Manual para crear Llaves Privadas y Públicas en Windows.

Gpg4win constituye una interesante aplicación de software libre con la que puedes cifrar archivos y correos electrónicos mediante el empleo de un sistema de llaves públicas y privadas.

El algoritmo de cifrado que emplea este programa también es libre y se denomina 'GNU Privacy Guard', la alternativa de código abierto a los sistemas de codificación patentados.

Gpg4win creará ambas llaves en función de los parámetros que especifiques. Para poder trabajar con el programa es necesario conocer la llave pública del destinatario.

El funcionamiento es el siguiente: la información se cifra con la llave pública del receptor y cuando éste recibe el documento lo descifra empleando su llave privada.

El programa instala un plugins para el cliente de correo 'MS Outlook' con la que es posible cifrar los mensajes desde la interfaz de esta aplicación.

Requisitos para instalar Gpg4win

- Sistema operativo Windows 2000, XP, Vista y 7. Funciona en sistemas de 32 y 64 bits.

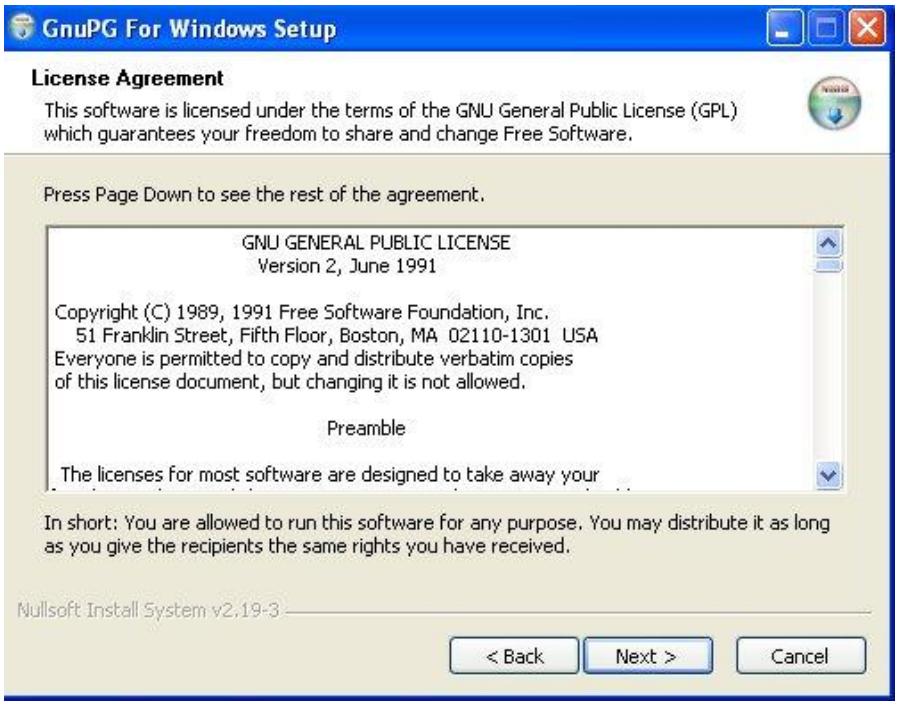
- El plugins para Outlook GpgOL con compatible con Microsoft Outlook 2003 y 2007, no así con la versión 2010.

- En la actualidad, el plugins para Explorer GpgEX sólo funciona con la versión de 32 bits.

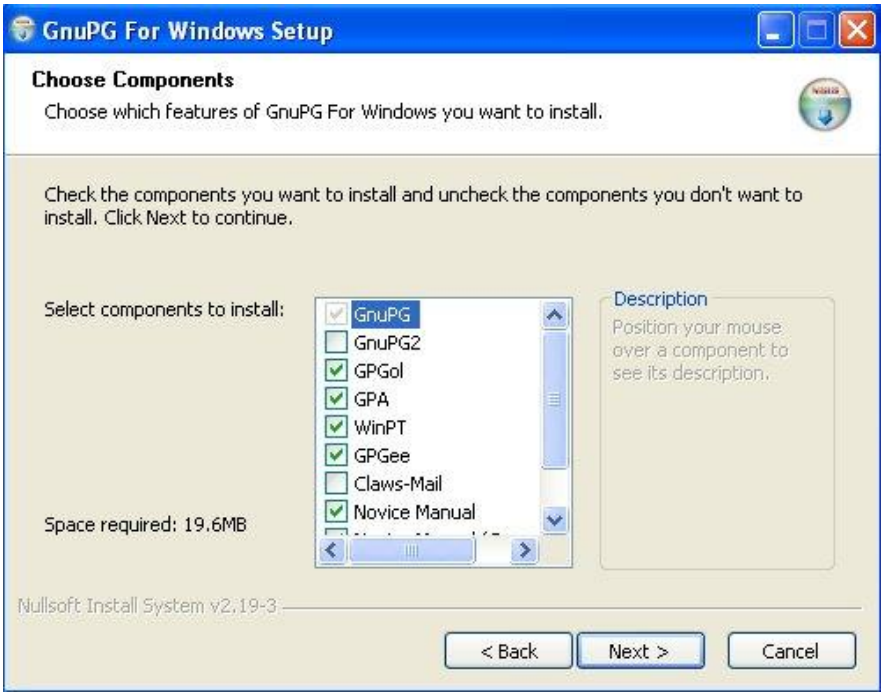
Instalación de la aplicación Gpg4win

Empezaremos descargando el software desde la siguiente URL: http://www.gpg4win.org/ (esto puede tardar unos minutos), una vez descargado, lo ejecutamos y saldrá algo como esto:

Esta imagen nos muestra las características del software, damos clic en siguiente.

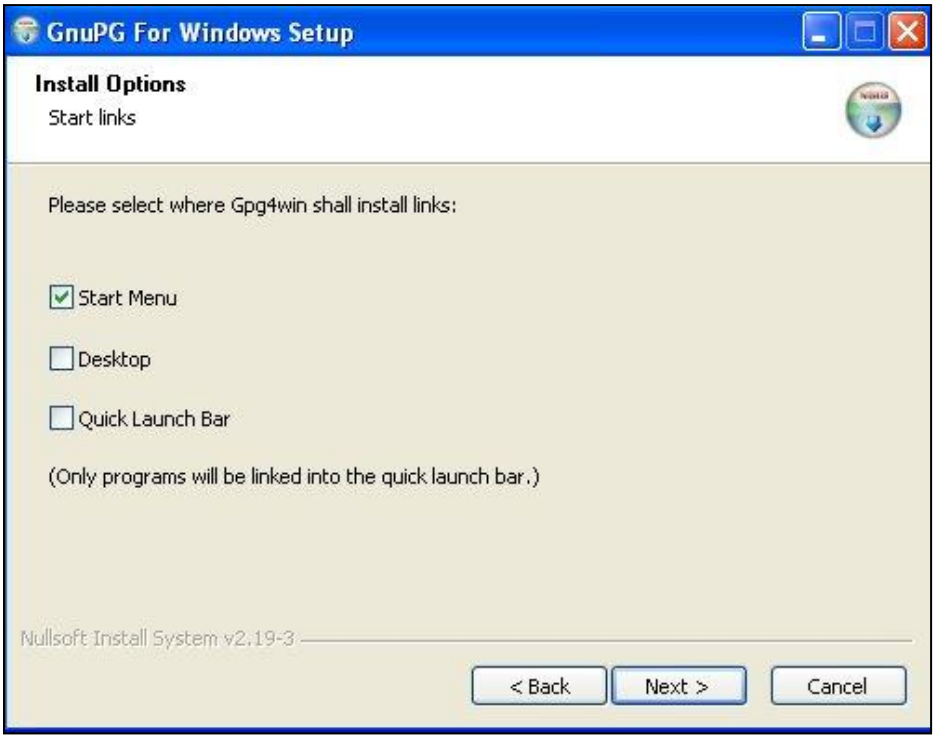


Le damos siguiente si aceptamos la licencia del producto



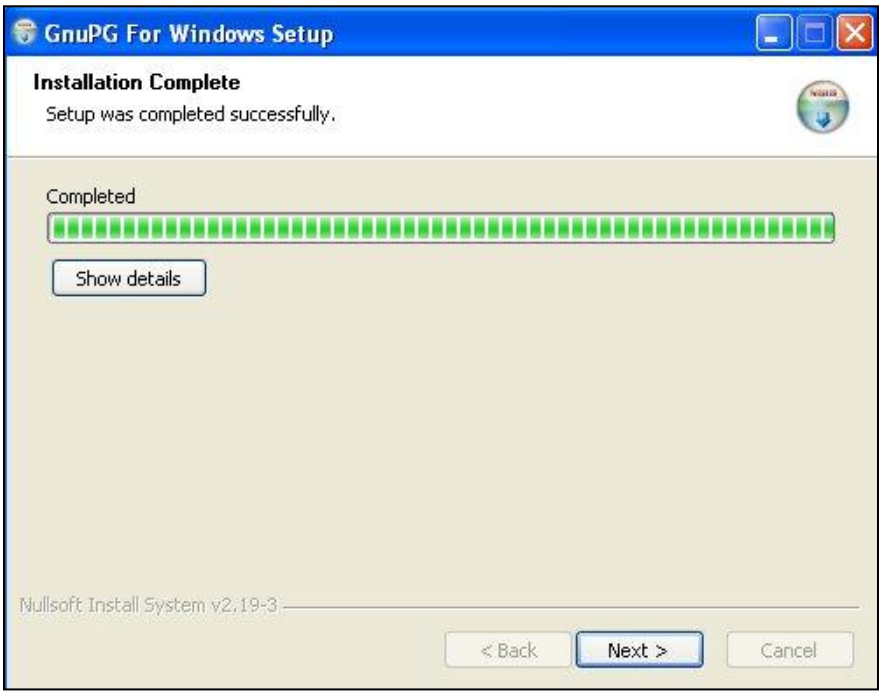
Si queremos, dejamos los complementos por defecto a instalar, si no lo podemos modificar según sus necesidades. Clic en siguiente.

Seleccionamos la ruta en la cual quedaran los archivos del software, en este caso, se dejo la ruta por defecto.



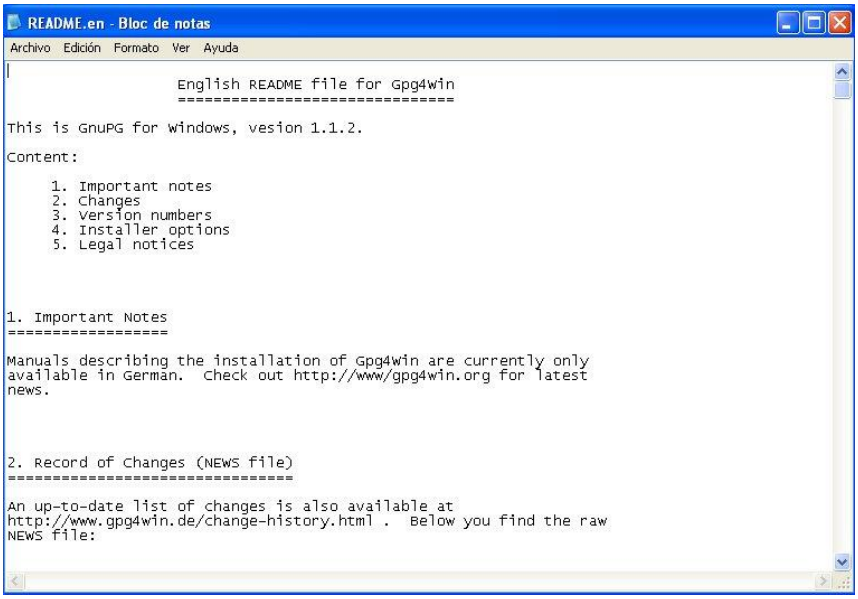
Este paso es para especificar donde quedaran los accesos directos al programa, en este caso en la opción de menú o inicio. Pulsamos siguiente.

Acá, podemos cambiar el nombre de cómo aparecerá el software en el menú de inicio de nuestra PC. Clic en Instalar.



(En algunos casos hay que mover el mouse en la barra para que cargue la instalación). Terminada la instalación damos clic en siguiente.

Es exitosa la instalación, le damos finalizar.



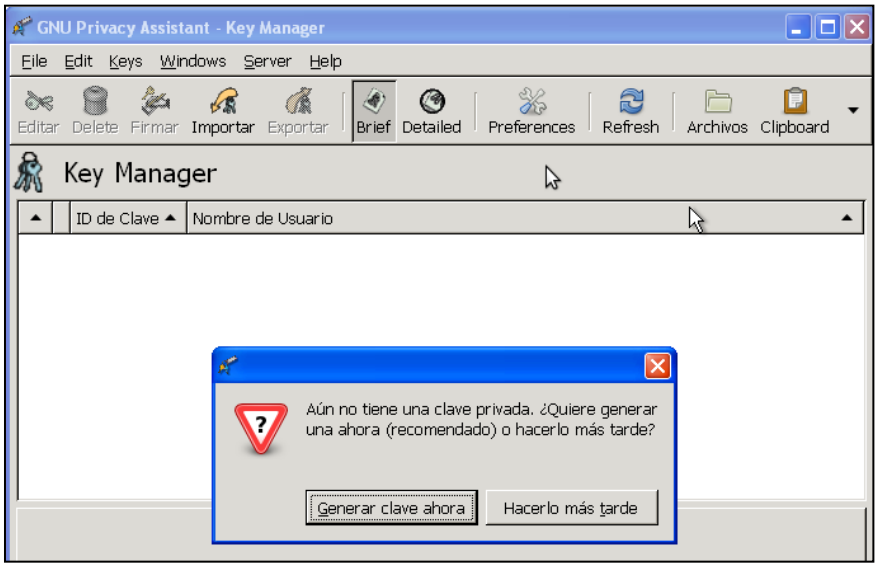
Cuando le damos clic en finalizar, nos muestra el archivo README, el cual nos ofrece información, acerca del software acabado de instalar en nuestro equipo.

¡Tenemos gpg4win listo para usar!

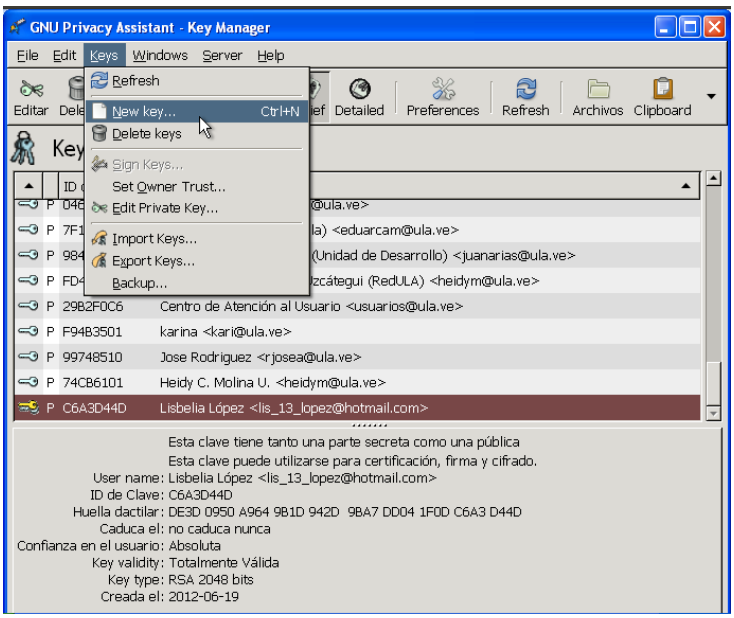
Pasos para la creación de un par de llaves Públicas y Privadas en Windows

1) Abrimos el siguiente icono.

2) Si es primera vez que se utiliza el programa, en el momento del inicio se le preguntara si desea generar una clave privada.



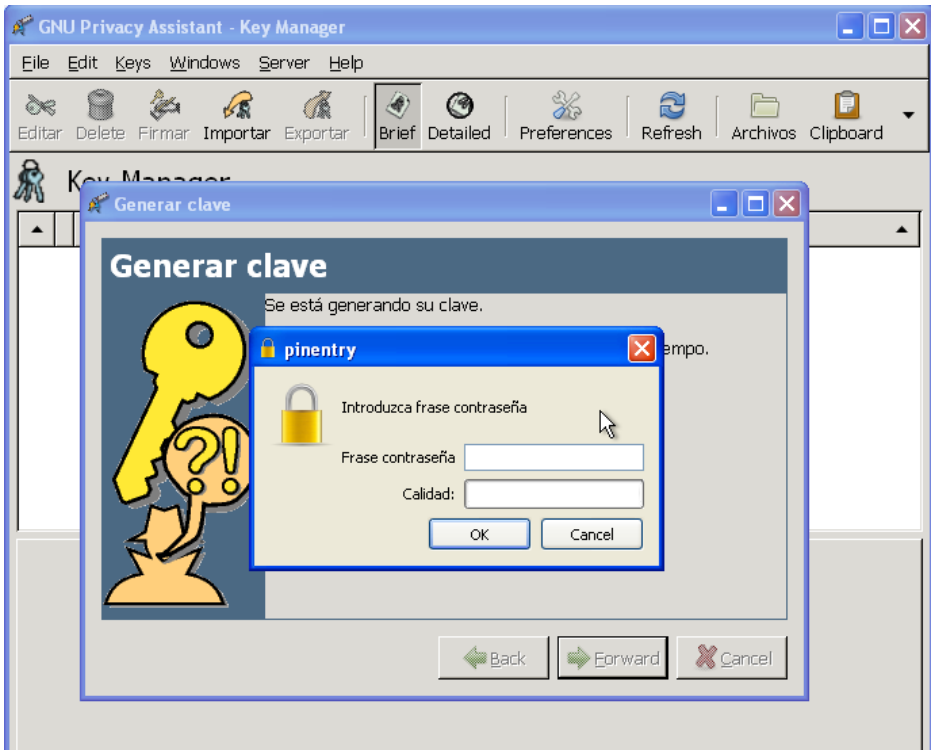
De no aparecer esta ventana, se debe hacer clic en la opción “Keys” y luego en el menú desplegable seleccionamos “New key...” También se puede pulsar las teclas Ctrl + N, para ingresar al gestor de generación de claves.



3) Para crear una nueva clave, se nos piden datos como:

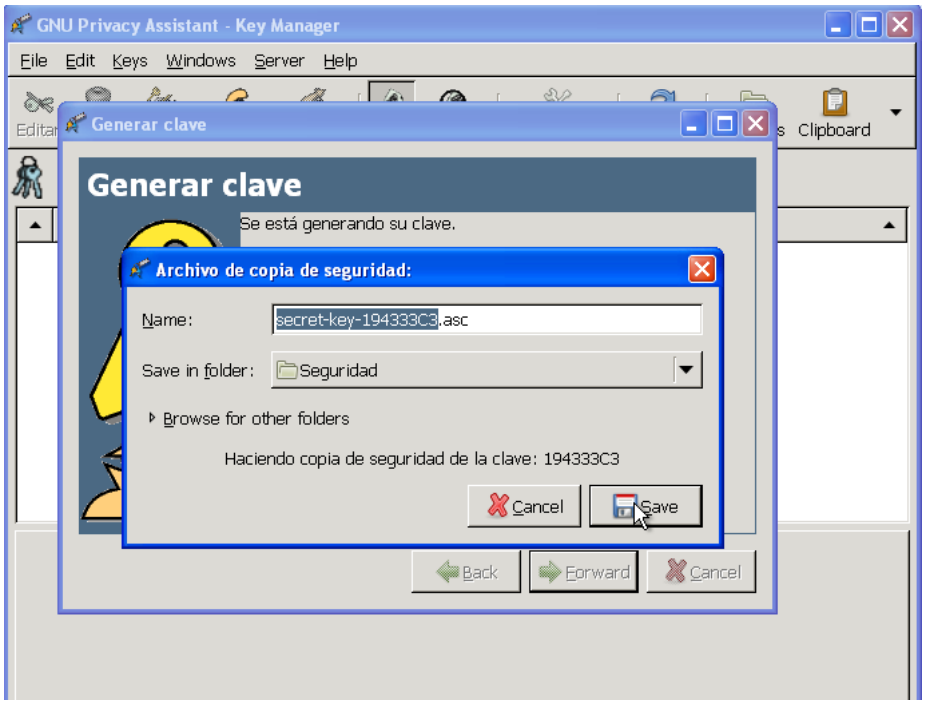
4) Ahora, nos pregunta si queremos crear una copia de seguridad, la cual podemos crear en el momento.

5) Luego se debe introducir la frase contraseña para nuestra llave privada, Desde un punto de vista de seguridad, la contraseña que desbloquea la llave privada es uno de los puntos más débiles en GnuPG (y en otros sistemas de cifrado de llave pública), ya que es la única protección que tiene el usuario si alguien se apoderara de su llave privada. Para una contraseña lo ideal es que no se usen palabras de un diccionario, y que se mezclen mayúsculas y minúsculas, dígitos, y otros caracteres.

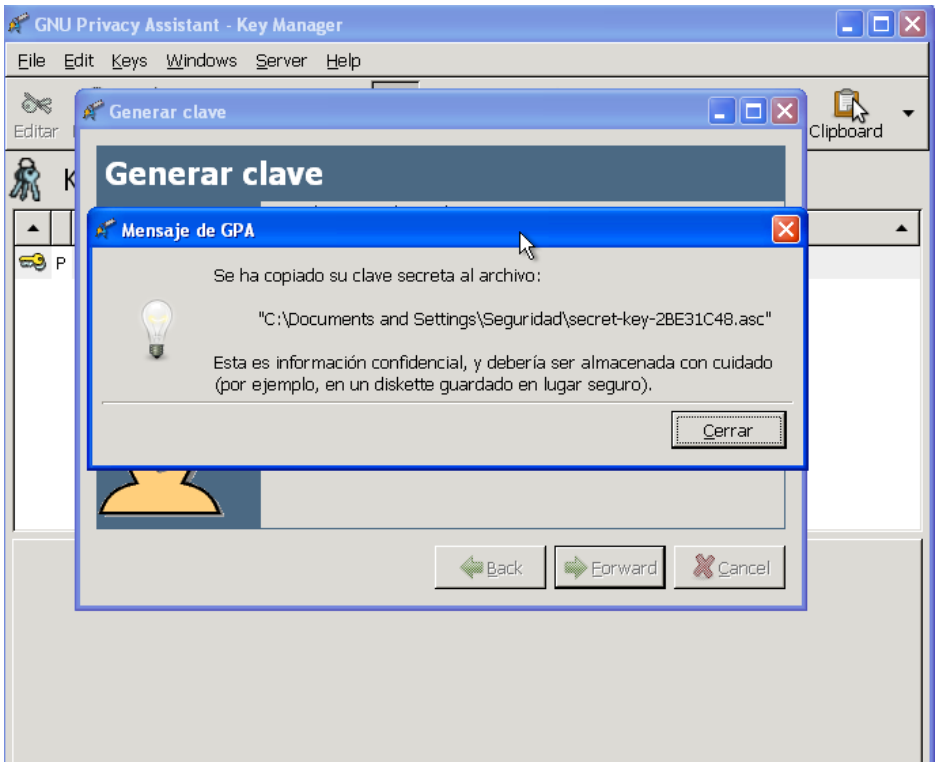


Luego, pedirá ingresarla de nuevo.

6) Si le hemos dado “crear copia de seguridad” anteriormente, creara la copia después de este paso (después de introducir la frase contraseña).

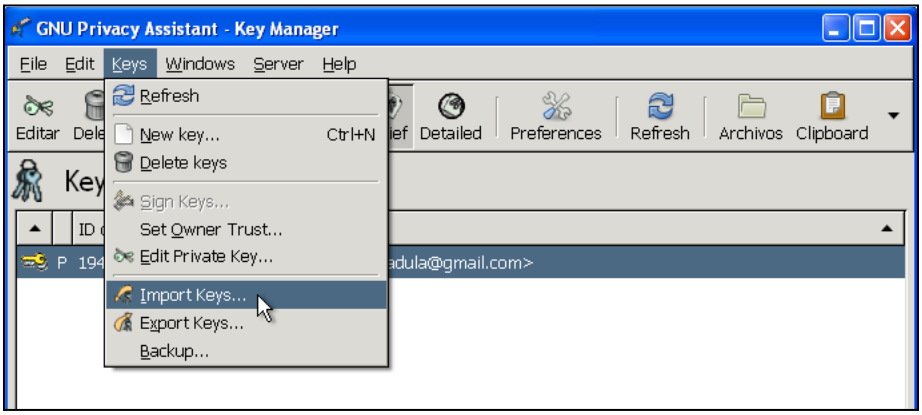


Y el aviso que confirma que verdaderamente se ha creado.

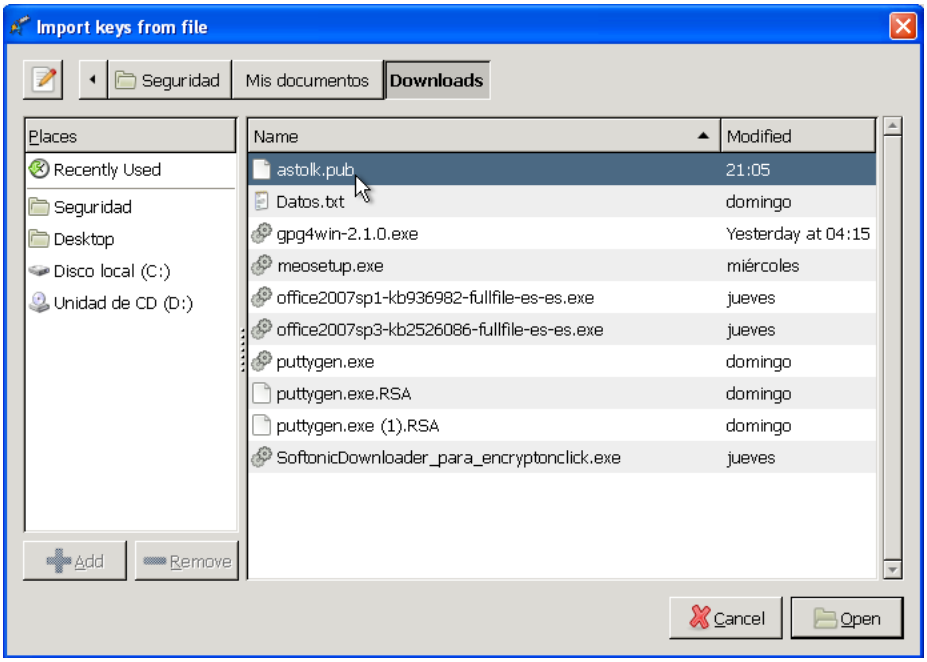


7) Importar llaves

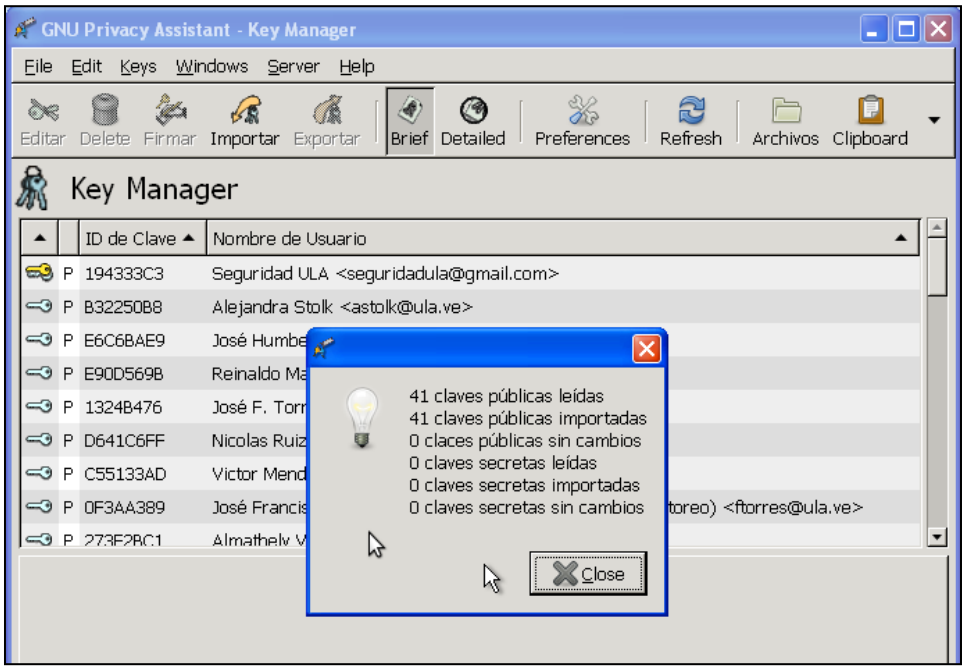
Si deseamos importar la llave de un amigo, buscamos la opción de importar.



Seleccionamos la llave pública que deseamos importar y damos clic en abrir.

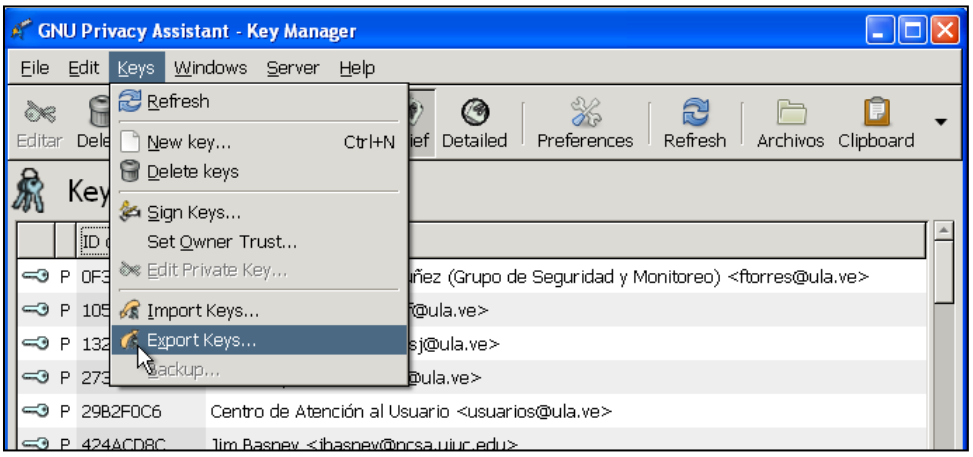


Es aquí cuando culmina el proceso de importación.

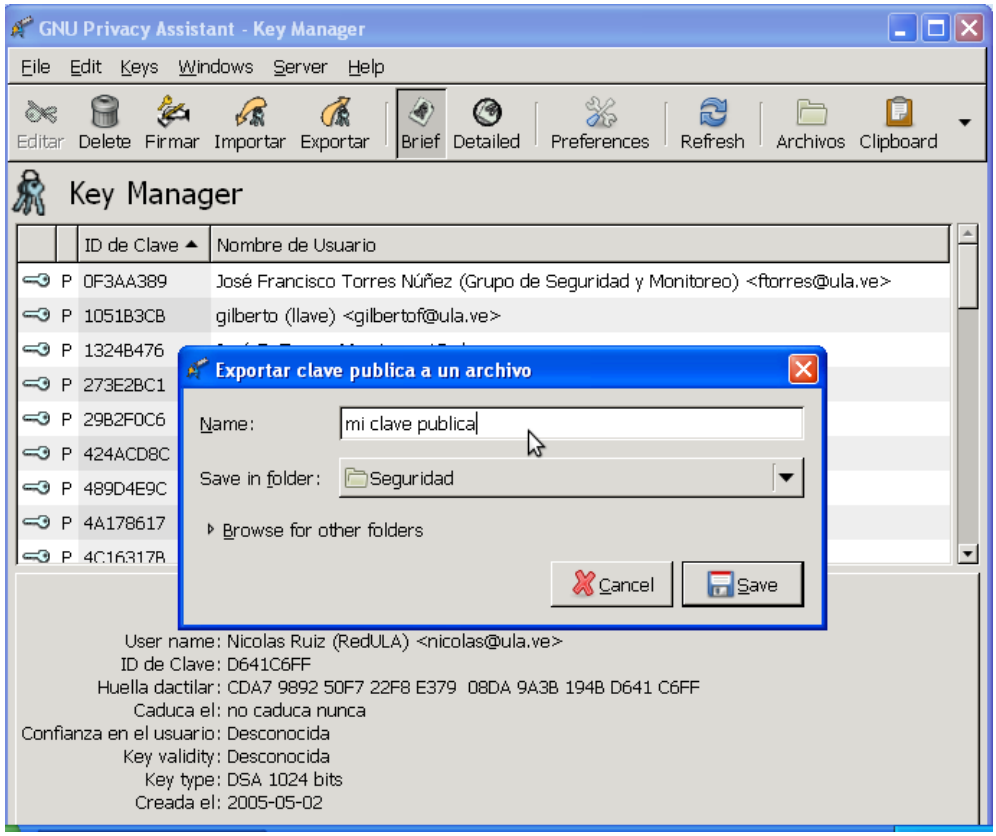


8) Exportar llaves

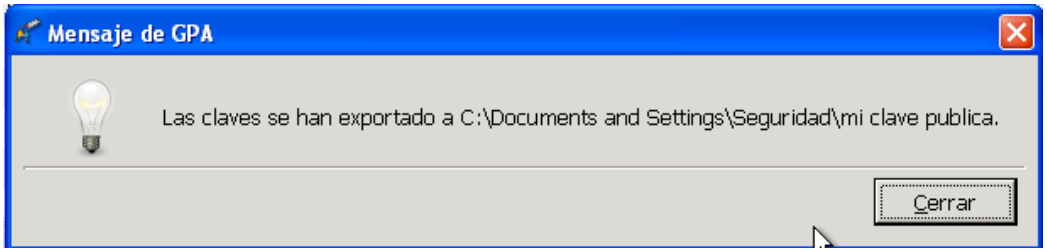
En la pestaña “Keys” seleccionamos las opciones de exportar.



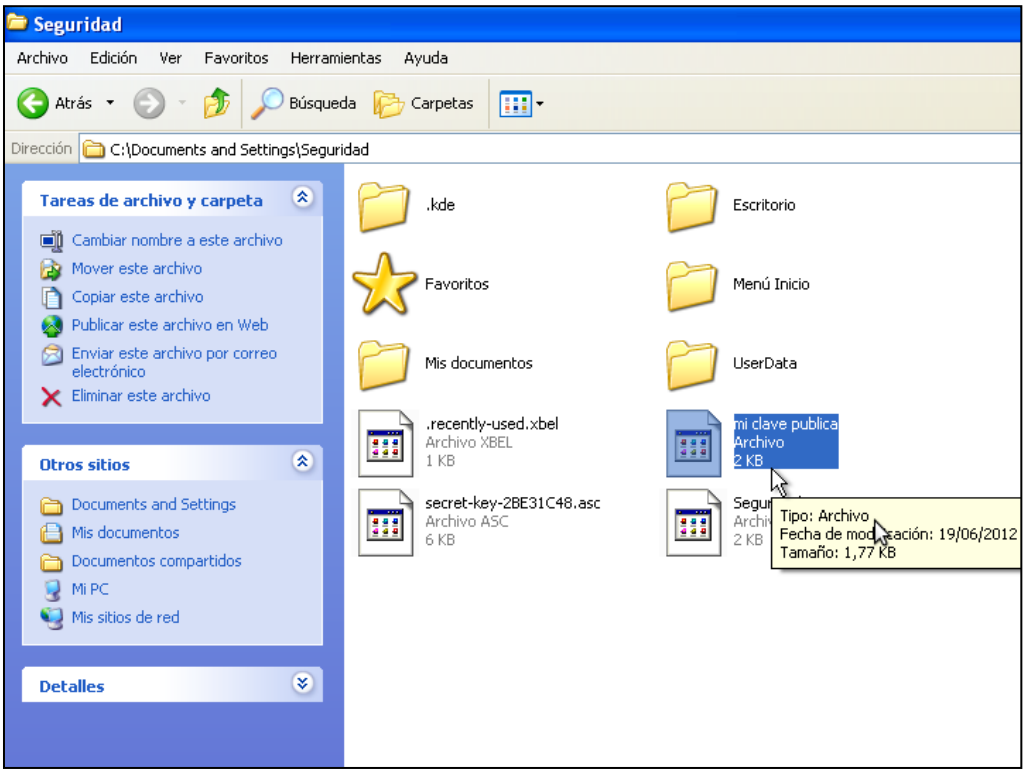
Las llaves se pueden exportar a archivos para que las podamos distribuir entre la gente que queremos que nos cifre o firme cosas o bien porque vamos a formatear el equipo y necesitamos salvarlas.



Colocamos el nombre del documento con nuestra llave pública y seleccionamos la carpeta donde se desea almacenar.

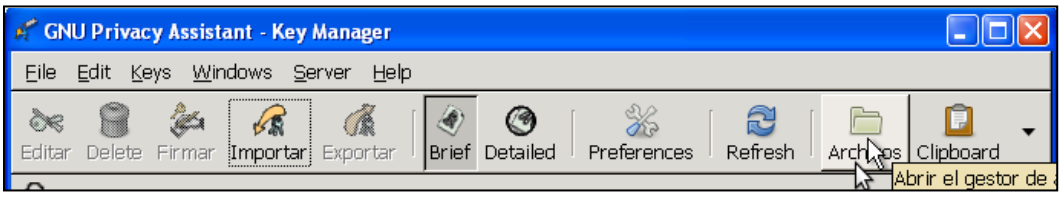


Podemos verificar si la clave se ha exportado correctamente:

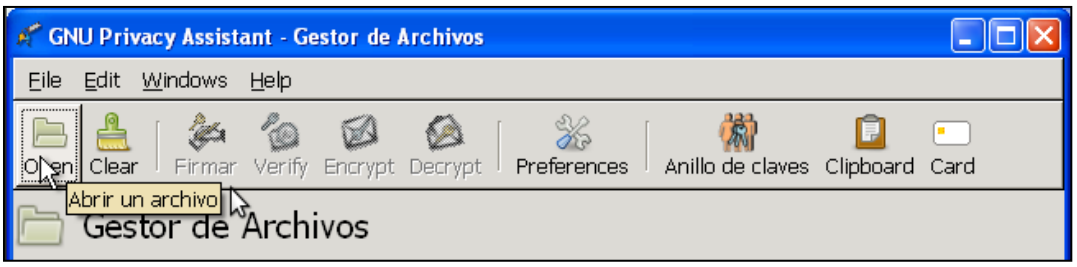


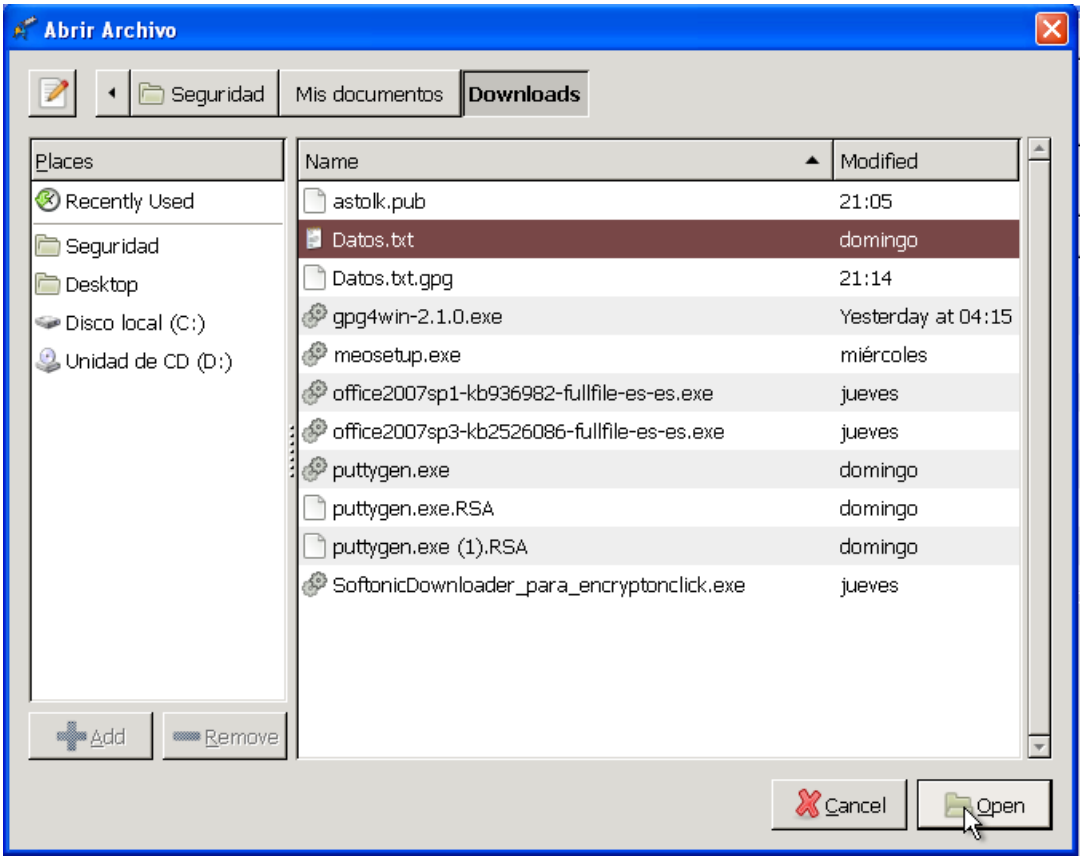
9) Cifrar Archivos

Para cifrar un archivo buscamos la opción de archivos.



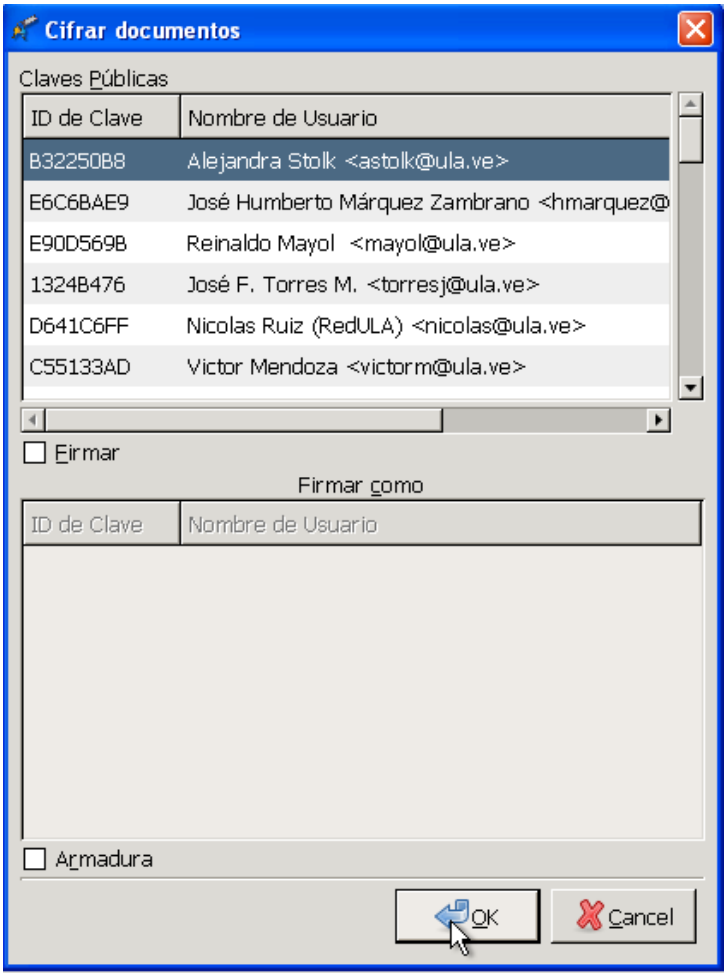
Luego Abrir y seleccionamos el archivo que queremos cifrar.

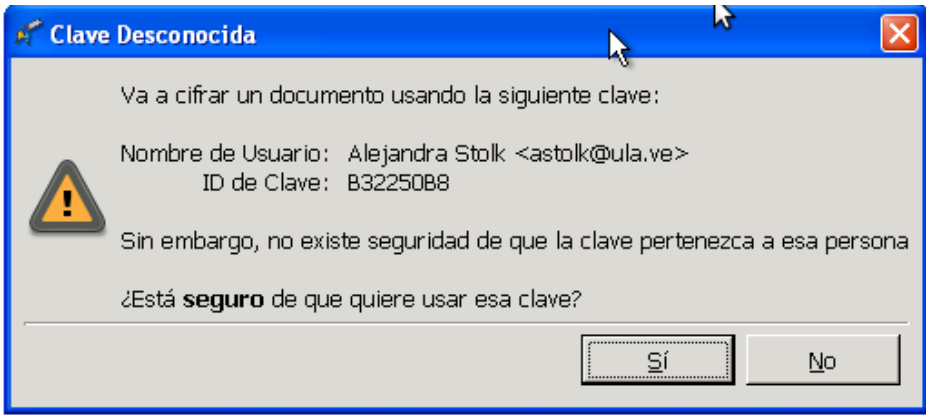




Una vez seleccionado el archivo hacemos clic en abrir y vamos a la opción de cifrar.

Seleccionamos la llave pública con la que deseamos cifrar el archivo, presionamos "si" en el aviso que sale a continuación y finaliza el proceso.



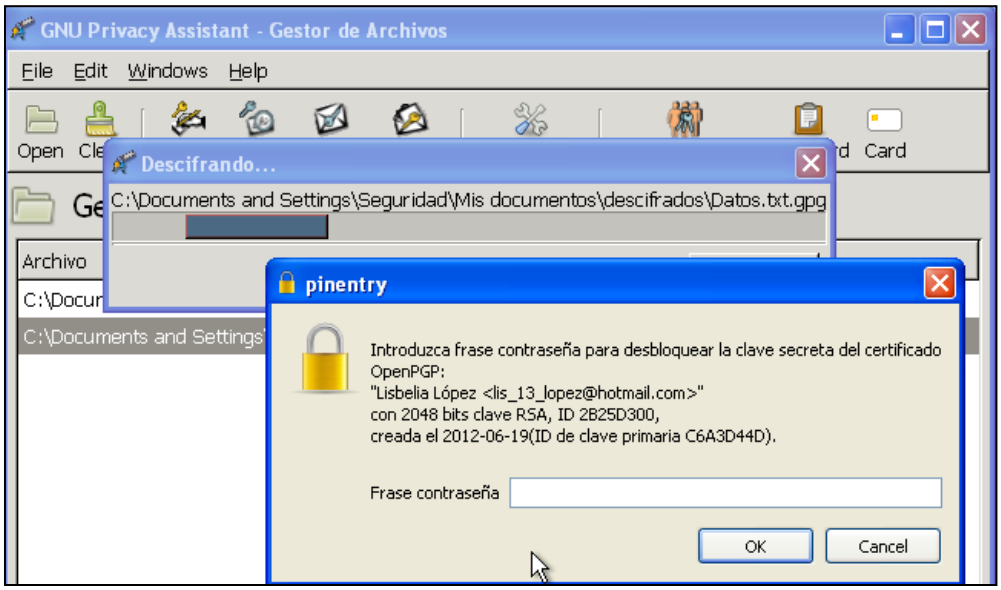


El archivo quedará almacenado con extensión .gpg.

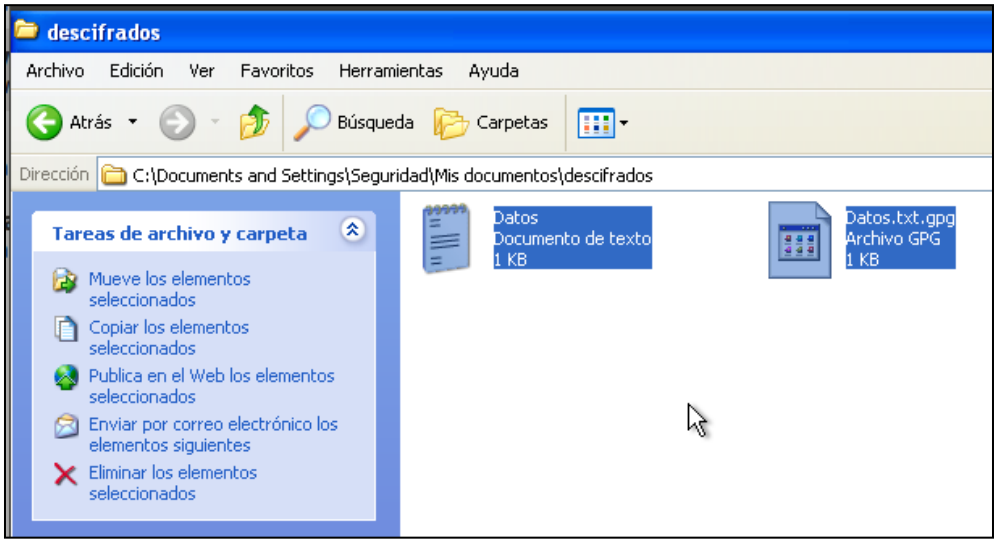
10) Descifrar archivos

Buscamos el archivo .gpg que se ha almacenado y seleccionamos la opción de descifrar.

Ingresamos la frase contraseña para descifrar el archivo



Verificamos si el archivo cifrado ha sido descifrado correctamente.



Cuando instalamos la herramienta gpg4win, se instalan complementos: Cleopatra y Claws-mail. De estas 2 herramientas puedes conocer más visitando estos enlaces:

Descargar Manual de Cleopatra:

http://docs.kde.org/stable/es/kdepim/kleopatra/kleopatra.pdf

Ver manual de Claws-mail

http://tuxlink.wordpress.com/2008/04/20/claws-mail-y-gmail/