

Muy bien. El video ya está hecho por completo y quería pedir disculpas, ya que la calidad del sonido y la imagen no son muy buenos. Además tuve que grabarlos de manera asincrónica por problemas de rendimiento. Si alguno conoce un programa mejor que el AutoScreenRecorder, puede decírmelo y ahorrarme malos ratos.

Link del video: [Laboratorio de encriptación y hashes by Roadd en Vimeo](#)

PD: en el zip, están los ejecutables de los programas que vamos a usar.

Basta de cháchara, empecemos.

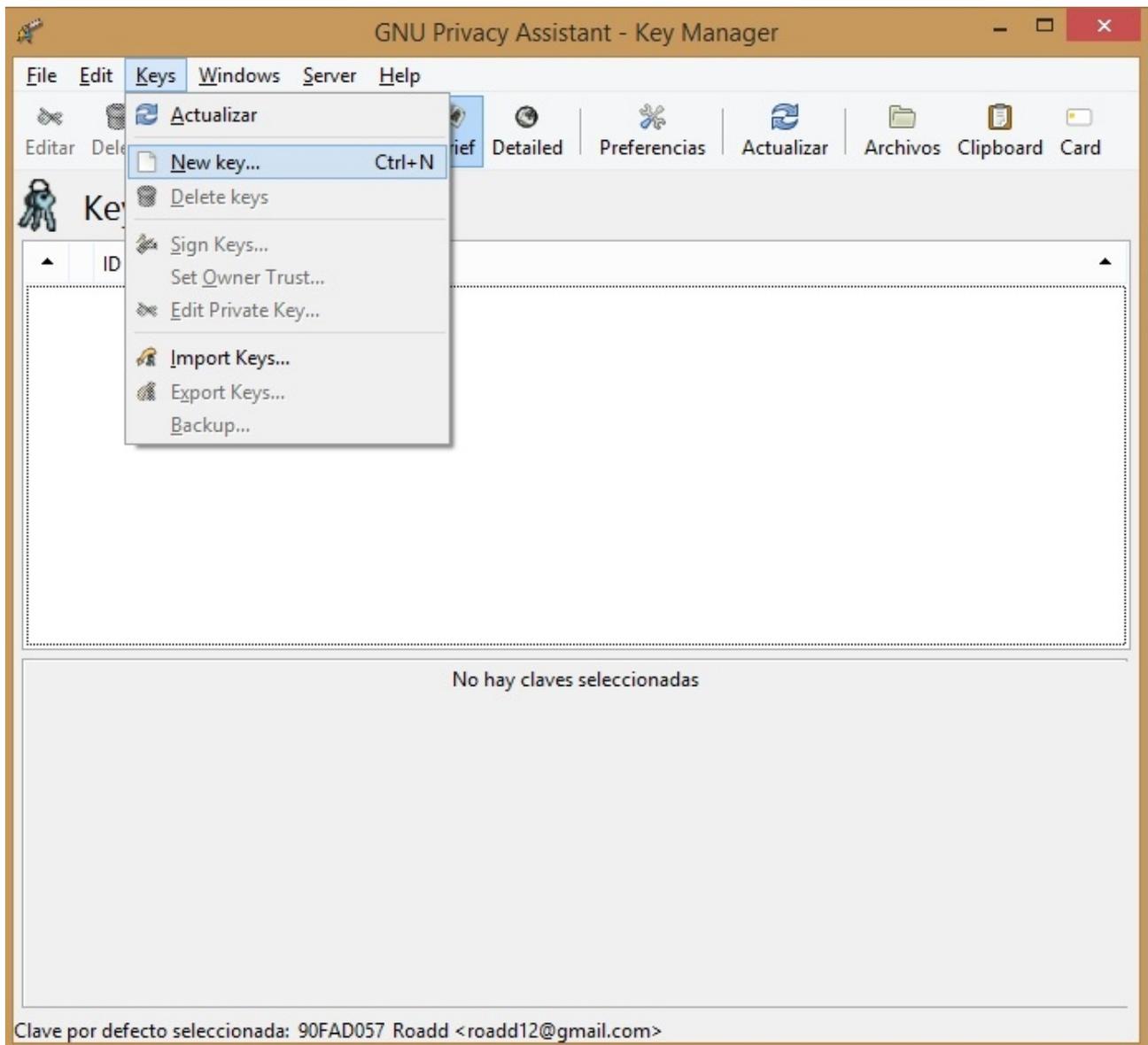
Aclaro de más, que el video contiene exactamente lo mismo que este tutorial escrito. Es sólo que por gustos, hago ambas cosas.

En este laboratorio, vamos a crear nuestras claves asimétricas, encriptar de manera simétrica, y comprobar la integridad de archivos mediante hashes.

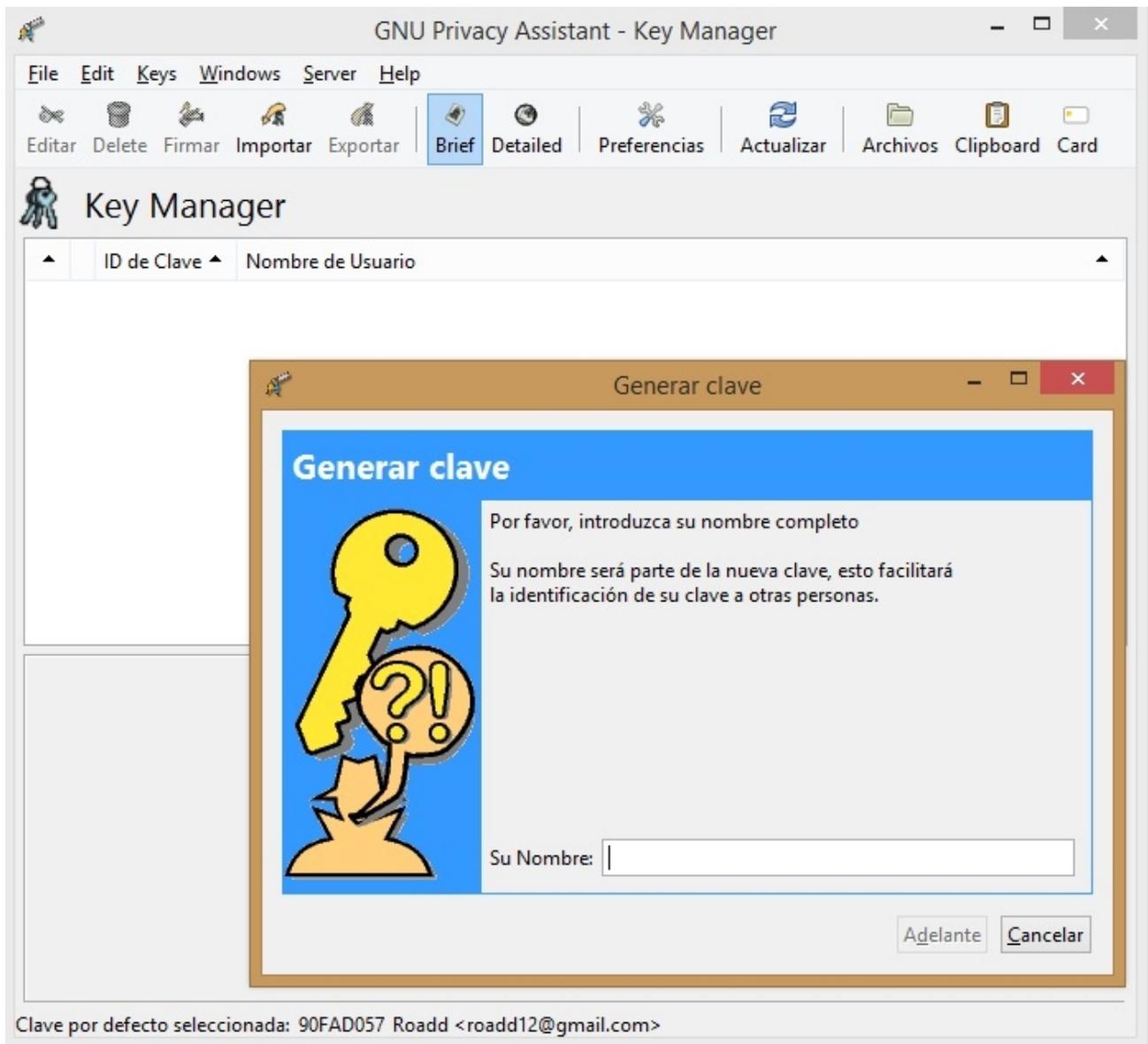
Primero instalemos y abramos el gpg4win (gpa). Fíjense, que también instala otro agente que se llama kleopatra, pero no vamos a usar ese en esta ocasión.



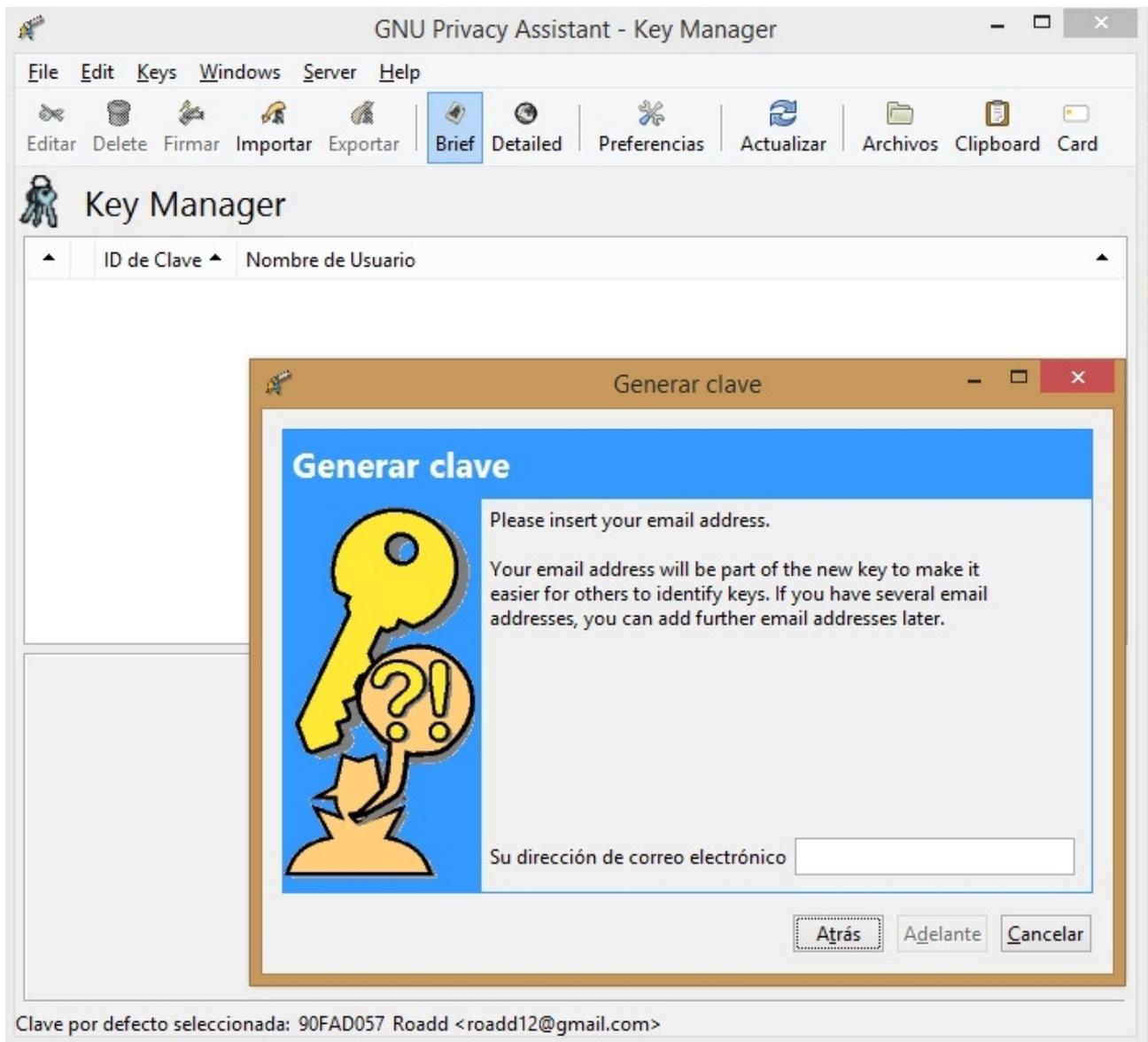
Si es nuestra primera vez que abrimos el soft y no tenemos creada ninguna llave, nos saldrá una ventana que nos dice si queremos crear. Pero vamos al caso universal. En el menú: Keys->New key



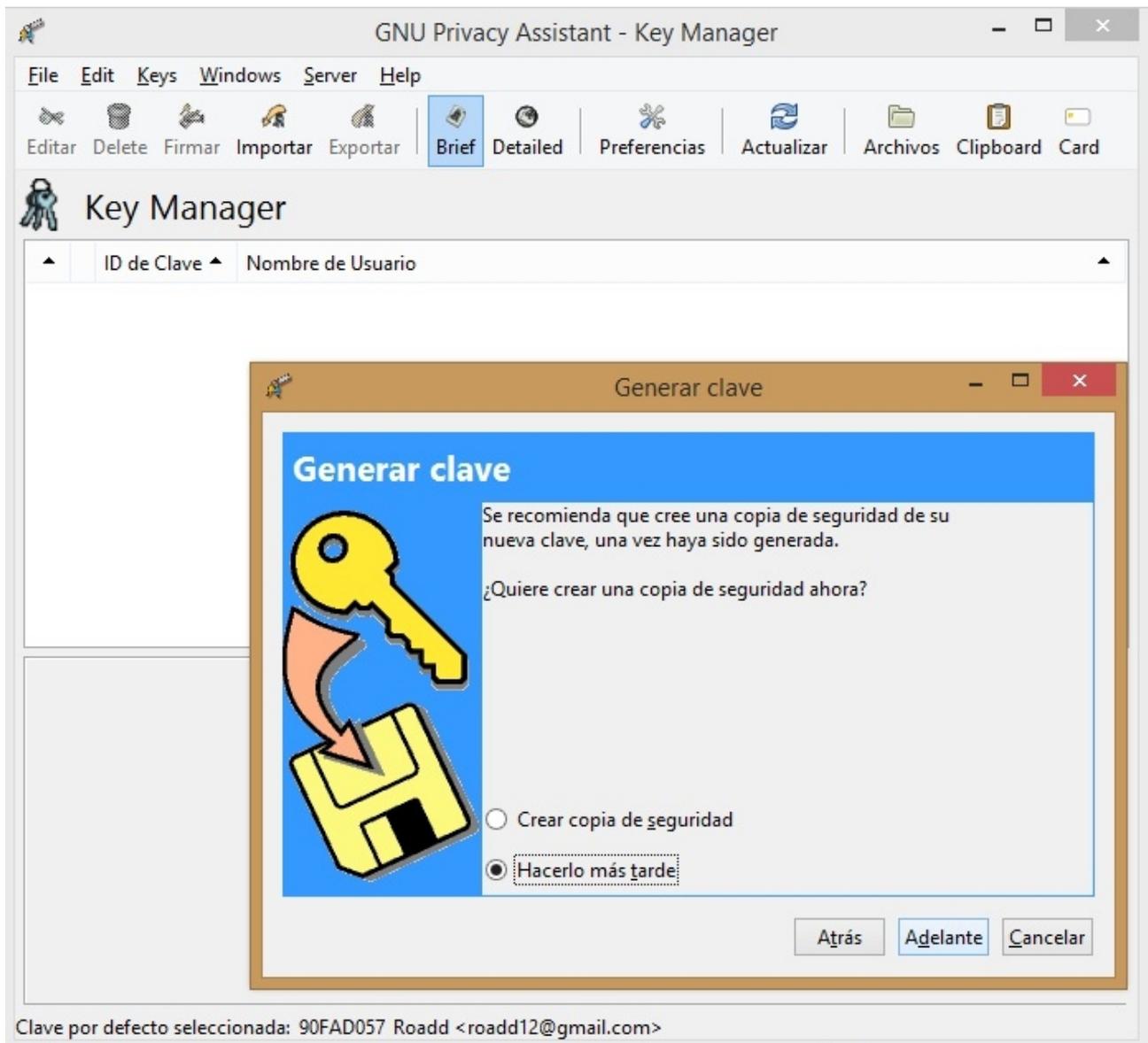
Ahora nos aparece una ventana que nos pide nuestro nombre. Pongan el que quieran.



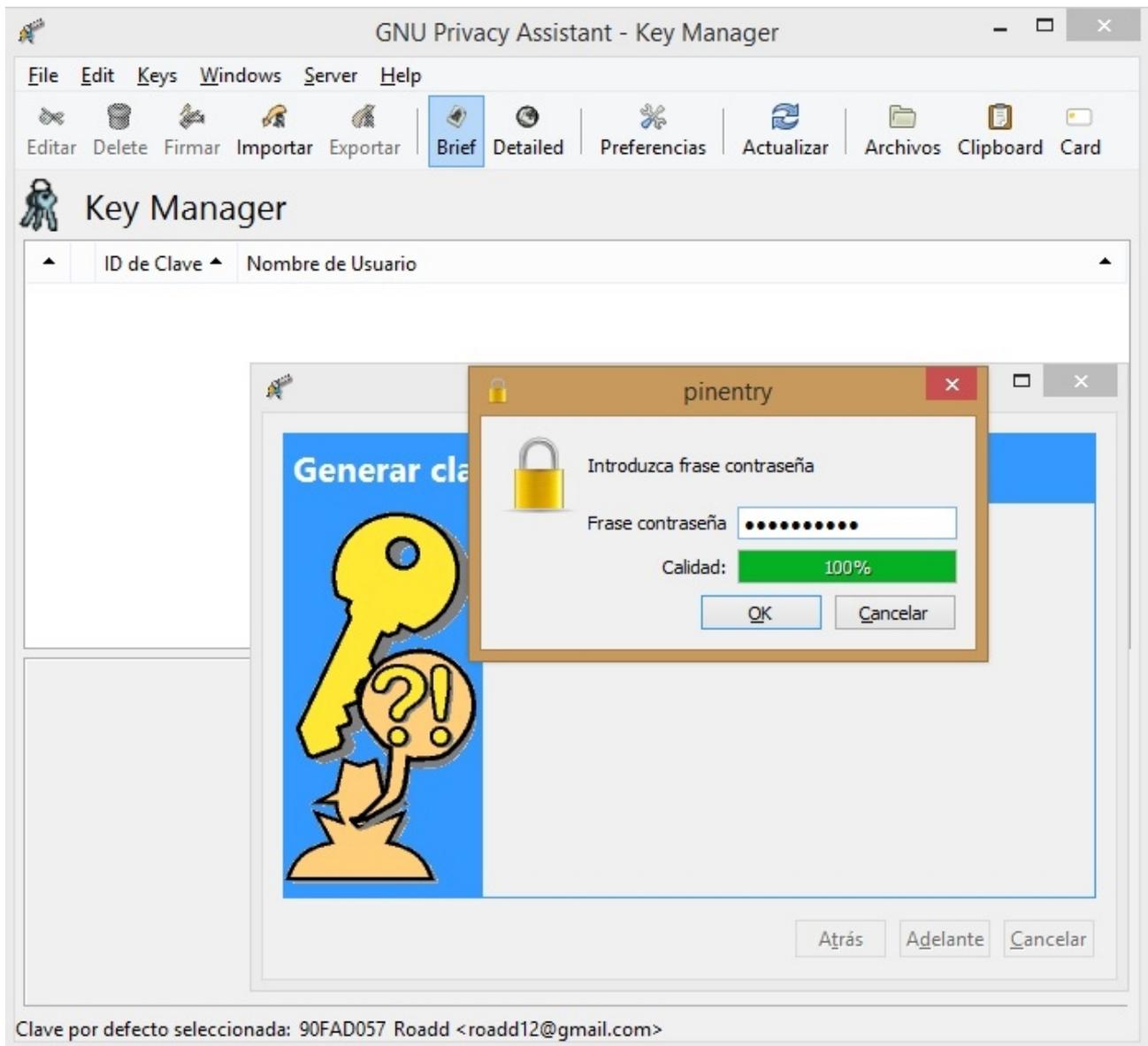
Ahora nos pide nuestro correo electrónico.



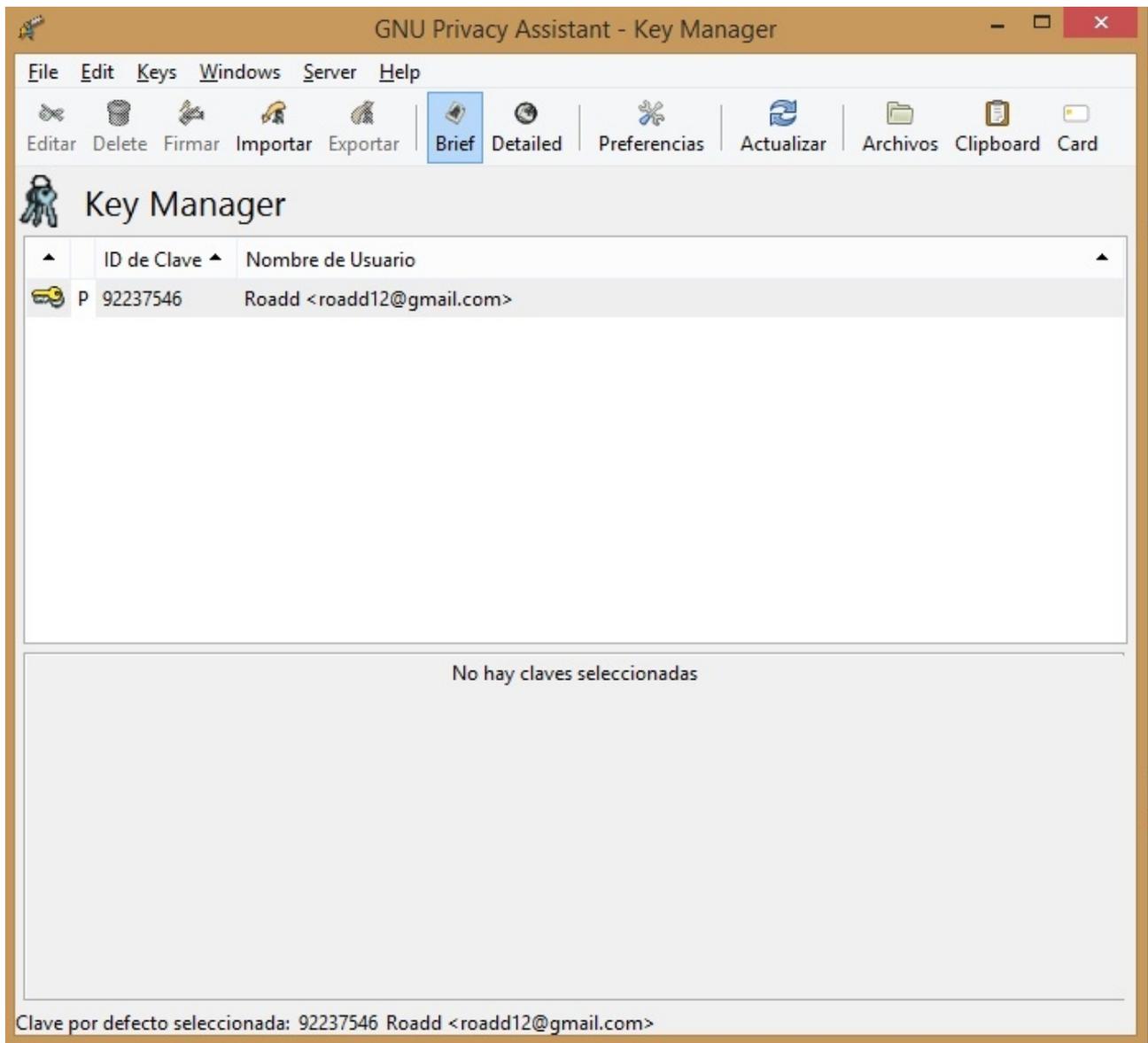
Muy bien. En esta última ventana, nos pregunta si vamos a generar una copia de seguridad a lo cual yo le contesto que no pero ustedes pueden hacerlo si quieren.



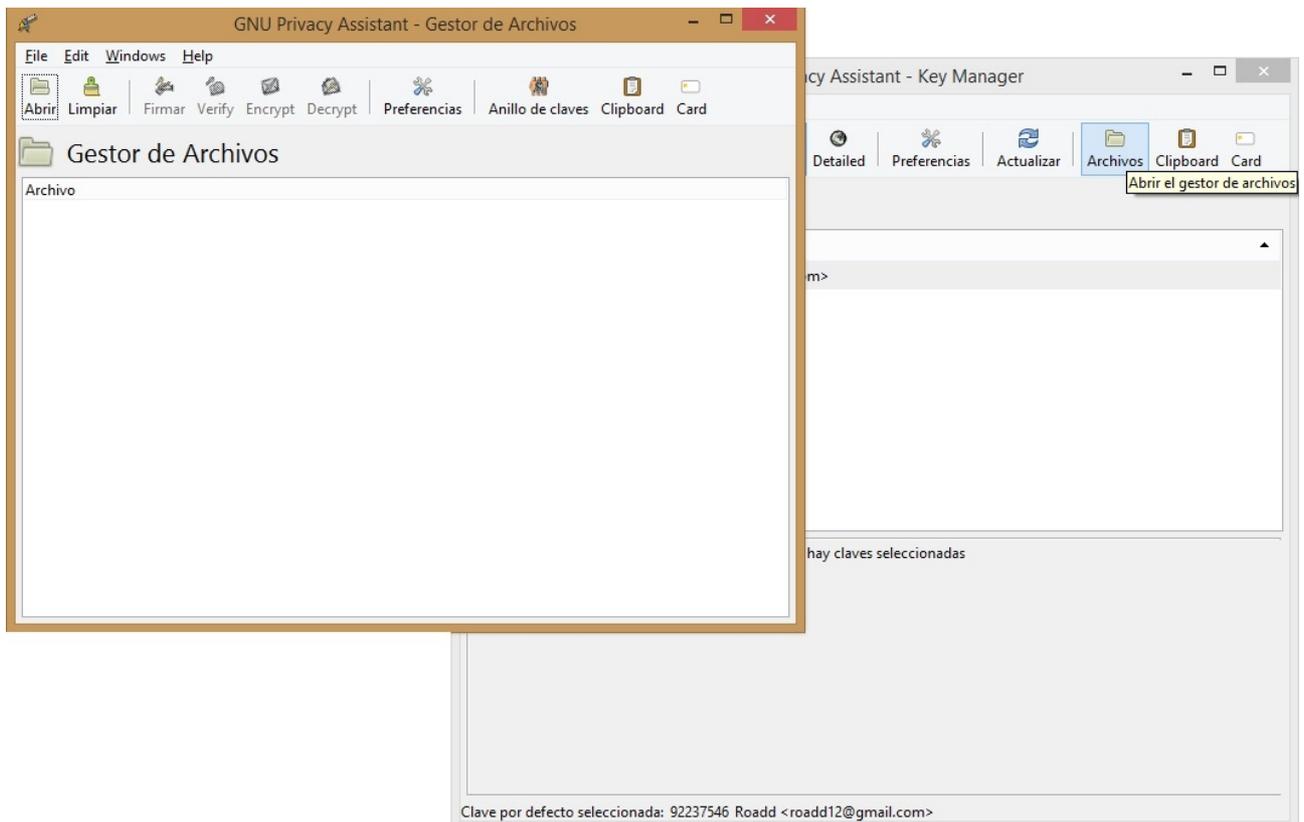
Luego nos pide una contraseña con la cual poder abrir los próximos archivos que se encriptarán con nuestra clave pública. Y también nos pedirá que la reescribamos por normas de seguridad.



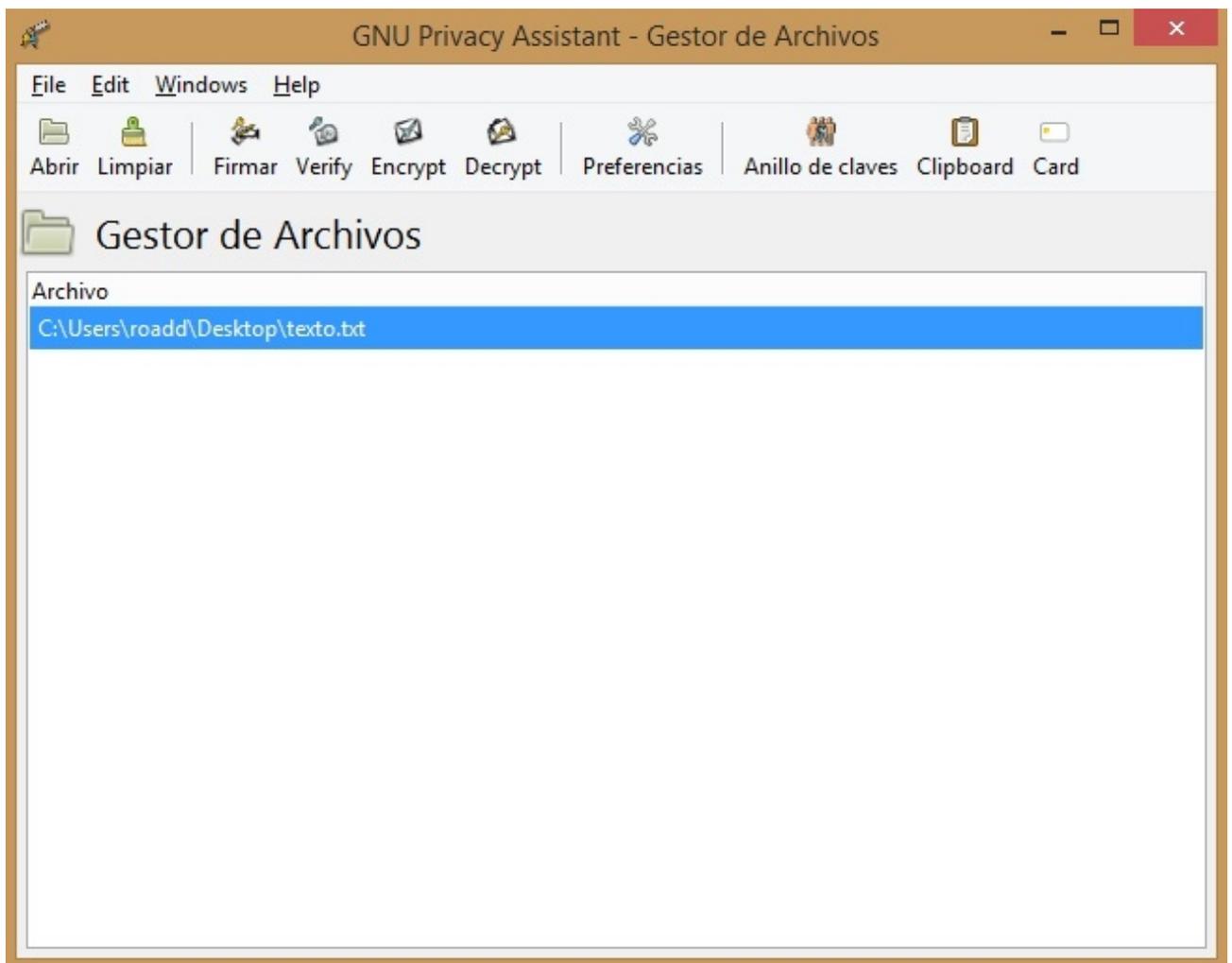
Excelente. Ya tenemos creadas nuestro par de claves.



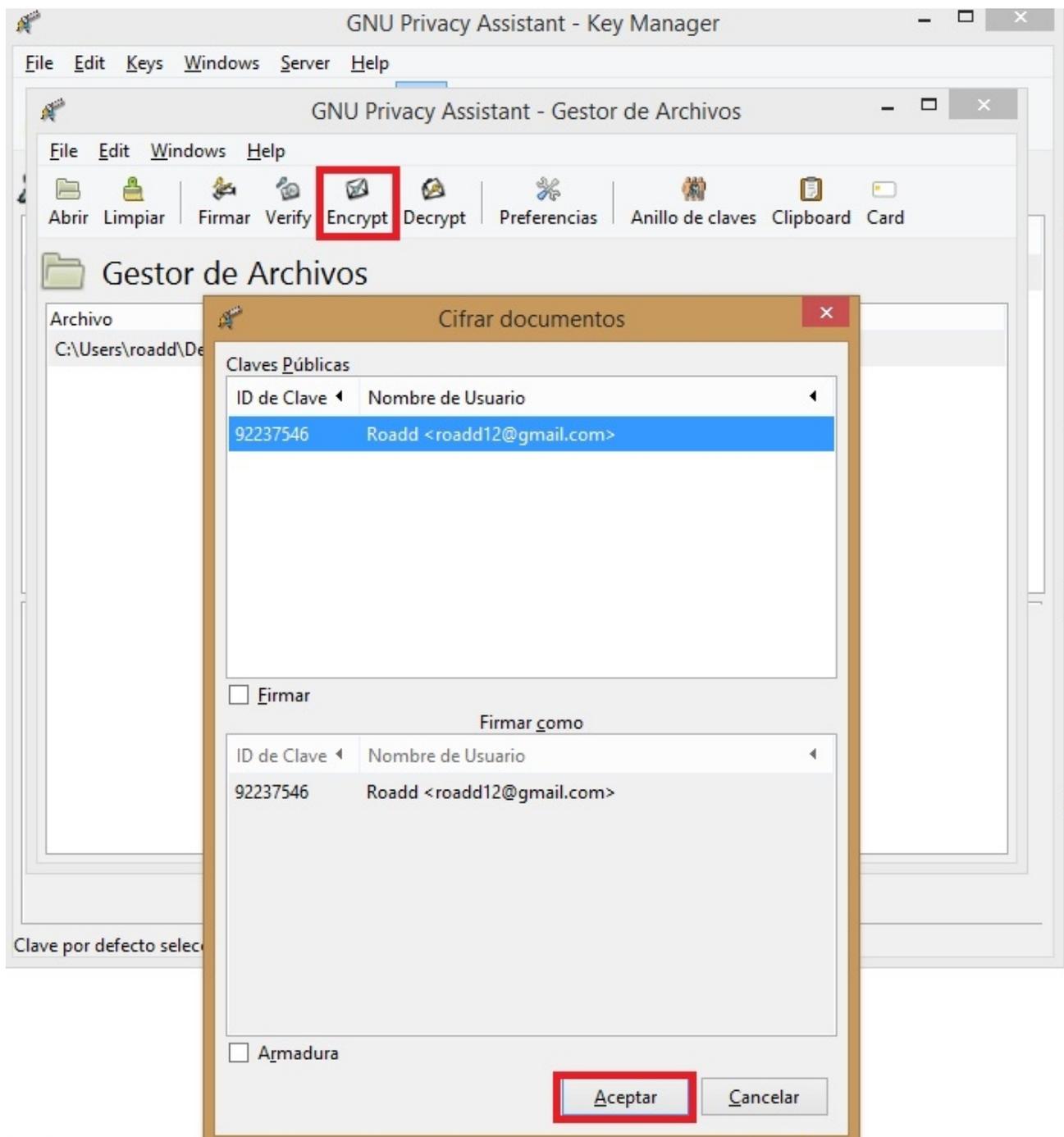
Vamos a la parte de archivo donde podemos gestar nuestros archivos para la encriptación, descryptación, firma y verificación de los mismos.



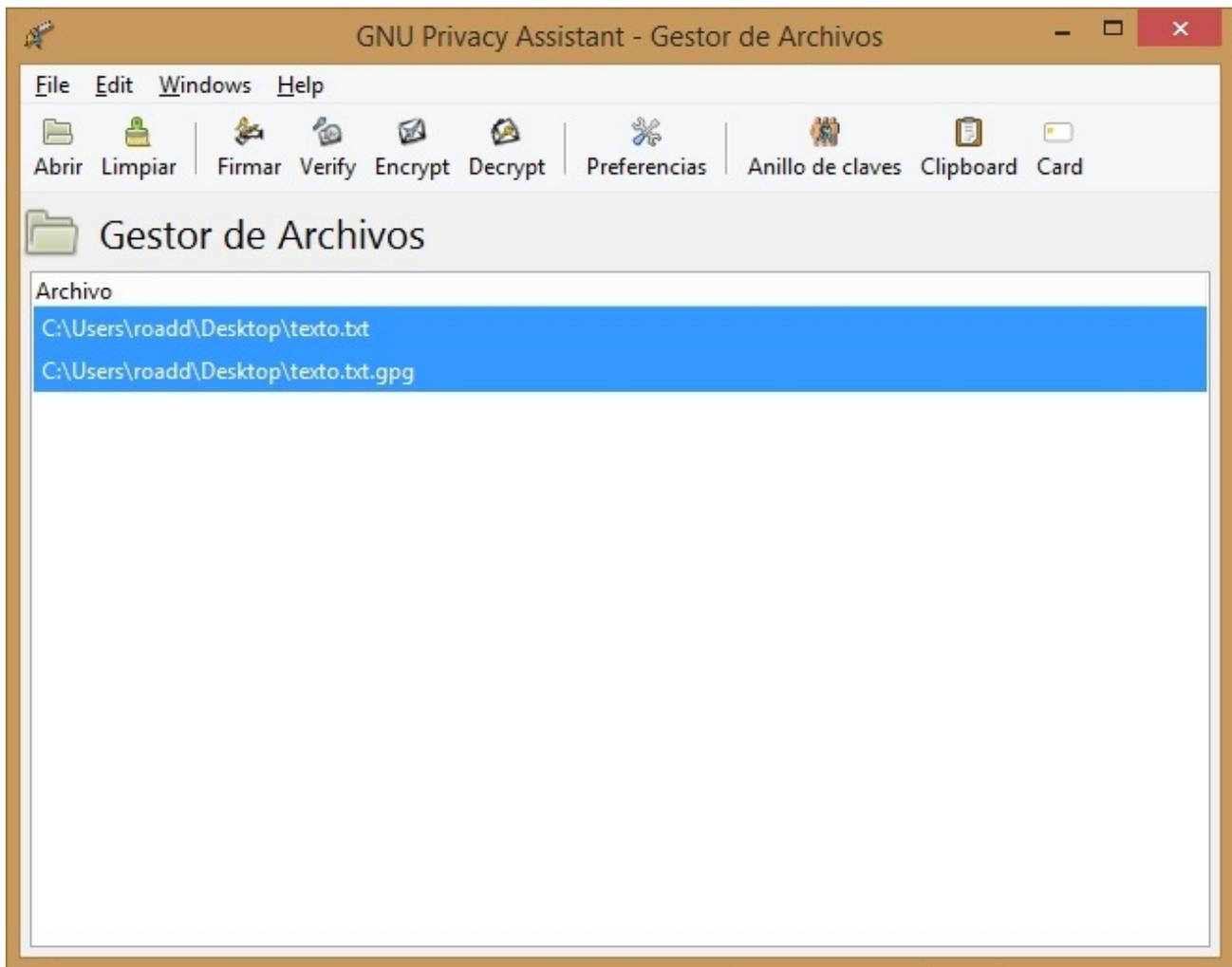
Entonces, iremos a “abrir” y seleccionamos alguno de nuestros archivos para poder encriptar. Yo seleccione un txt que tengo en el escritorio.



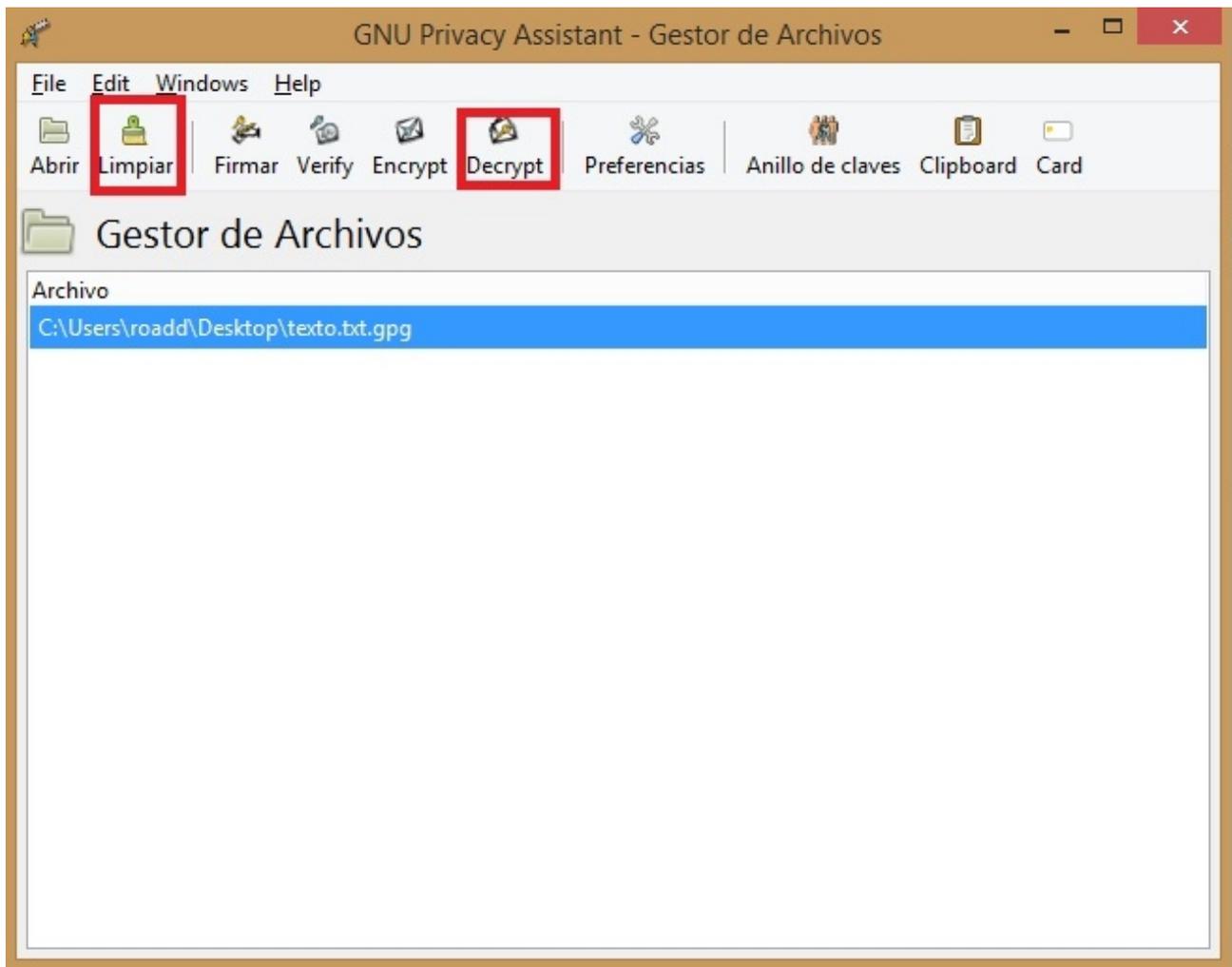
Le damos a encrypt y seleccionamos la llave pública que vamos a utilizar para encriptar el archivo. Luego le damos a aceptar.



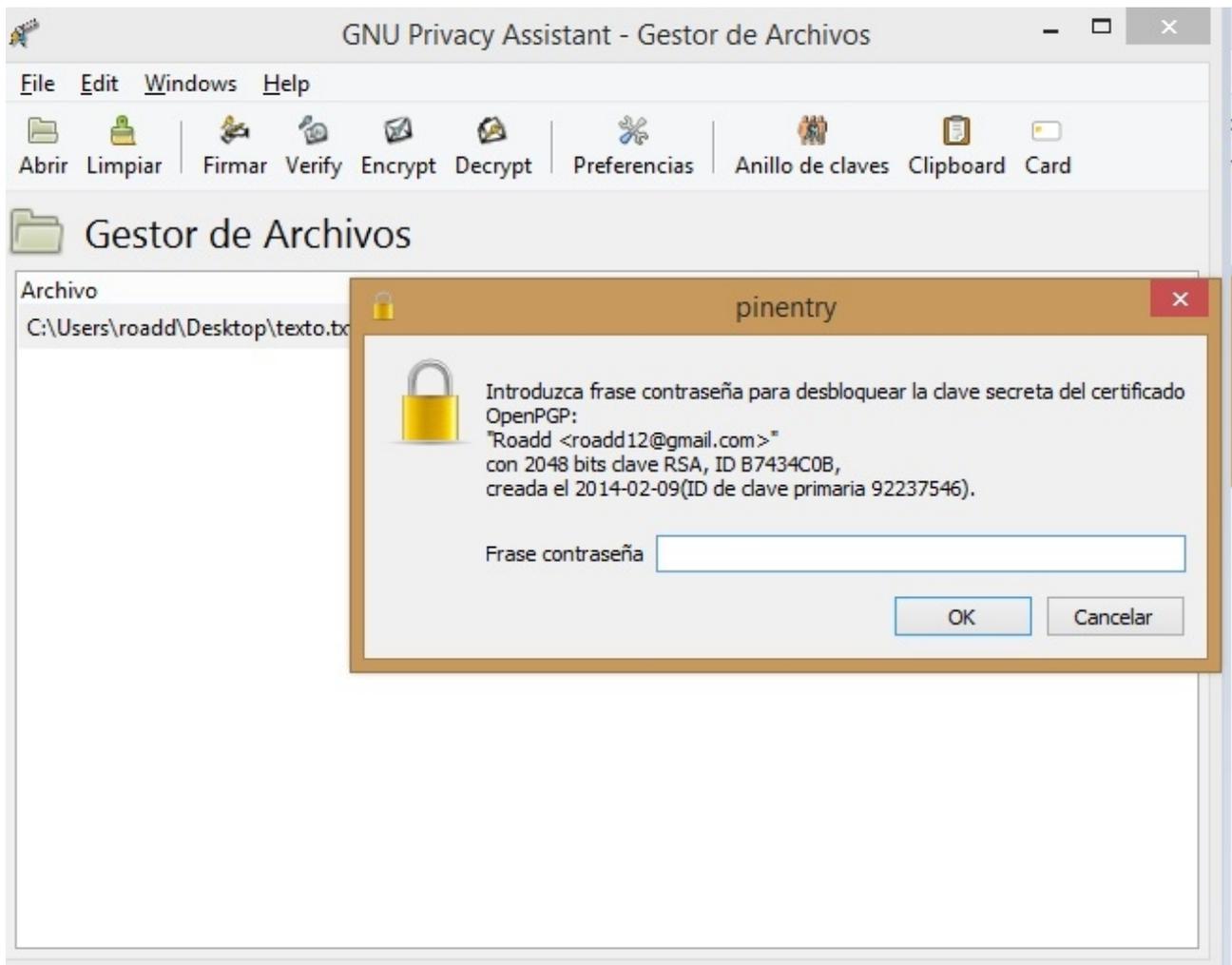
Y se generó nuestro archivo .gpg, encriptado que a menos que tengas la clave, no es posible de leer.



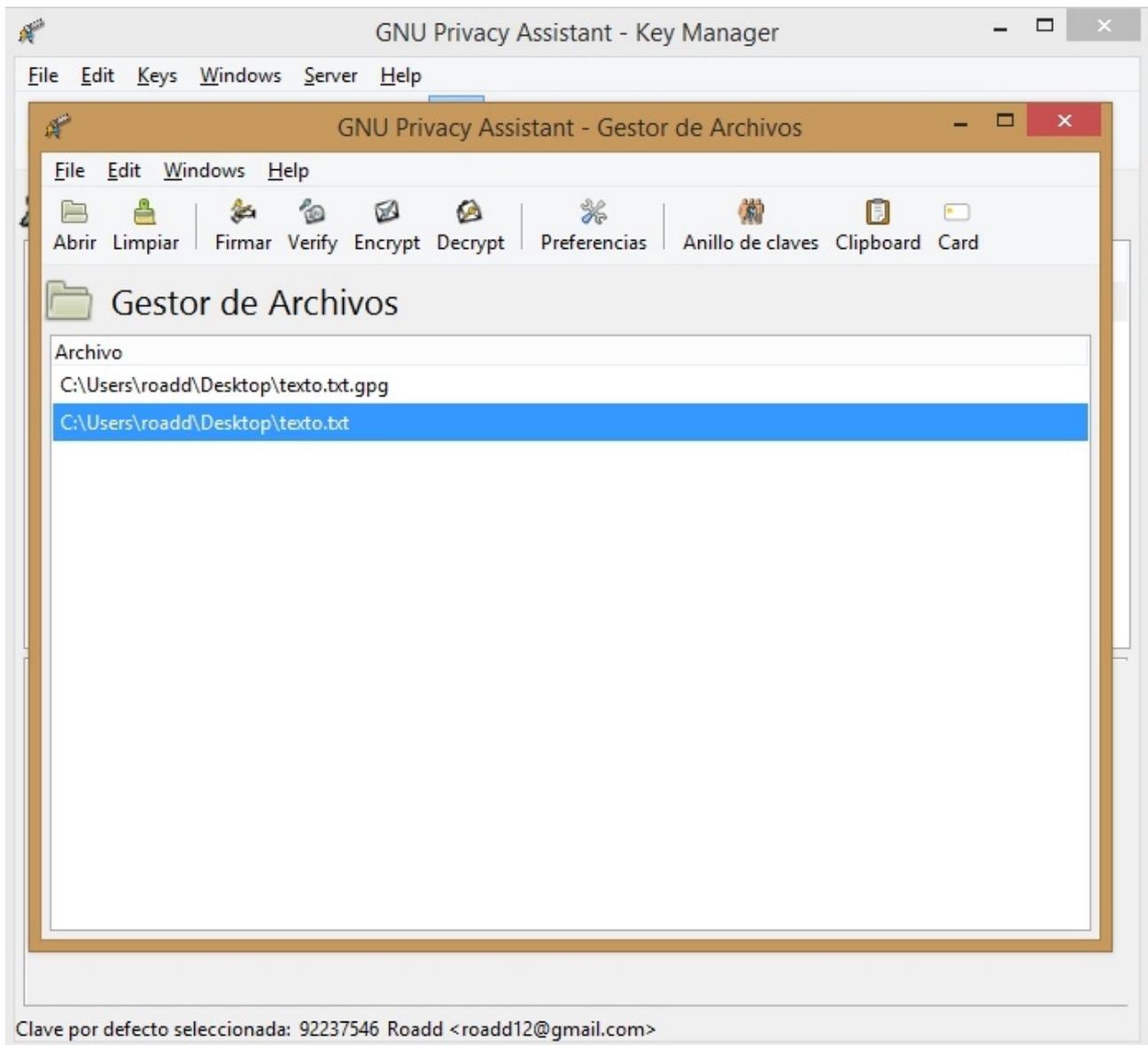
Muy bien, le damos a “limpiar” y abrimos nuestro .gpg para desencriptarlo. Luego seleccionamos la opción decrypt.



Entonces nos pide contraseña (en caso de que lo queramos descriptar en el mismo directorio en el que está el original va a pedirnos si queremos sobrescribirlo) y colocamos la que nosotros habíamos creado anteriormente.

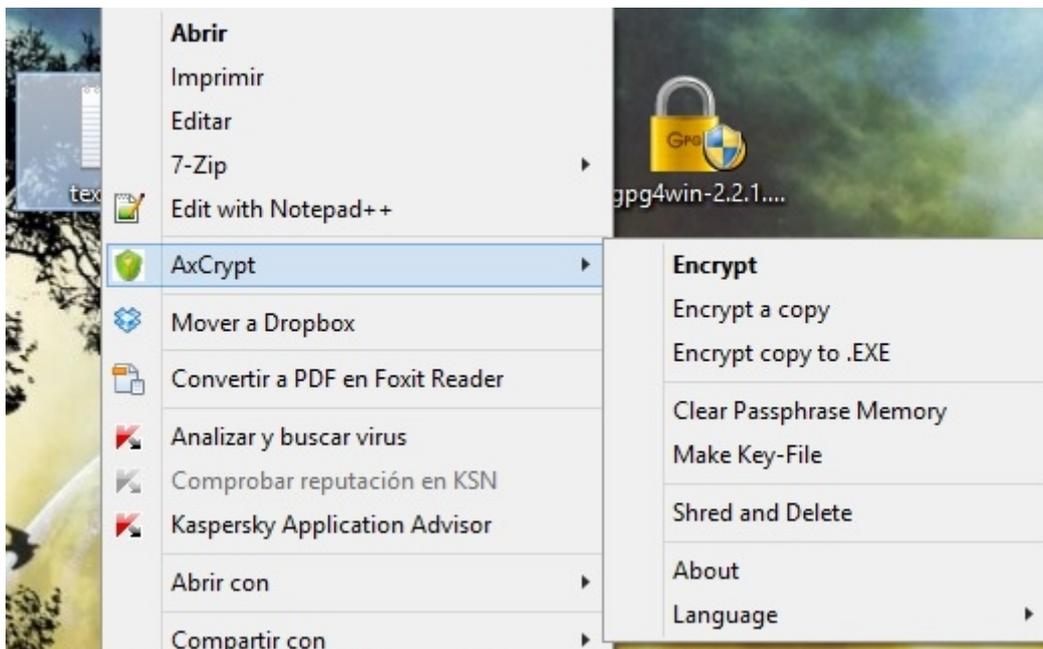


Y allí nos genera el archivo descriptado y fácil de leer :D.

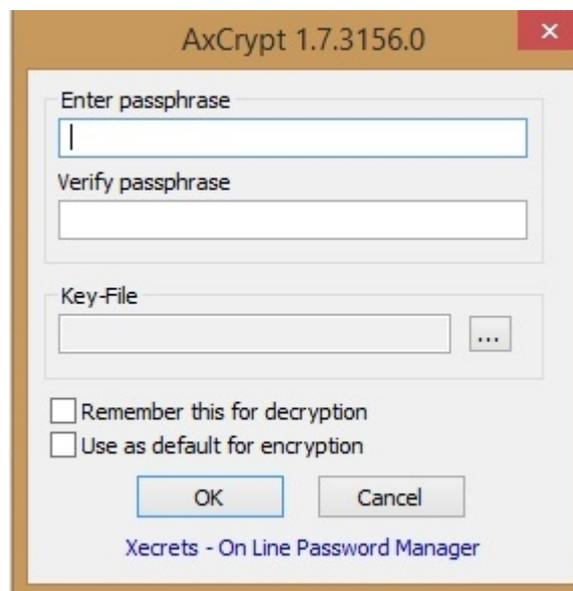


Ahora pasaremos a la encriptación simétrica.

En esta ocasión vamos a usar el AxCrypt. Instalemoslo y vemos lo fácil que es. Automáticamente, luego de la instalación, nos aparece en el menú de opciones con el click derecho, poder encriptarlo con el soft ya mencionado.



Entonces, en el menú que se despliega seleccionamos “Encrypt”, y nos aparecerá un cuadro donde debemos colocar la contraseña para poder descryptar el archivo. Además tenemos dos opciones que tildar que son: poner la contraseña como default (algo no muy apegado a la seguridad) y guardarla como clave de descryptación. Generemos la contraseña que nos plazca.

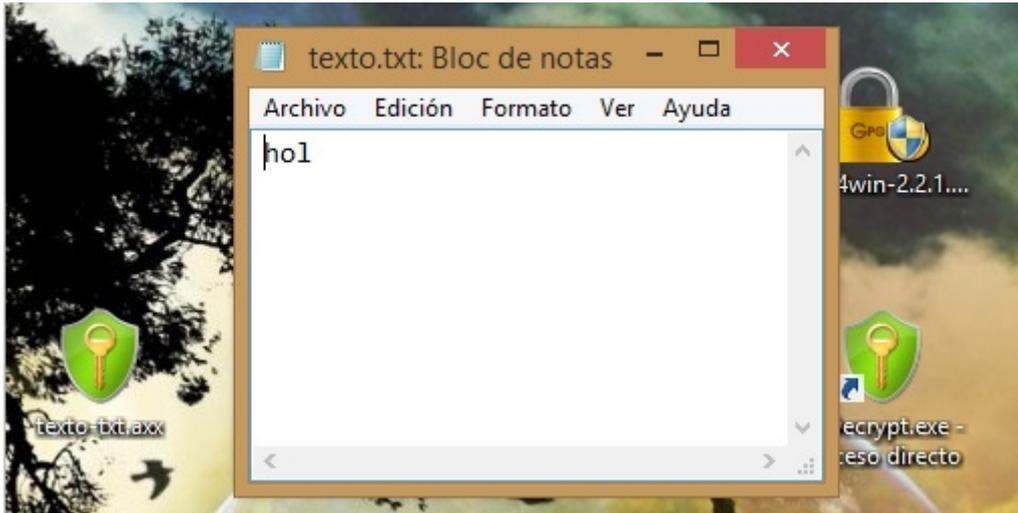


Vemos que hay un archivo nuevo que reemplazó al original. Tiene por extensión .axx. Si le damos doble click, nos aparece la ventana para colocar la clave que conocemos.



Y prestemos atención, que el archivo que descryptamos no aparece en el escritorio

desencriptado. Sólo podemos leerlo e interactuar con este, pero luego sigue encriptado.



Ahora, los hashes.

Vamos a usar la página www.onlinemd5.com, en la que tenemos 2 herramientas que quería mostrarles. Igualmente pueden usar la que quieran.

OnlineMD5

A screenshot of the 'OnlineMD5' website interface. The main heading is 'MD5 & SHA1 Hash Generator For File'. Below the heading, there is a text box that says 'Generate and verify the MD5/SHA1 checksum of a file without uploading it.' and a button labeled 'Seleccionar archivo' with the text 'Ningún archivo seleccionado' next to it. A large white box contains the instruction 'Click to select a file, or drag and drop it here(max: 4GB).'. Below this, there are several input fields: 'Filename:' with the value 'No File Selected', 'File size:' with '0 Bytes', 'Checksum type:' with radio buttons for 'MD5' (selected), 'SHA1', and 'SHA-256', 'File checksum:', 'Compare with:', and 'Process:'.

En la parte de arriba vamos a subir un archivo "pagina.txt" con el texto "hola" dentro. Y la página nos muestra el hash en md5 que genera. Guardemosló.

A screenshot of the 'OnlineMD5' website interface, showing the same tool as the previous screenshot but with a file selected. The 'Seleccionar archivo' button now shows 'pagina.txt'. The 'File checksum:' field now contains the MD5 hash '4D186321C1A7F0F354B297E8914AB240'. The 'Process:' bar at the bottom is filled with blue and shows '100.00%'.

Muy bien, ahora cambiemos el contenido del archivo. Por ejemplo, borrarle una letra. Ustedes pueden comprobarlo con cualquier cosa y todas las veces que quieran.

Para generar el hash del nuevo archivo tenemos que recargar la página.

Y allí volvemos a subir el archivo y comprobamos la coincidencia con el otro hash.

MD5 & SHA1 Hash Generator For File

Generate and verify the MD5/SHA1 checksum of a file without uploading it. pagina.txt

Click to select a file, or drag and drop it here(max: 4GB).

Filename: pagina.txt
File size: 3 Bytes
Checksum type: MD5 SHA1 SHA-256
File checksum: FEFB8EEDABD821FBEEEA6C35C38C1966
Compare with: 4D186321C1A7F0F354B297E8914AB240 ✗
Process: 100.00%

Vemos que ni cerca de ser el mismo. Pues claro, cada bit varía el resultado del hash. Pueden probar con cada hash que les guste, incluso intenten cambiando el nombre del archivo y fíjense que pasa ;).

Ahora pasemos a la parte de abajo de la web. Vemos que tenemos un cuadro de texto, y abajo nos colocará el hash del string, automáticamente. Es decir que pueden fijarse aún más como varía el hash, letra a letra.

MD5 & SHA1 Hash Generator For Text

Generate the hash of the string you input.

el perro se muer

Checksum type: MD5 SHA1 SHA-256
String hash: 38AC9149BD312AEE2068F1F09AE40DF3

Jueguen un poco, y aprendan. El laboratorio es importante para tener los conocimientos frescos:).

Espero que haya podido ser lo dinámico que quise. Nuevamente, perdón por la calidad del video.

Cualquier cosa pueden mandarme mail a: r0add@hotmail.com

Para donaciones, pueden hacerlo en bitcoin en la dirección siguiente:

1HqpPJbbWJ9H2hAZTmPXnVuoLkKp7RFSvw

Roadd.

Este tutorial puede ser copiado y/o compartido en cualquier lado siempre poniendo que es de mi autoría y de mis propios conocimientos.