SHELL_CLK 4.5

1. <u>**S.O.:**</u>

   WINDOWS 95/98/NT/XP

2. **SPECIFICATIONS:**

   Encrypting algorithm: CLK®

   Encrypting procedure: CLK®

   Encrypting - Decrypting speed (using a 2 GHz. processor): 265 Kb./s.

3. SUMMARY:

1- This software encrypts any kind of file and returns an unreadable file that can be decrypted with the same master key.

2- The program build or read a master key book (or database). Each master key contains up to 12 individual keys (10 text keys up to 64 characters, and 2 numeric keys). Using these keys, the software encrypts and decrypts, but <u>having activated a Master Key from a Key Book beforehand.</u>

3- The way this software encrypt and decrypt is totally innovative and the last keys close the encrypted file. As a result of it, it's almost impossible decrypt that file without the original key. What's more, this software can encrypt any file as many times as you want, increasing security.

4- A file can be used (verify key) that is independent from the key book and becomes key Nr. 23 of Win_CLK ´s algorithm. **IMPORTANT: <u>If you encrypted using 23th key, the selected file must be the same and without changes you must use to decrypt. Remember this file´s name in order to decrypt, because CLK doesn´t keep any track of this file.</u>** This function is optional. The software ask if you want to use 23rd key (verify key) before encrypting and decrypting.

5- This software also has an utility to erase files definitely and without tracks called " logic erase". This function, overwrite the source file with zero in the hard disk. Ater that, truncates it to just 1 byte and then erases it from the system.

4. **HOW TO USE:**

In order to encrypt and decrypt a file, there must be a Key Book present. The key book is a database that contains the master keys and his attached 12 keys. You can create as much key books as you want, and you can have as many master keys as you want in each other.

(ADVICE: You must remember which master key and what verify key you used in the encryption process. You'll need THE SAME KEYS WITHOUT CHANGE in order to decode. CLK doesn't keep any reference about these keys.)
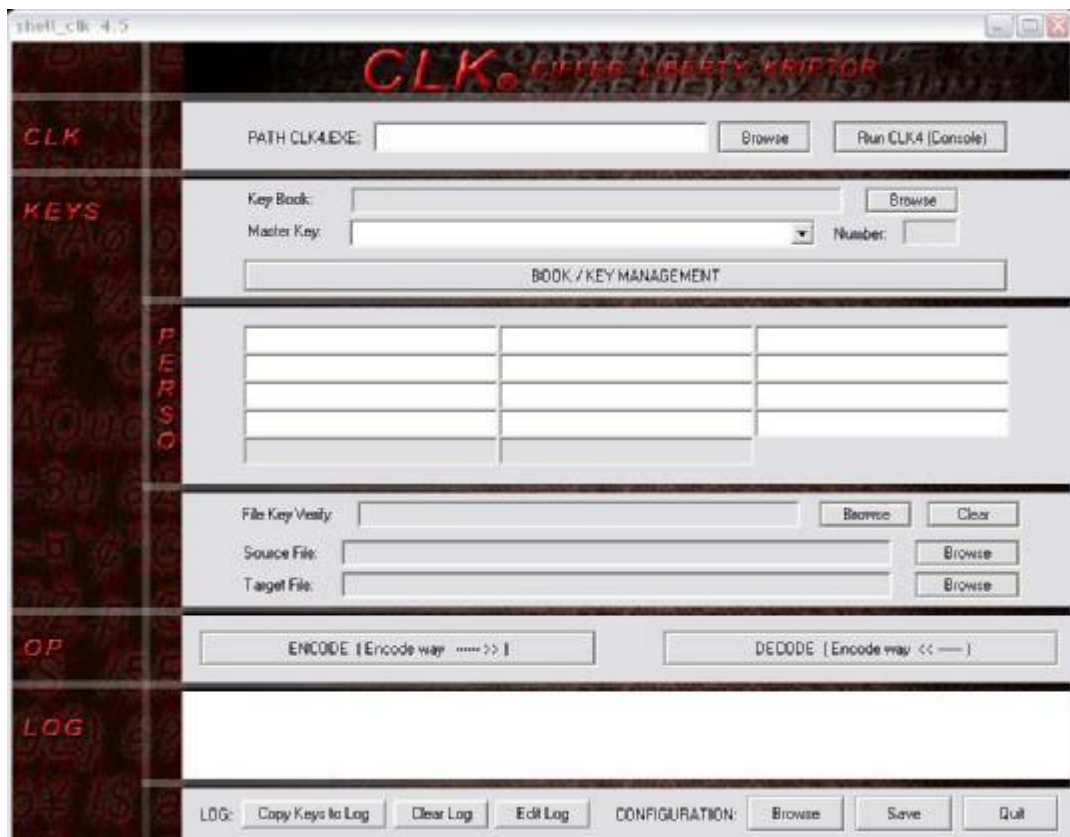

fig.- 1

How to create a Key Book:

1.- To create a new key book, click once over "KEYBOOK MANAGEMENT" (fig. 1). A new window called "KEYS" emerges. (fig. 2)

2.- Click over "NEW Key Book". Inside the emergent window, you must write the desired name and extension for you key book (example.- keys.clk). Click on "save". ADVICE: In order to complete the key book creation process, you must create a Master Key (see " How to create a Master Key"), If not, for security reasons, the key book WILL NOT BE SAVED.
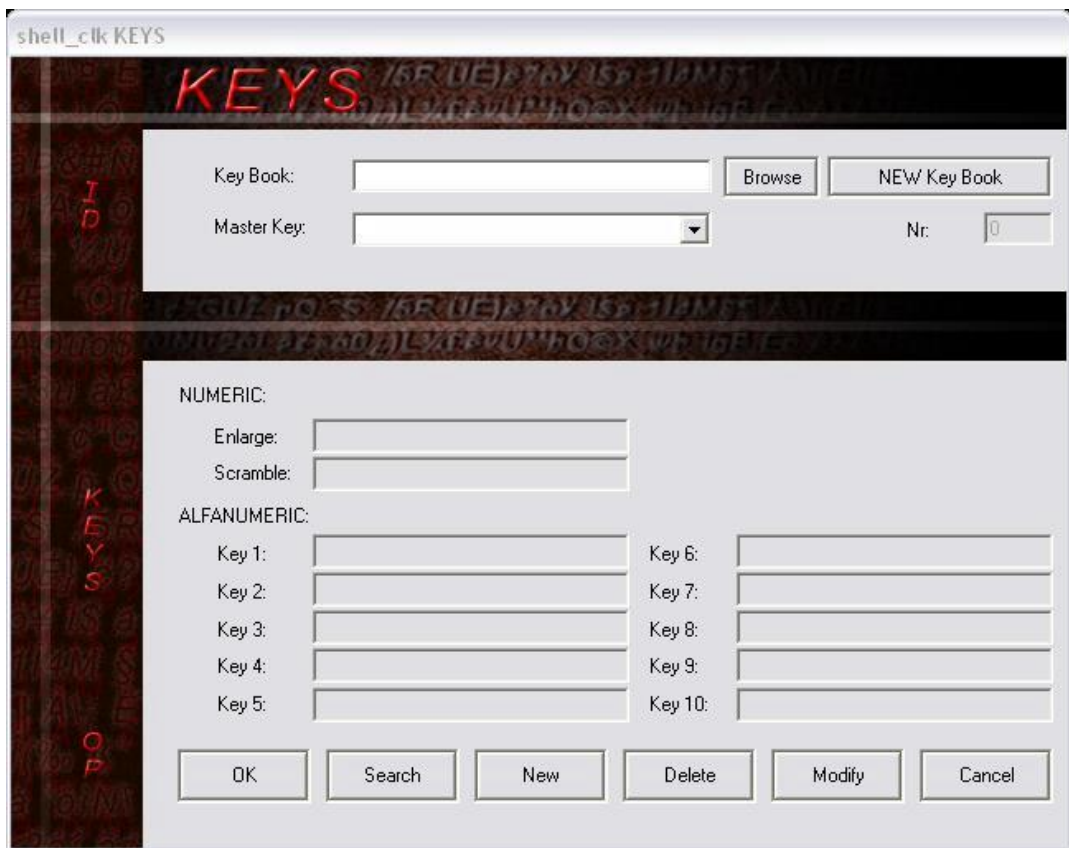
fig.- 2

How to create a Master Key:

1.- Click over NEW to create a master key (fig. 2). A new window called "NEW MASTER KEY" will pop up.(fig. 3)

2.- Fill the "Master Key" field with the desired name. ADVICE: A Master key and his 12 attached keys doesn't need to be unique (They can be repeated any number of times in the same key book. The only thing that is unique for each Master key is his number.

3.- Fill the numeric fields called "Enlarge" y "Scramble" with a minimum value of 1.

4.- Fill the alphanumeric fields that you want. Keys 1-10.

fig.- 3

5.- Click on "OK". ADVICE: If you created a NEW Key Book, it will be saved now in the previously designed path.

How to activate a Master key:

1.- In order to activate a Master key, you have to load a Key Book before (Select "explore" in the "KEYS" window (fig. 1). A new window emerge. Then, select the desired Key Book).

2.- Select the desired master key from listbox (fig. 4) Now the Keys from the selected Master Key are shown.
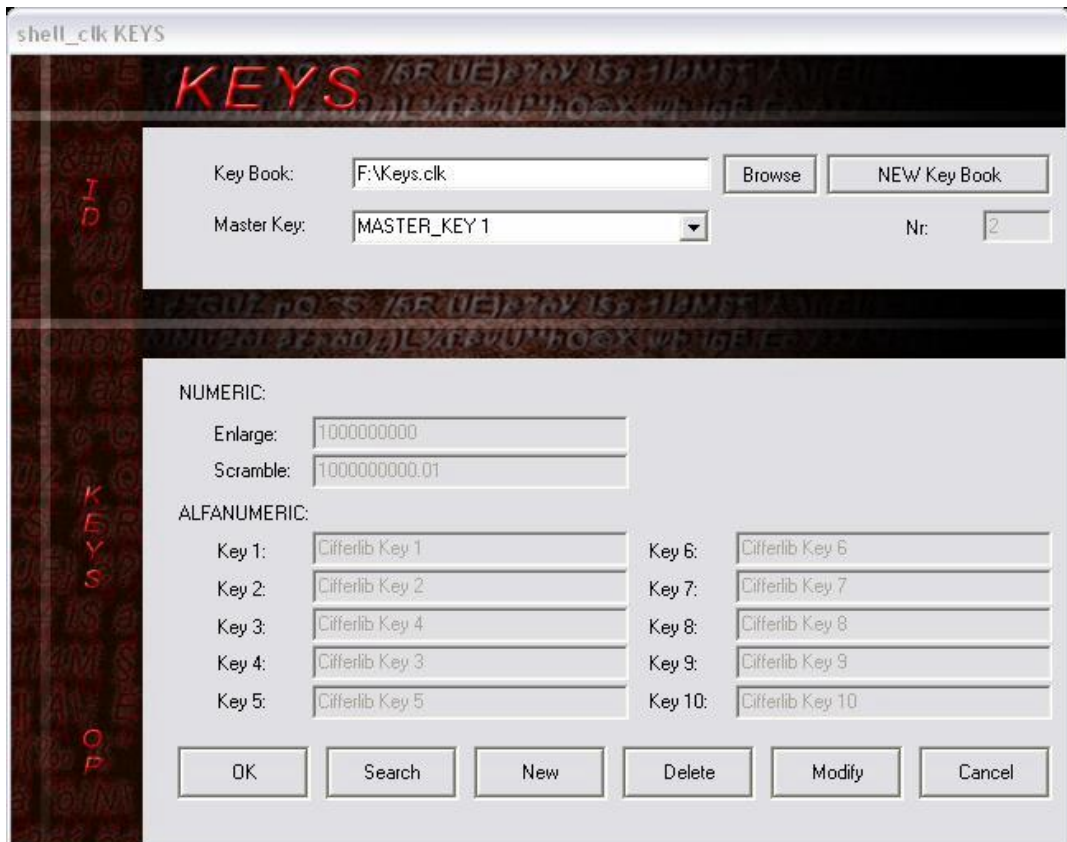
fig.- 4

3.- Fast activation: In the main window click on "Browse" located to the right, then select the Master Key on the listbox (fig. 1)

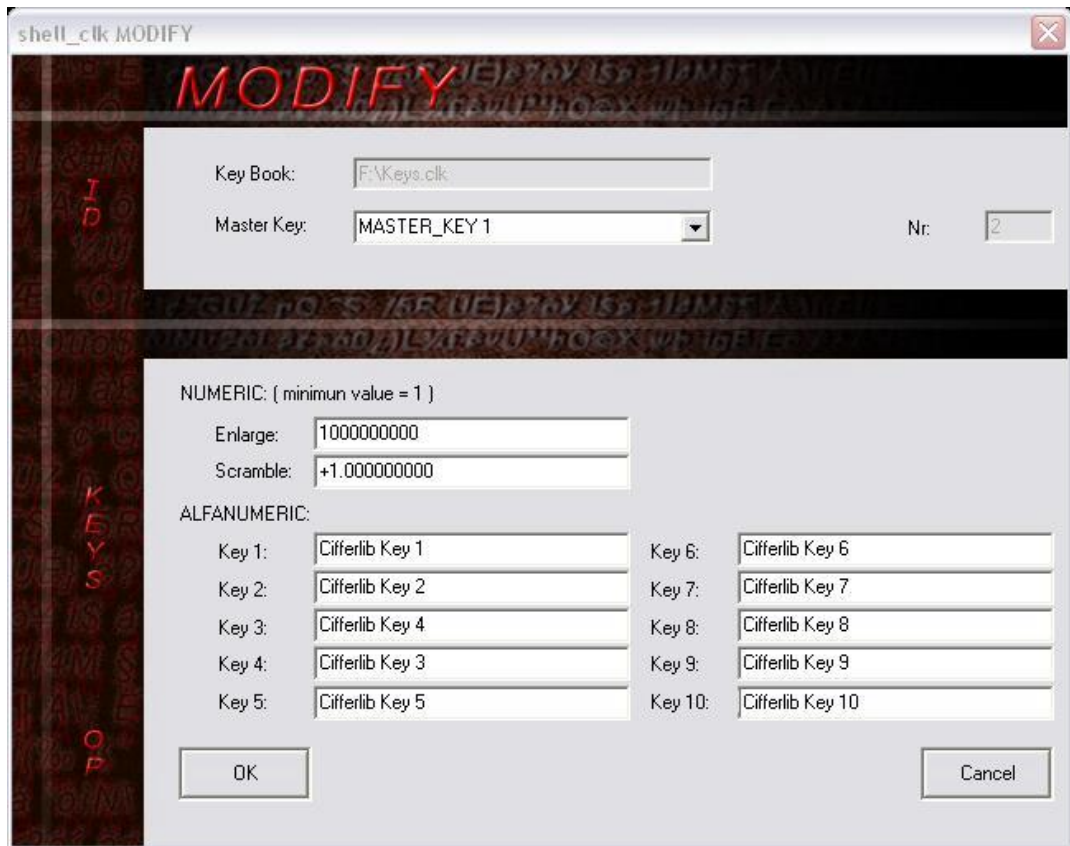## How to Delete a Master Key:

1.- To delete a master key and his 12 attached keys, you must activate the Master Key you want to delete (See "How to activate a Master Key")

2.- Click over "DELETE" (fig.4).

How to Modify a Master Key:

1.- In order to Modify any Key attached to a Master Key, first you must activate the Master Key you want to Modify (See "How to activate a Master key").

2.- Click on "MODIFY" (fig.4). A window called "MODIFY" will open. (fig. 5)
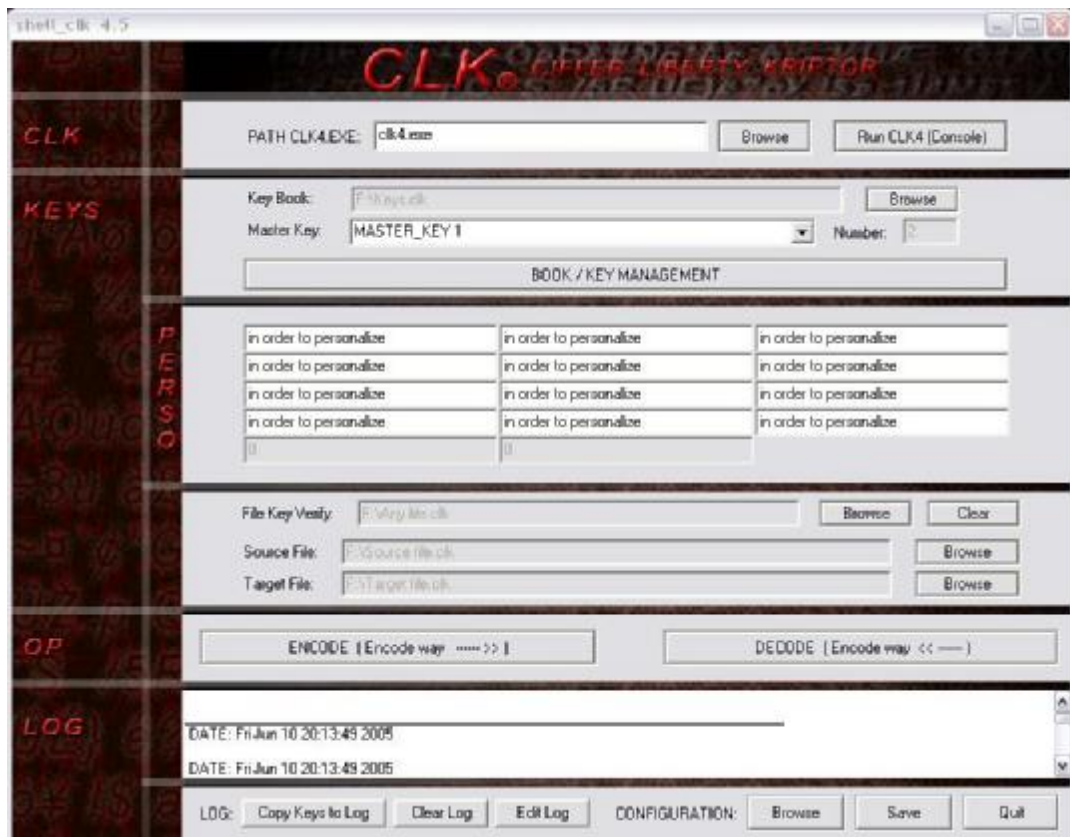

fig.- 5

3.- Modify any fields you want and click OK for saving changes.

How to Encode and Decode:

1.- In order to Encode or Decode a file, a Master Key must be selected first (See "How to activate a Master Key").

fig.- 6

2.- If you wish to personalize the algorithms it fills up the perso fields (fig. 6).

3.- Select the Source file, click over "Browse" button you see on the right side (fig. 6).

4.- Select the Target file, click over "Browse" button you see on the right side (fig. 6). A new window opens . You must write down the name and extension that you want for the target file (Example.- Target file.clk). Click on "save".

5.- If you want to use the File Key Verify, select it. To do it, click on the "Browse" on the right side (fig. 6).

(ADVICE: You must remember which Master Key and what File Key Verify you used in the encryption process. You'll need THE SAME KEYS WITHOUT CHANGE in order to decode. CLK doesn't keep any reference about these Keys.)

6.- Finally, click on ENCODE or DECODE button.

Log and configuration:

This software generate a log that can be edited and saved with user´s configuration.

The registered data:

       Path of Clk4.exe

       Key Book used

       Number of Master Key

       Source File

       Target File

       File Key Verify

       Personal parameters

       As an option, the used Master key and his 12 attached keys

1.- To register the used Master key and his 12 attached keys click on COPY KEYS TO LOG

2.- To Delete Log click on CLEAR LOG (fig. 6)

3.- To Save Log and Configuration click on SAVE.

4.- To Load a Configuration and his Log click on BROWSE and select one.

5.- To Edit Log click on EDIT LOG (fig. 6) A new window called "LOG" emerges. (fig. 7), Once finished click on SAVE to return.
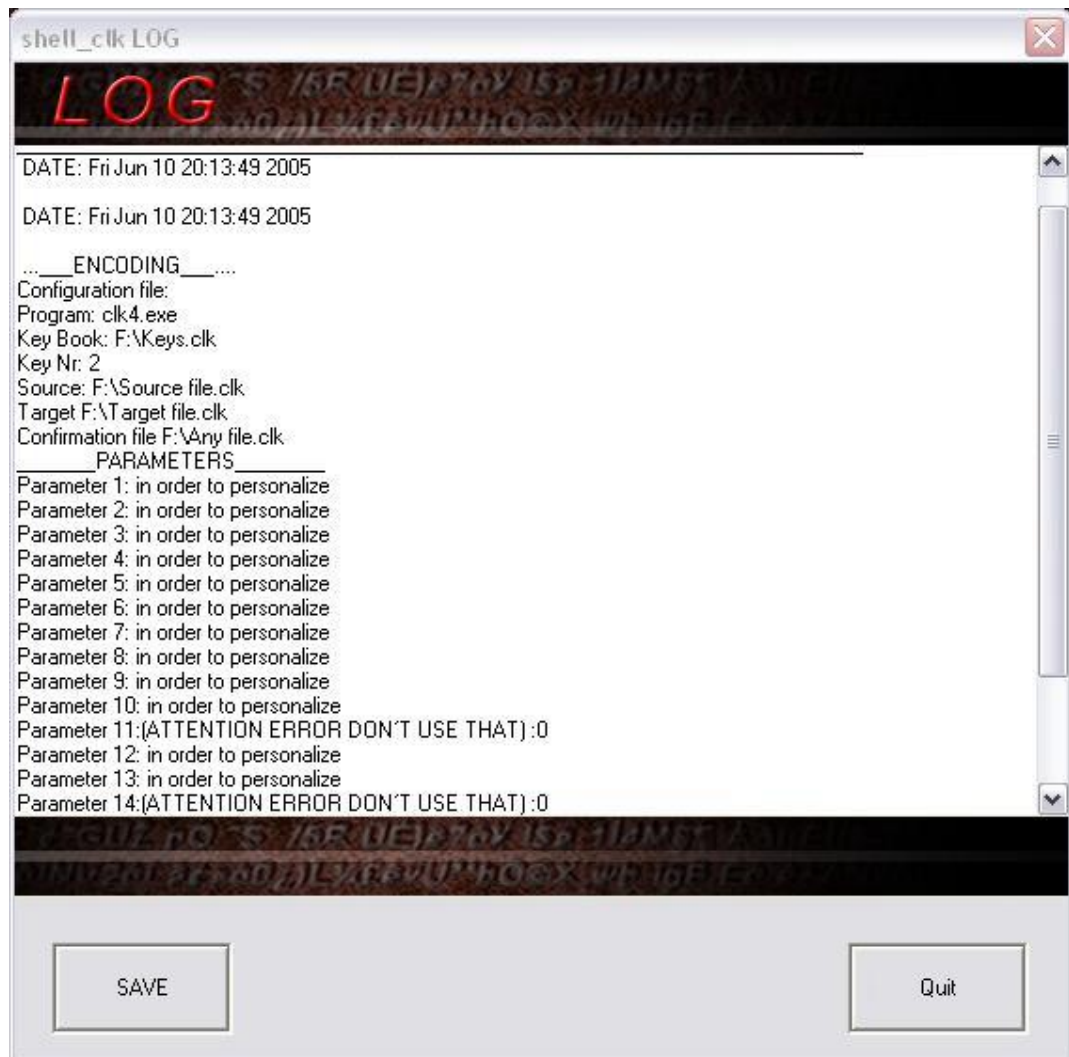
fig.- 7

FINAL ADVICE: CIFFERLIB HAS NO RESPONSABILITY OF ANY DATA OR MATERIAL LOST IN THE USE OF THIS SOFTWARE, EVEN IF IT HAPPENS FOLLOWING THIS MANUAL.