Categories

- Anti-X Radiation: 4
- Cables [Unlock/Flash...]: 58
- Cellular Mobile Phones: 1
- Connectors: 24
- Converters: 3
- Dual SIM Housings: 5
- Flash / Unlock / Repair Boxes: 4
- Gadgets: 9
- GPS Cables: 2
- GPS receivers: 2
- Housings: 2
- Infrared Adapters: 4
- PDA/Handhelds Accessories->: 7
- PICcards: 7
- Portable Handsfree: 2
- Rechargable Batteries: 3
- Repair / Spare parts->: 2
- SIM Cards Backups: 4
- Software: 3
- Support: 2
- Tools: 2

What's New?

Cables2.com Software Downloads

Select a category : All go

Sim Scan 1.33

```
I MUST WARN YOU THAT YOUR CARD MAY BE DESTRUCTED DURING THE WORK WITH THIS
PROGRAM !!!.


SIM SCAN is a program that allows functionality analysis of Yours GSM SIM
smart card.
Do not use this program on SOMEONE ELSE\'S SIM CARDS, and you may use it only
in educational purposes!
Smart card reader needs no power supply, since it is powered via RS232 lines.

With this program you can analyze:

ATR      (For any card)

CLA+INS (For any card, while comments are valid only for GSM SIM card)

FILES   (For any card, while comments and analysis are valid only for GSM SIM
         card)

Ki       (It is valid only for GSM SIM MoU A3,A8 ciphering algorithm.)
         SOME CARDS CAN BE DESTROYED USING THIS FUNCTION!!!
         ESPECIALLY PREPAID CARDS!!! BECAUSE THEY HAVE LIMITED RUNNING
         OF A38 FROM 10000 TO 65536 TIMES AND AFTER THAT A38 DO NOT WORK ANYMORE!!!
         During the work it is possible to interrupt the program by pressing
         any key. In case of interrupting, temp file will be saved, and later
```

Nokia 8310 cover conversion kit for Nokia 8210

Languages

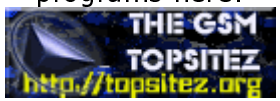
Currencies

Euro

Shopping Cart

..is empty!

Download unlock programs here:




```
        you may continue the analysis from the point you\'ve interrupted it.
        Also, at every 512 cipher texts temp file is automatically generated,
        so that the analysis could be continued if a communication error with
        card occurs.

Since almost all new SIM cards from 2000-2002 have limited running
of A38 to 65536, old method for finding Ki is useless.
I\'ve found new method for finding Ki that can find Ki in range
from 40000 to 80000 cipher text.
Process takes at last 8 x less cipher texts than first
version of \"Sim Scan\".

        New method can find 16 bytes Ki in next steps:

1) 2-R attack for getting first 2 bytes of Ki and take approx. 16000 cipher texts
2) 3-R attack for getting next 2 bytes of Ki and take approx. 758 cipher texts
3) 4-R attack for getting next 4 bytes of Ki and take approx. 758 cipher texts
4) 5-R attack for getting last 8 bytes of Ki and take approx. 832 cipher texts

That gives approx. 18348 cipher texts for finding Ki.

Since step 4 requires great resources and takes lot of time
for calculation on standard PC, only steps 1,2,3 are implemented in this
version of \"Sim Scan\"

Using steps 1,2,3 Ki can be found in:

        2 x 2-R attack (2*16000)
      + 2 x 3-R attack (2*758)
      + 1,5 x 4-R attack (1,5*758)
      + brute force on 2 bytes (2)
        ------------------------
      = approx. 34655 cipher texts.

For this method Ki can be found in 99% of SIM limited to 65536.
process takes on P2 715 Mhz and resonator of 10,24 Mhz less than 60 min!
If you want to use this method select \"F5-F1\" in \"Sim Scan\"

If you use \"F5-F3\", Finding Ki will take:

        2 x 2-R attack (2*16000)
      + 2 x 3-R attack (2*758)
      + 1 x 4-R attack (1*758)
      + brute force on 4 bytes (2)
        ------------------------
      = approx. 34274 cipher texts.
```

```
For this method process takes on P2 715 Mhz approx. 12 hour
because of using brute force on last 4 bytes.

In option \"F5-F2\" and \"F5-F3\" you have to set A38 limit and
when limit is reached program will start to use brute force.

Note:    First time when you use option \"F5\" for finding Ki, program
         will create \"par2.bin\" and process will take on P2 715 Mhz
         approx. 1 hour.


After finding Ki, IMSI and Ki will be stored in file and you can use
later to write IMSI and Ki using \"F6\" to GSM a38 SIM based on Gold Wafer
card (PIC 16F84 + 24lc16).
Source for Gold-Silver card can be found on my site: http://users.net.yu/~dejan


REQUIREMENTS

- Pentium II processor with 64MB RAM
- Win9x


;-----------------------------------------------------------

Update:

v1.33
         Improved algorithm for geting Ki from SIM MoU a38 cards.
         (Added 4-R attack).

v1.21
         Added function F6 for writing IMSI and Ki to GSM SIM Gold Wafer
         (PIC 16F84 + 24lc16).
         Improved algorithm for geting Ki from SIM MoU a38 cards
         (Added 3-R attack).

v1.10
         Fixed some bugs.

         Using Setup you can to set COM port and COM port speed.

         If you want to change COM port speed (that will speed up
         ALL SimScan function!) you\'ll need to use appropriate resonator
         in Smart Card Reader!
```

```
        You can use resonator of 10.240 Mhz from old cordless phone
        and it will speed up about 2.5 x to 3 x using COM port speed 28800.
        It seems that all SIM card works fine on that speed!

        Also, this version support entering PIN 1.


**********************************************************************
Program is tested on Win95,98 and on Intel cpu\'s P1, Celeron.
If you have any problem with this program then just DO NOT USE IT!!!
**********************************************************************


Dejan Kaljevic
```

Download Now!

Tuesday 08 October, 2002 **2190413 requests since Friday 01 June, 2001**