



Jonweb Technology Trade CO., LTD.

<http://fa.jonweb.net> , <http://english.5130cn.com>

Kindly offer Factory Automation Parts with lower price.

CRACKING THE MITSUBISHI “KEYWORD”

A Technique to discover the password or “keyword” stored in Mitsubishi A series and FX series PLC's.

Written By Aisha Liang (<http://www.5130cn.com>)

Application Software required:

Melsec GX Developer

Comlite 32 (Available free from <http://english.5130cn.com>)

NOTE:

This technique is intended as a work around when you have been left with a password protected PLC and the original installer has gone bust!

Introduction

The keyword within a Mitsubishi processor consists of a string of characters in the range 0-9 and A-F, in the case of the A-Series these are six characters long and in the FX they are 8 characters long. If a keyword has been set within the processor, it is required in order to read the program from the PLC to be able to monitor / modify the program. If you haven't got the key, you can't get in.

Mitsubishi Electrics China technical support have been asked if it is possible to identify or get round the keyword, their answer is no, you must clear the PLC memory and start again. Not very good if you do not have the original code to begin with! I read an article on the forum on www.5130cn.com (<http://english.5130cn.com>) where someone was asking the question on keywords and one user suggested the use of Comlite32 to discover what was going in and out of the com port. I can't tell from the discussion threads whether or not it was successful so I had a go myself and documented the findings for the use of others.

(Note that ComLite32 does not work with NT/2000 – I used W98)

Setting The Keyword

A1S Processor

I had a distinct advantage over some users, whereby I did not have a protected PLC to crack, I had an unprotected one which I could set any keyword in it so I knew what I was looking for. On the **A1s processor**, using GX Developer, I set the keyword to ABCDEF, then closed the file. I started ComLite32 to monitor com1 in single line mode. I then did a “read from PLC” into a blank project. When “Param & Prog” is selected, switch to ComLite and start logging. Switch back to GX Developer and hit the execute button. A dialog then appears asking for the keyword, at this point type in any keyword (e.g. 123456), the dialog will appear again (because the keywords don't match). At this point, switch back to ComLite and see what you've got. It will appear something like this:

Address: Rm 902, ShangDi Garden 23#, HaiDian District , Beijing, China (ZIP: 100085)

地址: 北京市海淀区上地佳园 23 号楼 902 室 (邮政编码: 100085)

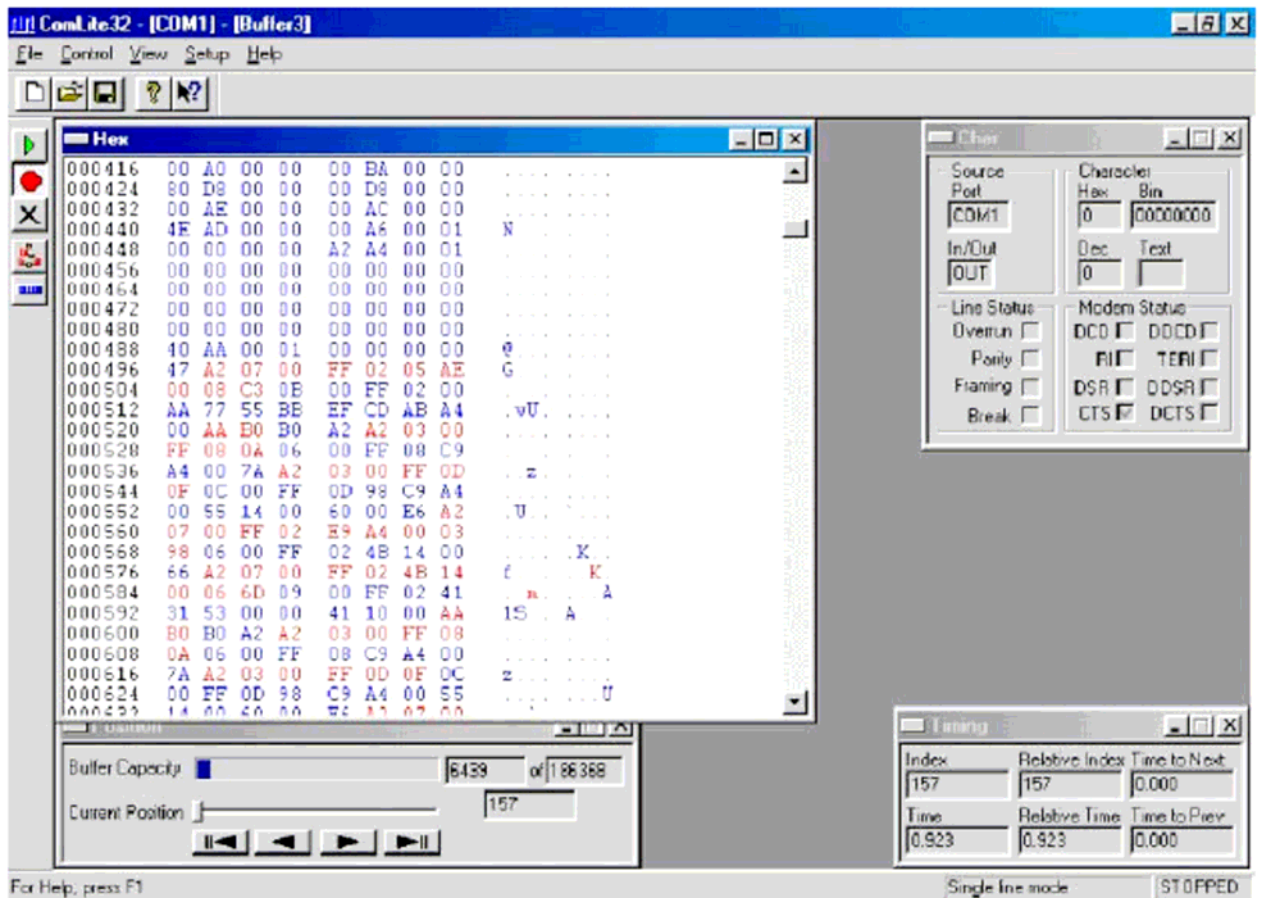
电话 / TEL: +8610-6298 8280 / 8636 0099 传真 / FAX: +8610-6298 5883



Jonweb Technology Trade CO., LTD.

<http://fa.jonweb.net> , <http://english.5130cn.com>

Kindly offer Factory Automation Parts with lower price.



The red data is what your PC is sending, Blue data is sent from the PLC.
 It looks like the PC sends a command to the PLC asking for the keyword, the PLC then sends it back and GX Developer compares the two, if they match, it allows you to continue. The red **A2 07 00 FF 02 05 AE 00 08 C3** looks like the request for the keyword. What the PLC sends back is **0B 00 FF 02 00 AA 77 55 BB EF CD AB A4 00**. Looks meaningless, doesn't it? Until you know that the keyword that I set was ABCDEF. So, if you ignore the last two characters (A4) and work backwards in packets of two we get AB CD EF. I thought that this must be too simple, so I used a different CPU and a different keyword. This time I used "A1B1C1" as the keyword. Did the same routine as above and this time I got:

```

000888 00 00 00 00 00 00 00 00 .....
000896 00 00 00 00 00 00 00 00 .....
000904 00 00 00 00 40 AA 00 01 .....
000912 00 00 00 00 47 A2 07 00 ..... G
000920 FF 02 05 AE 00 08 C3 0B .....
000928 00 FF 02 00 AA 77 55 BB .....
000936 C1 B1 A1 50 A2 07 00 EF ..... P
000944 02 00 B1 00 00 B9 03 01 .....
000952 FF 02 FF FF FF FF FF FF .....
000960 FF FF FF FF FF FF FF FF .....
XXXXXXXX FF FF FF FF FF FF FF FF .....
  
```

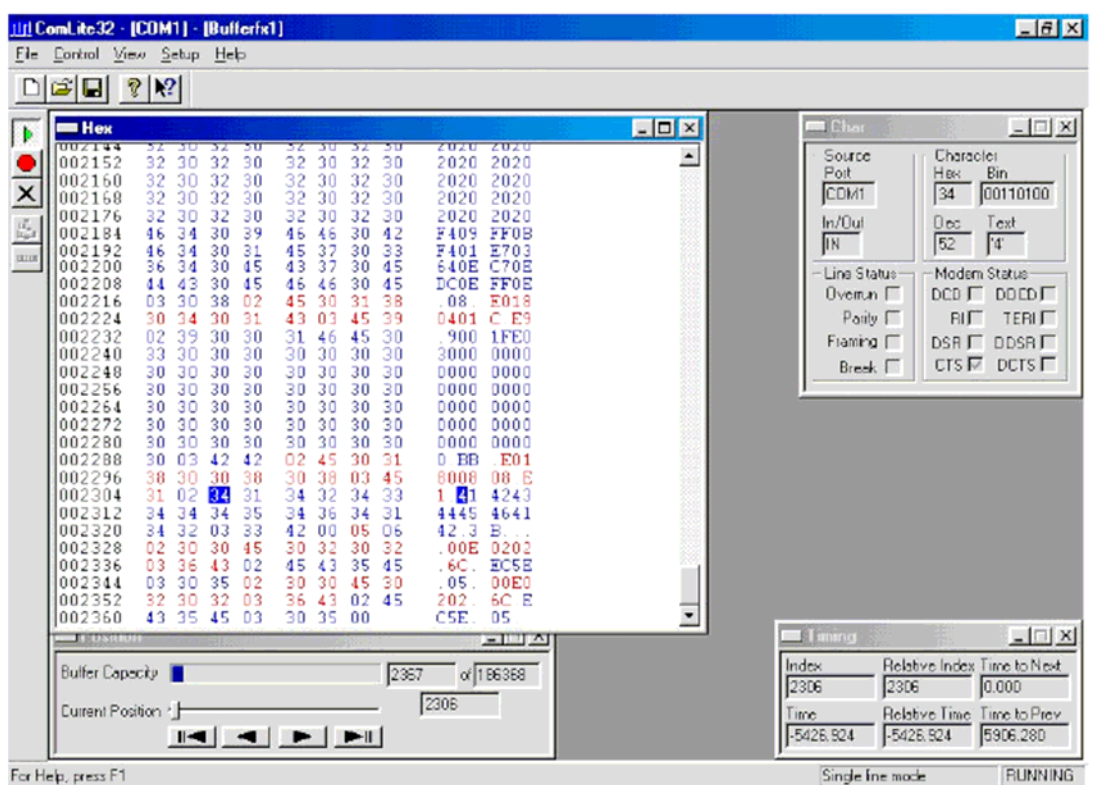
Same command to get the data from the PLC (**A2 07 00 FF 02 05 AE 00 08 C3**) and the data back was **0B 00 FF 02 00 AA 77 55 BB C1 B1 A1 A4**.
 Working backwards ignoring the last packet we have A1 B1 C1 .

Address: Rm 902, ShangDi Garden 23#, HaiDian District , Beijing, China (ZIP: 100085)
 地址: 北京市海淀区上地佳园 23 号楼 902 室 (邮政编码: 100085)
 电话 / TEL: +8610-6298 8280 / 8636 0099 传真 / FAX: +8610-6298 5883

FX Series PLC's

The keyword structure in the FX - CPU is somewhat different to that of the AnS-Series, you now have 8 characters instead of 6. Though I did think that it would work the same way. Not quite. The FX CPU that I used was an FX2N128MR, with this model being newer and more advanced than the A1s may explain the differences, however, the AnS-Series technique may work on older FX's or F1/F2 processors. I haven't got one to try it on but would welcome any feedback.

I approached the FX the same as the AnS-Series using the keyword "ABCDEFAB", with the ComLite logger running I could not see the pattern ABCDEFAB or AB EF CD AB anywhere in the data. The pattern that I did see was quite interesting though I kept seeing a pattern of 34's, i.e. 34, 31, 34, 32, 34, 33, 34, 34, 34, 35, 34, 36, 34, 31, 34, 32.



We know in the code that each number represents an ASCII character, these numbers were then translated from ASCII and the result was 4 1 4 2 4 3 4 4 4 5 4 6 4 1 4 2. Group them into twos and you get 41 42 43 44 45 46 41 42 .

What is the character equivalent if these values are in ASCII??

They magically appear to be A B C D E F !!

The request for data from PC to PLC works in a similar way: 02 45 30 31 38 30 30 38 30 38 03 45 31.

The next block of data is the key sent back from the PLC, this time it's in the correct order. Ignoring the first two characters (the 02) the next sixteen blocks (I'm calling a 34 one block) represent your keyword. All you have to do is take the first two blocks (34 31) convert each one into an ASCII character (4 1) put the two together (41) and then convert that hex



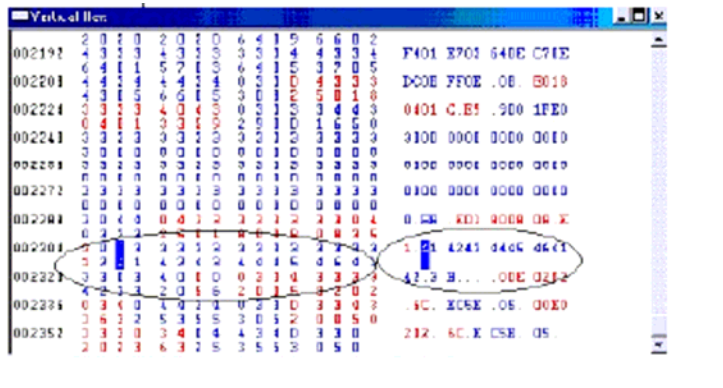
Jonweb Technology Trade CO., LTD.

<http://fa.jonweb.net> , <http://english.5130cn.com>

Kindly offer Factory Automation Parts with lower price.

number into an ASCII character (A), do this for the next 7 blocks of two that you can see and that should equal the keyword.

It looked simpler to me when I viewed it as "Vertical Hex" in ComLite – I could see straight away how they had split the ASCII number up.



Now, looking back, I can see it in the normal hex view though, but there are always more than one way of solving a problem.

What's Next??

Mitsubishi Small Q PLC ---Yes, we have done it , maybe No.1 of the world...



Any Ideas & Comments are welcome at 010-86360099@sohu.com .

Or click this link to keep contact <http://fa.jonweb.net/jiemi> .

Address: Rm 902, ShangDi Garden 23#, HaiDian District , Beijing, China (ZIP: 100085)
地址: 北京市海淀区上地佳园 23 号楼 902 室 (邮政编码: 100085)
电话 / TEL: +8610-6298 8280 / 8636 0099 传真 / FAX: +8610-6298 5883