[**LOFTER-网易轻博**](http://www.lofter.com)

[LOFTER-网易轻博 logo](http://www.lofter.com?act=qbbkss_20151027_08) [加入LOFTER 免费冲印20张照片>](http://blog.163.com/zhangrui_399/blog/static/6563859020105111810271/#guidearea)

[似水流年](http://blog.163.com/zhangrui_399/blog/static/6563859020105111810271)

**转帖：西门子手机发送AT指令**

**Siemens3508手机AT指令发送短信的实验**

**凡夫**

    最近利用Siemens3508旧手机做了AT指令发送短信的实验。有人可能认为我费那么大劲折腾累不累，告诉你这可是废物再利用，可以利用旧手机里的GSM/GPRS模块做无线远程多点分布数据采集、监控、遥控等，主要是想与RFID模块结合，远程读取电子标签。现在GPRS按流量计费，可以24小时连续在线，无传输数据也就不产生流量，很方便。可以用单片机、GSM/GPRS模块、数据采集模块（如传感器、RFID模块）组成远程终端。这就要求用单片机的串口与GSM/GPRS模块通信。基于这样的目的进行了AT指令控制GSM/GPRS模块的实验。  
    Sie

**Siemens3508手机AT指令发送短信的实验**

**凡夫**

    最近利用Siemens3508旧手机做了AT指令发送短信的实验。有人可能认为我费那么大劲折腾累不累，告诉你这可是废物再利用，可以利用旧手机里的GSM/GPRS模块做无线远程多点分布数据采集、监控、遥控等，主要是想与RFID模块结合，远程读取电子标签。现在GPRS按流量计费，可以24小时连续在线，无传输数据也就不产生流量，很方便。可以用单片机、GSM/GPRS模块、数据采集模块（如传感器、RFID模块）组成远程终端。这就要求用单片机的串口与GSM/GPRS模块通信。基于这样的目的进行了AT指令控制GSM/GPRS模块的实验。  
    Siemens3508手机的GSM模块和西门子的TC35i模块的AT命令集基本一样，TC35i模块的AT命令集资料网上可以搜索到的。由于没有手机数据线，就拆开了手机，Siemens 3508手机数据线接口，一共12脚分别定义为：  
1）充电IN-（充电负级或DATA地）  
2）AUDIO\_L（耳机左声道）  
3）充电IN+（充电正级）  
4）DC+（3.6V供电正极）  
5）DATA\_OUT（数据输出）  
6）DATA\_IN（数据输入）  
7）MODE（线控MIC模式选择）  
8）CTRL（线控按键输入端）  
9）GND（话筒地）  
10）MIC\_IN（话筒正极）  
11）AUDIO\_R（耳机右声道）  
12）AUDIO\_GD（音频地）  
    我们只需把1、5、6脚引出即可，它的串口是3.3V的TTL电平，要和电脑串口连接，还需用232接口电路芯片转换为232电平。接口电路做好后连接好各部分，用超级终端建立串口连接，我的台式电脑设置是COM1、波特率19200、数据位8、停止位1、奇偶校验无、流控制无，连接成功。注意，我的笔记本没有串口，用USB转串口线也可以连接，在执行AT指令时基本正常，发短信可以发出，但是串口死掉了。我的Nokia3230手机用蓝牙（映射串口）和电脑超级终端连接不成功，不知何故，不然可以做做GPRS实验，留待日后研究。  
    好了以上准备工作做好了，可以发AT指令玩转手机了。  
   
 一）基本指令：  
 发送指令  
 AT  
 返回  
 OK  
 表示连接成功。

 AT+CGMI

 SIEMENS  
 OK  
 返回厂家信息。

 AT+CGMM

 3508i  
 OK  
 返回模块信息。

 AT+CGMR  
 12  
 OK  
 返回固件版本号。

 AT+CGSN

 449247374930903  
 OK  
 返回IMEI序列号。

 AT+CIMI

 460007251202938  
 OK  
 返回SIM卡的IMSI。

 AT+CCLK?

 +CCLK: "09/11/04,11:11:41"  
 OK  
 查看当前日期和时间。

二）发送短消息

    先看看手机支持哪些字符集：  
 AT+CSCS=?  
 +CSCS: ("GSM","UCS2")  
 OK  
 可以看到Siemens3508手机支持"GSM"和"UCS2"两种字符集。

     设置对象使用UCS2字符集：  
 AT+CSCS=UCS2    
 OK     
 这样就可以发中英文字符了。

 AT+CMGF=?  
 +CMGF: (0)  
 OK　　  
 查看短消息支持的格式，其格式只有PDU模式一种，没选择。

 下面开始发短信：  
 接收手机号：  13812345678  
 短信中心号：8613800270500   
 短信内容：你好，Hello!

 方法一：　  
 AT+CMGS=32  //设置后面要输入的PDU字串的长度(实际长度/2-1)  
 > 0011000B813118325476F80008A7124F60597DFF0C00480065006C006C006F0021   //输 入的PDU字串，包含了接收手机号码、信息内容等有效内容。稍后详细分析如何得到这个字串。输入后要按“ctrl+z”，显示->  
 +CMGS: 210    
 OK  //表示发送成功，如果返回ERROR表示发送不成功。

 现在我们来详细分析一下如何得到那个PDU字符串。  
 1)首先分析原PDU串中最前面的0011000B81  
　　 按顺序依次表示：  
 00--短消息中心信息的长度，这里的0意味着，采用modem中已存的短消息中心的信息。  
 11--说明信息体格式的字段，普通短信和wap push在这个字段上会有区别的。（普通短信就用11）  
 00--一般取00，采用默认的发送号码。  
 0B--接收手机号码长度的十六进制表示。中国大陆应该都是0B（11=0BH）。  
 81--本部分表明了接受手机号码的类型。这里采用81。  
　　  
 2)接下来是3118325476F8  
　　 接收的手机号码是13812345678，手机号是11位奇数，末尾加F，将原号码变为13812345678F，然后我们把第一位和第二位交换，第三位和第四位交换，以此类推。这样就得到3118325476F8。

 3)再接着是0008A7  
 00--协议标识(TP-PID) 是普通GSM类型，点到点方式。  
 08--用户信息编码方式UCS2。  
    在PDU Mode中，可以采用三种编码方式来对发送的内容进行编码，它们是7-bit、8-bit和UCS2（16-bit）编码。  
    7-bit编码用于发送普通的ASCII字符，它将一串7-bit的字符(最高位为0)编码成8-bit的数据；  
    8-bit编码通常用于发送数据消息，比如图片和铃声等；  
    UCS2编码用于发送Unicode字符。  
    PDU串的用户信息(TP-UD)段最大容量是140字节，所以在这三种编码方式下，可以发送的短消息的最大字符数分别是160、140和70。这里，将一个英文字母、一个汉字和一个数据字节都视为一个字符。  
 A7--信息有效期  
　　 　　  
 4)最后是124F60597DFF0C00480065006C006C006F0021  
   “你好，Hello!”字符串转化为UNICODE代码即为4F60597DFF0C00480065006C006C006F0021，而12（16进制）则等于unicode字符串的长度除以2，即36/2。UniCode编码转换，以中文为例，一个中文字符是两个字节，直接对高位字节和低位字节进行十六进制转换就可以了。如“欢迎”，UniCode 编码是 6B22 8FCE ，这同时也就是转换的结果，如果发送的串中有英文字符，那么在前面补全00 ，以保证一个字符对应两个字节。  
　　    
   
 方法二：　  
 AT+CMGS=41  //设置后面要输入的PDU字串的长度(实际长度/2-1)  
 > 0891683108200705F011000D91683118325476F8000800124F60597DFF0C00480065006C006C006F0021  
 按“ctrl+z”，显示->  
 +CMGS: 211    
 OK  //发送成功  
 两种方法的PDU码有什么区别呢？还是顺序分析：

 08 - 指的是短信中心号的长度，也就是指(91)+(683108200705F0)的长度。   
 91 - 指的是短信息中心号码类型，91是TON/NPI遵守International/E.164标准，指在号码前需加 '+ '号，此外还有其它数值。   
 683108200705F0 - 短信息中心号码。这需要根据不同的地域作相应的修改。前面的(08)+(91)+(683108200705F0)实际上就是短消息中心地址（Address of the SMSC）。

 11 - 文件头字节   
 00 - 信息类型（TP-Message-Reference）   
 0D - 被叫号码长度   
 91 - 被叫号码类型   
 683118325476F8 -被叫号码，经过了位移处理，实际号码为 "8613812345678 "。上面的（00）+（0D）+（91）+(683118325476F8),构成了整个短信的第二部份目的地址（TP-Destination-Address）。

 00 - 协议标识TP-PID,这里一般为00 。  
 08 - 数据编码方案TP-DCS（TP-Data-Coding-Scheme）,采用前面说的USC2(16bit)数据编码 。  
 00 - 有效期TP-VP（TP-Valid-Period）。   
 12 - 长度TP-UDL（TP-User-Data-Length），也就是后面紧跟的短信内容的UniCode编码4F60597DFF0C00480065006C006C006F0021的长度 36 / 2 = 18 的十六进制12 。  
    方法二是在PUD码中指定了短信中心号8613800270500，和国际代号86，注意用方法二在手机里不能预设短信中心号，方法一手机里有没有设置短信中心号，都发送成功了。  
　　  
    以上是在查阅有关资料后对PDU字符串的分解分析，不尽全面或有偏差，但是按这个基本规律对其它信息进行编码发送也是成功的。当然手工计算产生PUD码很繁琐易出错，网上也有人编了程序自动产生PDU码。

　  还有很多指令可以玩，如电话、电话簿、振铃、音量、密码等等，这里就不跑题赘述了。

<http://lubert.blog.sohu.com/135838451.html>

展开全文

2000万年轻人都在用，现在下载有好礼相送

[Apple Store 下载](http://www.lofter.com/app/QRCodedownload?act=qbbkss_20151027_05) [Android 下载](http://www.lofter.com/app/QRCodedownload?act=qbbkss_20151027_04) 

[Apple Store 下载](http://www.lofter.com/app/QRCodedownload?act=qbbkss_20151027_05) [Android 下载](http://www.lofter.com/app/QRCodedownload?act=qbbkss_20151027_04) 



[直接下载](http://lofter.com/app/QRCodedownload) [应用宝](http://android.app.qq.com/myapp/detail.htm?apkName=com.lofter.android) [豌豆荚](http://www.wandoujia.com/apps/com.lofter.android) [360手机助手](http://zhushou.360.cn/detail/index/soft_id/90765) [小米应用商店](http://app.mi.com/detail/16938)

[Apple Store 下载](http://www.lofter.com/app/QRCodedownload?act=qbbkss_20151027_05) [Android 下载](http://www.lofter.com/app/QRCodedownload?act=qbbkss_20151027_04) 