KARTRIDGE

COPIES CARTRIDGES TO DISK!

WORKS WITH 8K or 16K CARTRIDGES
INTEGRAL RESET SWITCH
OPTIONAL EXTERNAL RAM ALLOWS "UNTOUCHABLE" MEMORY EXPANSION
SIMPLIFIES CRACKING CARTRIDGES TO OBTAIN CODE FOR ROM BURNERS

Some cartridges require external RAM not included in this package.

KARTRIDGE KRACKER

GENERAL DESCRIPTION

The Kartridge Kracker (KK) system is designed to allow the user to copy the contents of any 8K or 16K cartridge to disk. This is implemented through the ability of the KK board to prevent autorunning of cartridges.

FEATURES

* Cartridge control switches allow manual control of C64 hardware memory configuration lines. RAM socket tilted for easy switch access.

* RAM socket allows use of 8K or 16K VIC style RAM expanders for "ROM EMULATION" on programs which do not operate in normal C64 RAM space.

* RESET switch is integral thus eliminating the need for soldering and drilling your computer.

* Simplifies transferring of cartridge contents to ROM burners.

OPERATING INSTRUCTIONS

As may be expected, the hardest part to using the KK will be in the actual "cracking" of the cartridge as this requires a little detective work on your part. This involves finding out the size (8K or 16K) and "configuration" of your cartridge. To simplify matters we have provided a step by step procedure for you to follow but it will help if you are aware of some simple facts. First of all the configuration of memory for cartridges is controlled by two lines from the computer called Game and Exrom. If you look at switches 7 and 8 you will see a GM and an EX on the PC board. These two switches control the three possible configurations. Next are the two memory block select lines on switches 4 and 6. These lines normally go to the cartridge and allow it to be "selected" by the computer when the correct address is sent out by the microprocessor. The actual block locations represented by these lines changes under the control of the game and exrom lines! The effect of this is that for 8K cartridges there are actually six possible configurations - three if it uses ROML and three if it uses ROMH. Since 16K needs both 8K select lines (one for each "half" of 16K) there will be only the three configurations as mentioned earlier. Table 1 shows the possible combinations by switch number for 8K and Table 2 for 16K. The table will be

refered to in the procedure.

- - TABLE 1 - -

TEST #	KK SWITCH # 7	8	6	4	COMBINATION (Write Down)
1	ON	OFF	ON	OFF	2-6-7
2	OFF	ON	ON	OFF	2-6-8
3	ON	ON	ON	OFF	2-6-7-8
4	ON	OFF	OFF	ON	3-4-7
5	OFF	ON	OFF	ON	3-4-8
6	ON	ON	OFF	ON	3-4-7-8

- - TABLE 2 - -

1	ON	OFF	ON	ON	2-6-7
2	OFF	ON	ON	ON	2-6-8
3	ON	ON	ON	ON	2-6-7-8

OPERATING PROCEDURE

Make sure computer and all peripherals are turned OFF before plugging in KK. KK can normally be left plugged in with all switches in off position. Computer can be powered up with switches in other than off position but in some configurations the computer will lock up.

KRACKING KARTRIDGES

1. With all power OFF and all KK switches OFF, plug cartridge to be cracked into rear KK slot.

2. Turn ON computer. Using table 1, set KK switches as shown under "TEST #1". Press reset. If game runs, you have found out configuration for that cartridge. If game does not run try TEST #2, then #3 and so on until you find the test that causes it to run. Do not forget to press reset for each test, after setting the switches. One of the six settings should cause the cartridge to operate. If not it is probably a 16K cartridge and you should go directly to that procedure.

3. After finding the correct configuration, write down the numbers which correspond to that TEST#. This will be the combination to use when running the program in expansion RAM.

4. Switch all KK switches OFF. Set switch 8 ON and press reset. 30719 Bytes free message should appear.

5. Using information from above, if the combination starts with a 6 then turn on switch 6. However if it starts with

a 4, turn on switch 5.

6. LOAD "KRAC*",8,1 [RETURN]. When loaded, type SYS3291 [RETURN]. Follow prompts. Insert pre-formatted disk to hold cartridge data. NAME should be less than 16 characters - do NOT use quotes.

7. If you wish to make additional disk backups of this cartridge, repeat from SYS3291.

8. NOTE: The cartridge program on your disk is saved with a starting address of $4000. This is where the KK places external RAM during Loading. If you wish to load program into C64 RAM at other locations you can either change the load address on the disk with a disk editing program or use a machine language monitor to transfer the program from $4000-$6000 to where you want it.

9. NOTE 2: Some cartridges have other compoonents besides ROM memory. There is no way to duplicate such circuitry without building a special printed circuit card for each variation along with associated circuitry. Obviously this falls outside the realm of capability for this system. At present the majority of cartridges do not use other circuitry.

CRACKING 16K CARTRIDGES

A 16K cartridge is addressed as two 8K cartridges and so will be saved in two passes. The following procedure assumes that you have already determined that the cartridge is definitly a 16K.

1. With computer power and KK switches OFF, plug in 16k cartridge.

2. Turn ON computer and using table 2, try each TEST combination followed by pressing the reset button until you locate the combination which causes the cartridge to run normally.

3. Write down the "combination" shown corresponding to the TEST just performed.

4. Turn OFF all KK switches. Turn ON switch 8 and press reset. 30719 byte message should appear.

5. Load "KRAC*",8,1 then when done, type SYS3291 [RETURN] **Turn switch 6 ON. Insert preformatted diskette you wish to use to save cartridge on.

6. Follow promot. For NAME use 1 followed by program name to indicate first half. Do NOT use quotes. Total length must less than 16 characters. Example 1GAME

7. When done turn OFF switch 6 and press RESET. Then turn on switch 5.

8. Type SYS3291. KK title should appear, if not then reload it.

9. Follow prompts. Use 2 in front of name to indicate second half. Example 2GAME

10. This completes 16K cracking procedure. You now have two "halves" of the program. Both will be loaded to $4000 and end at $6000. When using KK external 16K RAM they will be routed to the correct location by the RUN procedure. If attempting to RUN in C64 RAM you can either change the load addresses using a disk editor or transfer the programs a half at a time to the corresponding C64 location.

LOADING-RUNNING KRACKED PROGRAMS

This section covers loading and running 8K and 16K programs using an external VIC style RAM (block switchable 8K or 16K -Note 16K cartridges cannot be run in 8K RAMs)

1. Switch all KK switches OFF. Press reset. Turn ON switches 1 and 9. Set external RAM card so that 8K RAM is in block 1 as identified by RAM manufacturers instructions.

2. Press reset. 38911 message should appear. Load Kracked program from disk using "prg name",8,1 format.

3. When done loading switch #9 OFF. For 8K cartridges, go to step 4. --- For 16K do not change KK switches yet. First switch first half of RAM out of block one and switch second half into block one then repeat step 2. When DONE switch 9 and 1 OFF. Next switch first half of RAM into block one, second half into block 2. NOTE It does not matter which half (8K section) of the external RAM is considered first half or second half. Just pick a side and stick to it!

4. Turn on switch combination that you wrote down for the cartridge you have just loaded. Press reset and the program will RUN! NOTE: It is a good ides to use combination as part of program name so you have it in your directory at all times.

USING C64 RAM

This information is intended for those inclined to experiment with the use of internal RAM to run kracked cartridges. You should be alerted to the fact that this is one of the simplest things for a cartridge manufacturer to prevent and so many cartridges may not run in internal RAM. One of the easiest ways to prevent use of RAM is to use a routine in the cartridge program which tries to erase itself in part or whole. If the program is in ROM or write protected external RAM, it cannot be erased or changed. However if it is in internal C64 RAM of which you have no control of the read/write lines, it will be erased or destroyed by such a routine. For this reason the

process of using internal RAM is interesting but hardly effective. For competent machine language programmers, these protection routines could be located and taken out.

To effectively handle kracked cartridge use in C64 RAM you will need to obtain and learn to use a monitor program. The monitor should be able to reside under $8000 and not in the $4000 to $6000 block.

The method you will follow should begin by looking for the cold start and warm start addresses at the begining of the program. Load the program as well as a monitor and look for the cold start and warm start address. Remember the KK cartridge will initially load to $4000 in your C64 RAM and the first two bytes will be the cold start address in standard 6502 LO byte HI byte format. The second two bytes at $4000 ($4002 & $4003) will be the warm start address. Write these down then transfer the program to its normal resident address. Typically the normal resident location of the cartridge will be $8000 or $A000 or possibly $E000. The cold and warm start addresses should give you a clue to this.

METHOD ONE... On some programs after transferring you can simply SYS to the warm start or in other cases the cold start address. Remember that if you are using SYS that you need to first convert the hex value you obtained for the warm and cold start addresses into decimal. If you use a monitor program to make the transfer, it is usually easier to use the Go command of the monitor. If all fails, you may be encountering some form of protection.

METHOD TWO... If the location is $A000 or $E000 you will need to disable the ROM in those locations before trying to execute a program at that address. This can be done by changing the byte at $0001. For disabling BASIC ($A000) change $0001 to $36. To disable both BASIC and KERNAL ($A000 and $E000), change $0001 to a $35. Remember that any monitor that uses KERNAL or BASIC would be disabled by this. In other words a basic POKE will work but will also cause loss of control. The most certain way to maintain control is to use your own machine routine to do this. After disabling the ROM concerned, you can try a SYS or press reset. Don't forget to previously load and transfer the program to the normal resident address!

METHOD THREE... Another possibility to experiment with is to set the KK switches 7 and 8 to the configuration normally used by the cartridge AFTER first loading and transferring the program to the resident address. After getting everything set up you will usually have to use the reset switch as you may not have control of the system. (Depends on setting of 7 and 8)

As stated earlier there is not a foolproof way of running in C64 RAM due to the many variables and possible protection methods. Your best bet is to experiment as much as you can and even try combinations of the above methods as they may apply.

Once you have determined the method for a particular cartridge, you will find it helpful to modify the diskette load address so that the program will load directly to the resident address and not require transfer from $4000. Products such as "The Software Protection Handbook" provide disk editors and programs to identify starting Track and Sector for use in modifying "load to" addresses. In general, the procedure is to identify which track and sector contains the first block of the cracked program and then use a disk editor to change the bytes which control the "load to" location.

BURNING PROMS

One of the unique advantage of "Kracking" cartridges is that the kracked cartridge program recorded on the diskette is by nature ready to be "burned" in a programmable read only memory. Any commercially available PROM programmer box that plugs into your C64 should be able to handle this. Although the specific details of use will vary from one burner to another the general idea is the same. This is to download the kracked cartridge to the PROM burner unit then follow the burners instructions on burning the PROM! Once again keep in mind that the kracked program is addressed at $4000. With the burned PROM, this will make no difference as it is an 8K block and can reside at any 8K block location. Normally the cartridge wiring itself will determine where the cartridge resides. In the case of 16K cartridges you will need to load half, transfer it to the burner then load the other half and transfer it to the burner (assuming your burner can handle 16K PROMS).

Although the cost of PROM and blank cartridge may total around $15 there are some programs which you may feel important enough to back up this way. If you don't own a burner and don't expect to use one enough to justify the cost, you may be able to get some help from a local user group.

WARRANTY

This product is warranted by the manufacturer to be free from defects and materials for a period of 90 days from date of purchase. No other warranty is expressed or implied. The use of this product should be by someone of adequate technical experience. Neither the manufacturer nor it's agents can assume any liability for incidental or consequential damages that may arise out of use or misuse of this product.

* * * WARNING * * *

Failure to follow instructions or properly install this accessory may present a hazard to person and property.

KARTRIDGE KRACKER

NOW you can own this unique and powerful tool which will allow you to dump the contents of 8K and 16K cartridges onto disk!! But whats really great is that you can also RUN the cartridges programs without plugging in the cartridge! The KRACKER gets YOU INSIDE the cartridge! Put all your favorites on disk and get rid of the clutter. This package provides you with the software and hardware needed to get started. Program on disk included. (Some cartridges require use of external RAM not included)

MADE IN THE USA

KARTRIDGE KRACKER ERRATTA

INSERTS

General description add: The KK system is provided with the KK circuit board, and the KK disk containing the KK program plus a free public domain monitor program which is provided for those who wish to do more experimenting with the data contained in the ROM cartridges. Use of the system requires a user supplied 8K or 16K RAM expander of the VIC 20 variety. (Not included)

Kracking Kartridges step 5 change to read: Using combination from above, if the second digit is a 6 then turn on switch 6. However, if the second digit is a 4, turn on switch 5 (five).

Kracking Kartridges step 6 should read: LOAD "KAR*",8,1 [RETURN]. ....

Loading-Running Kracked Programs step 3 sentence one: When done loading, switch #9 and #1 OFF.

Loading-Running Kracked Programs step 3 add after "then repeat step two" for the second half of the cartridge saved on disk (2GAME).

USING C64 RAM

Insert at beginning: Note: It is only possible to run a few cartridges in C64 RAM without some modification of the program code, and even this requires some familiarity with machine language and use of editor assemblers. A monitor and a brief set of instructions is provided on the disk for this purpose.

MANUAL CORRECTION

SOFTWARE LOADS WITH

LOAD "KAR*",8,1

SYS3291