

西门子STEP7解密全攻略



本书由 **PLC 解密网** 倾情奉献

<http://www.plcjiemi.com>

TEI:13969908936


QQ:596181637

E-mail:plcjiemi@qq.com

西门子 STEP7解密全攻略之 S7-200CN解密

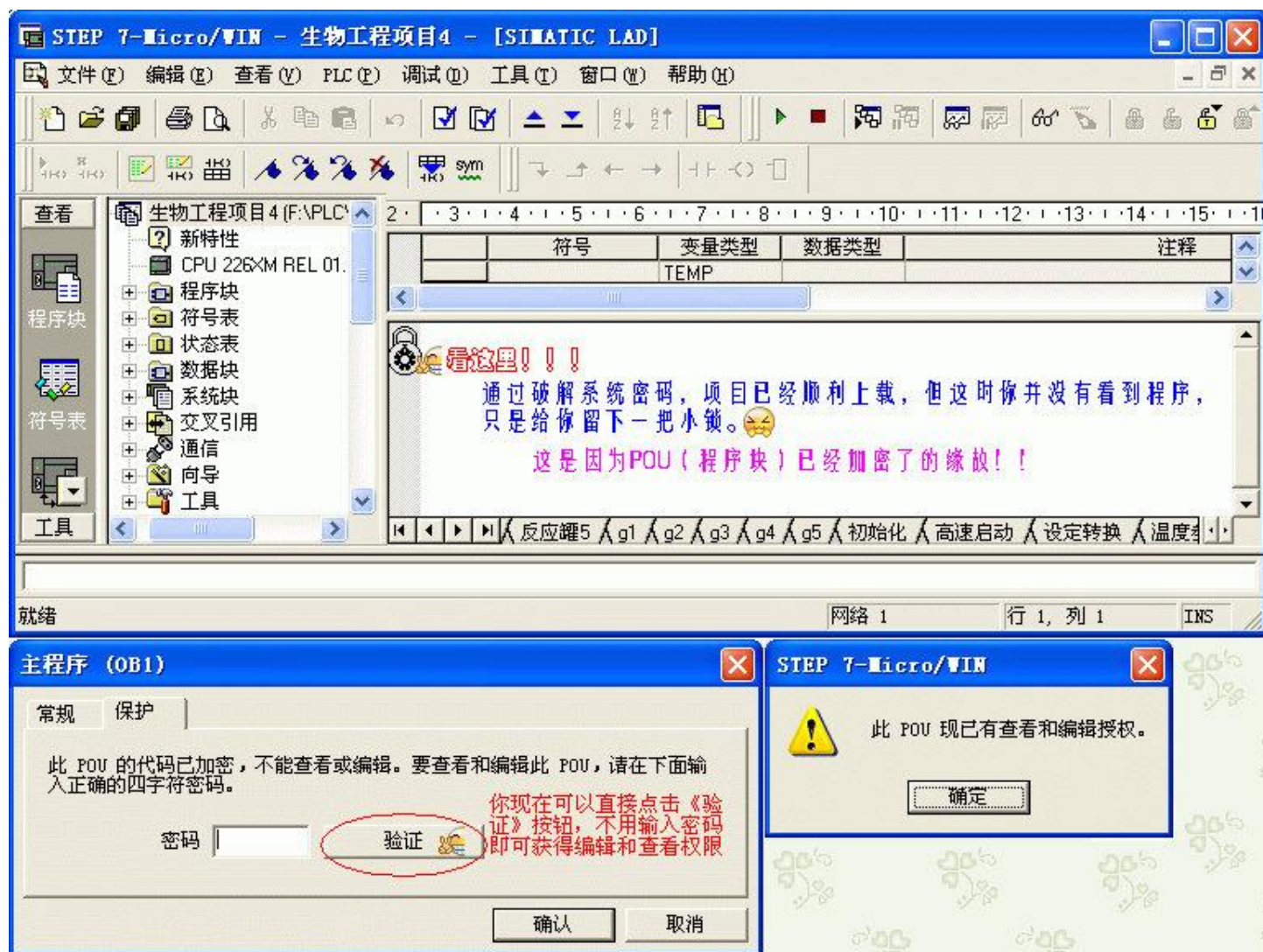


1 西门子 S7-200的 PLC密码共分三个层次，我们最为关心的就是系统密码，因为它直接影响到程序的上载，也是我们所要破解的关键一层密码。其次就是 POU密码，对于西门子的 200PLC,你虽然已经破解了系统密码，也上载了程序，但是每个 POU都显示一把小锁，你并打不开程序，直接影响我们对程序的编辑。再一个就是项目密码，是程序员做完项目后为保密而在编程软件的“文件”下的“设置密码”下而生成的。然而下载后并没有这个密码，所以这层密码并不是我们所要考虑的问题，如果网友有需要的话，可以 [点击下载](#)。

2 首先连接好与 PLC的 PPI编程电缆，如果您还没有编程电缆，那么你就自己开发一根吧！ 看下面的解密软件图，是 2010年开发的不用注册的完全授权版本，您只需下载解压后便可使用。如果您还没有下载请在此 [点击下载](#) 设置好 S7200的波特率、站号，如果提示连接错误可以进行《地址搜索》，搜索完成后点击《读取密码》按钮，密码便出现了！关于本软件的具体使用说明及适用范围请》》》这里进入




3 解子程序 (pou密码)是需要替换 STEP 7-MicroWIN的 datamangers200.dll文件，这样在《查看》菜单的《属性》里面的《保护》不用输入密码就可以打开子程序；请看破解流程图



4 关于破解补丁的安装替换方法：

如果您所使用的编程软件是 STEP 7-Micro/WIN V4.0.6.35 SP6版的。把 (datamanagers200.dll) 拷贝到 "C:\Program Files\Siemens\STEP 7-Micro/WIN V4.0\bin\文件夹下覆盖原文件就可以了。解子程序最低需要 STEP 7-Micro/WIN V4.0.3.08 SP3版,随西门子软件版本的更新分别为 SP4 SP5 SP6,现在已经达到 SP7版,低版本或别的版本不行。各自的版本需要各自的破解补丁,彼此不通用。各版本的破解补丁本站提供免费的下载,解压后按说明安装即可。关于各种版本的破解补丁已经单独打包,如果需要您可以在此 [点击下载](#) 如果 我所 讲的这些您还是不明白,请看下面视频吧!

5 关于 PLC版本为 02版 (cn) 的系统密码破解说法：

点击[这里](#)你先看一下西门子公司说法！新版本的 plc 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。所谓的新版本是怎么区分的？第一看硬件在 PLC 的底部标签的最下面一行就记录了版本号。第二看 PLC 正面标记的 CPU 的型号如 226 CN，如果带有 CN 字符，那么版本号肯定也是 02 版。第三就是通讯读版本号，你用 STEP 7-MicroWIN 连接 PLC，点击[上载](#)按钮，这时弹出的对话框中就清楚的显示了 PLC 的 CPU 型号及版本号。所以说区分新旧版本看的是版本号，带 CN 的只是其中的一种，还有不带有 CN 的也是具有四级加密功能的。也可以这样说凡具有四级加密功能的就称之为新版本。破解这种版本确实有一定的难度，但也并不是象西门子公司所说的无法破解，凡事总有破绽。

现在 CN 的解密套装已开始发售，详情请点击[进入](#)。现在基本可以确定 PPI 协议所能破解的西门子 S7-200 PLC 的范围：02.00 版以下的，包括部分 02.00 版本（确切的说是最高只有 3 级加密功能的 plc），通过本软件就可以轻松破解，02.00 版以上的，包括 02.00 版（精确定位是 - 具备 4 级加密功能的 2.0 版本）和所有的 200CN 型号，只有拆机解密，迄今为止还没有更好的办法！关于版本号，你通过本软件就可以探测到。

6 编程软件的下载：（此版本为西门子官方提供的正式直接安装版，非升级版本）

  s7 - 200 的最新软件 STEP 7-MicroWIN V4.0.9.25 SP9 版请在这里 [点击下载](#) 

西门子 STEP7 解密全攻略之 MMC 密码破解

 look! 这就是一张 512K 的 MMC 卡 

 狂破 S7- 300 400

方法 1: 请先打开《MMC 读卡软件》，破解时先用普通 MMC 读卡器（电脑城、手机店有售，10 元左右或您的电脑本身就有），读出 S7-300 或 400 的 MMC 卡。在软件窗口选择对应的移动磁盘，按一下《读取》按钮，这时在弹出的‘建立文件’对话框中输入你要建



立的文件名，点击《确定》按钮，读取开始了.....待读取完成，程序密码就会出现，看下图。有了密码这样你就可以在线把程序下下来.切记!!如果出现《格式化》对话提示请及时退出,退出后在重新载入.否则出现数据或程序丢失概不负责.附赠一个 300-400 卡写入软件（写卡软件未加密直接解压打开就是），当你不小心将卡格式化,一般情况就报废了,因为数据格式不同，有此软件可写入映像数据,可在 PLC 重新下载程序使用.



方法 2:通过上面的方法你已经破解了 plc 密码，但是如果你以后再次使用，又忘记了密码，而读取 MMC 卡又相当费时（要 10 - 20 分钟），那么一个更为方便快捷的方法又来了 - - - 刚才您已经建立了一个名为***.s7img 的文件，那么现在您再用<MMC 卡解密>这个软件打开该文件，按一下<密码>下的<S7-300>，稍等密码就会出现。有了密码这样你就可以在线把程序下下来，如果程序加了锁再用<S7 程序解密>这个软件解锁即全搞定。这也是唯一能破解 300-400 的软件。



🔧 S7程序解密：

S7程序解密 ,用于加锁解锁 S7 300/400的 OB FB FC DB块。当你有解密软件解密后将程序上传到电脑后 ,很多程序块是加了密的 ,只能显示一个个小锁 ,有此软件可轻而易举打开 .使用前请备份原 Project 以防不测。



🔧 MMC被误格式化的救星来了！

可以将 MMC整个打包读出来写成一个 IMG文件，就象你原来用 HD-COPY给软盘做的 IMG镜像文件一样。当然被误格式化成电脑文件格式的 MMC卡也可以用附带的标准 IMG文件来恢复。比如你把 8M MMC给格式化成 16.7M的 FAT格式，结果电脑认识了，PLC却不认识了，这时候可以用 <MMC写卡软件>拿 8M MMC的 IMG文件来恢复，恢复完就还是 PLC能认识的 8MMC了。软件版本的不同可能导致您无法写入 S7 IMG 文件，所以解压包里共提供 V0.9和 V1.0两个版本，以供选用。



🚩接下来请看 西门子 300 解密全攻略之 [程序还原篇](#)

西门子 STEP7解密全攻略之 MMC程序还原



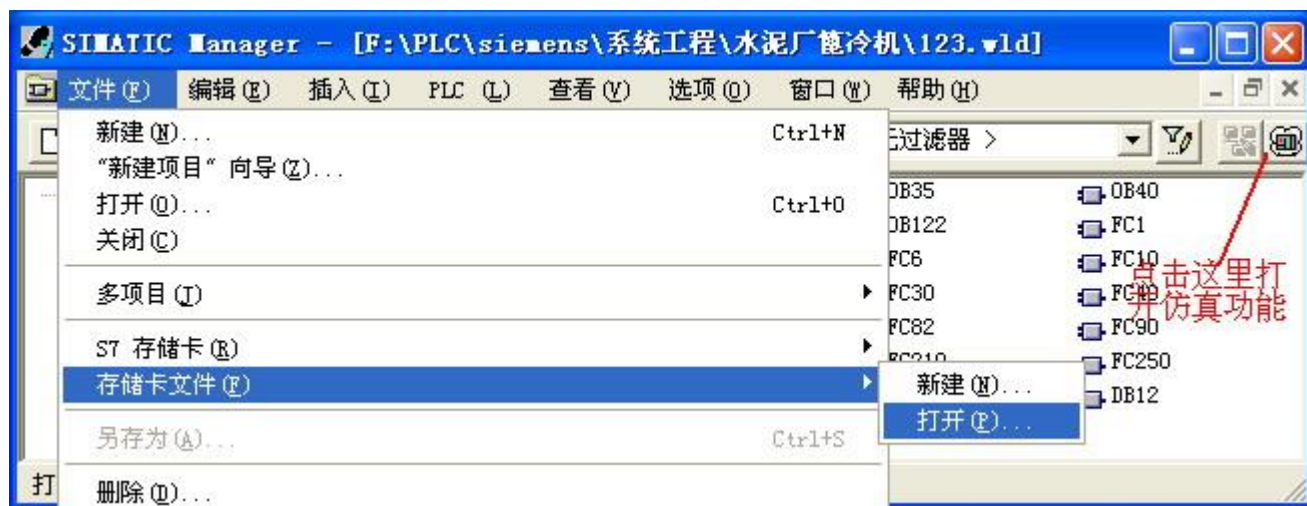
🚩模拟与测试

如果您现在还没有卡，或心里没底不敢轻易使用 MMC 卡，那么就先来模拟一下吧！您需要找来一个普通的随意大小的 U 盘或普通相机或手机的 MMC 卡，仿真当作 S7 的 MMC 卡来作我们的试验品。S7-300 的解密软件您可能已经下载，那么现在就请打开 <MMC写卡软件>，打开<映像文件>文件夹里的<S7-300 2080 压机程序>写入到 U 盘。到此，您已经拥有了一个仿真的 MMC 卡了，现在可以按照上面的解密方法破密码了.....不过此方法仅供学习模拟适用，不能代替 S7 的 MMC 卡，也并非绝对不行，如果修改 CID 和 CSD 数据的话 plc 也能认识，但是民用 mmc 卡和工业 mmc 卡的技术参数必定不同，比如温度参数，S7 的 MMC 卡上限温度是 80 度，而普通 MMC 卡只有 60 度。等等原因，所以不建议替代，如果哪位网友替代成功请来信告诉我！

🚩怎样打开卡内的程序：

用 <MMC读卡软件>读出来的文件是一个后缀名为 s7img的文件，这是一种映像文件，这种文件是编程软件无论如何也不可能打开的，那么就需要转换了。具体操作如下图所示：

- 1 运行 <S7 MMC卡转换与解密软件>，点击 <文件> 下的 <打开>，选择你所读出的 S7img文件。
- 2 点击 <转换>下的 <s7img到 wld>，这时会弹出完成消息框，点击 <确定>按钮，到此时转换过程全部完成。
- 3 运行 s7 300 400的编程软件的管理器 <SIMATIC Manager>，在 <文件>选择项里的 <存储卡文件>下点击 <打开>，选择你刚才所转换的 *.wld文件，程序就打开了！遗憾！但是你看不到硬件组态。



编程软件建议使用 STEP7 V5.4中文版或更高，如果您还没有此软件请 [点击下载](#) 

安装本软件是需要授权的，如果你还没有，请在这里 [点击下载](#) 

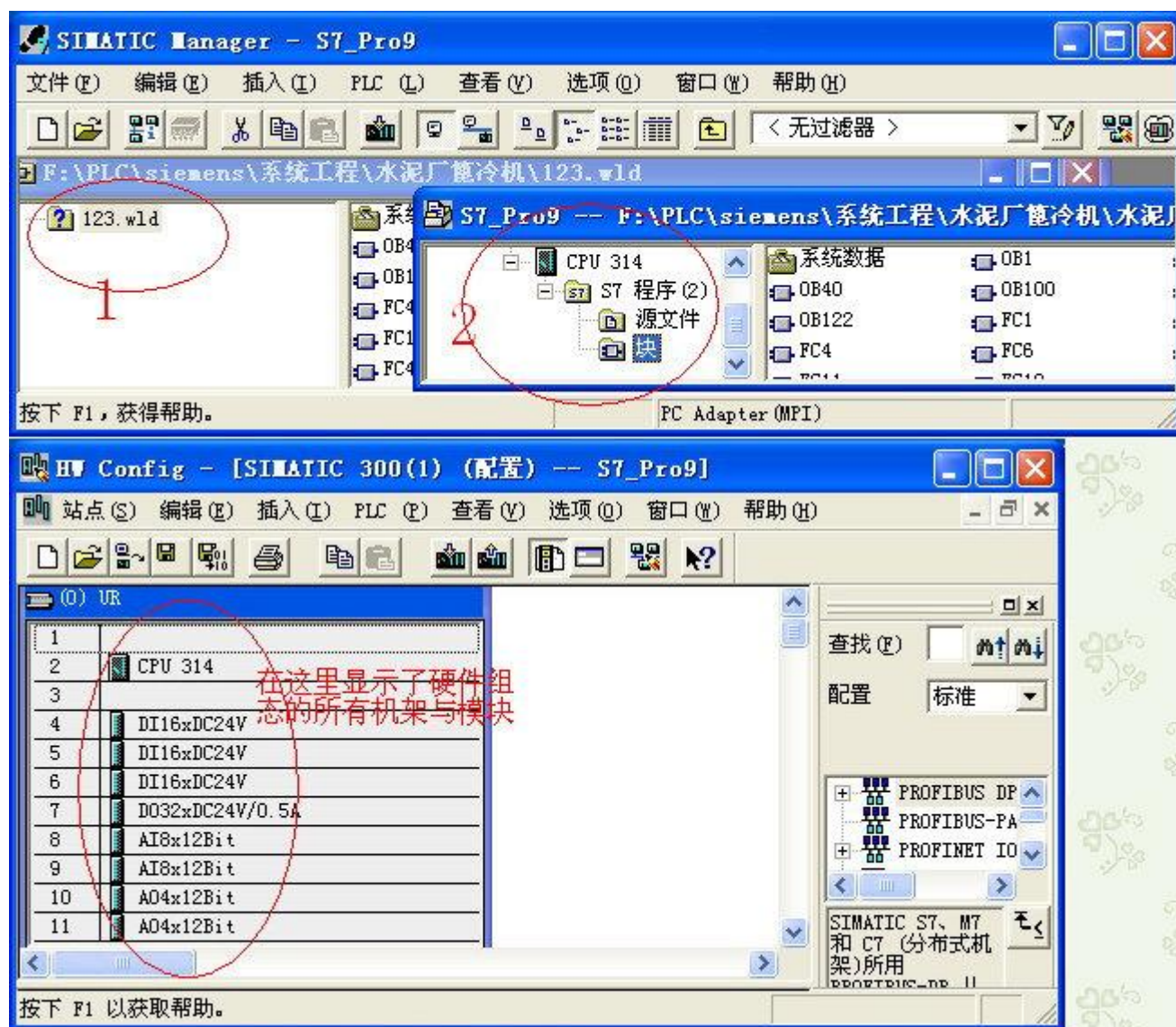
卡文件的还原转换

您打开的卡文件如下图 1 处，只有文件名，并不像 2 处有 cpu 型号及硬件组态，完全不如使用 MPI 电缆下载的好看、好懂。没有关系，我们可以使用仿真软件将其转换。如果您还没有安装西门子公司的 PLCSIM

仿真软件那么请 [点击下载](#)  如果您还不会使用仿真请先看一下视频教程。安装完成后管理器

《SIMATIC Manager》的右上角就会出现如上图指示的一个图标，点击一下便可启动仿真功能。现在不要启动，我们要做的下一步是要复制如下图 1 中右框里的所有的块，当然包括最重要的系统数据块，接下来你点击《文件》下的《新建项目向导》，在弹出的对话框中不必选择 cpu 型号及其他选项，直接《确定》。这时你已经新建了一个工程，在下图 2 右侧栏里右单击鼠标选择“粘贴”，会复制刚才 1 处 123.wld 卡文件的所有块，到这里你就需要启动仿真了！仿真启动后你点击下载按钮，这样一路“确定”、“是”便把工程下载到了仿真机里了。

最后一步点击管理器《SIMATIC Manager》中 PLC 下的 将站点上传到 PG，在弹出的对话框中点《视图》按钮，这时 可访问的节点 栏里会出现 2 CPU841-0 等字符，你点击使其发蓝，再点击《确定》按钮，程序上传了..... 上传完毕后你会发现刚才新建的项目又多了一个项目，你现在可以删除刚才新建的项目，只留下刚刚下载的一个，到这里程序的还原已全部完工！现在我们来看一下刚才还原的程序是不是和用 MPI 电缆下载的一样。点击 SIMATIC 300(2) 在右侧筐里会显示 硬件 和 CPU*** 再双击 硬件 出现如下图所示，好了，接下来你自己看吧！



上接 西门子 300 解密全攻略之密码破解篇

浅谈西门子 S7-400 PLC解密

现在西门子 PLC 大阵营中 LOGO、S7-200CN、S7-300 都已经被破解的体无完肤，根本就无密码保护可言了，密码保护形同虚设。LOGO 在网上已大量流传软件，下载就可以使用。即使是没有软件，其 4 位密码，很快可以暴力破解。其软件下载地址：<http://plcjiemi.5d6d.com/thread-412-1-1.html>

至于 S7-200 早期版本，更是泛滥成灾。软件下载地址：<http://www.plcjiemi.com/2010vjemi.htm> 再看最新的版本就是 02 版以上产品比如 CN 系列，增加了 4 级保护，可以禁止程序上载，无论是否已知密码。

但是这种也已经被拆机破解了，现在这种拆机解密虽然还有几百元的收费，但是用不了半年，就公开免

费了。

对于 S7-300 的产品，为了适应当前的市场，增加 MMC 卡，这正好给破解提供了一个好的破解方法，直接做卡的镜像、克隆，便可以找到密码。此软件也早已泛滥。下载地址:

<http://www.plcjiemi.com/mimapojie.htm>

下一个就轮到西门子 STEP 7 阵营中老大级的人物 S7-400 了！提到这个产品就不禁让人头皮发麻，这个产品多数应用了 PC 卡，就是比 MMC 卡要大的那种，尺寸外形刚好可以插到您的笔记本的 PCMCIA 卡槽。看下面我自己拍的照片，我们来认识一下这位风云老大！第一幅图是卡正面，反面没有字，就不拍了。再看看他的接口，其实跟你的 PCMCIA 引脚定义卡槽的网卡一样一样的。看下面下面我们再来看看他的脸，正面，关键是这里，订货号型号都在这里了，LOOK!这是 FLASH 卡，还有一种我所见到过的 RAM 卡



我们再来看看 S7-400 产品，看右面图。

通过上面我们已经认识了西门子 S7-400 这种产品，言归正传，我们来探讨怎么解密的问题。

破解思路 1、暴力破解

你先到这里下载这个软件 <http://plcjiemi.5d6d.com/thread-413-1-1.html> ,使用串口电缆解密要 3 年，为了提高速度说要用 CP5611 卡来通讯，关于 CP5611 卡的使用你看这里 <http://plcjiemi.5d6d.com/thread-130-1-3.html> 对于此种解密我不抱有信心，你看看网上最多的 WINRAR 解密，就是暴力破解，并且不用通讯，解密一个 6 位字符密码都要 1 个月，何况还要通讯呢？岂不是更慢！，我是没有测试过，也不想浪费这个感情，大家有测试过的，请发表演讲！



破解思路 2、直读解密

这可是最上乘的武功，我等此生是无能为力了，但是我说这个直读解密 S7-400 也并非空穴来风，夸夸其谈。想当年国家为力实现钢铁冶炼中的转炉国产化，不再进口，就组织了国内各大自动化技术研究机构来破解西门子 S7-400PLC,最后由天津传动研究所某位大侠攻破，用的是 PROFIBUS 通讯解密。直到现在都传为佳话，但是解密方法至今还是一个迷，估计是国家最高机密吧！像我等解密发烧网民，即没有实验室，也没有资金支持，搞这个那是天方夜谈，但是像西门子产品研发人员，中国院士里的人员，搞这个还是绰绰有余的，只是出于等等原因不便公开罢了，非但不公开，就连一点蛛丝马迹也没见到过啊！真是悲哀！！

破解思路 3、PCMIA 驱动解密

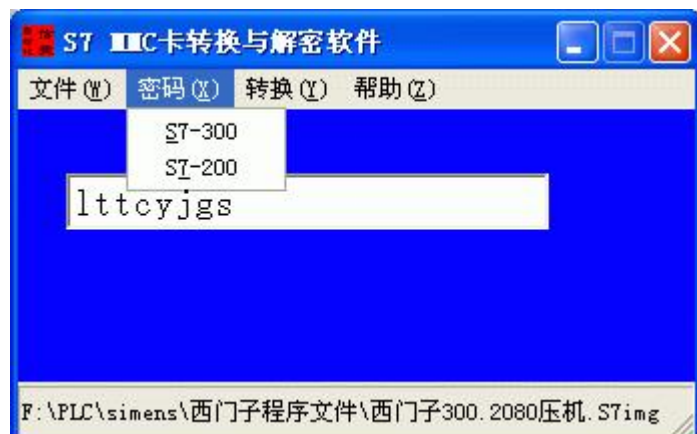
上面我们也提到了，这种卡其实可以直接插到您电脑的 PCMIA 卡槽，硬件可以与通用 PC 机兼容。这种我是做过实验的，插上去后，电脑提示要求安装驱动，天哪我到哪里找驱动啊，自己又不会开发，不过搜到了一个。看这里 <http://plcjiemi.5d6d.com/thread-253-1-1.html> 说安装驱动后便可以显示盘符，跟电脑硬盘一样，我也安装了，但是还是要驱动。伤脑筋，我是没有成功，有实验过的网友也请把实验结果写出来。

破解思路 4、读卡解密

像 S7-300 的产品，直接用普通读卡器就可以读出 MMC 卡，破解密码，是否 S7-400 的也照样可以应用此种方法呢？答案是:NO .为什么这么说呢，你先看看最流行的破解 MMC 卡的软件，看下面的软件图。密码显示下拉窗中有 S7-300,也有 S7-200 为什么就没有 S7-400 呢？是这个软件破解不了 S7-400 吗，非也！，并非破解不了，这个软件只是破解镜像克隆文件的，你只要有文件，知道密码算法，怎么会显示不了密码呢？原因是根本没有人能做得了 S7-400 PC 卡的克隆文件。没有文件，何谈解密啊，这就是之所以这个软件没有 S7-400 选项的原因。如果您对西门子 S7-300 的解密还不甚了解的话呢，你先到这里看看，不然以后的文章你也看不明白。这里 <http://www.plcjiemi.com/mimapojie.htm>

根据上面的思路来看，只要能做了 S7-400 PC 卡的镜像文件就可以找到密码了，对这个思路是正确的。下面我们来看看能读这种卡的设备。第一就要数西门子公司 PG 了，什么 PG 啊？我也不甚了解，更说不好，我没见过，没用过。据说是西门子公司出品的一种笔记本电脑，售价 3 万以上，预装 STEP 7 一切软件，不但软件支持，连西门子的一旦硬件都支持，可以读西门子的公司出品的各种卡，当然包括 MMC 卡和 S7-400 的 PC 卡啦！不过此价值级别的稀世宝物，我等低级网民就无福消受了！但是经网友实验，加密的卡你不输入密码根本就读不了，也做不了备份，也不能做克隆。没戏了，真失败，也有道理，西门子公司怎么会搬起石头来砸自己的脚呢！3 万多的东东也搞不了这个，那么还有没有其他的呢？有！

看这里 <http://plcjiemi.5d6d.com/thread-372-1-1.html> 标题是：siemens 专用读卡器 Prommer 的使用。正文：要是能自己做一个就好了，现在只能看看流口水，版主能不能研发一个。在此感谢这位网友提供的优质资料和好的想法。大家先来看看这个宝贝又是什么样子的！



不错！不错！真的不错，样子好丑，就是不知好不好用，会不会又像西门子的 PG 一样啊！没有用过，

没有发言权，有使用过的网友请赶快发表演讲！但是我看了后面网友的回复气也泄了一半：西门子售价人民币 7569 元 靠！！买个市面上出售的能读 MMC 卡的读卡器才 10 元，简直就是抢劫，我才懒得研究它呢！不过能解密的话我还是非常非常滴喜欢的啊！！

难道市面上就没有能读这种卡的廉价读卡器了吗？我是一直在找，但是一直是未找到。一天一位网友给我发来这个，说能解，我半信半疑，没有用过，给大家看看，有用过的讲话！

分享解密的经过：因为我以前做过西门子的 S7-200CN 的拆机解密，很是顺手，想通过拆卡来解密，我不但想了，而且做了，做过电子维修的网友一看就知道了，西门子的这种卡不是简单的一个存储器芯片那么简单，还加了一个管理芯片，就是那个方形的 CPU，读写的数据都要通过它过滤一遍，那么经过他过滤的数据还能看吗？最后读出的数据就是一团乱码，最终失败。

那么是不是就真的没有办法解决了呢，西门子 S7-400 的加密就真的那么神吗？也并非如此！凡事总有破绽，没有解决不了的密码，功夫不负有心人，只要努力，机会还是有的。我已经成功的破解了几台 CPU412 - 2 CPU412-1 CPU414-2DP 等几个品种，解密速度只需几秒时间，有同样爱好的网友，可以加我好友，找我私聊。

PLC 解密网 二〇〇九年十二月十二日星期六