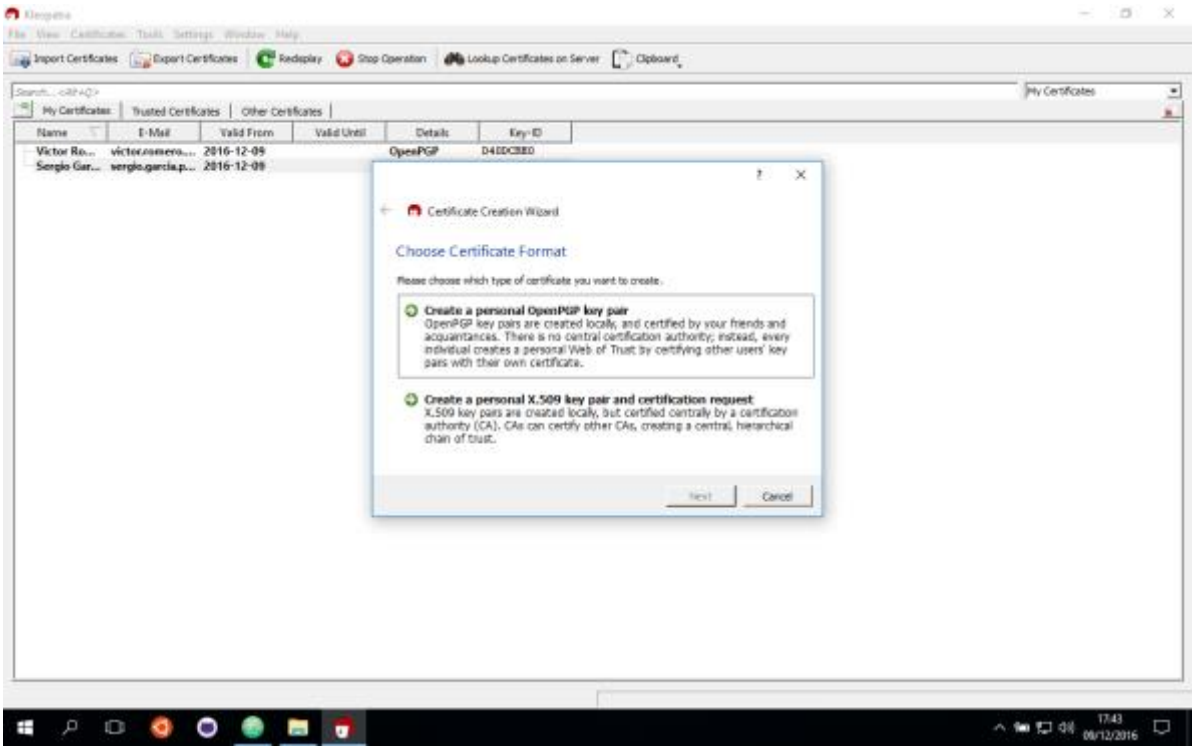
Certificados, firma digital y criptografía
Práctica SL5
Informe de prácticas

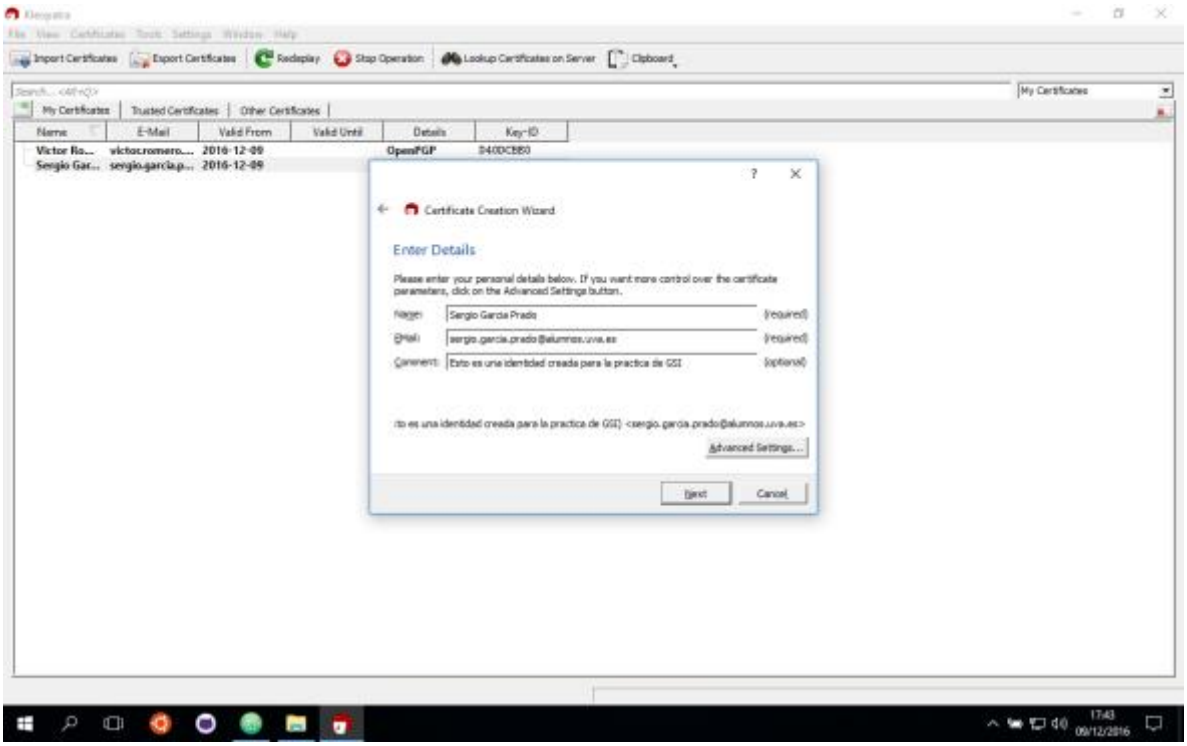
1. **Describa los pasos que se deben seguir si se desea enviar un mensaje firmado a una persona empleando certificados.**

   Para enviar un mensaje firmado a una persona enviando certificados lo primero de todo es crearse una identidad que nos identifique, a través de la cuál otras personas podrán comprobar que somos nosotros. La herramienta Kleopatra permite este proceso mediante los siguientes pasos:

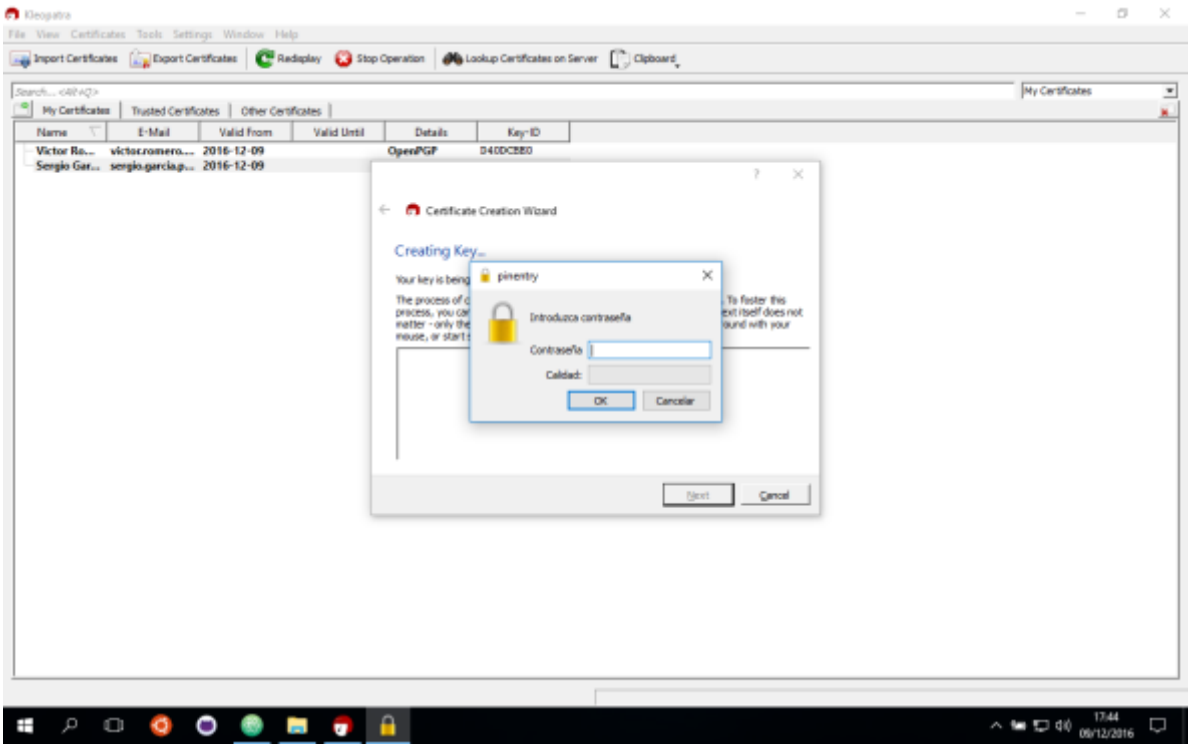


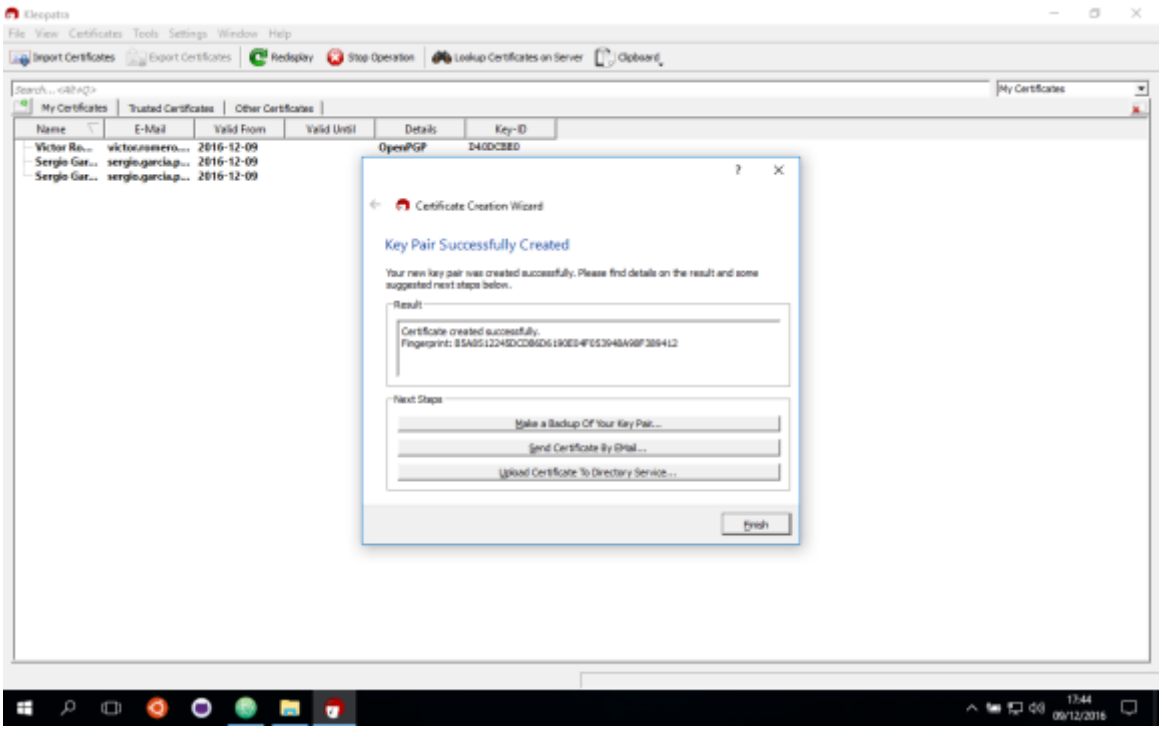
   Seleccionamos el método de certificado mediante identificación OpenGPG el cuál utiliza algoritmos de clave pública o asimétrica, los cuáles utilizan dos claves, una de ellas se da a conocer entre los interesados y es denominada pública, mientras que la otra se guarda en secreto y es denominada privada. La estrategia que utilizan estos algoritmos se basa en la necesidad de la clave contraria para el descifrado.

   El paso siguiente es introducir nuestros datos personales para que esta identificación quede relacionada con el usuario.



A continuación se pide una clave o keyphrase que nos permitirá acceder a nuestra clave privada tal y como se ha expuesto anteriormente.





Una vez hecho esto, la identidad ya está creada, por lo que se debe hacer es compartir con quienes se desee compartir mensajes, de forma segura mediante el sistema de envío cifrado y/o de manera firmada con lo que se puede verificar quién es el remitente.

Nótese que estas dos cuestiones son distintas, ya que enviar el mensaje de forma cifrada no implica indicar quién ha sido el remitente, ni enviar un mensaje indicando quién es el remitente implica enviar de manera cifrada el mensaje. A pesar de ello existe la opción de realizar las dos acciones simultáneamente.

Los siguientes pasos del proceso consisten en enviar el certificado de identidad a todas aquellas personas a las que se desee demostrar el origen del fichero.

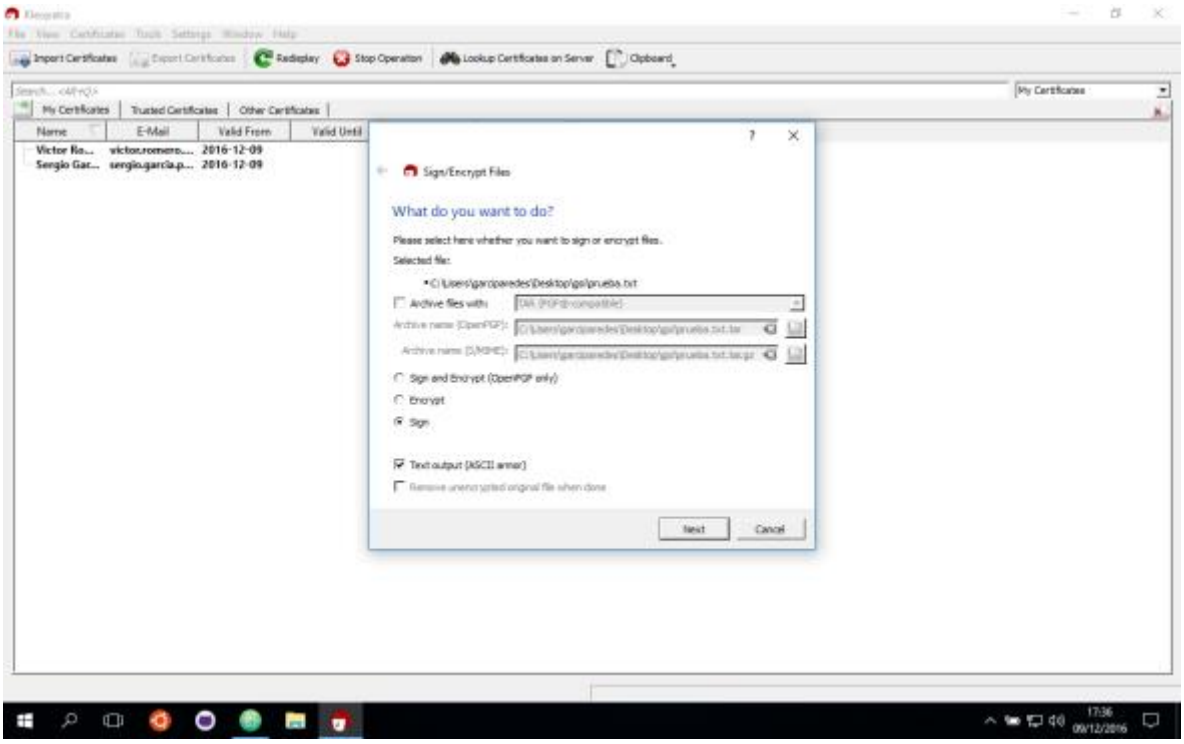
A continuación, se realiza el proceso de firma del mensaje, el cuál se indica en las capturas de pantalla que se adjuntan a continuación. Lo único que hay que hacer es indicar el fichero que se desea firmar junto con la identidad.

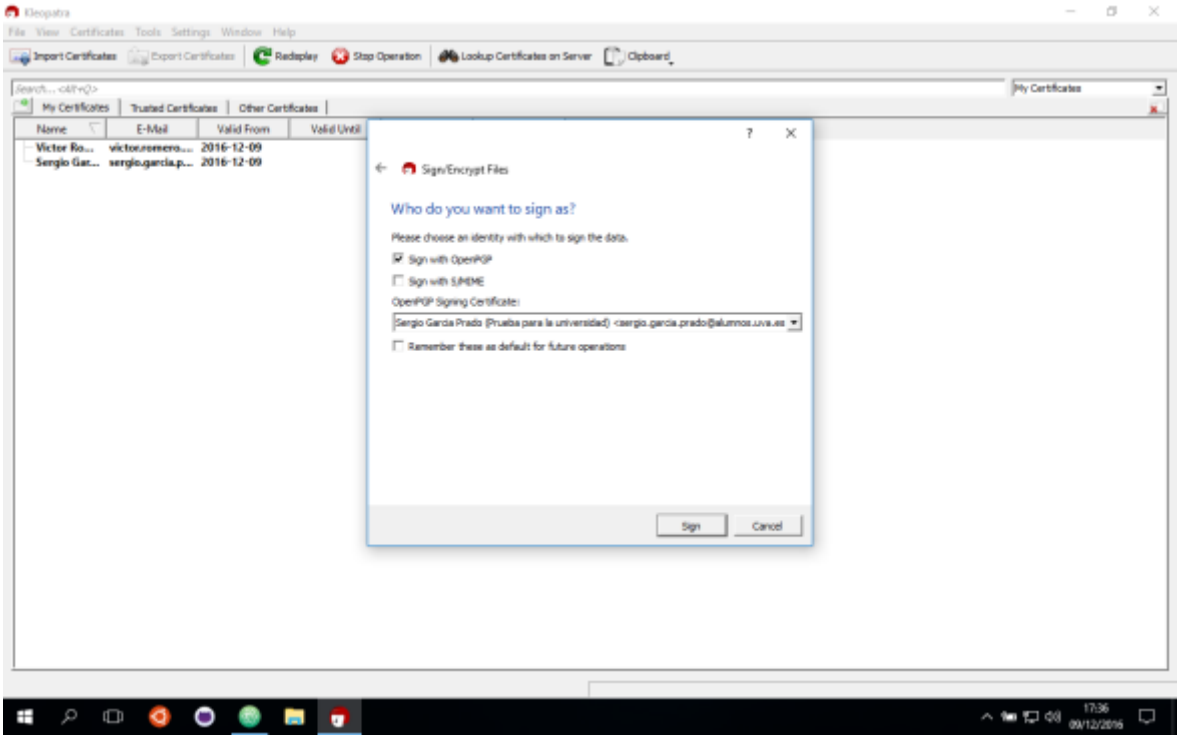
Tras completar estos pasos se genera un nuevo archivo que contiene la firma del mismo. Esta firma consiste en un resumen del fichero mediante algún algoritmo como MD5 o similar, que después se cifra con la clave privada de la identidad.

El proceso que realizará posteriormente el destinatario será realizar el mismo proceso de resumen mediante un algoritmo como MD5 o similares. También descifrará con la clave pública de la identidad el resumen o firma enviado junto con el usuario y si estas dos coinciden significará que la integridad del fichero continúa intacta por lo que la firma será válida.

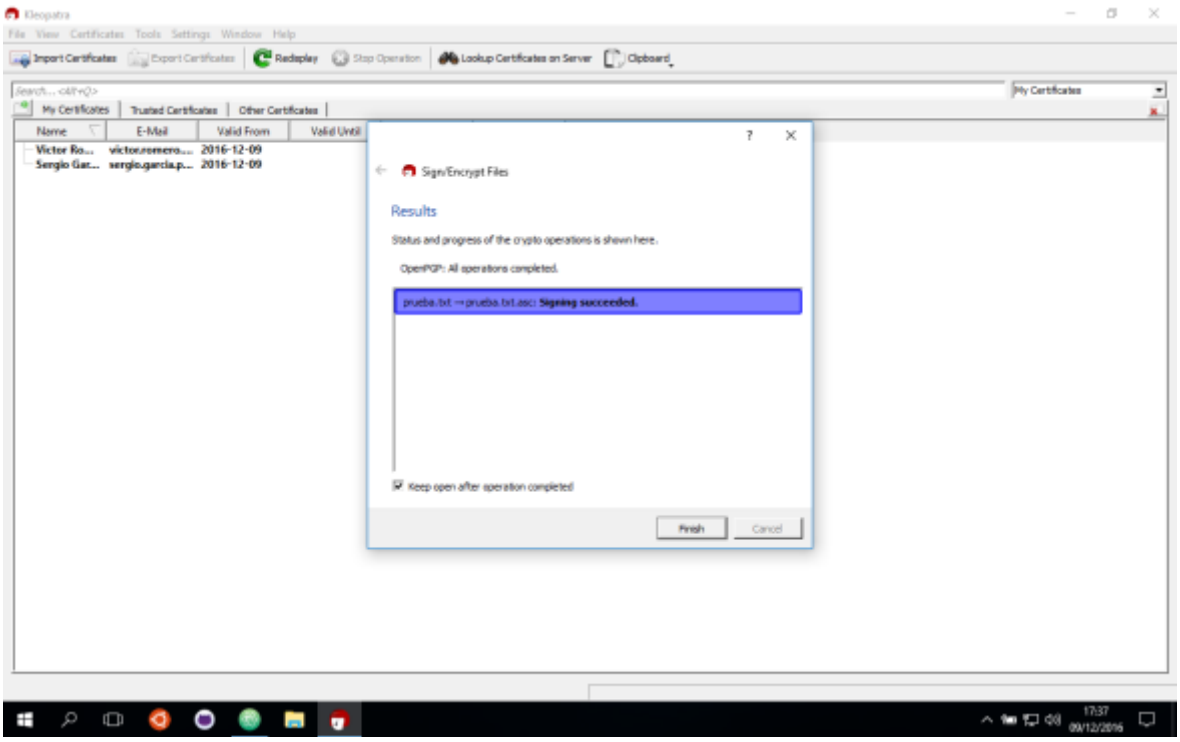
En el ejercicio 4 se exponen los dos casos mostrando las capturas de pantalla que muestran

la salida del Software Kleopatra.





Nótese que en este paso se pedirá la contraseña de la identidad que firma debido a que se utilizará la clave privada de la misma.



2. **Al crea una identidad, debemos introducir una "frase de paso" (keyphrase). Posteriormente, el software nos solicitará dicha frase en determinadas ocasiones. Comente y explique cuándo y para que lo solicita.**

   Cuando se crea una identidad GPG se piden los siguientes campos: *nombre completo*, *email* y *descripción* opcional además de los tamaños que tendrán las claves, así como el algoritmo que se desea utilizar. Además, tal y como se indica en el enunciado de este ejercicio, se pide también una keyphrase.

   La estrategia que utiliza GPG es la de algoritmos de cifrado de clave pública para enviar información de forma segura. Esta idea es importante a la hora de entender cuándo se pide la keyphrase.

   Cuando se desea firmar un archivo, lo que se pretende es demostrar la autoría/modificación del mismo, para comprobar esto, otras personas utilizarán la clave pública que se les suministra para verificar que ha sido firmada con la privada que solo el propietario posee.

   En el caso de querer cifrar un archivo para que solo una persona lo pueda leer, la operación es la inversa. Lo que hay que hacer es cifrarlo con la clave pública, que todo el mundo conoce, pero que solo se puede descifrar con la privada, para que solo lo pueda descifrar la persona que posea la privada, con lo que se consigue que solo esta lo lea.

   Por ejemplo, al firmar un archivo se pide dicha keyphrase, sin embargo, no es necesaria a la

hora de verificar una firma de otra persona ya que en este caso no debe utilizar ninguna keyphrase secreta.

Lo mismo ocurre cuando se cifra un mensaje para otra persona, al utilizar la clave pública de esta no es necesario introducir la clave (a menos que además de cifrarse, se vaya a firmar, en cuyo caso, como se ha expuesto en el párrafo anterior, sí que sería necesario). En el momento de descifrar un mensaje cifrado dirigido a una persona en concreto, sí que es necesario utilizar la keyphrase porque se utilizará el algoritmo de cifrado.

Como conclusión, podemos decir que la keyphrase se solicita al usuario únicamente cuando es necesario el acceso a la clave privada del mismo para la operación correspondiente.

3. ¿Qué diferencias existen entre un password y una keyphrase? Desde su punto de vista, ¿cuál es mejor y por qué?

La principal diferencia entre una *password* y una *keyphrase* es la longitud de cada una de las mismas. Generalmente esto se debe a que una *password* no permite introducir caracteres en blanco o espacios. Por el contrario, las *keyphrases* sí que permiten esto, por lo que se pueden utilizar oraciones completas como claves de acceso.

La principal ventaja que tiene una *password* frente a la *keyphrase* es su facilidad para ser recordada en la memoria de una persona. Esto, a su vez lo convierte en una gran vulnerabilidad ya que facilita su descubrimiento mediante fuerza bruta o diccionarios de claves comunes.

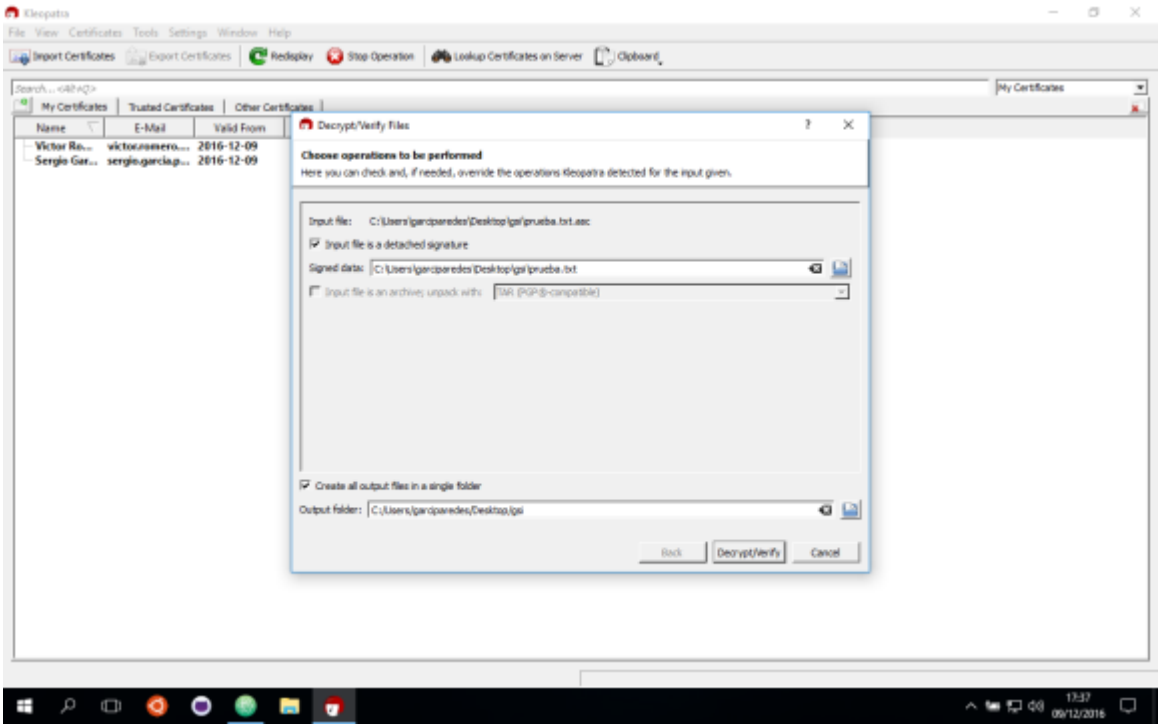
La ventaja principal de una *keyphrase* es su mayor nivel de seguridad debido al mayor tamaño de la clave que se utiliza, lo cual imposibilita el ataque por fuerza bruta. Por el contrario, el problema de este sistema consiste en la dificultad para recordar dicha clave por parte del usuario que la utilizará.

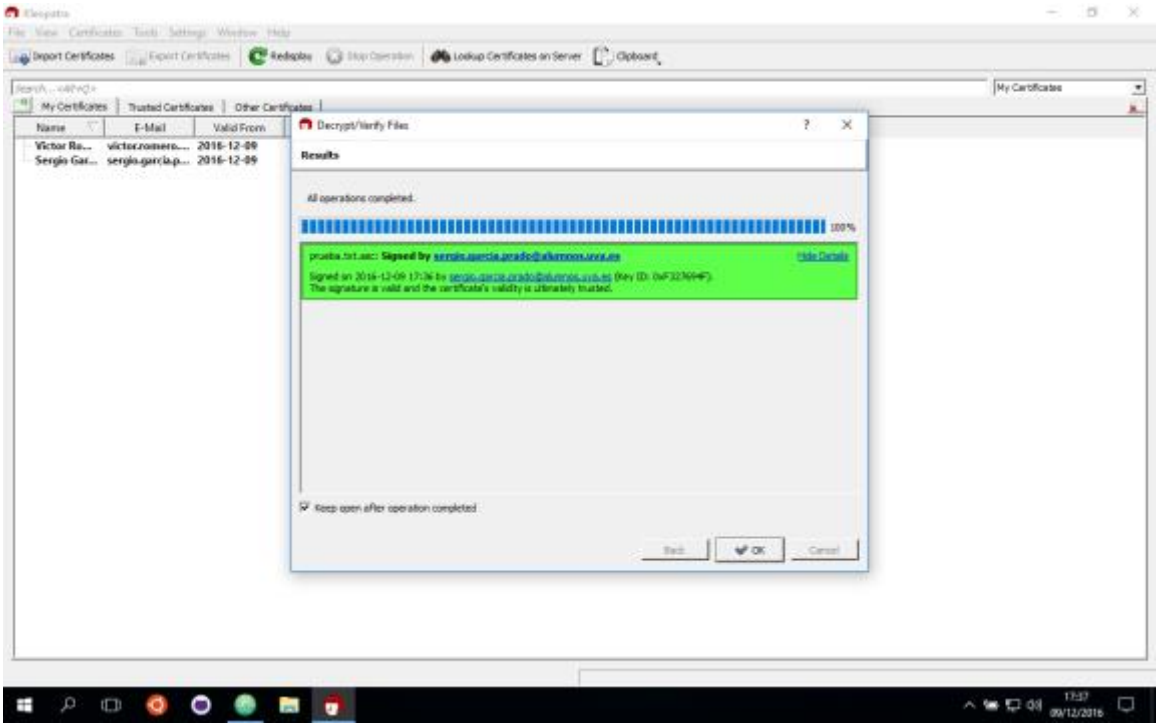
Bajo mi punto de vista creo que no existe una alternativa mejor que la otra sino que están orientadas a fines diferentes. Mientras que la *keyphrase* es una mucho mejor alternativa para ser manejada por una máquina, por su capacidad de almacenamiento "ilimitado", la *password* tiene sentido cuando debe ser recordada por una persona.

A pesar de ello, cada vez están ganando más adeptos otros métodos que sustituyen el uso de *passwords* de usuario como sistemas basados en telemetría (huella dactilar, imagen facial, etc.) u otras alternativas que se siguen apoyando en claves de tamaño corto pero utilizan métodos adicionales como verificación en dos pasos que tratan de ser fáciles de usar para las personas.

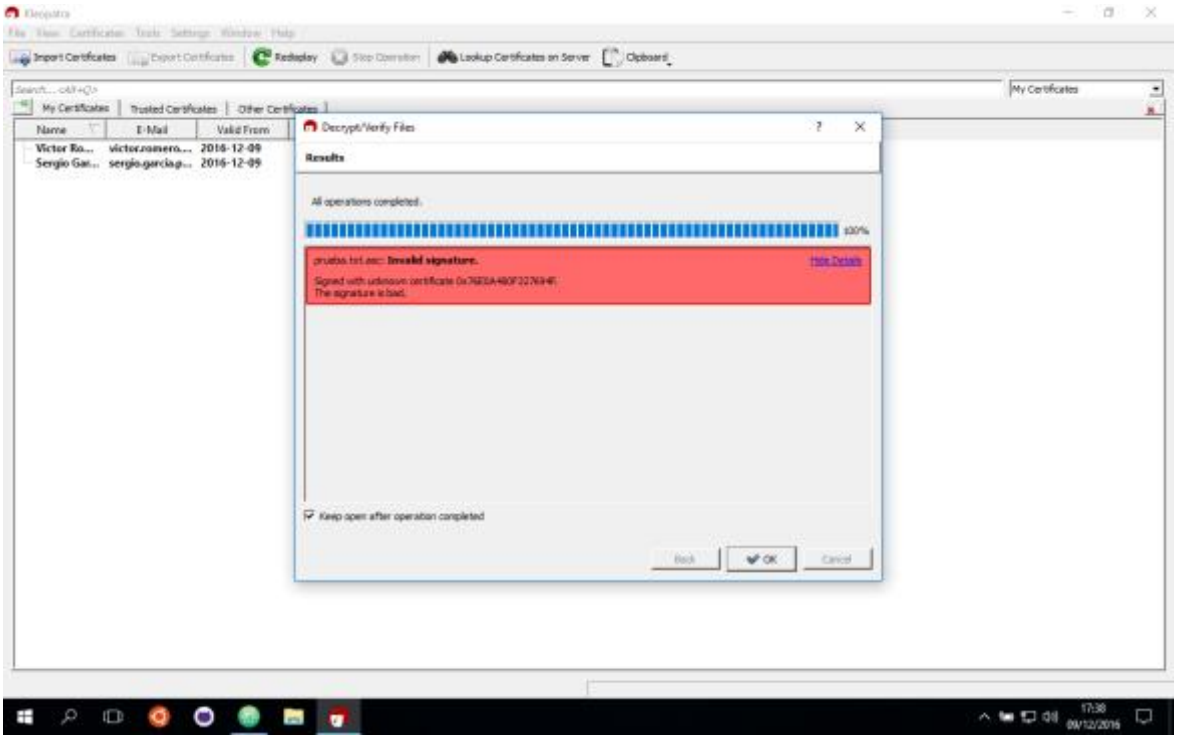
4. Al verificar una firma digital se coteja tanto la firma como la identidad del remitente. Capture el mensaje que obtiene al verificar una firma recibida (usando Kleopatra) tanto sobre el fichero recibido como sobre el fichero recibido modificado. Comente los resultados.

Para ver los resultados de verificar la firma sobre un fichero que no ha sido modificado se muestran las siguientes capturas de pantalla:





Tras modificar el fichero y utilizando la misma firma para validar el fichero el resultado obtenido es el siguiente:



Los motivos por los cuales sucede esto ya han sido descritos en el ejercicio 1. Tal y como se dijo allí esto tiene que ver con la diferencia entre los resúmenes obtenidos por vía del fichero a con el contenido y la firma de la identidad que tras ser descifrada debería coincidir con el mismo.