PLAY MATES ISSUE 5 EXTRA

By Mark Riley

Using Romantic Robots INSIDER.

1.If you can,read all of Phil Howards "Insider Dealing" series in A.A.

2. (i)Search for all occurences of 3E,no. of lives

(ii)Disassemble at the locations listed

(iii)Note the locations that the no. of lives is loaded to

```
    i.e.     3E,04           ld a,4
             32 F9 34        ld 34F9,a
```

This loads 4 (hopefully the no. of lives) into location 34F9

(iv)Search for all occurences of 32 F9 34 Ideally,there should only be 3 locations given:one each for setting the lives,decreasing them and increasing them.

(v)Disassemble at those locations given and check for 3D just before the 32 instruction.

(vi)Replace 3D with A7 and return to the game.

(vii)You might find that 32 F9 34 is only found at the address you already have.This could mean that the lives are decreased and increased using another register.

3.Some games load the lives with the A register but decrease them using the HL register.

In this case search for all occurences of &35 (dec(HL)).Check that the lives location is mentioned just before the &35 instruction.Replace any of these with 00.

The instruction 36 F9 34 puts the number at that location into the HL register.

Also check for D6 01 (sub HL).This method is used in Wec Le Mans and in Chase HQ.(Both written by the same programmer).Replace the 01 with 00 to stop the timer.

The instruction DAA after D6 01 indicates that the result of the decrease is converted to decimal numbers,usually for display.

4.If you have a M/Face poke for any games,use the Insider to disassemble the game at that location.Remember that when you input the disassemble address,make this address a few bytes before the location you want to study i.e. if the poke is at location 02F3,make the disassemble address as 02ED.This ensures that the location you require is on the screen for you.

Poke 02F3,00 for inf.lives in Arkanoid (Budget version)

5.Check to see if you can redefine the control keys and if you can note how many keys there are to change.Then use the TEXT option to look for odd words in the program that might fit the redefinition. i.e. Exolon has 5 control keys.Using the TEXT option shows the word ZORBA.Inputting this as your key controls will result in infinite lives.(You can change the keys once ZORBA has been put in.)

6.You can try checking for FE FF (CP FF).This usually follows a decrement instruction and checks for lives going below 0.I have not found this to be very useful but it is something to bear in mind.

7.Try to get hold of the Z80 Instruction Set.This will give you all the necessary information for checking registers.
PROGRAMMING THE Z80 by Rodnay Zaks is very good-trouble is it costs about £23.95.The ISBN is 0-89588-069-5.
MASTERING MACHINE CODE ON YOUR AMSTRAD 464/664/6128 goes some way to helping learn m/c,but the best feature is a comprehensive explanation of most of the Z80 instruction set.It costs £8.95 and the ISBN is 0-907563-91-0.

8.Check out the normal tape/disc pokes in Cheat Mode.These alone can sometimes enable you to find the necessary pokes with the M/face very quickly.
For example;
This is a poke from AA51 for the game Xenon.(I have not got it)

```
10 DATA 21,49,00,22,c9,03
20 DATA C3,84,03,3E,C9,32
30 DATA 0B,08,C3,78,05
40 FOR X=&40 TO &50
50 READ A$
60 POKE X,VAL("&"+A$)
70 NEXT:MODE 1
80 OPENOUT "W":MEMORY &350
90 LOAD"XENON"
100 CALL &40
```

Using the multiface,you could poke the instruction C9 into location 080B.This would most likely give infinite energy.
The thing to look for is the set of data info commencing 3E.
In the above example it is 3E,C9,32,0B,08
This means; 3E C9 - load the A register with C9
32 0B 08 - puts the contents of the A register into memory location 080B
(C9 is RET or return in m/c and,in another poke,could be 00 or A7)
There may also be multiple 32's.
i.e. a poke gives infinite energy,lives and time:in the listed poke there is the sequence 3E,A7,32,08,92,32,07,56,32,34,53
This would (probably) mean that you should poke A7 into the following locations to get the infinite whatevers;
9208 5607 5334
Remember,the location is ALWAYS given as LOW byte,HIGH byte.When using the INSIDER,the column on the left shows the actual code,the centre column shows what the code really means.The column on the right gives the symbolic representation of the code.

==================

** IMPORTANT **

When using the INSIDER to poke a game,make a note of the instruction you are replacing.You don't need to know what it means,but,if the poke does not work,you must replace the original instruction to ensure that the changes you make are done only one at a time.Also,after poking a location,return to the game to test it before moving on to try another poke.

==================

The instruction &27 can be particularly useful.It is the Decimal Adjust Accumulator (DAA).This converts the contents of a register to a decimal number,usually for screen output.

Say you have a driving game with a timer that decreases,use the find facility to search for all occurrences of 27.There will be lots of locations listed,note them all down.Then disassemble to examine all of the locations given.If the DAA instruction is not listed in the centre column,ignore that location.If it is,check out the previous couple of instructions to see if there is a decrement instruction.Even if there is,or you cannot figure it out,replace the &27 with &00 (No Operation).Return to the Game.Examine the counter.If it is showing non-numeric characters,then you have found the right location,near which will be the instruction for decrementing the timer register.Replace the decrement instruction with &00,or,if the instruction is D6 01 (subtract 1 from the HL register),replace the 01 with 00.This will subtract 0 from the register,so giving infinite time.

Another alternative is to search using the TEXT option for the "GAME OVER" message.Note the rough address that it starts and disassemble before the message.Say the G of GAME OVER is at location AAAA,use the FIND option to find all occurrences of AAAA.If there are any,note the locations.If there aren't,try searching for AAA9 or AAA8 or AAA7 as there may be control characters before the message itself.Any locations given should indicate an Absolute Jump.

This means that the code will jump to the end game routine depending on a calculation executed just before the JP instruction.All you have to do is find how the calculation works and neutralise it.

It may be that there are no Absolute Jumps,in which case the jump to the end game routine is made by a JR (Jump Relative) instruction.In this case,you have to search through the code from &80 bytes before the routine to &80 bytes after it.Carefully examine the code in the CENTRE column,looking for any references to a JR instruction that goes to a location very close to the end game routine.Again,if you find it,look for the calculation method and disable it.

i.e.The code in the centre column may look like this;

```
LD A,(0123)      load A register with contents of location 0123
DEC A            reduce the number by one
CP FF            is it below zero ?
JR AAAA          yes - jump to end game routine
LD (0123),A      put new number back into original location
RET              return to game
```

This may not be strictly accurate,but should give you an idea of what to look for.In this case,the poke needed must replace the DEC A instruction,using either 00 or A7.

It is sometimes easier, if the game has it, to search for the routine that increases the lives. (Although 'lives' is always being used, it could equally be ammo, time or whatever feature you want.)
Most games rarely check for too many lives, so the routine is very simple i.e.

```
3A 23 01                      LD A,(0123)
3C                            INC A
32 23 01                      LD (0123),A
```

Using the FIND option, you would search for all occurrences of 3C 32. After noting the addresses given, disassemble to them and note the memory locations involved, in this case 0123. Then search for 3A 23 01 and again disassemble to them and one of them will be the routine that decreases the lives.

If you are sure that you have found the location that initially sets the lives, but cannot find the decrement method, replace the initial lives with a larger number. Do not use FF though, as this may be what the game checks for, so it will always be a "GAME OVER".
i.e. The game has 5 lives which are loaded into memory location 2345 as follows;

```
3E 05
32 45 23
```

If you cannot find the decrement method, replace the 05 with a number such as F0, to give lots more lives.

Make sure that you know how to poke the correct location. A typical INSIDER display will be similar to this;

```
6789 C9           RET                 ignore these shapes/letters
678A 3A 22 32     LD A,(3222)
678D 97 01        SUB 01
678F FE FF        CP FF
rest of prog......
```

The location to poke is 678E, replacing 01 with 00. You could poke 678D as well, but there would be no point to it.
If you are anything like me, the Hexadecimal system will give you real headache when you first start using it, but it does get easier.

When doing a search using INSIDER, always press '3' and enter 0 as the start address.
When doing a TEXT search using FIND option 2, always try both for the upper case and lower case of the word. CAPS LOCK will not work so you will have to keep one finger on SHIFT.

Poking EAGLES NEST.

1.Play the game to find out what's what.
There is AMMO of 99 which can can increase/decrease
There are KEYS which can increase/decrease
HITS can also increase/decrease.50 HITS = dead.
2.Press the red button to bring in the INSIDER.
3.Press F to select the FIND option.
4.Press 1 to select number search.
5.(Try to find infinite AMMO first)
Enter 3E (return) 63 (return) (return) [63 is HEX for 99]
6.Press 3 and enter 0 as start of search address.
7.Press 4 to start search.
8.The message **NOT FOUND** appears.
9.Search again for 3E 99,repeating steps 6 and 7.
10.It will stop searching and display FOUND AT 01E8 - write this down,and press 4 to continue the search.
11.Two more FOUND messages appear,giving the locations 157D and 367C.Remember to always press 4 to continue the search until all code between 0000 and FFFF has been examined.
12.Disassemble to location 01E0 and press either RETURN or SPACE until location 01E8 is in the most left column.
13.You will see 3E 99 3A 1B 00.This indicates that the number 99 has been put into memory location 001B.
14.Press ESCAPE to return to the Main menu,and disassemble to 1570.
15.Again you will see the sequence 3E 99 3A 1B 00 at 157D.
16.After pressing ESCAPE again,disassemble to location 3670 and there it is again;3E 99 3A 1B 00 at 367C
17.So we have 99 loaded into the same loaction in 3 places.
18.We now assume that the ammo is decreased in hopefully a simple way.
19.Return to the FIND option.Press 1,1B,return,00,return,return,3,0, return and 4 to commemce the search.
20.This will show all the locations where 001B is,and one of them should be next to the decrement instruction.
21.Doing the search as before will turn up 3 locations: 0900,0A8A, and 0A93.
22.The last 2 locations are very close so we will start there.
23.Return to the Main menu and disassemble to 0A80.
24.At location 0A90 is a 3D (DEC A) instruction.
25.Return to the Main menu and press P
26.Enter the address as 0A90 and enter 00 as the poke.
27.Press R to return to the game.
28.Press ESCAPE to check the ammo state,unpause the game,press FIRE a few times,press ESCAPE and BINGO ! infinite ammo.

Okay,now to get infinite keys.

1.I tried searching for all occurences of 3E 01,3C 32 but there were far too many and I could not find a constant memory location.
2.Hoping that things were simple,I thought to check for 3D FE FF which reduces the register by one but checks to see if the result is below zero.This search found only one location at 19A2.
3.Disassemble to examine this location,then poke 00 into location 19A2.
4.Return to the game - now you have infinite keys.

Now for infinite hits.

1..In the game,when you get to 50 hits,you are dead.Therefore the program must check to see if this condition is met.
2.Search for all occurrences of FE 50.I am assuming that it uses the decimal 50,not the hex 50 because the ammo was in decimal.This instruction compares the result of a register with the number in the statement,making a decision possible on the result.
3.There are 4 locations given: 08AC,0A1B,2A61,2A72
4.Starting with the first,disassemble to view 08AC.
5.You will find that the memory location 001D is loaded into the A register and then compared to 50.
6.Replace the 50 with a lower number (I used 10) by poking 10 into 08AD.
7.Return to the game,find the enemy and using the pause button,keep track of the number of hits needed to kill you.You will find that only 10 hits will kill you now,not 50.This means that we have found the part of the program that checks your state of health and that memory location 001D contains the current number of hits.
8.Search for all occurrences of 1D 00
9.I found 22 between 0000 and 8537.
10.Remember that we are searching for an increment instruction involving location 001D.
11.The first 6 locations,when disassembled,do not have such an instruction.
12.At location 25EE,you find that the number at 001D is loaded into the A register,increased by one with the instruction C6 01 and the result converted into a decimal number with the 27 instruction.
13.Go back to the Main menu and poke 00 into location 25F1 which makes the program add 0 instead of 1.
14.Return to the game,find the enemy and try to get killed - you can't.

So there you have it.Poking 00 into the following locations to give infinite Ammo,Keys and Hits respectively: 0A90,19A2,25F1
Unfortunately,the game somehow checks to see if you have cheated. When you enter your name onto the High score table,it is changed to LAZY.I haven't got a clue how this checking is done.

I hope that this has helped you to learn a little more about the INSIDER.The best way to learn is to use it on those games for which you already have a M/face poke.Disassemble to examine what the poke does.This will enable you to see how to use the program.Write down the way in which lives are decreased and,when trying to poke a game,bear in mind all the methods you have seen used.

Try and use it as often as possible so you get more used to it.

I realise that what I have written is rather disjointed - but that's the way I think.I'm sorry if it has been hard to follow.

If you require any help with poking games with the INSIDER,please write,but remember to enclose a SSAE !

From:-
Mark Riley,2 Primrose Way,Kirby Muxloe,Leicester,LE9 9AX

***

Wow that was a mega-read wasn't it, but I hope you agree it was worth it ? I was going to split this article over two issues because of it's length. But I've decided to do all of it in one go and make it a supplement to issue 5. Mainly because I feel it will be some thing you will be digging out quite often and having to search two issues for the part you want will be lot of trouble.

I had planned a 3 part article on this self same subject but Mark has done it far better than I ever could. I may still do it in a much later issue as a reminder of the main points in Marks article.

It just leaves me to say thanks to Mark Riley for his hard work and help in producing Play Mates issue's 4 and 5.
