criptonita 0.0.1 GPLv3

Creado por: Alejandro Cisneros
Actualizado: 11/06/2021
Licencia: GPLv3
Uso

El script de criptonita es una implementación automatizada de herramientas como gpg GNU Privacy Guard para sistemas operativos Linux que nos permite hacer el uso de herramientas de cifrado y descifrado sin necesidad de memorizar comandos, gracias a su automatización, criptonita cuenta con métodos de cifrado simétrico como
3DES, IDEA, TWOFISH, BLOWFISH, AES, AES 192, AES 256. y algoritmos de cifrado asimétrico RSA y ElGamal.

Ejecución de script

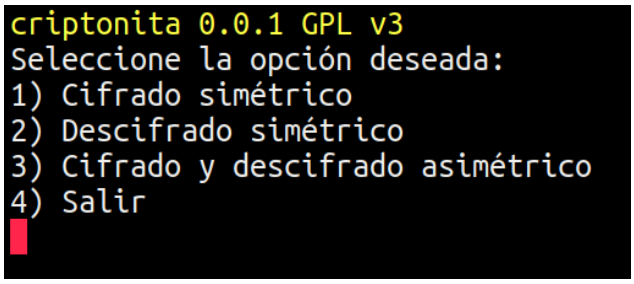
Para ejecutar el script necesitas descargar criptonita.sh cuyo programa se puede ejecutar como cualquier script en Linux "$ *bash criptonita.sh*" o
"*./criptonita.sh*" recordando que para ejectura un script en Linux es necesario el previo otorgamiento de permisos con el uso del comando *chmod:*

Ejemplo

chmod 700 criptonita.sh
./criptonita.sh

En cuyo ejemplo primero se le otorgan los permisos al script para posteriormente ejecutar

Cuando ya hemos ejecutado el script lo primero que veremos será un menú de opciones

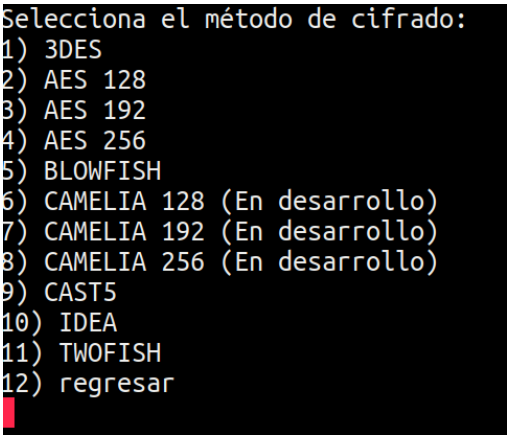


Para seleccionar una opción solo requiere ingresar el número y presionar ENTER

1) Cifrado simétrico

Cuando seleccionamos la opción de cifrado simétrico estamos hablando de cifrar con una contraseña un un archivo cualquiera incluso directorio el cual solo podrá ser vuelto a visualizar con el uso de esta misma contraseña, en otras palabras solo la persona con la contraseña podrá ver dicho archivo.

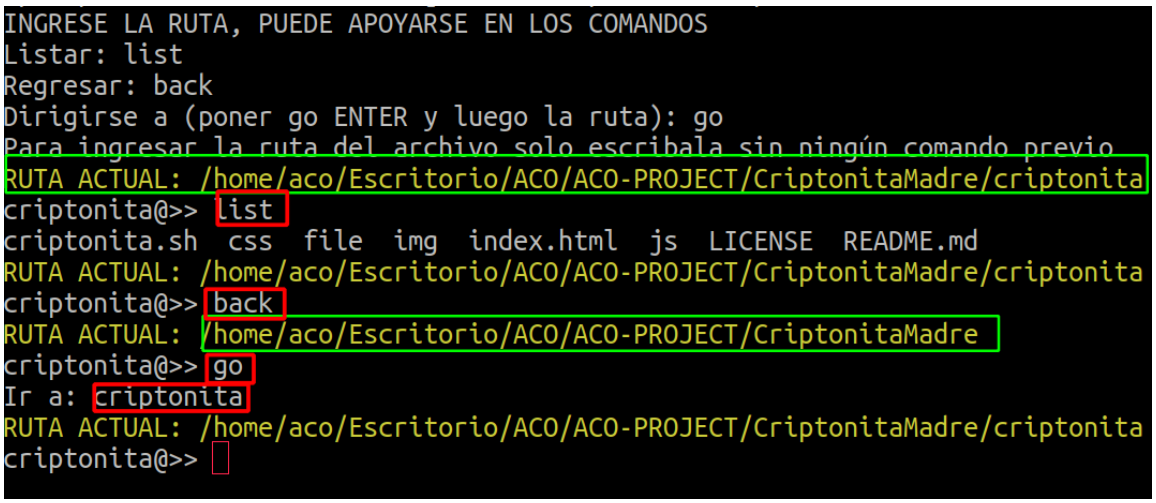
Una vez seleccionada esta opción vemos el siguiente menú de métodos de algoritmos



#NOTA: CAMELIA 128,192 Y 256 no se encuentran en funcionamiento aún, hasta próximas versiones
Una vez seleccionado el método de cifrado vemos el prompt de criptonica:

El prompt de criptonita

Es una herramienta que permite ejecutar comandos básicos para navegar por los directorios como si de tu terminal se tratara, aunque cambiando la sintaxis
podemos listar con el comando ***list*** (análogo a un "*ls*"), podemos regresar a la carpeta madre con ***back*** *(* análogo a "*cd ..")* y podemos ir a una ruta específica con el comando ***go*** (análogo cd pero en dos líneas) en el cual se debe de considerar la sintaxis adecuada: primero se escribe **go** se presiona ENTER y se procede al llenado de la ruda a donde te quieres mover desde el prompt de criptonita; Ejemplos:



En este ejemplo se lista el contenido de la carpeta criptonita ***list***
Se sale de la carpeta criptonita a la carpeta madre ***back***
Presionamos el comando ***go*** ENTER y en la siguiente línea ingresamos la ruta a movernos en este caso regresamos a el directorio criptonita

Es importante ver que en el prompt de criptonita podemos usar rutas absolutas y relativas a la posición de RUTA ACTUAL

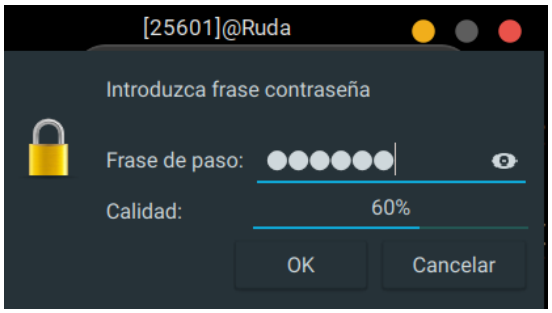
Para hacer alusión a un archivo
Para indicar el archivo a cifrar solo hace falta poner la ruta de su archivo a cifrar criptonita detectará si se trata de un fichero o un directorio para el proceso de cifrado; Ejemplo:

El cifrado de un archivo en el escritorio llamado contraseñas.txt
#Nota: Recuerde que el método de cifrado fue seleccionado en el paso anterior en el menú de métodos:

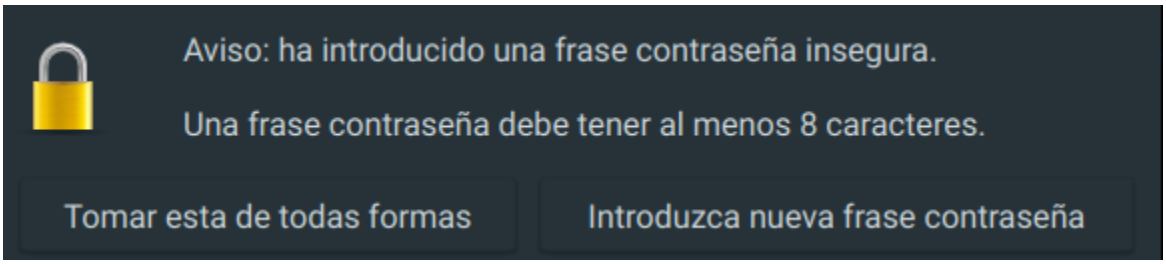
```
RUTA ACTUAL: /home/aco/Escritorio/ACO/ACO-PROJECT/CriptonitaMadre/criptonita
criptonita@>> /home/aco/Escritorio/ravtzn.txt
```

En este caso ponemos de ejemplo el uso de una ruta absoluta para señalar el fichero ravtzn.txt el cual vamos a cifrar con el método previamente seleccionado.

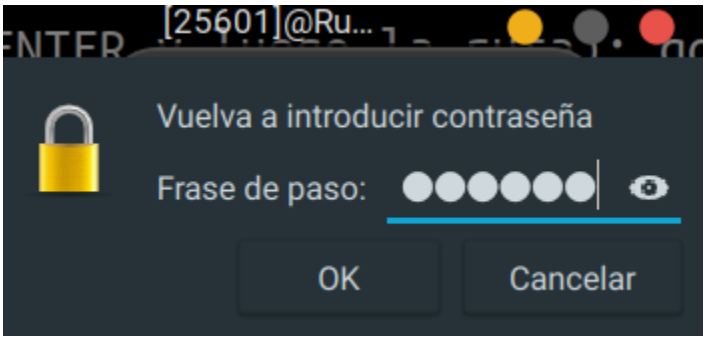
Al presionar ENTER criptonita le pedirá una contraseña en un cuadro de dialogo en el que deberá registrar su contraseña dos veces para verificar:



Si su constraseña es debil, criptonita le advertirá de dicha falta de complejidad en su contraseñas:



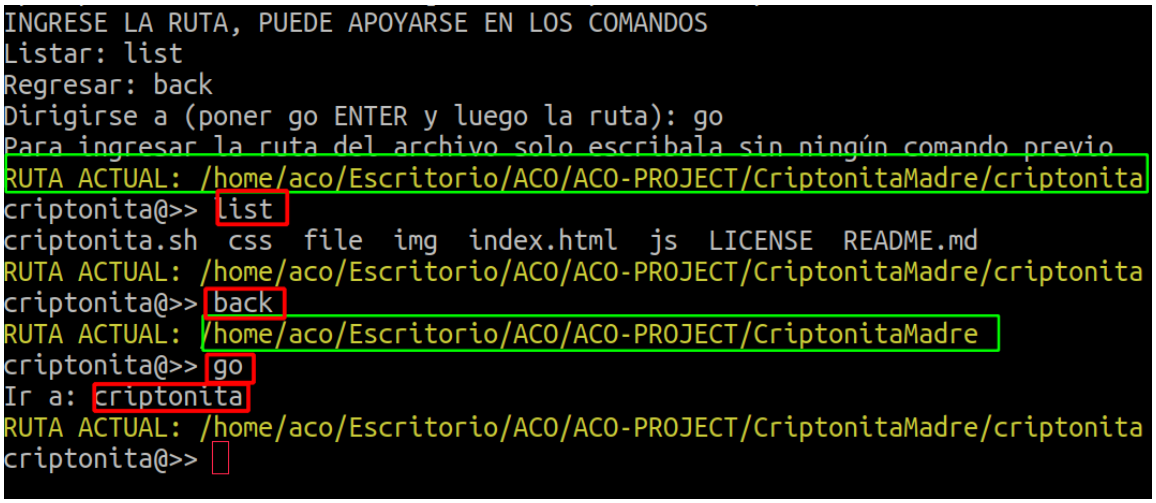
Aquí puede decidir continuar a pesar de la debilidad de su contraseña o regresar e ingresarla de nuevo; pasado este punto se le pedirá la confirmación de su clave



Si todo sale bien, su archivo esterá cifrado en la ubicación indicada, podrá corroborar su contenido cifrado.

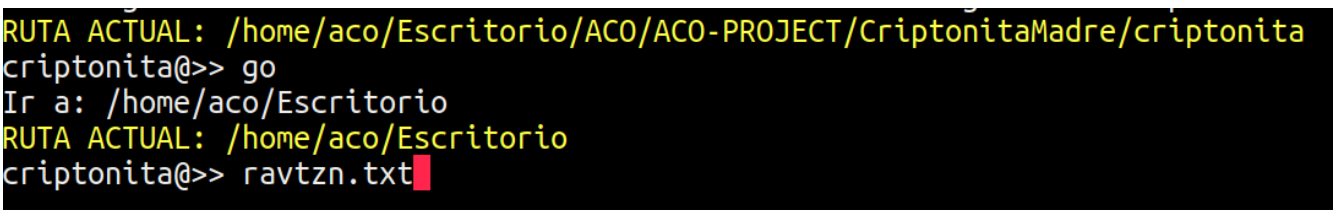
2) Descifrado de archivos

Cuando seleccionamos en el menú principal la opción de “Descifradi simétrico” inmediatamente vemos el prompt de criptonita, el cuál resulta una misma instancia del prompt que explicamos en la opción de cifrado, por lo que tenemos los mismos comandos y la misma implementación de las rutas (para indicarlas solo se ponen y se pueden utilizar de manera absoluta o relativa al la RUTAACTUAL):



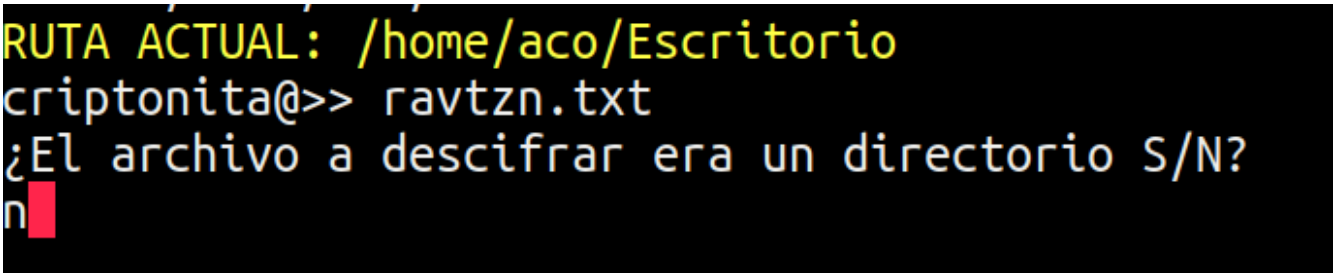
Esta vez voy para descifrar un archivo del escritorio llamado ravtzn.txt me moveré en el prompt de criptonita a dicha ubicación e indicaré la ruta del archivo de manera relativa a RUTA ACTUAL señalada con verde en la imagen anterior.

Ejemplo de descifrado para archivo en Escritorio

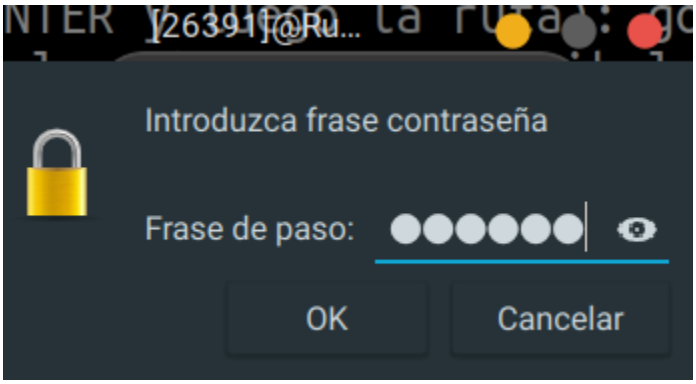


Una vez puesta la ruta, podemos dar ENTER

criptonita detectará si se trata de un archivo cifrado, detectará el método de cifrado, pero no puede detectar si se tratava de un directorio o fichero, por lo que se deberá responder con “s” para si o “n” para no en caso correspondiente, en el caso de ejemplo se trata de un fichero por lo que la respuesta a dicha pregunta es n (porque no se trataba de un directorio cuya información debe saber el usuario al ser propietario o autorizado de la información):



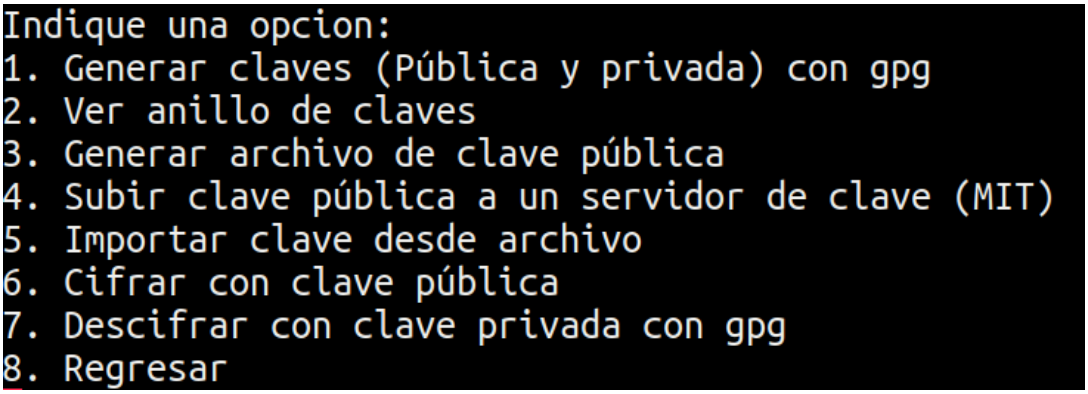
Posteriormente presionamos ENTER para ver la petición de contraseña:



La cual de ser correcta descifrará el archivo indicado y estará disponible en la carpeta donde previamente estaba el cifrado.

3) Descifrado y cifrado asimétrico

Criptonita cuenta con opciones para realizar cifrado y descifrado asimétrico las cuales podemos ver en su menú de opciones



De no conocer la terminología usada para cifrado asimétrico se recomienda informarse para poder utilizar estas funciones ya disponibles en **criptonita,** para probar estas funcionalidades se sugiere ir provando en el orden en el que se presentan en el menú.

El presente material de documentación está en pleno desarrollo, gracias por su comprensión…

4) Salir

Simplemente es la opción que nos permite salir del script