WARNING: DONT USE THIS GUIDE FOR ANY ILLEGAL PURPOSES. USE THIS FOR EDUCATIONAL PURPOSE ONLY

ITEMS NEEDED

1. Plain Wafer Card
2. Sim card reader
3. Software to extract Ki & IMSI
4. Wafer Card Programmer
5. Software to program the wafer card

INTRODUCTION

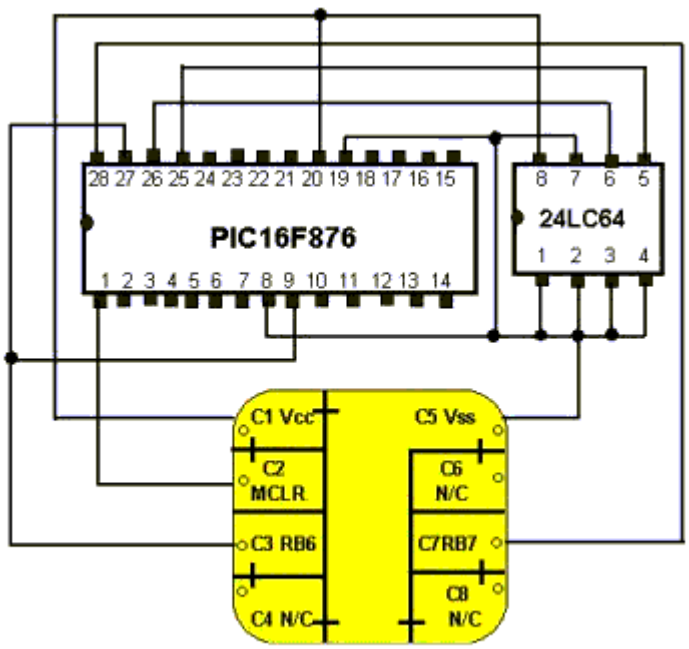
This is a simple and complete guide to sim cloning. With the help of this guide, you will be able to get your sim cloned. This guide is applicable for cloning COMP128V1 version simcards. Eventhough the newer algorithms can't be cloned now, almost 75% of us are using the cards with the COMP128V1 algorithm. Here comes the relevance of this guide. The working on new algorithms COMP128V2 & COMP128V3 are going on and lets hope to get this new algorithms cracked soon. Please dont use this guide for cheating or harming others. Use this at your own risk and the author will not be responsible for any further issues.

TIPS

Always search internet to find the items, softwares and news. Use search engines. They are free and especially for our needs. You may not get these items from your local electronic shops. The main reason is that only a few people know about this. A major group of electronic shops dont know what a silver wafer card is and what a wafer card programmer is.

Wafer Cards

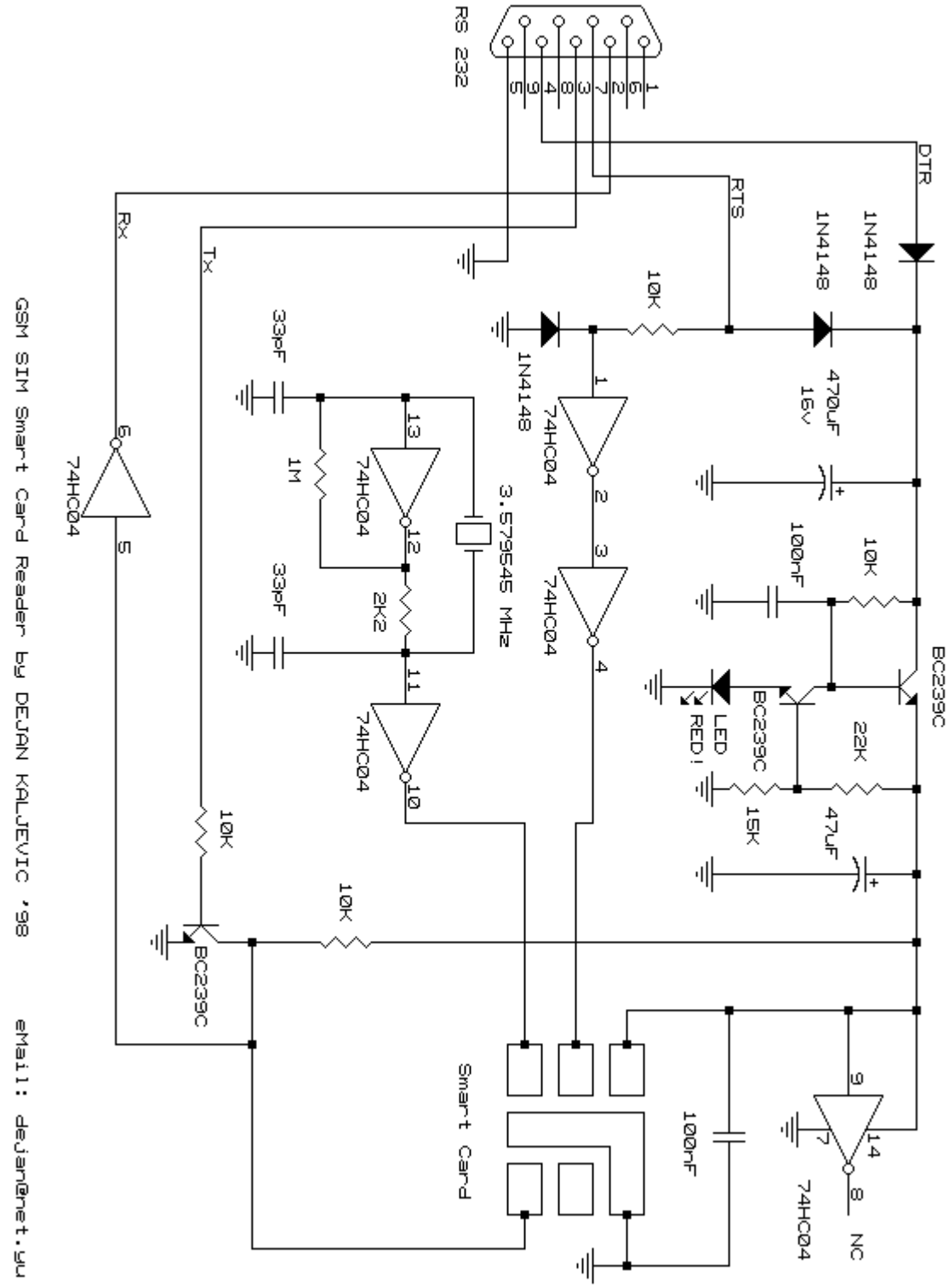
The sim cards we get from the operator are not programmable. So we need to find some plain wafer cards for the purpose. There are mainly three types of wafer cards suitable for GSM cloning. Gold Card, Silver Card and Green Card. Out of these Silver Wafer Cards are used most. So we will take a closer look at Silver wafer Card. Silver wafer card consists of a PIC 16F876 and an EEPROM 24C64. These two electronic components are wired as shown in the below circuit.



You can buy plain silver cards from http://www.pulsat.com and if you dont find one there just search for "silver wafer card" at http://www.yahoo.com or http://www.google.com. If you can't find a plain wafer card in your place or if you can't get one from the internet, you can try the alternate method of manufacturing a silver wafer card by wiring the above circuit. It works fine with almost all the handsets. The only drawback is that, it won't fit inside the handset. We need to place it outside the handset.

Sim Card Reader

You can construct your own sim card reader economically with the following schematic. It uses minimum components and works with almost all the scanning softwares. If you need to increase the speed of the scanning you can replace the 3.57Mhz crystal with a 6.12MHz or 7.14Mhz. The simcards will not support a speed of more than 10Mhz. Also you can try other simcard readers from various providers. It can be USB too. But make sure about the compatibility with the software you are using.



WARNING: DONT USE THIS GUIDE FOR ANY ILLEGAL PURPOSES. USE THIS FOR EDUCATIONAL PURPOSE ONLY

Software to extract Ki, IMSI & ICCID

We need some software to extract the secret key Ki stored in our simcard, The scanning time depends on the software, usage, programmer and the simcard. Some cards take less than 30 minutes and some can take upto 36 hours. I suggest Woron Scan 1.09 for the scanning. Its is a pretty one and much faster. You can download it from the internet. This program took maximum of 6 hours and a minimum of 25 minutes to me. The main feature of this program is, it can recognise whether the card is COMP128 V1 or not. This helps us in wasting the time and wasting our original simcard.

The next one is Sim Easy which can be downloaded from http://simeasy.tlzj18.com. With this software you can scan for Ki and it can be used to edit the contacts stored in the simcard. Yes, we can read the messages too with this software. Some simcards will not work with this software. You can simply cheat the program to connect with those simcards too. Just remove the simcard and press connect in the menu. Then insert the simcard back within a second. You can now use that simcard with this program.

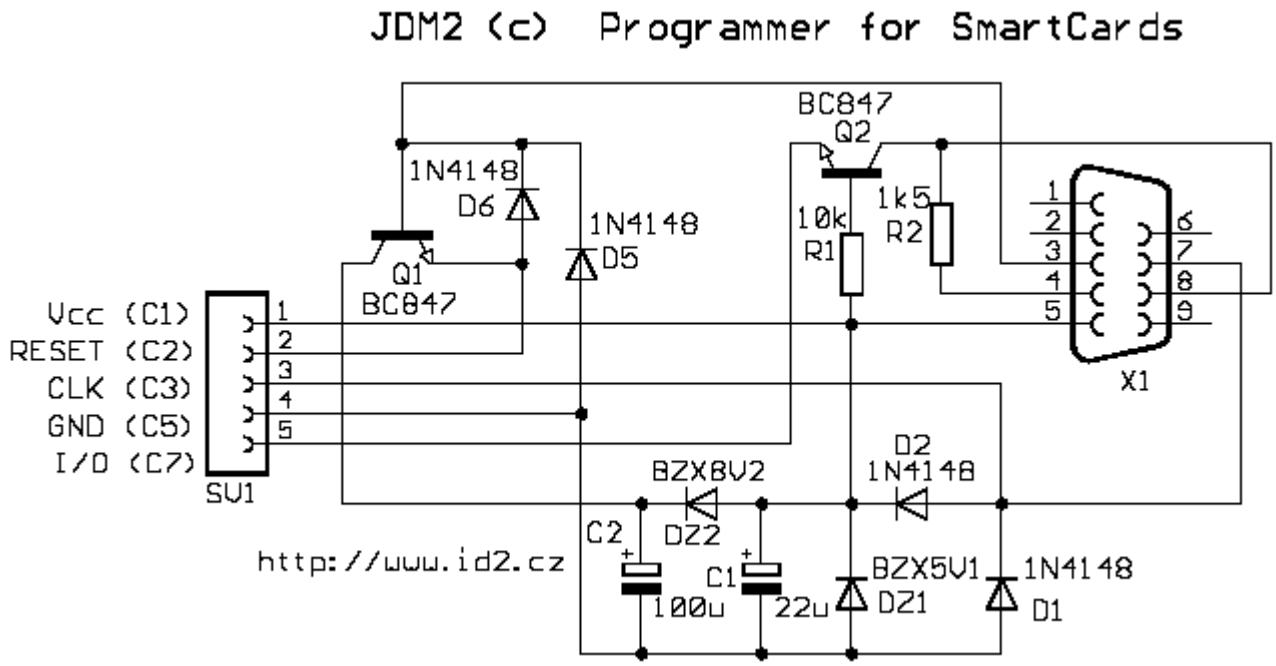
Cardinal from http://www.mgfware.com and Dejans SimScan from http://users.net.yu/~dejan can also be used to extract Ki from the simcards.

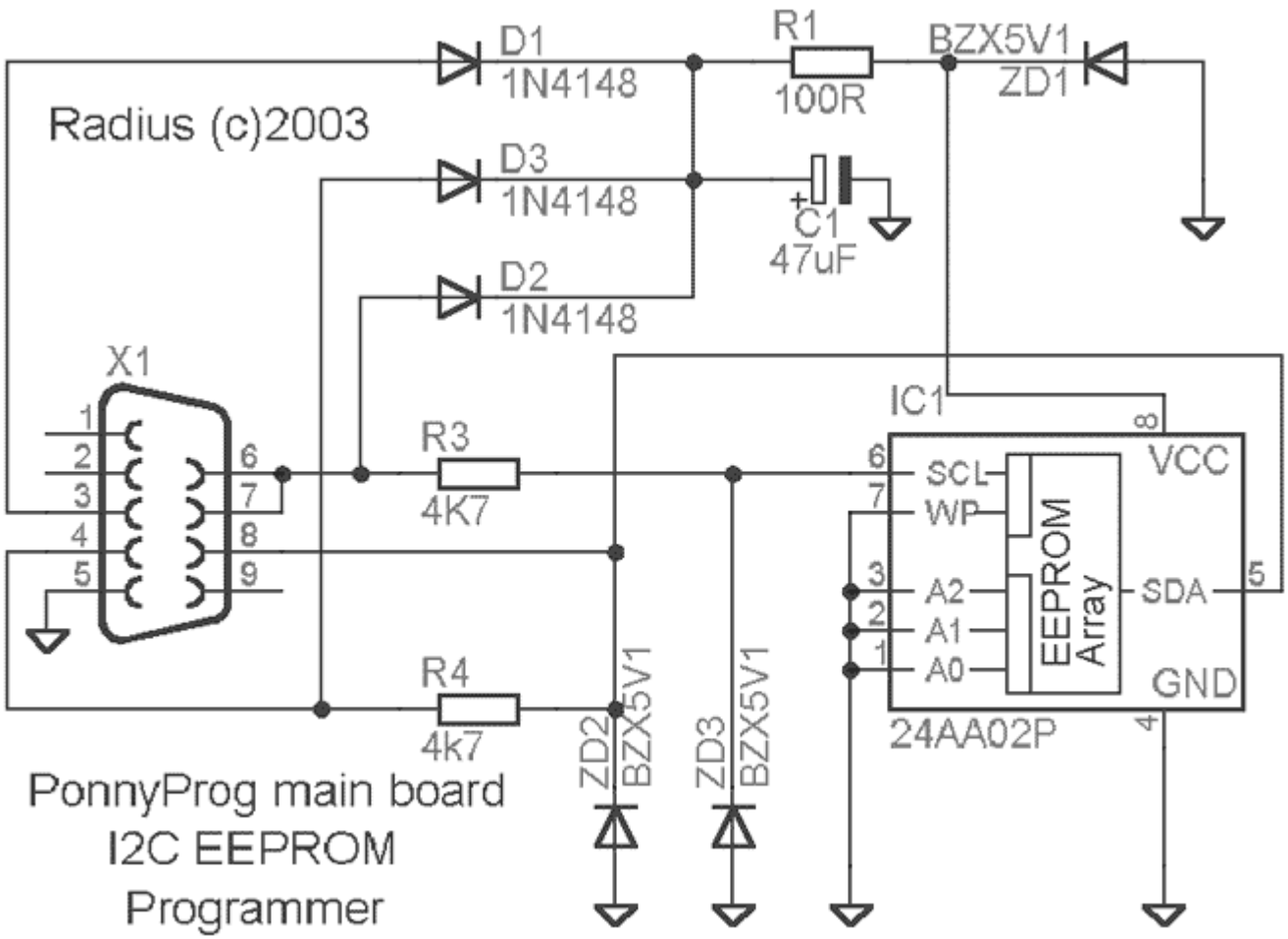
Wafer Card Programmer

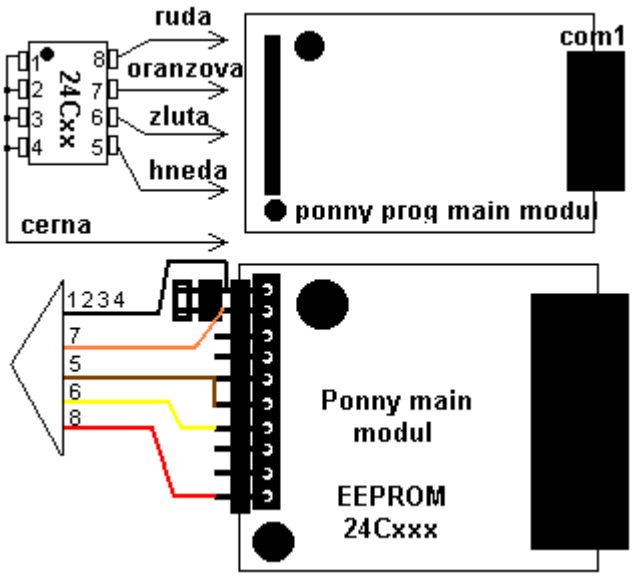
This programmer consists of two programmers incorporated into one. One PIC programmer and one EEPROM programmer. The logic behind the programmer is, the EEPROM inside the wafer card is programmed through the PIC. I suggest Millenium 2000VX MAX programmer for programming the wafer card. It is a very economical programmer without any housing. Even though it is cheap and looks like scrap, it is too powerful and suits best for our needs. Almost all the wafer cards used in GSM can be programmed with it. You can get one from http://www.pulsat.com/satellite/site/details.php?product_id=62. You can also use programmers like Dynamite programmer and updated versions of Millenium programmer. Any way i dont prefer you to make your own programmer. Eventhough you are an expert in electronics and computer, you have to waste much of your time to program the wafer card. Anyway the below circuits will give you and idea for the programmer.

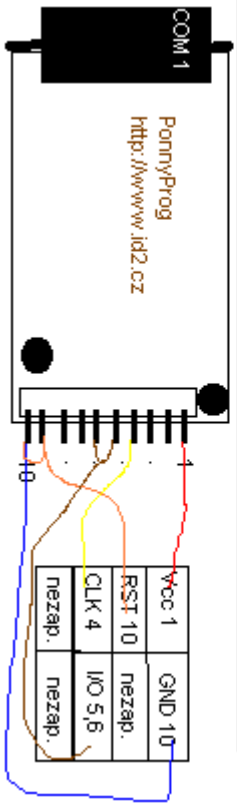
Here is the circuits for a PIC programmer and EEPROM programmer. The first one JDM2 programmer is for programming the PIC and the second one is an EEPROm programmer. But these are induvidual programmers for your reference only. I am not sure about its working, since i haven't constructed it. Anyway the source says its 100% working.

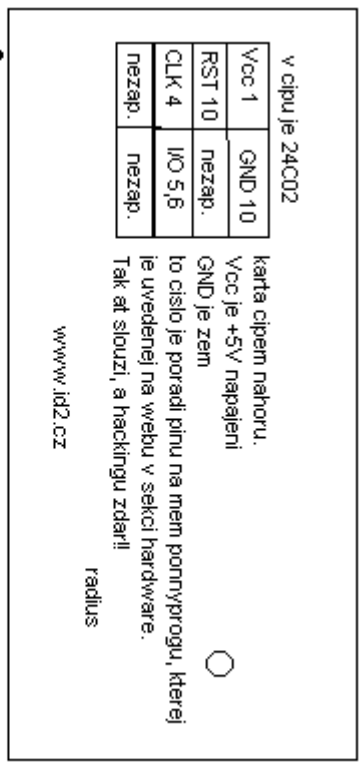
The third one is the programmer which works as both smartmouse and phoenix. This works fine with ICProg. The only drawback is that this would not be as easy for a beginner. Anyway just try your luck with this programmer. The PCB layout is also attached, if you wish to make your own circuit board. The bitchmouse programmer has two jumpers with it and the jumper settings are also mentioned in the schematic. One is for inverting the reset pulse and other is to change the woking frequency, for increasing the speed.

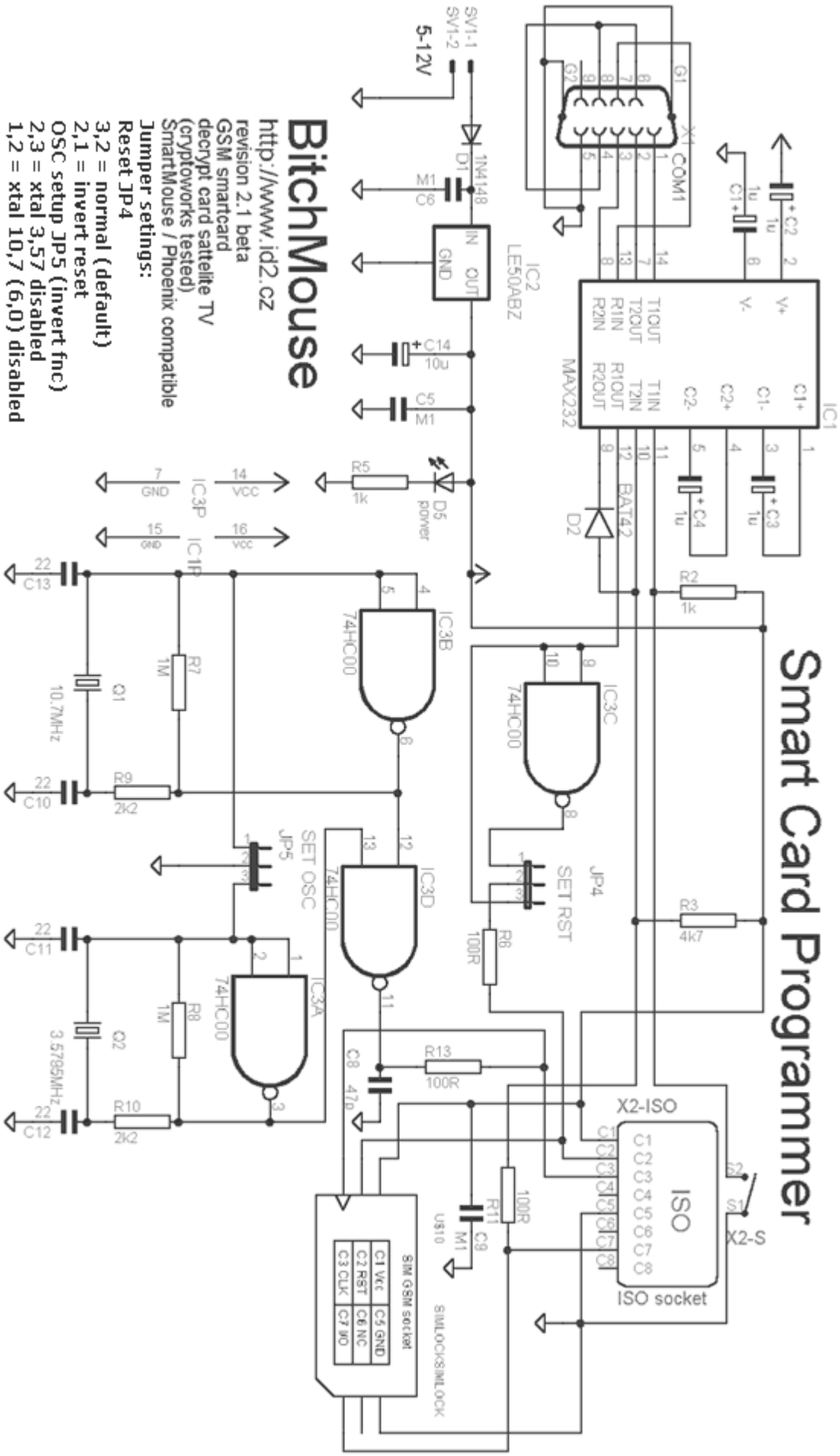


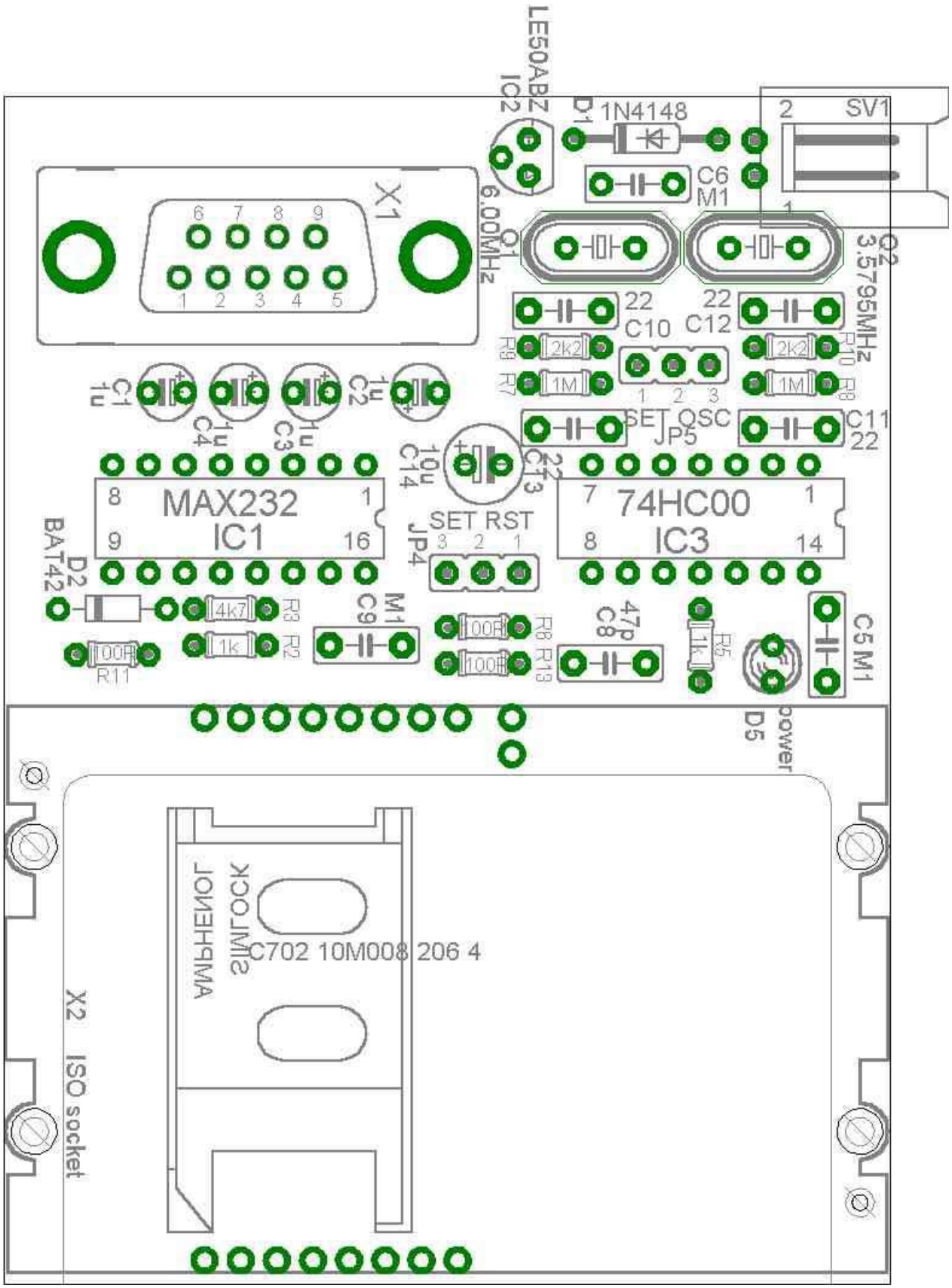












WARNING: DONT USE THIS GUIDE FOR ANY ILLEGAL PURPOSES. USE THIS FOR EDUCATIONAL PURPOSE ONLY

WARNING: DONT USE THIS GUIDE FOR ANY ILLEGAL PURPOSES. USE THIS FOR EDUCATIONAL PURPOSE ONLY

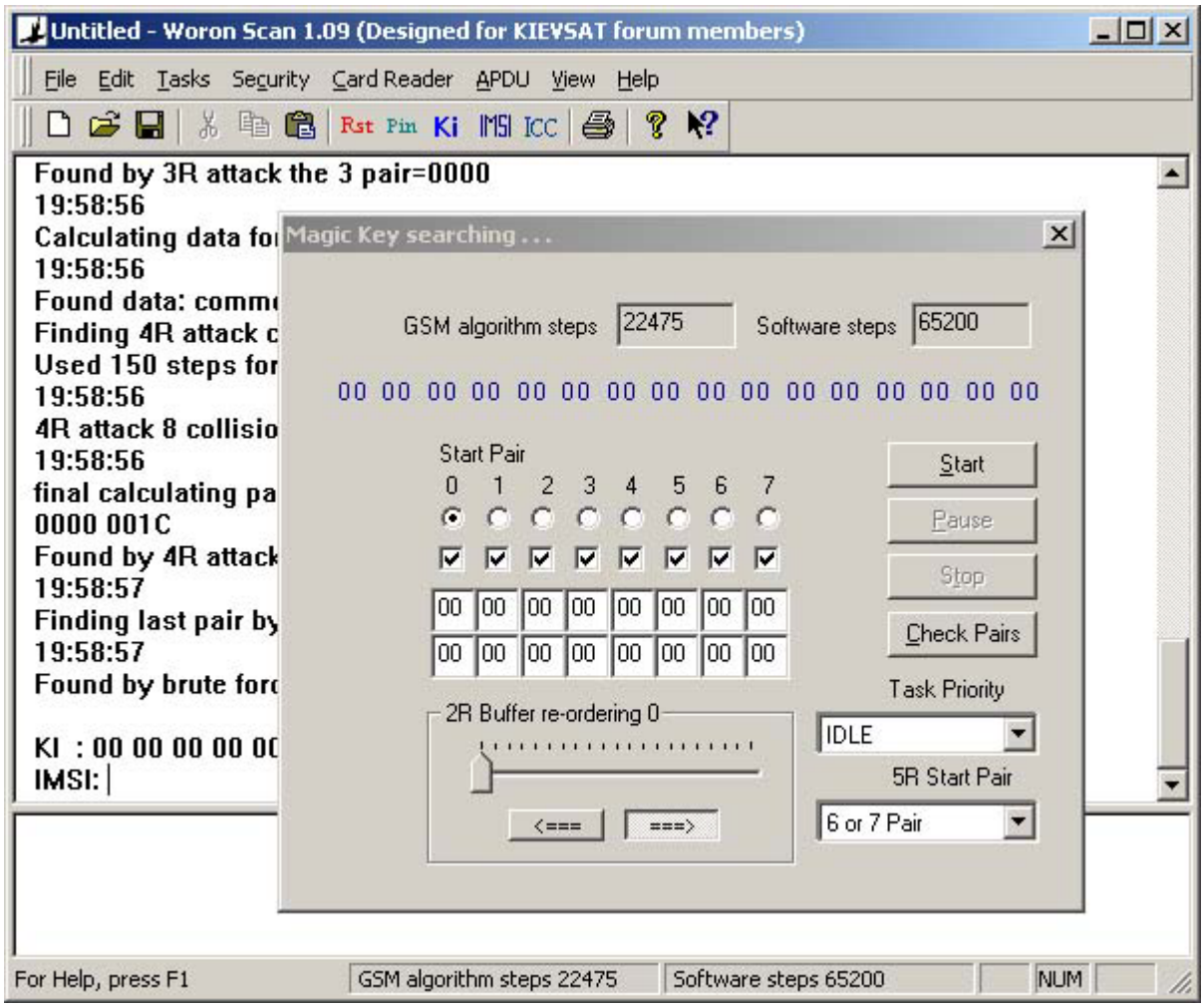
Software to program the wafer card

Before checking the software to program the wafer card, we need to choose what to be programmed on the plain wafer card. Anyway we need one file for PIC and one for the EEPROM. We can make the plain wafer card in to a 10 in 1 simcard, a 16 in 1 simcard or even a simcard with only two numbers. But if we have the provision, i suggest to utilise the maximum from it. So i suggest a 16 in 1. Inorder to make this dream come true, we need some additional softwares too. I suggest SimEmu 6.01 from http://www.simemu.cjb.net or pic-ador from http://borodza.com/pic-ador . With these softwares you can create the hex files for PIC and EEPROM.

Inorder to program these files to the wafer card, we need the software compatible with the programmer. If you are using a Millenium 2000VX Programmer you can use CardMaster with it. If using a Dynamite Programmer, the programming software usually comes bundled with the programmer. You can use ICProg also.

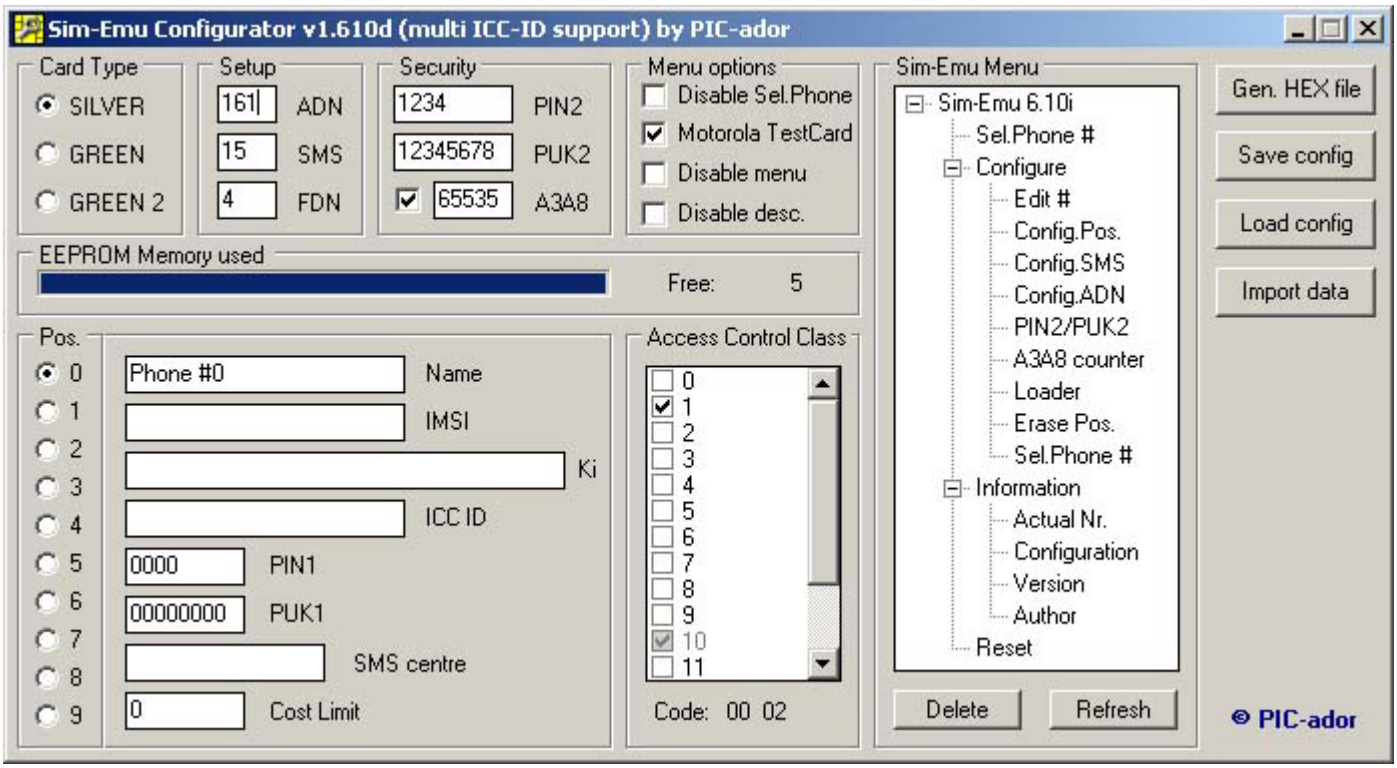
PROCESS

STEP1 : Insert the simcard in the simcard reader and use the software to extract the Ki, IMSI and ICCID of your simcard. Here i used Woron scan 1.09

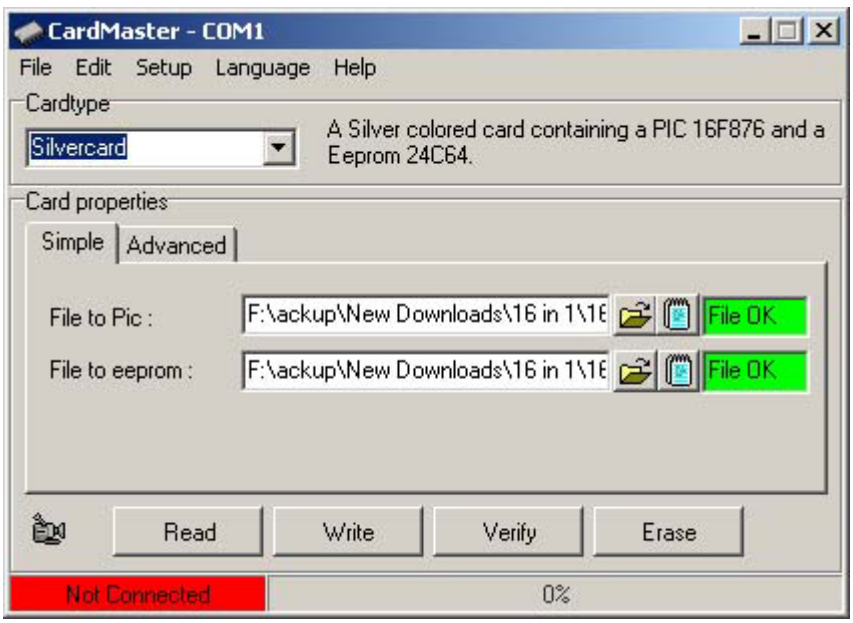


STEP2 : Make the files for PIC and EEPROM with SimEmu Configurator or 16 in 1 SimEmu Configurator by Pic-ador. If you are using the SimEmu Configurator by Pic-ador uncheck the A3A8 checkbox under security. Please dont enable this even from the sim services menu. If enabled, it counts back to zero and when it reaches zero, all bad things can happen to your simcard. In the configurator you can set the number of ADN, FDN and SMS. You can use the formulae "16448 = (ADN - 51) x 32 + SMS x 176 + FDN x 32 must be less than 6480" for silver wafer cards. Then generate the Hex files for PIC and EEPROM by clicking the Generate Hex file. With this configurator, in addition to the 16 number slots, you can make the simcard a Motorola Test card too. In 16 in 1 configurator the positions are from 0-9 and from A-F. Each position can be customised by induvidual PIN an PUK codes.

WARNING: DONT USE THIS GUIDE FOR ANY ILLEGAL PURPOSES. USE THIS FOR EDUCATIONAL PURPOSE ONLY



STEP3 : Now we have the files to be written to the Silver Wafer card. For this we need the Wafer card programmer and the software for programming. Here i am using the Millenium 2000VX Max programmer and the Cardmaster 2.1 software. Connect the programmer and run the software. Select the type of card you are using. Select the port by clicking setup > port. If the port set by you is correct the red colour with message on ststus bar changes to yellow and shows no simcard. Insert the simcard and load the files for PIC and EEPROM in the file to PIC and file to EEPROM fields respectively. Dont change any other settings. Now you are at the last stage. Press F3 or click edit > Auto Program. You can watch the status bar about what is happening. Programming the pic.. programming the eeprom... programming the pic.... verifying.... and atlast you will get the message that the card is programmed succesfully. Here you may ask the question why the PIC is programmed again after programming the EEPROM?. The PIC is first programmed with the eeprom loader to program the EEPROM. then the EEPROM is programmed through the pic. After that the contents in the pic is erased and the actual file is programmed in the PIC.



STEP4 : Now you are completed. Take the card out of the programmer, cut it to the size of the normal simcard and put it in the handset. After switching on, the handset asks for PIN code. Enter any four digit number. This will be the PIN for your first position "0". It asks for the PUK too for the first position. The phone switches on with no network or "Sim card not registered error". This is normal because no operator information is there on the simcard. Now we are moving to the final step of your

dream. Browse through the menu and find the Sim Tool Kit. Now it should be named as Sim-Emu 6.01. Open it and you can see the menus Configure, Select Phone and Information. Select Configure and go to config postion. It asks for the position. You can select any position from 0-9 and A-F. After selecting the position it asks for a PIN and PUK. Always provide different PIN and PUK for each positions. It helps us to switch to a number directly when the handset is switched on. After PIN and PUK it asks for KI, IMSI and ICCID. You can now recall the extracted values from STEP1 and enter it to appropriate fileds. Now you are done. You have a cloned simcard and moreover you are going to have a simcard with 16 cloned mobile numbers.

A WORD FROM THE AUTHOR

I am a Computer hardware Engineer and I started this as a project for my Diploma in 1998. I managed to impress the invigilator by showing the basic things that can do with a simcard reader. I was able to extract the ki in the beginning itself, but due to lack of information or a proper guide i was not able to do the rest of the things. The main issue was with the wafer cards. At first i thought that, with a simcard reader and a used sim card i was able to program the card. But continuous searching provided me the basic knowledge. The next major issue was the availability of wafer cards. I searched almost every corner of india and nobody knows what a Silver Wafer card is. Atlast after 4 years, one of my friends brought me some Silver wafer cards from UK. I searched many forums about sim cloning and i cant find one succeeded from India. But i got some guides from some forums. But those were outdated and use only two simcards in 1 and were bit confusing too. So after experiencing these difficulties, i planned to make a guide for sim cloning. **DONT USE THIS GUIDE FOR ANY ILLEGAL PURPOSES. USE THIS FOR EDUCATIONAL PURPOSE ONLY.** I think i tried to explain each and everything in detail and if you have any questions or suggestions, please let me know. **sujithsidhardhan@gmail.com**

DISTRIBUTION

You can freely make copies of the archive and distribute them as long as no alterations are made to the contents.

DISCLAIMER

IN NO EVENT SHALL I BE LIABLE FOR ANY DAMAGES WHATSOEVER (INCLUDING WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, OR ANY OTHER PECUNIARY LOSS) ARISING OUT OF THE USE OR INABILITY TO USE THIS PRODUCT.
ALL THE SCHEMATICS & TRADEMARKS PROVIDED HEREIN ARE PROPERTY OF THEIR RESPECTIVE OWNERS OR COMPANIES

THANKS

Mr. KrishnaRaj & Mr. Binu for purchasing the programmer & wafer cards for me

Mr. Dejan Kaljevic for his circuits and software

SimEmu for his sim emulation oftware

Pic-ador for his sim emulation software

pulsat.com for the wafer cards

volny.cz/id2 for circuits

promosatuk.com for the programmer

forum.gsmhosting.com for the information