

# 西门子 STEP7解密全攻略

本书由 [PLC解密网](http://www.plcjiemi.com) 倾情奉献

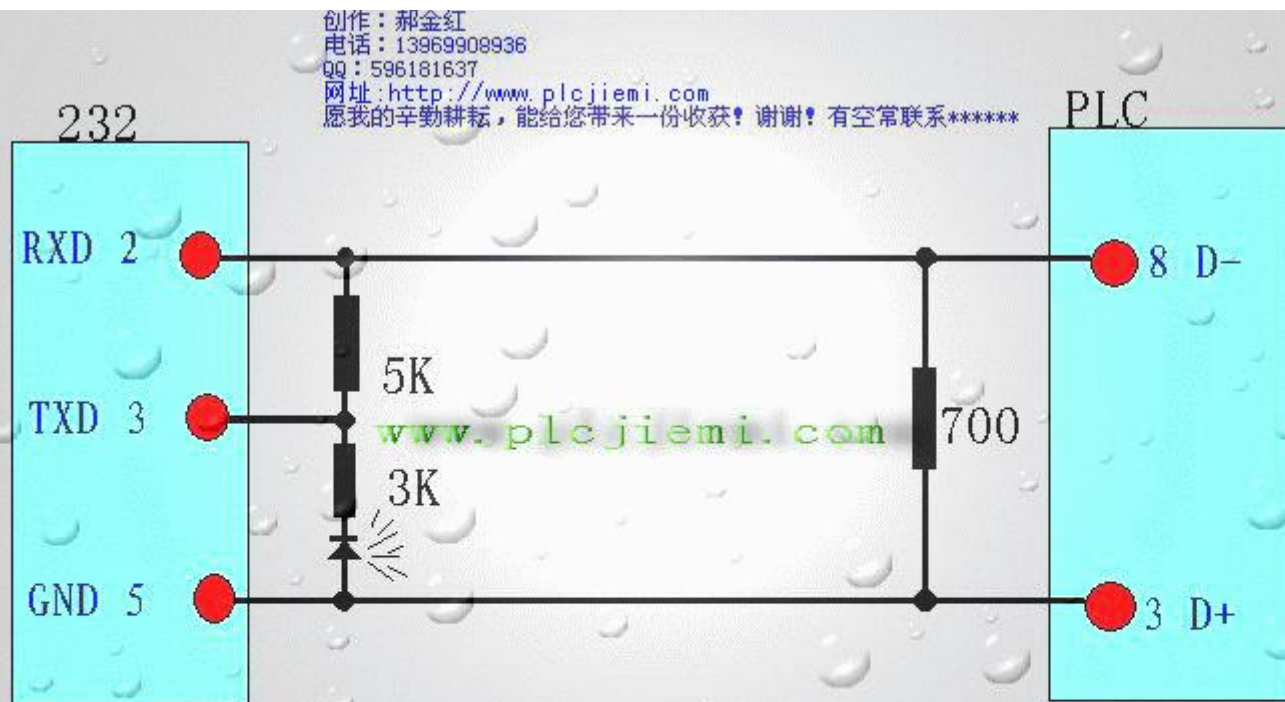
<http://www.plcjiemi.com>

[TEL:13969908936](tel:13969908936) [13054900817](tel:13054900817) [QQ:596181637](qq:596181637) [E-mail:plcjiemi@qq.com](mailto:plcjiemi@qq.com)

## 西门子 STEP7解密全攻略之 200CN解密细说

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，可以来信索取。

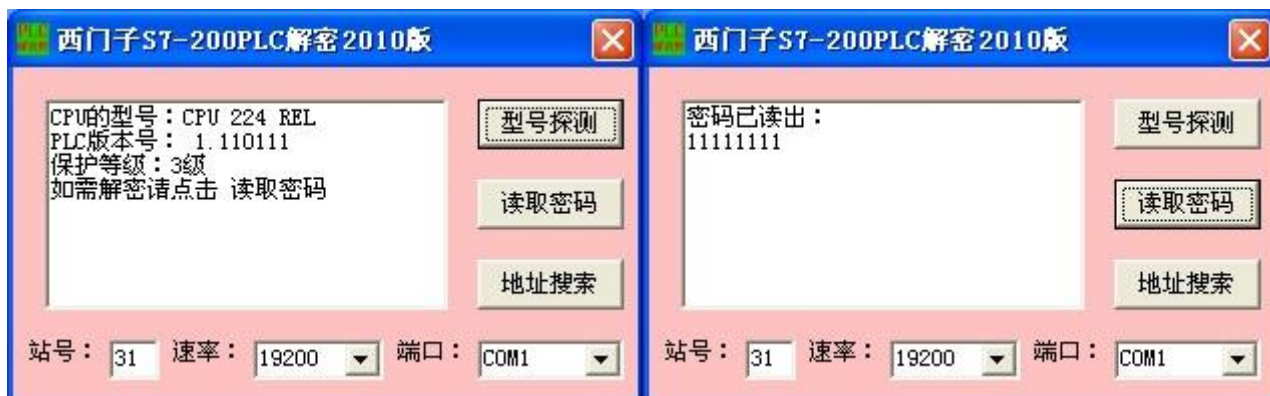
2 首先连接好与 PLC的 PPI编程电缆，如果您还没有编程电缆，那么你就自己开发一根吧！



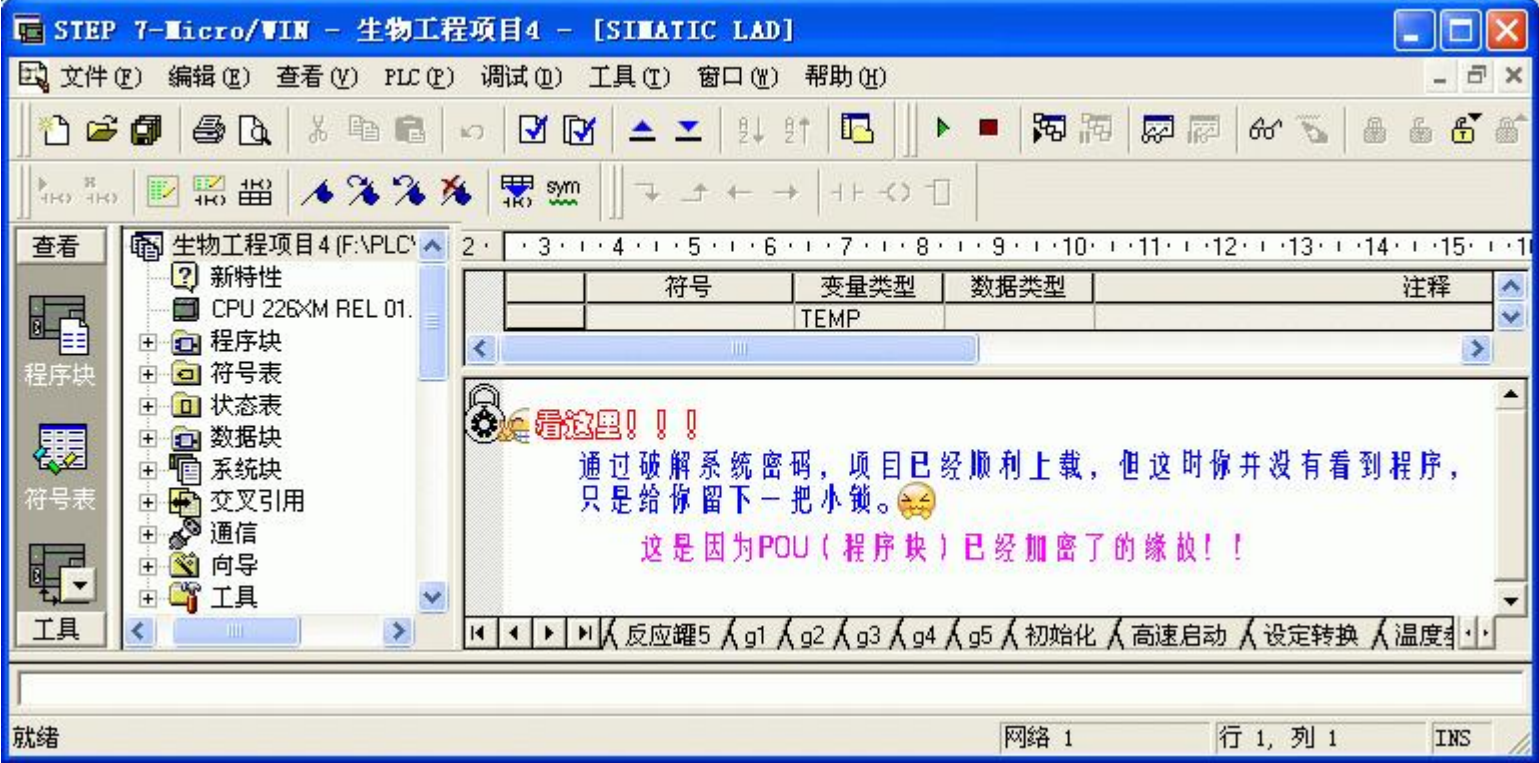
### 西门子S7-200编程电缆

在S7-200 CN CPU224下在以9.6kbps 和19.2kbps 都能通过

看下面的解密软件图，是不用注册的完全授权版本，您只需下载解压后便可使用。设置好 S7200的波特率默认为 9600kbps，点击《解密》按钮，密码便出现了！



3 解子程序 (pou密码)是需要替换 STEP 7-MicroWIN的 datamanagers200.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版、SP5版本、SP6版本，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。各版本的破解补丁随解密软件一并下载，解压按说明安装即可。关于三种版本的破解补丁已经与解密软件一同打包，如果您没有此软件可以在此 [点击下载](#)，也可以来信索取。

#### 5 关于 PLC版本为 02版 (cn) 的系统密码破解说法：

你先看一下西门子公司的说法！

SIEMENS

西门子  
微自动化  
软件

概述

超级树

数据块页

改善的可用性

PID自动调谐

诊断选项

趋势图

内置的PTO向导

菜谱向导

数据日志向导

内存卡

项目保护

字符串数据类型

新的指令

TD支持

杂项

Servicepack 1&2

Servicepack 3 & 4 **25**

Servicepack 5

最新的等级 4 密码保护

等级 4 密码保护防止显示或上传 CPU 里面的程序。

无论你是否已知密码，等级 4 密码保护限制对 CPU 数据的读取和写入。

这个功能为用户的程序提供更好的保密。

LEVEL 4

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。

其破解思路：关键是能够修改降低它的保护等级，密码的破解不是关键。我们通过拆机读取它的 EEPROM, 找到了其密码和保护等级数据位的存放地址，密码的解码方式已破译，现在 CN的解密套装已开始发售，详情请[点击进入](#)。

6 关于编程软件的下载：




# 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载下来。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载下来，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 8MMMC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 8MMMC的 IMG文件来恢复，恢复完就还是 PLC能认识的 8MMMC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

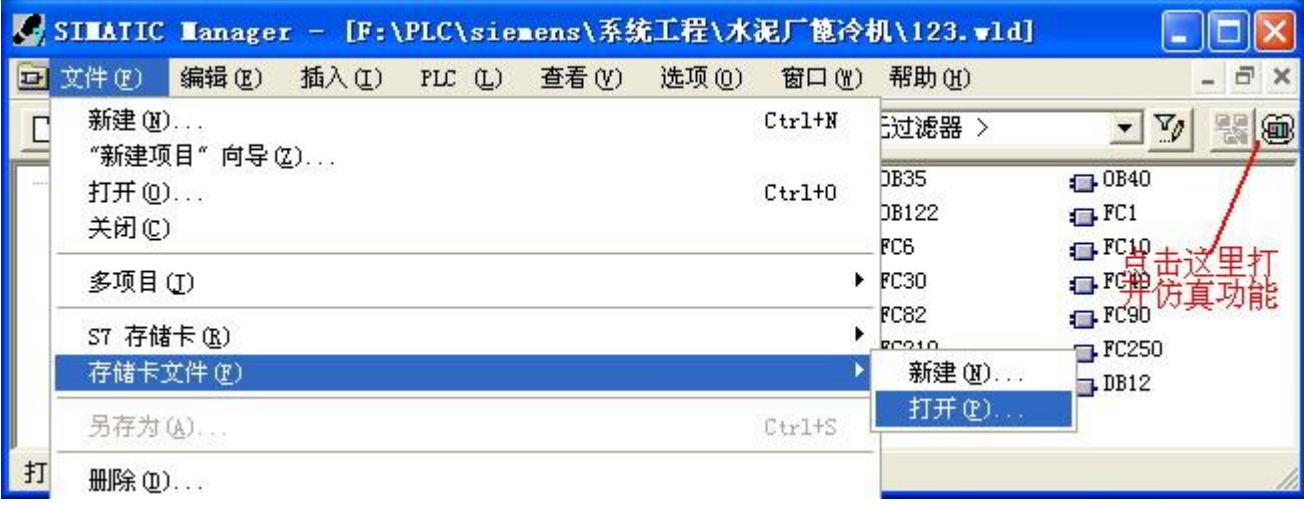
如果您现在还没有卡，或心里没底不敢轻易使用 MMC 卡，那么就先来模拟一下吧！您需要找来一个普通的随意大小的 U 盘或普通相机或手机的 MMC 卡，仿真当作 S7 的 MMC 卡来作我们的试验品。S7-300 的解密软件您可能已经下载，那么现在就请打开 [MMC写卡软件](#)，打开<映像文件>文件夹里的<S7-300 2080 压机程序>写入到 U 盘。到此，您已经拥有了一个仿真的 MMC 卡了，现在可以按照上面的解密方法破解密码了.....不过此方法仅供学习模拟适用，不能代替 S7 的 MMC 卡，也并非绝对不行，如果修改 CID 和 CSD 数据的话 plc 也能认识，但是民用 mmc 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 V5.3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

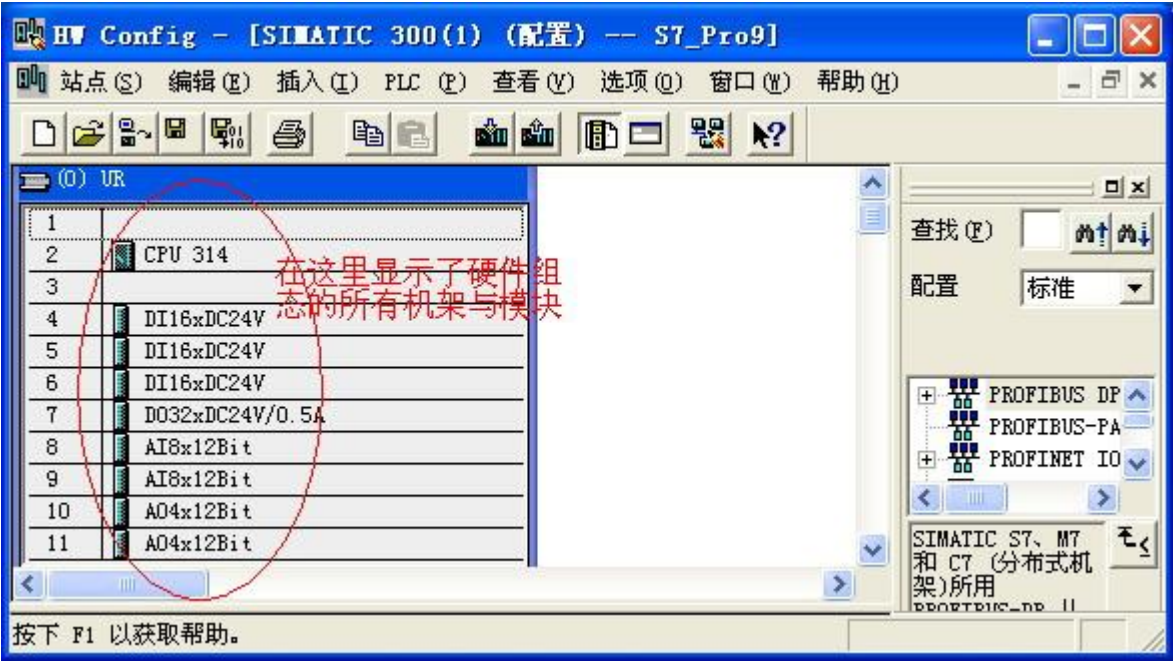
您打开的卡文件如下图 1 处，只有文件名，并不像 2 处有 cpu 型号及硬件组态，完全不如使用 MPI 电缆下载的好看、好懂。没有关系，我们可以使用仿真软件将其转换！如果您还没有安装西门子公司的 PLCSIM 仿真软件那么请 [点击下载](#) 此软件安装也是需要授权 KEY 的，请在这里 [点击下载](#) 如果您还不会使用仿真请先看一下视频教程。安装完成后管理器 <SIMATIC Manager>的右上角就会出现如上图指示的一个图标，点击一下便可启动仿真功能。现在不要启动，我们要做的下一步是要复制如下图 1 中右框里的所有的块，当然包括最重要的系统数据块，接下来你点击《文件》下的《新建项目向导》，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在刚才新建的项目下又多了一个项目，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！



最新推介

软件名称	软件说明	授权方式	下载
三菱 PLC 解密软件	可解 FX0 、FX0S 、FX0N 、FX1N 、FX1S 、FX2 、FX2N、 FX2NC、 A 系列和 FX3U 的一段密码，Q 的不能解	免费下载	
松下 PLC 解密软件	可解 FP0、FP1、FP2、FP2SH、FP3、FPM、FPC、FP5、FP10、FP10S、FP10SH 等系列密码 FPX 和 FPG 不可解	免费下载	
永宏 PLC 解密软件	可解永宏 FB、FBA、FBN、FBE、包括 ID 密码，显示完整密码 FBS 系列可解版本号为 4.52 以下型号	免费下载	
深圳合信 PLC 解密	可解深圳合信产仿西门子 PLC 的全部密码,包括 4 级密码和特有的超强加密 <a href="#">点击进入</a>	电话联系	<a href="#">关于合信</a>
LGK 系列解密软件	LG 解密软件,可解 K 系列 PLC 型号,如果需要破解 K120S.K120SE 最新版本 V2.9 系列 CPU 密码,请联系我	免费下载	
富士 PLC 解密软件	可解富士 NB、NJ、NS、SPB 等 N 系列 PLC 密码，无次数限制	免费下载	
AB PLC 解密软件	可解 AB 的 ML1200、SLC-500 等型号 PLC 显示完整密码	免费下载	

三菱触摸屏解密	三菱 F930、F940、A900、F900 触摸屏解密软件	免费下载	
GP 触摸屏解密	可解 proface 触摸屏全系列密码， 无限制复制版，如设置 禁止上载 则无能为力	免费下载	
eview 触摸屏解密	本软件可以解 EView 全系列,包括以下型号:EMT510T,MT510L,MT508S,MT506S,MT506L 等全部型号	免费下载	
S7-300PLC 解密软件	西门子 S7-300 系列 PLC 解密软件，直接读出 MMC 卡的密码，无次数限制无限制复制版,如果您要破解无卡的 S7-300 型号(如 CPU314)和 S7-400 的型号密码请联系我 点击查看详细的使用说明	电话联系	<a href="#">联系方式</a>
S7-200PLC 解密软件	可以解 S7-200PLC 密码 ( 212、214、215、216、222、224、224XP、226、226XM ) 直接用 PC/PPI 编程电缆读出密码，可解系统密码和子程序密码。解密时间只需 1 秒。可解除 CN 以外的和版本号 2.0 以下的全部型号	免费下载	
S7-200 CN PLC 解密	西门子 S7-200CN(02 版)全授权解密套装今起发售，期待您的关注，详情请 <a href="#">点击进入</a>	电话联系	<a href="#">联系方式</a>
欧姆龙直读版解密	欧姆龙 PLC 解密软件,可解 C200H,C200HS, C1000H, C2000H, CPM1, CPM2*-S*, CQM1、CPM1A、CPM2A 等系列,可解 C 系列四位密码，瞬间显示密码，关键词：直读版，非穷举法解密，速度快	免费下载	
富士触摸屏解密	可解现有的富士触摸屏的所有型号	免费下载	
松下触摸屏解密	可解现有的松下触摸屏的所有型号密码	免费下载	
白光触摸屏解密	可解日本白光全系列触摸屏密码，强力推荐>>这个解密网上免费的很少	免费下载	
台达 PLC 解密软件	可解台达 ES、EX、SS、EP、SA 等系列型号，显示完整密码，无次数限制无限制复制版,EH 的到论坛下载	免费下载	

注 :为了活跃论坛，部分软件移至论坛下载，您只需简单注册一下就可以