FIRMA Y ENVÍO DE MENSAJES ENCRIPTADOS CON OpenPGP usando el programa GPG4Win (versión 2.1.0).

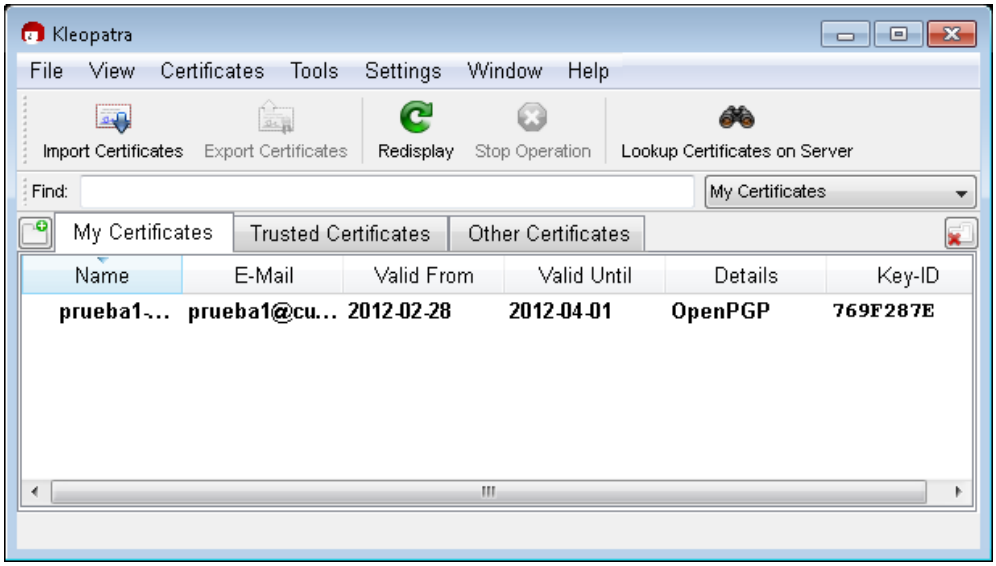
Práctica de la asignatura *Informática Jurídica* de la licenciatura en Derecho de la universidad de Valladolid.

1- Pensar una identidad ficticia (usar algo como minombre.alumno@uva.es) y una frase de paso fácil de recordar.

2- Agruparse en equipos de dos (uno en cada ordenador). Los miembros de cada equipo se van a intercambiar claves y mensajes firmados y encriptados.

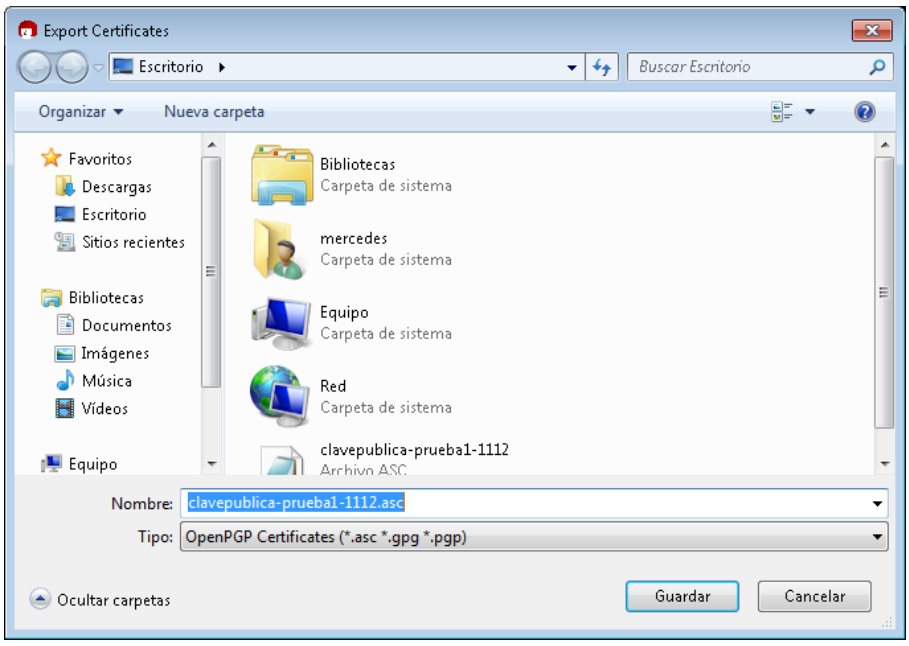
3- Ir al programa en nuestro ordenador: menú de Inicio, GPG4win, ejecutar el programa de nombre 'Kleopatra'.

4- Crear un nuevo par de claves para nuestra identidad (la que acabamos de crear en el paso 1).

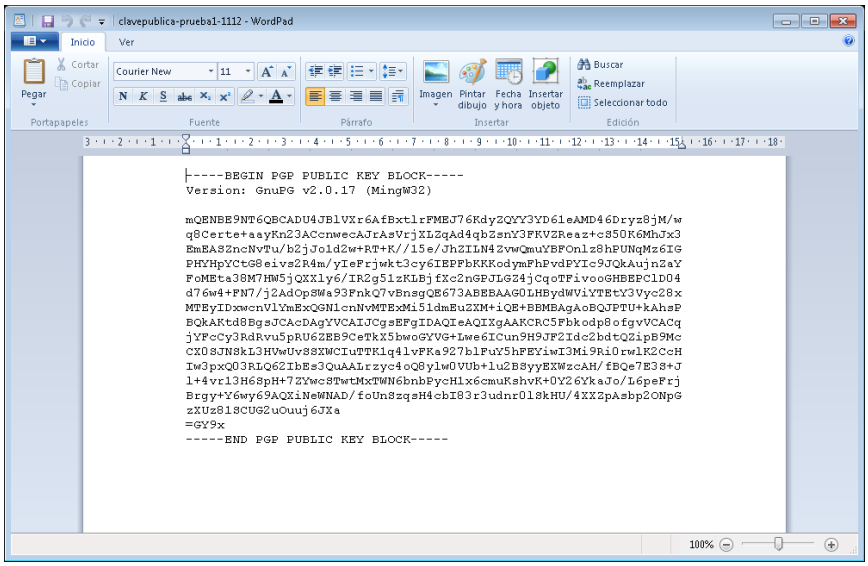


5- Editar la clave y cambiar la fecha de expiración (una semana más tarde). Se necesitará proporcionar la frase de paso para poder cambiar propiedades de nuestra clave privada.

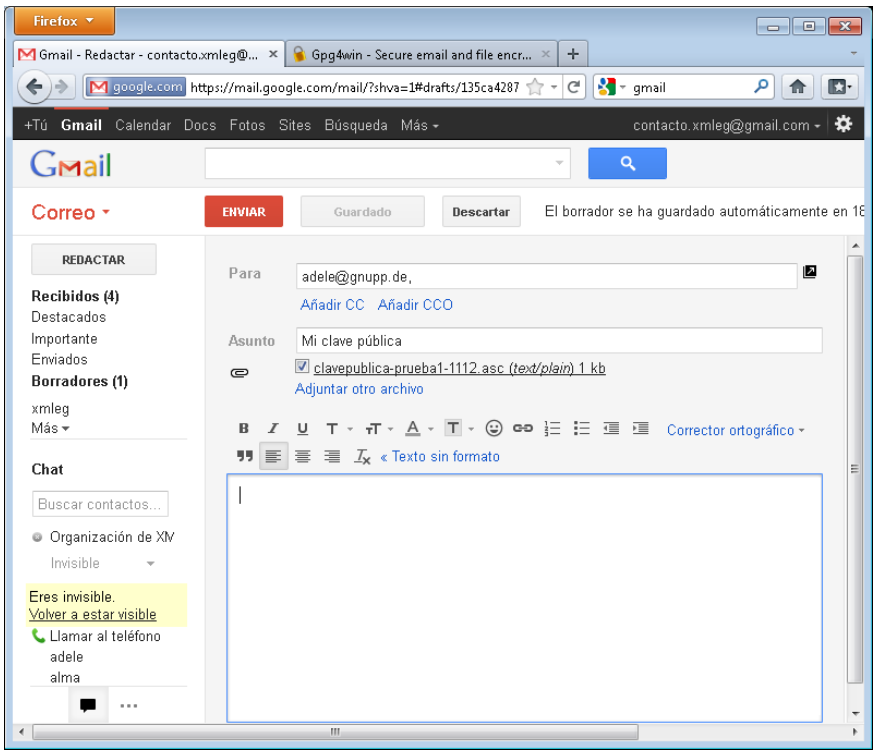
6- Exportar la clave. Escoger un nombre de fichero tipo *minombre_key.asc*. Seleccionar el escritorio para su ubicación.



7- Abrir este fichero con WordPad (¡NO con Word!): vamos a echar un vistazo a nuestra clave pública.

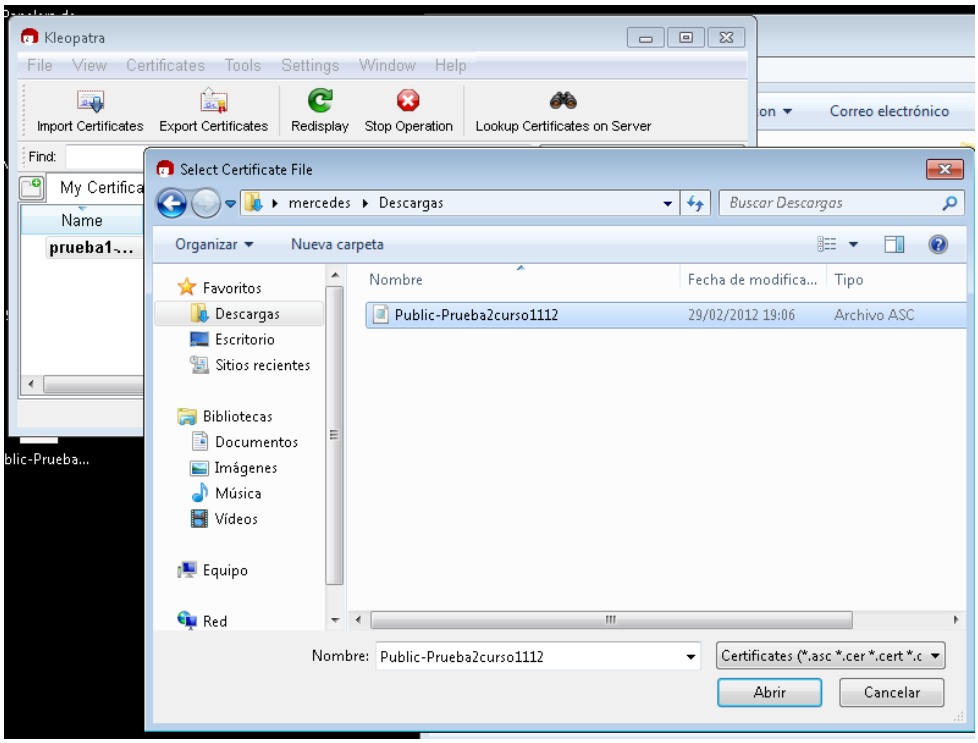


8- Crear un nuevo mensaje de correo. Adjuntar el fichero que contiene nuestra clave pública. Poner de subject "Mi clave pública" y enviarlo a nuestra pareja de equipo.



9- Abrir el correo que nos ha enviado nuestro compañero. Guardar el fichero adjunto, con un nombre parecido a *miamigo_key.asc*.

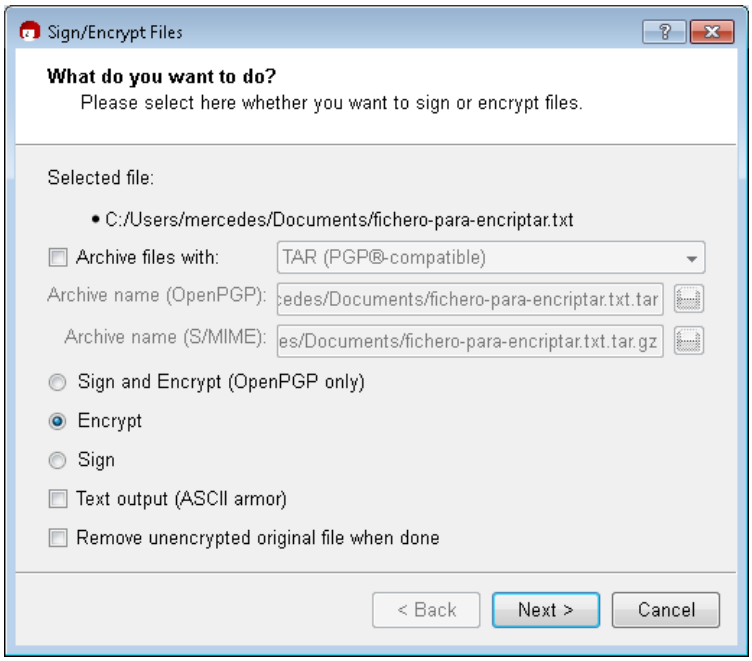
10- Ir a Kleopatra de nuevo y seleccionar "Importar clave". Cuando nos pregunte, seleccionar el fichero que acabamos de guardar.



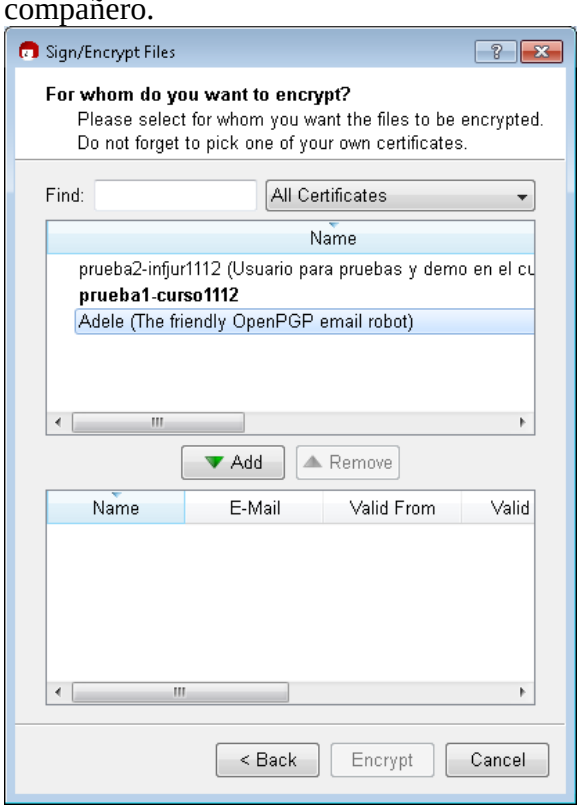
Hemos creado un par de claves, exportado nuestra clave pública, e importado la clave pública de otra persona a nuestro anillo de confianza. Vamos a enviarle un mensaje encriptado con su clave pública.

13- Crear un nuevo fichero de texto y escribir cualquier cosa (por ej. "Este es mi primer mensaje encriptado") en el contenido. Guardarlo.

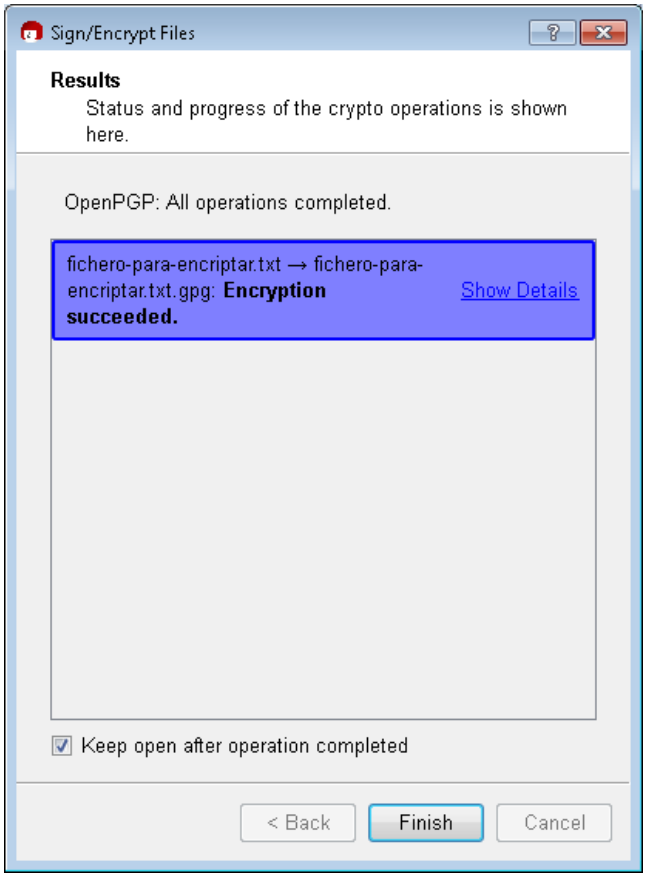
14- Ir de nuevo a Kleopatra y seleccionar en el menú de Fichero (File) la opción “Sign/Encript Files…”. Cuando nos pida seleccionar un fichero, buscar el fichero que acabamos de crear. Aceptar las opciones por defecto que nos ofrece Kleoptra (Encript).



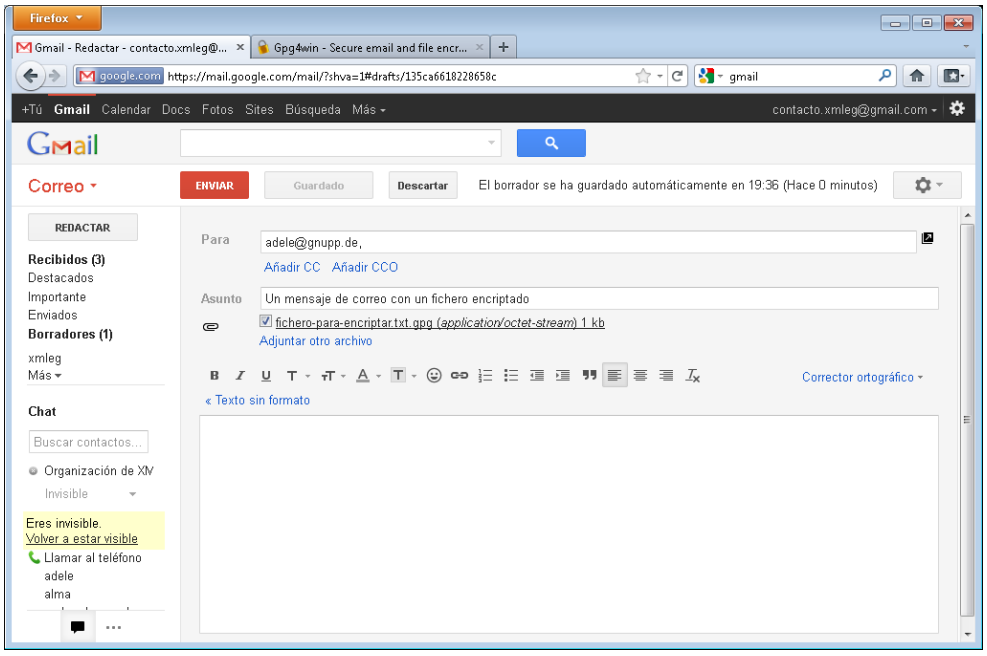
15- Cuando nos pregunte para quién queremos encriptar, seleccionar el certificado de nuestro compañero.



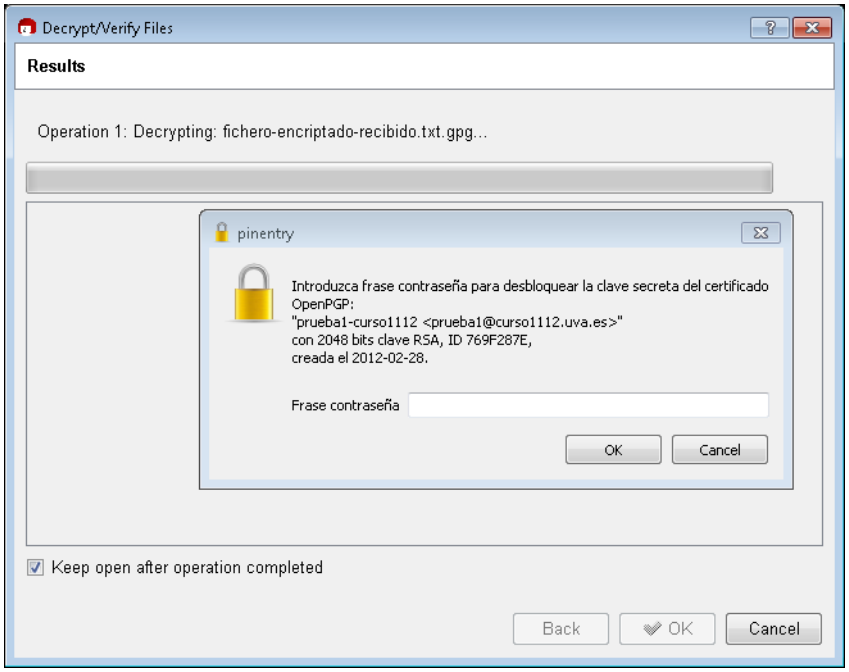
Si tiene éxito, recibiremos un mensaje como el que se ve en la figura, donde Kleopatra nos informa de que así ha sido.



16- Enviarlo a nuestro compañero. Poner cualquier subject (por ej., "Te envío mi mensaje cifrado").



17- Abrir el correo que acaba de enviarnos nuestro compañero. Guardar el fichero adjunto en nuestro ordenador. Ir nuevamente a Kleopatra y seleccionar en el menú de Fichero (File) la opción “Decrypt/Verify files…”. Nos pedirá nuestra frase de paso (*pregunta para pensar*: *¿por qué?*)



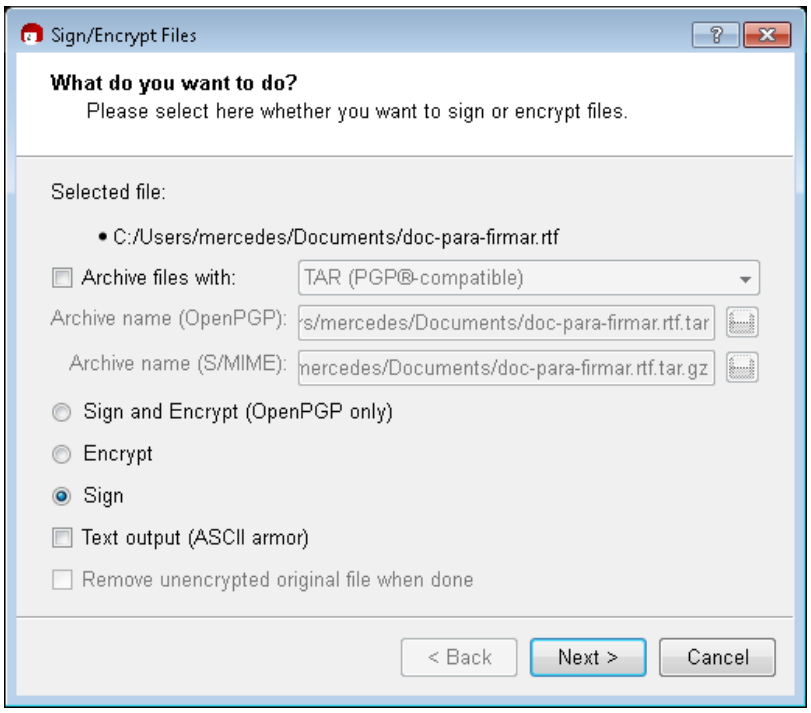
Si todo va bien recibiremos un mensaje de confirmación como el que aparece en la figura y Kleopatra habrá guardado un fichero con el mismo nombre, pero que ya no será de tipo PGP. Este fichero lo podremos abrir para leer el mensaje de nuestro compañero.

18- Abrir el fichero que para poder leer el mensaje que nos ha enviado nuestro compañero.

Acabamos de recibir un mensaje encriptado con nuestra clave pública, y lo hemos leido (desencriptado) usando nuestra clave privada. Vamos a firmar un documento, para enviarlo a nuestro compañero.

19- Hacer el mismo proceso del paso 13 (en este caso se trataría de "Mi primer documento firmado").

20- Ir de nuevo a Kleopatra y seleccionar en el menú de Fichero (File) la opción “Sign/Encript Files…”. Cuando nos pida seleccionar un fichero, buscar el fichero que acabamos de crear. En este caso, seleccionar una opción distinta a la que nos ofrece Kleopatra por defecto: “Sign”, tal como se muestra en la figura.



Nos pedirá nuestra frase de paso (*¿por qué?*).
Si todo va bien, Kleopatra nos mostrará un mensaje confirmando el éxito de la operación y guardará el fichero con la firma en nuestro ordenador --lo reconoceremos porque tiene el mismo nombre que el fichero original, pero la extensión '.sig'--.

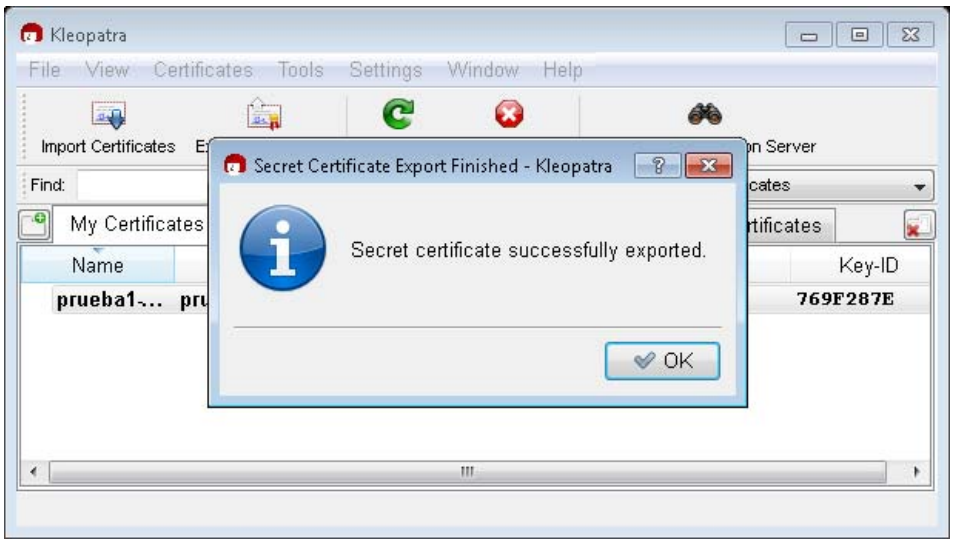
22- Enviar un correo a nuestro compañero con este fichero como adjunto.

23- Abrir el correo que acaba de enviarnos nuestro compañero. Guardar el fichero adjunto.

24- Ir a Kleopatra y seleccionar desde el menú de Fichero (File) la opción "Decrypt/Verify Files…". Para verificar la firma, es necesario que Kleopatra encuentre el certificado público de nuestro compañero en nuestra lista de certificados (para lo cual debemos haberlo importado previamente).

Acabamos de recibir un mensaje firmado y hemos verificado la firma. Hemos aprendido a crear un par de claves GPG, a exportar e importar claves, a intercambiar mensajes encriptados, y a firmar y verificar una firma digital. Por último, vamos a hacer una copia de seguridad de nuestras claves y nos la vamos a llevar en un USB o algún dispositivo al que sólo tengamos acceso nosotros.

25- Ir nuevamente a Kleopatra, seleccionar uno de nuestros certificados, y desde el menú de Fichero escoger la opción "Export Secret Keys". Nos preguntará qué nombre queremos darle y lo guardará con la extensión '.gpg'.



26- Copiar este fichero a nuestro lápiz de memoria.

27- Borrarlo del ordenador que hemos utilizado.