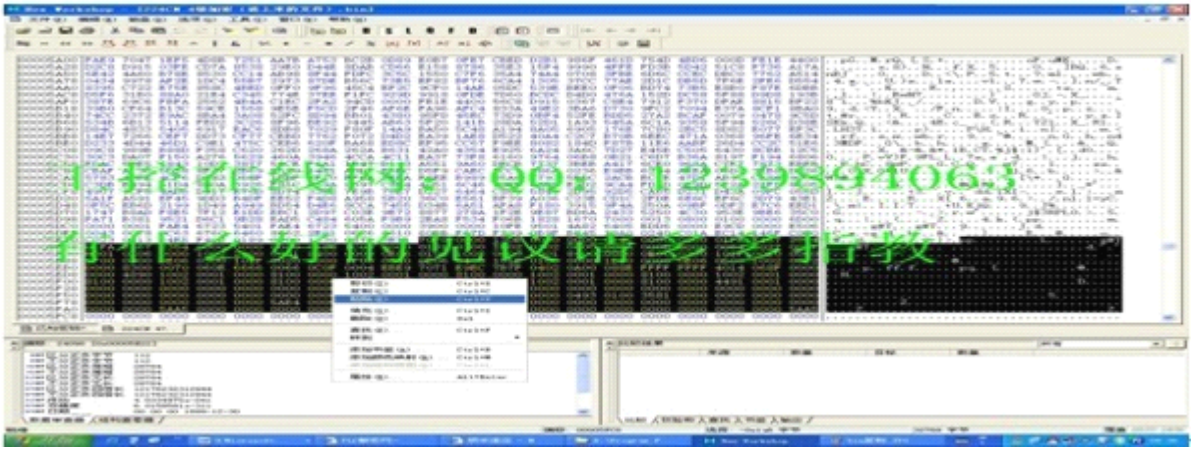
⑧：打开 4 级的 BIN 文件，把(226cn 为 a5f7，224cn 为 5ebf)04 级改为 03 级保存，然后用“S7－200 拆机解密软件”读出 bin 文件密码，此时读出的密码就是排列成的密码，但是文件不能写回 24C 的否则 PLC 报错。

224cn 密码区:5ec0 到 5ec7.　　226cn 密码区:a5f8 到 a5ff.　　224 密码区:3e76 到 3e7d.　　226 密码区:a690 到 a697.　　222 密码区:1e76 到 1e7d .

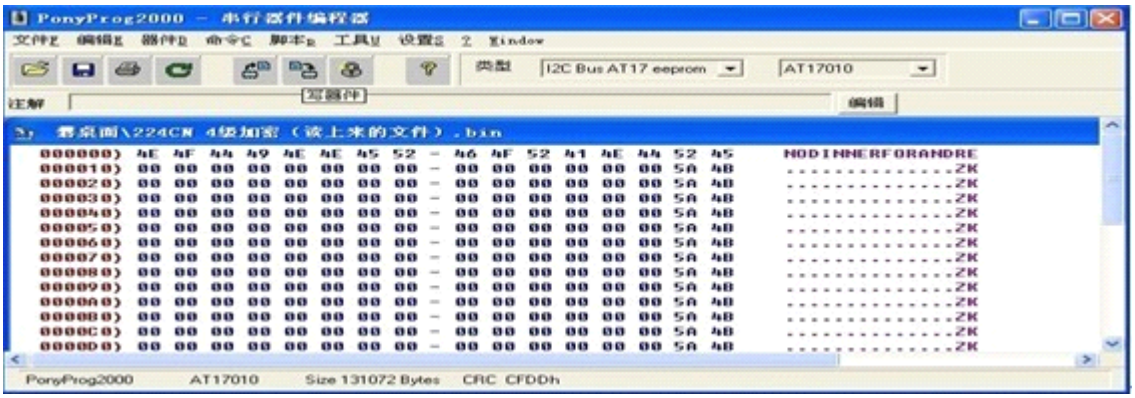
九：接下来我们现在要找出系统块的在 BIN 文件中的位置：那么块的位置在哪里呢？请安装 winhex 软件，。打开你刚才所保存的 4 级的 BIN 文件，再打开同型号的 CPU 型号的 3 级文件，举例 224CN。看图，你拖动鼠标选择 5e22 到 5fcf 之间的数据，然后在选择区域右单击鼠标，在随后弹出的选择框中点击“复制”，



十：然后点击激活你要破解的 4 级 BIN 文件，找到相同的地址，就是开始位置的 5e22 到 5fcf 的数据，记住替换**只能是相同 cpu 同版本替换**，并且所有块的起始位置都是从 5e22 开始的，这是规律。你现在可以在 4 级密码文件选中的数据文件上单击，在弹出的选择框中选择“粘贴”，



你可以点击保存，原有的 4 级**系统块**就被替换成 3 级**系统块**，重新写入 24C 芯片，



再用热风枪焊接，安装、上电,这时 PLC 如果没有报错误的话就可以上载程序了。

CPUU226CN 替换系统块 a55a 到 a71f

最后把停电保持数据等恢复回去

至此。S7-200CN（新版 PLC）4 级加密已成功破解。

如果没有三级密码的同型号的 BIN 文件可以采用以下方法，备份好读出的文件，执行 PLC 清除操作，在系统块里设置好 3 级密码，下载到 plc 里，在读出 BIN 文件，复制系统块。替换

有问题交流联系我 QQ ： 1300358487

2011-05-23