

SHELL_CLK 4.5

1. ENTORNO OPERATIVO:

WINDOWS 95/98/NT/XP

2. CARACTERÍSTICAS:

Algoritmo de cifrado: CLK®

Procedimiento de cifrado: CLK®

Velocidad de cifrado y descifrado (con procesador a 2 GHz.): 265 Kb./seg.

3. RESUMEN:

1- Este programa encripta y codifica cualquier tipo de fichero independientemente de su extensión y da como resultado un fichero ilegible, que se puede decodificar y descifrar con la correspondiente clave maestra.

2- El programa crea o lee un libro (o base de datos) de claves maestras. Cada clave maestra está compuesta por 12 claves individuales (10 claves de texto con 64 caracteres de longitud máxima, y 2 claves numéricas: un número entero y un número doble con signo). Por medio de éstas claves el programa codifica y decodifica, **habiendo activado antes una clave maestra de un libro de claves.**

3- La forma de encriptar de este programa es completamente innovadora y las últimas claves cierran lo codificado, de tal forma que es prácticamente imposible descifrar sin tener la clave original; además este programa puede codificar algo ya codificado previamente cuantas veces se quiera, con lo que se multiplica la seguridad.

4- Incluye un fichero a seleccionar por el usuario (fichero confirmación), que no se queda grabado en el fichero de claves y que se convierte en la clave 23 de los algoritmos Shell_CLK 4.5 . **IMPORTANTE: Si ha encriptado con la clave 23, el fichero seleccionado tiene que ser el mismo y sin modificar que aplique para descifrar. Es responsabilidad del usuario acordarse de éste fichero y su nombre, así como de que esté disponible por Shell_CLK 4.5 para su descifración correcta, ya que el programa no graba ningún dato referente a éste fichero.** Esta función es opcional. El programa

pregunta si se quiere aplicar la clave 23 (fichero de confirmación) tanto al encriptar como al desencriptar.

5- Este programa también tiene una utilidad para borrar ficheros de forma definitiva y sin dejar rastros llamada "borrador universal". El borrador universal sobrescribe con ceros en el disco, todo el contenido físico de un fichero seleccionado, después lo trunca dejándolo en un solo byte conteniendo un cero y posteriormente lo borra del sistema.

4. **MODO DE USO:**

Para poder codificar y/o decodificar un fichero debe existir un Libro de Claves. El libro de claves es una base de datos donde se almacenan las claves maestras con sus 12 claves asociadas. Puede crear tantos libros de claves como quiera, y en cada uno de ellos, pueden existir tantas claves maestras como desee.

(NOTA: Usted debe recordar qué clave maestra y qué fichero de confirmación utiliza para codificar, ya que necesitará LOS MISMOS y SIN MODIFICAR para la decodificación. CLK no guarda referencia alguna sobre estos datos.)

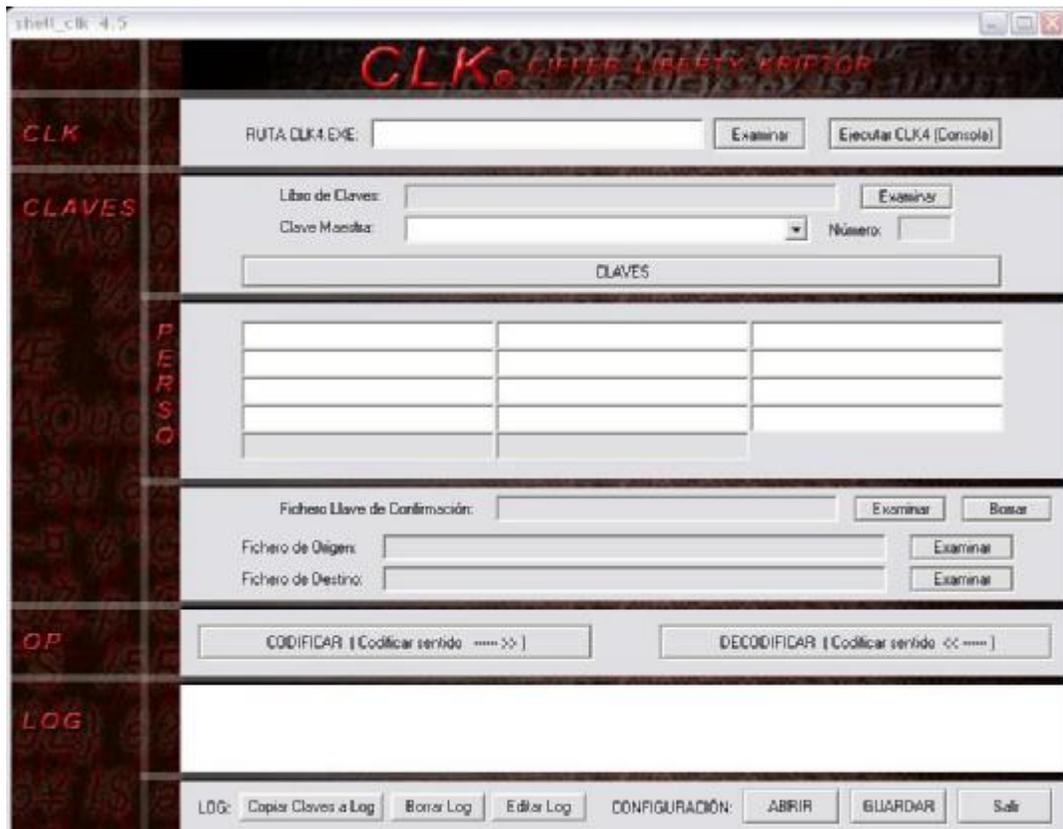


fig.- 1

Cómo crear un Libro de Claves:

1.- Para crear un nuevo libro de claves, haga click sobre CLAVES” (fig. 1). Se le abrirá la ventana “CLAVES” (fig. 2)

2.- Pulse sobre “Crear Nuevo libro de claves”. En la ventana emergente, usted debe escribir el nombre y la extensión que desee para su libro de claves (ej.- claves.ck). Pulse “guardar”. NOTA: Para que la creación del libro de claves sea completa, debe dar de alta una clave maestra (ver “Cómo crear una clave maestra”), de lo contrario, por seguridad, el libro de claves NO SE GUARDARÁ .

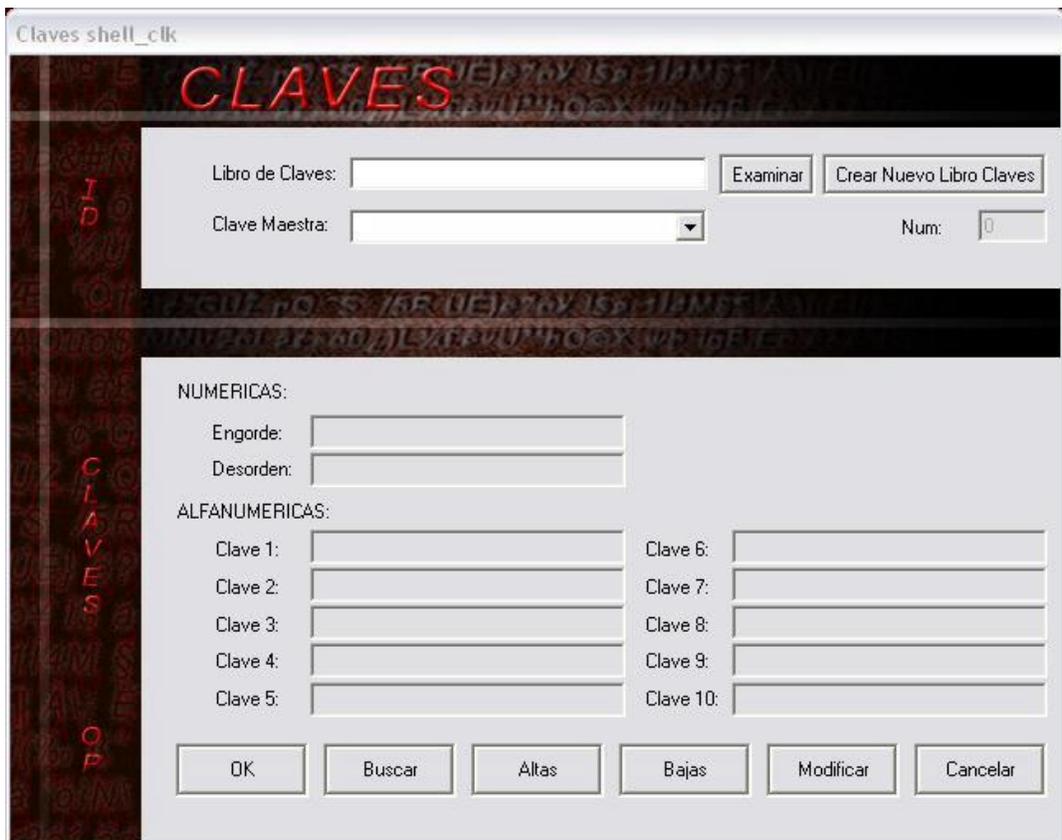


fig.- 2

Cómo crear una Clave Maestra:

1.- Para crear una nueva clave maestra haga click sobre ALTAS (fig. 2). Se le abrirá la ventana “ALTAS” (fig. 3)

2.- Rellene el campo “Clave Maestra” con el nombre que desee asignarle. NOTA: Una Clave Maestra así como sus 12 claves asociadas no tiene por que ser único (pueden repetirse indefinidas veces en el mismo Libro de Claves, lo que es único para cada Clave Maestra es su número de clave).

3.- Rellene los campos numéricos “Engorde” y “Desorden” con un valor mínimo de 1.

4.- Rellene los campos alfanuméricos que deseé, las claves (1-10).

Altas shell_clk

ALTAS

Libro de Claves: F:\Claves.clk

Clave Maestra: Clave Maestra 1 Num: 1

NUMERICAS:

Engorde: 10

Desorden: 10

ALFANUMERICAS:

Clave 1: Cifferlib Clave 1 Clave 6: Cifferlib Clave 6

Clave 2: Cifferlib Clave 2 Clave 7: Cifferlib Clave 7

Clave 3: Cifferlib Clave 3 Clave 8: Cifferlib Clave 8

Clave 4: Cifferlib Clave 4 Clave 9: Cifferlib Clave 9

Clave 5: Cifferlib Clave 5 Clave 10: Cifferlib Clave 10

OK Cancelar

fig.- 3

5.- Presione “OK”. NOTA: En caso de haber creado un nuevo libro de claves en este momento SE GUARDARÁ en la ruta que usted haya designado previamente.

Cómo activar una Clave Maestra:

1.- Para activar una Clave Maestra, debe cargarse previamente un Libro de Claves (haga click en el botón CLAVES se le abrirá la ventana CLAVES (fig. 2) seleccione examinar y en la ventana emergente seleccione el Libro de Claves a utilizar).

2.- Seleccione del desplegable la Clave Maestra que deseé (fig. 4) y se podrán visualizar las claves contenidas en la Clave Maestra seleccionada.



fig.- 4

3.- Activación rápida: En la ventana principal haga click sobre el botón de examinar situado a la derecha, después seleccione la Clave Maestra del desplegable (fig. 1)

Cómo borrar una Clave Maestra:

1.- Para borrar una Clave Maestra y sus 12 claves asociadas, primero debe activar la Clave Maestra que desea eliminar (ver “cómo activar una Clave Maestra”).

2.- Haga click sobre “BAJAS” (fig.4).

Cómo modificar una Clave Maestra:

1.- Para Modificar cualquiera de las claves contenidas en una Clave Maestra, primero debe activar la Clave Maestra que desea modificar (ver “cómo activar una Clave Maestra”).

2.- Haga click sobre “MODIFICAR” (fig.4). y se le abrirá la ventana “MODIFICACIONES” (fig. 5)



fig.- 5

3.- Modifique los campos que desee y presione OK para guardar los cambios.

Codificar y Decodificar:

1.- Para poder codificar y/o decodificar un fichero previamente se debe activar una Clave Maestra (ver “cómo activar una Clave Maestra”).

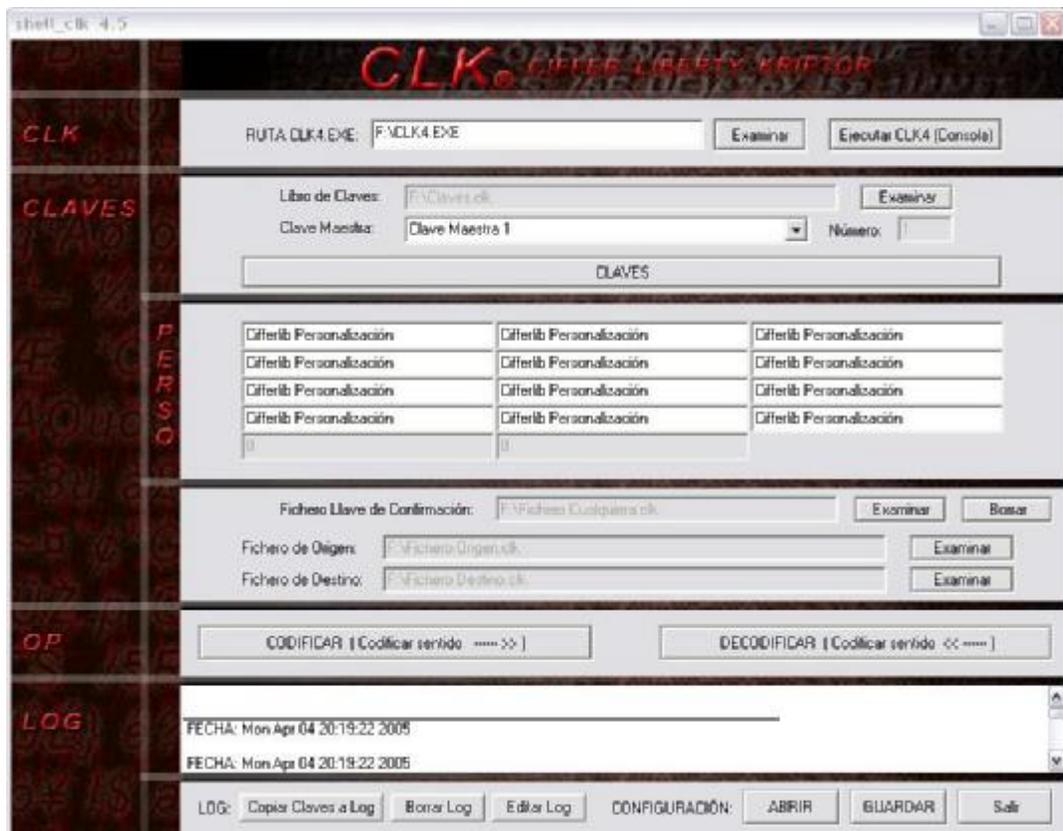


fig.- 6

2.- Si desea personalizar los algoritmos rellene los campos de personalización (fig. 6).

3.- Seleccione el Fichero de Origen, para ello haga click sobre el botón “EXAMINAR” de su derecha (fig. 6).

4.- Seleccione el Fichero de Destino, para ello haga click sobre el botón “EXAMINAR” de su derecha (fig. 6). En la ventana emergente, usted debe escribir el nombre y la extensión que desee para el fichero de salida (ej.- Fichero Destino.clk). Pulse “guardar”.

5.- Si desea usar el Fichero de Confirmación selecciónelo, para ello haga click sobre el botón “EXAMINAR” de su derecha (fig. 6).

(NOTA: Usted debe recordar qué clave maestra y qué Fichero de Confirmación utiliza para codificar, ya que necesitará LOS MISMOS y SIN MODIFICAR para la decodificación. CLK no guarda referencia alguna sobre estos datos.)

6.- Finalmente haga click sobre los botones CODIFICAR (paso de los algoritmos de izquierda a derecha) o DECODIFICAR (paso de los algoritmos de derecha a izquierda) según deseé.

Log y configuración:

Este programa genera un log que puede ser editado y guardado junto con la configuración utilizada por el usuario.

Los datos registrados son:

Ruta Clk4.exe

Libro de Claves utilizado

Número de Clave Maestra

Fichero de Origen

Fichero de Destino

Fichero de Confirmación

Parámetros de Personalización

De forma optativa la Clave Maestra utilizada así como sus 12 Claves asociadas

- 1.- Para añadir las Claves asociadas a la Clave Maestra empleada haga click sobre COPIAR CLAVES A LOG
- 2.- Para Borrar el Log haga click en BORRAR LOG (fig. 6)
- 3.- Para Guardar el Log y la Configuración haga click en GUARDAR.
- 4.- Para Cargar una Configuración y su respectivo Log haga click en ABRIR
- 5.- Para editar el Log haga click en EDITAR LOG (fig. 6) Se le abrirá la ventana LOG (fig. 7), Una vez editado haga click en GUARDAR para volver.

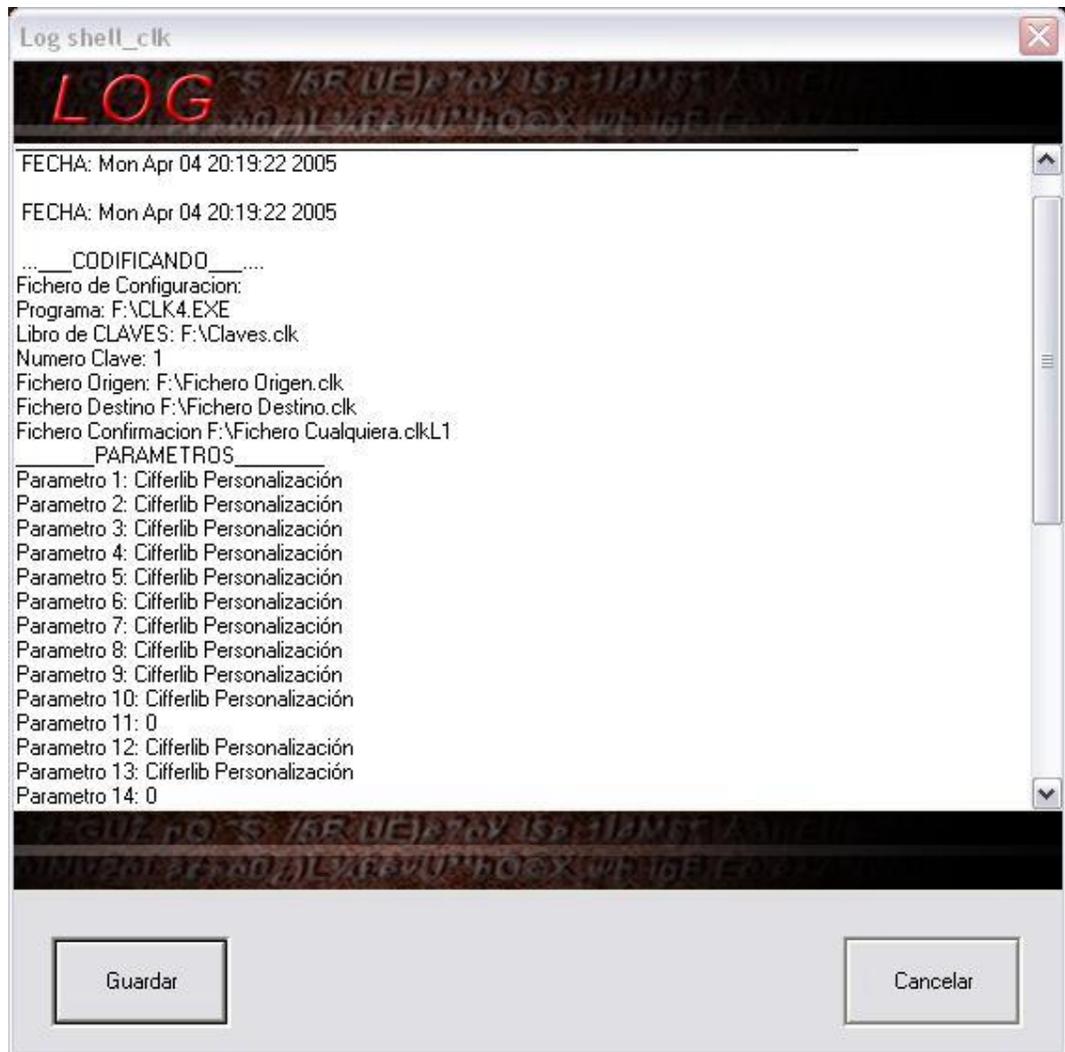


fig.- 7

NOTA FINAL: CIFFERLIB NO SE HACE RESPONSABLE DE LA PÉRDIDA DE DATOS QUE PUDIERA PRODUCIRSE POR EL USO DE ESTE SOFTWARE, INCLUSO SI ESTUVIERA PROVOCADO POR EL SEGUIMIENTO DE ESTE MANUAL.