Requerimiento 2

Te proponemos practicar con el cifrado asimétrico de la información. Para ello, primero debes contar con el entregable de la actividad 2 (será un fichero “pdf”) y el objetivo es volver a enviarlo a tu profesor, pero cifrado.

TAREAS:

Instalación de Gpg4Win en tu MV Windows 10

Generación de una pareja de claves (privada y pública) personales tuyas.

Exportación de tu clave pública y almacenamiento en un servidor externo en Internet (así cualquiera podrá verificar los documentos que firmes)

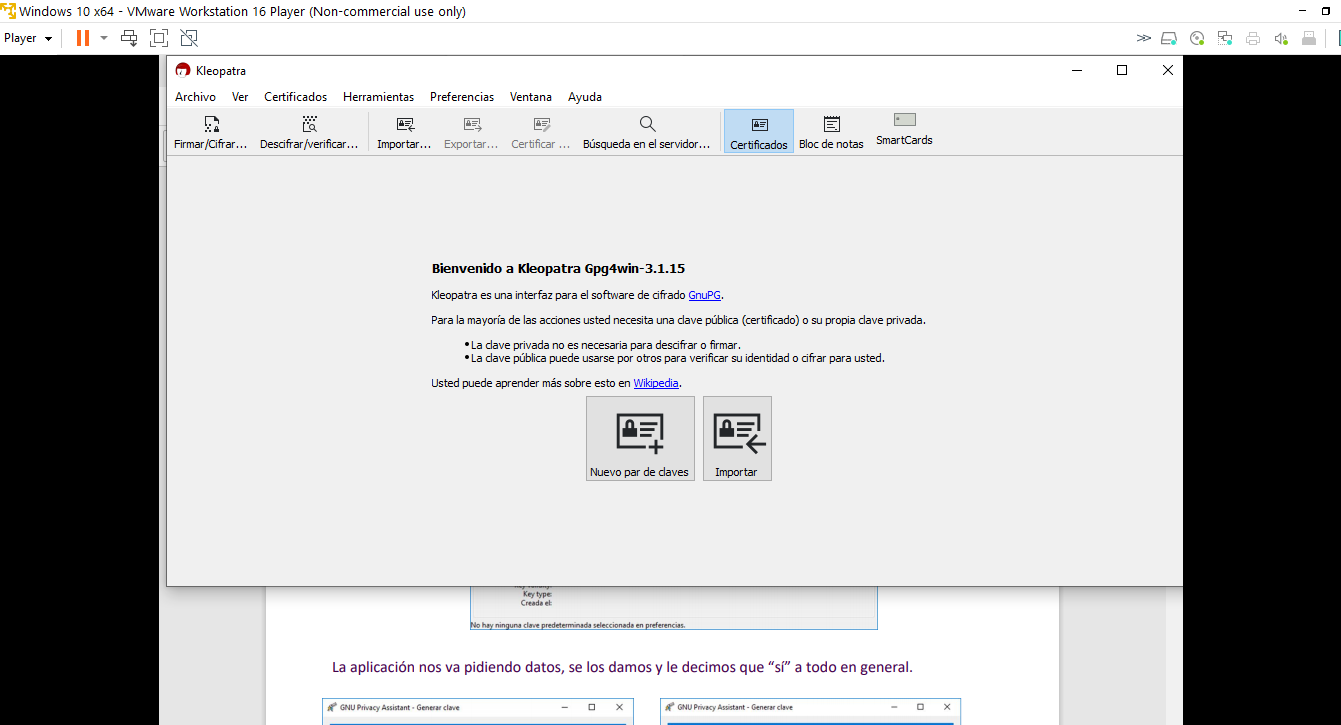
Cifrado del documento entregable de tu práctica AI4 con la clave pública de tu profesor. Para esto primero tendrás que bajártela desde un servidor externo y luego importarla en tu sistema de claves.

Envío a tu profesor (por el medio acostumbrado) del documento cifrado que él podrá ver con su clave privada.

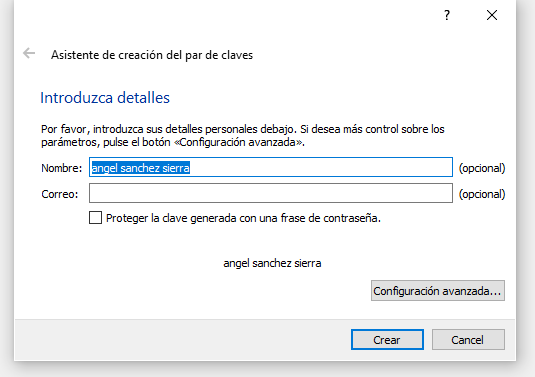
NOTA: por facilidad y para que practiques con Cpg4Win, hemos realizado la práctica entera en entorno Windows, para que lo hagas en una sola máquina virtual, pero igualmente podría hacerse en entorno Linux.

Procedimiento de cifrado asimétrico de la información en MV Windows 10:

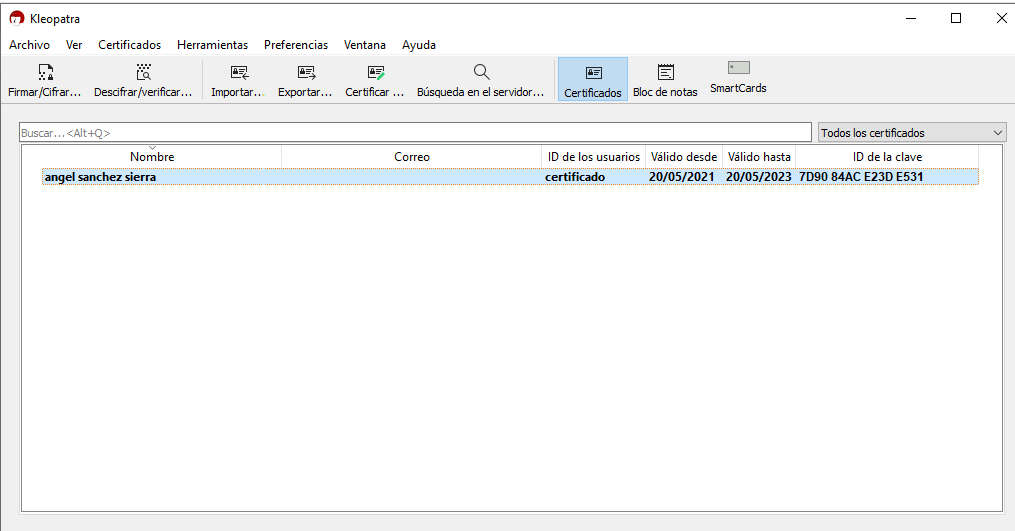
Primero he descargado la aplicación de Gpg4Win en mi MV



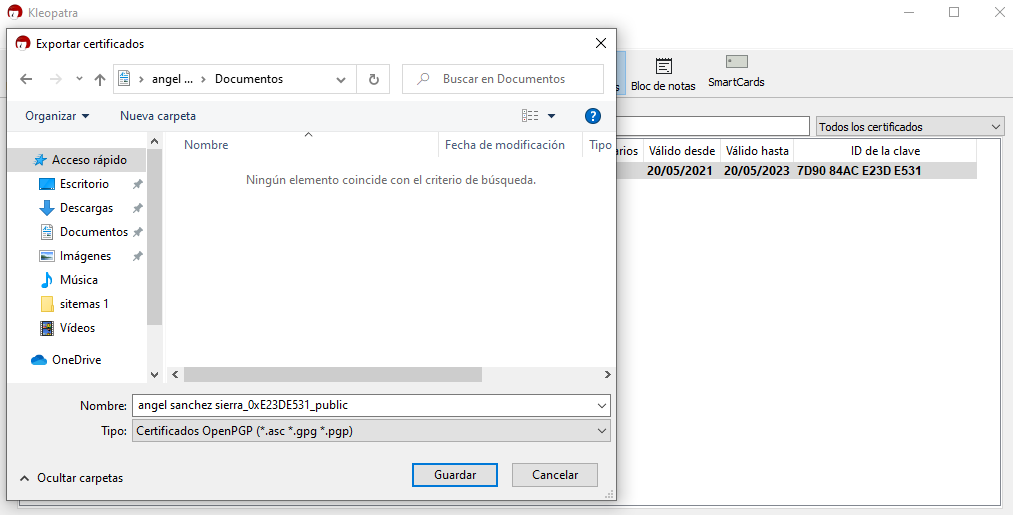
Al completar la instalación nos ofrece crear ya una pareja de claves. Las cuales procedo a crear.



Al final de este proceso nos indica que mis claves se han creado correctamente



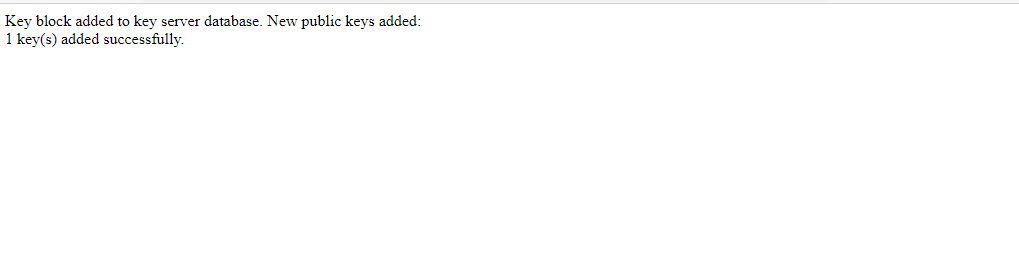
Una vez creada la pareja de claves ingreso a la otra aplicación del paquete (Kleopatra) y desde allí exporto mi clave pública.



Ahora voy a subir mi clave pública a un servidor en Internet. El que se nos ha dado por defecto es este: “pgp.rediris.es”.



Simplemente he pegado el contenido ASCII del fichero de claves que he generado en el cuadro inferior y dar a “submit”.

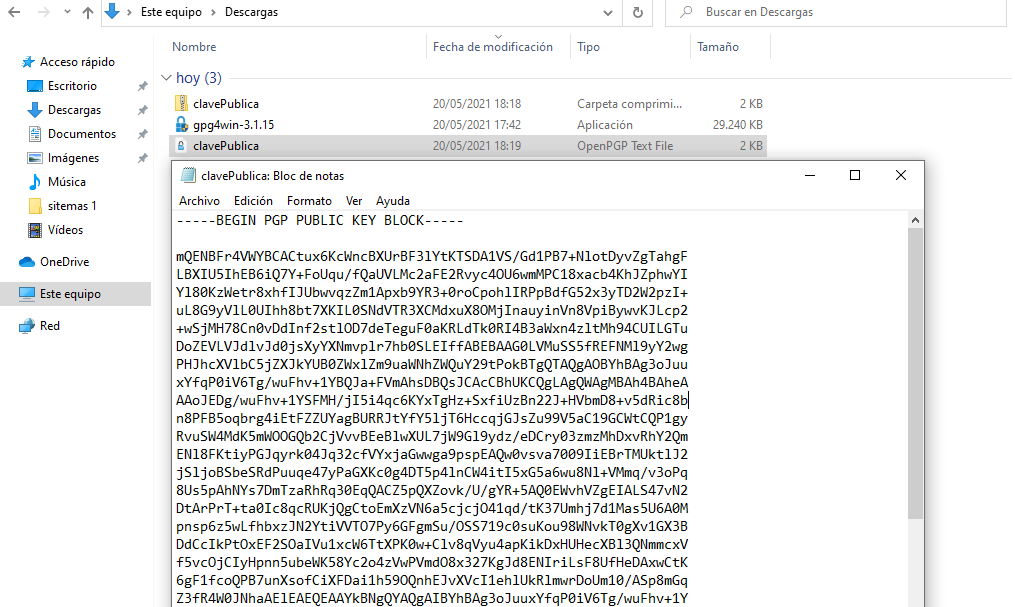


Si a continuación introduzco en el cuadro de búsqueda mi nombre veo que encuentra la clave pública que acabo de subir:

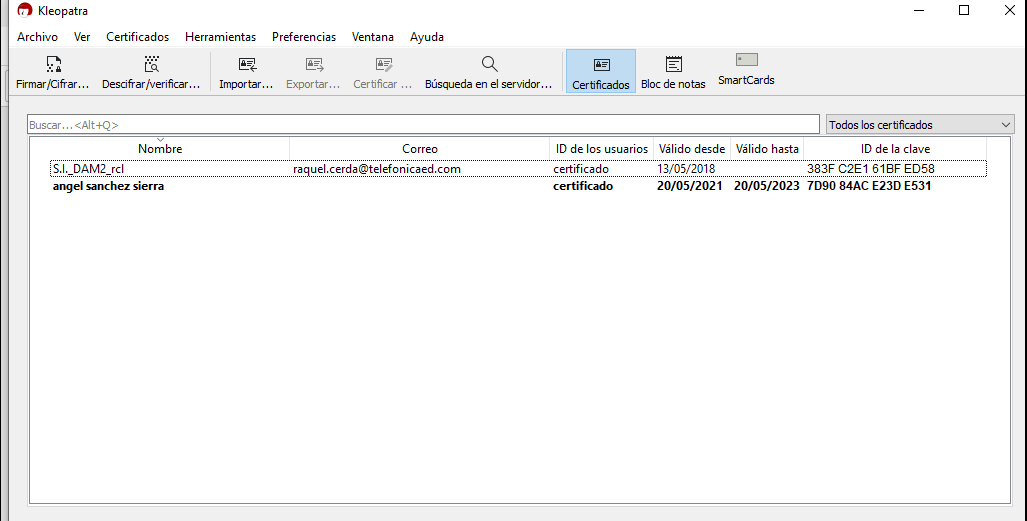


Ya tengo mi clave subida al servidor, pero para encriptar el archivo a enviar necesito la clave pública del profesor. Entonces la bajo desde el mismo servidor. Buscando por “Profesor MP0483”.

A continuación me la descargo primero y luego la importo a mi sistema. Para ello simplemente hago un copia/pega del código ASCII y lo almaceno en un fichero al que luego pondre la extensión “asc”.

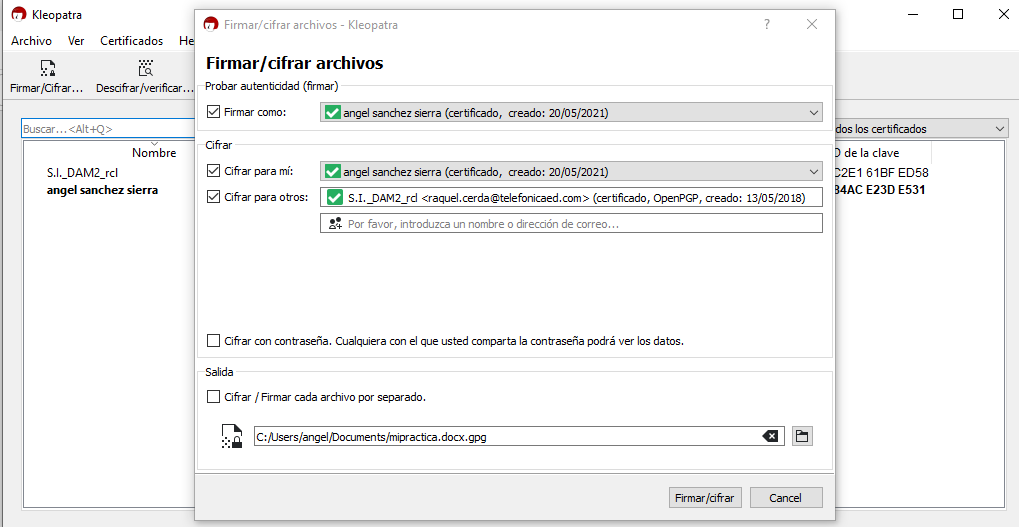


En este momento puedo comprobar que en el sistema ya tengo tanto mis claves (las que he generado) como la clave pública del profesor que he importado.

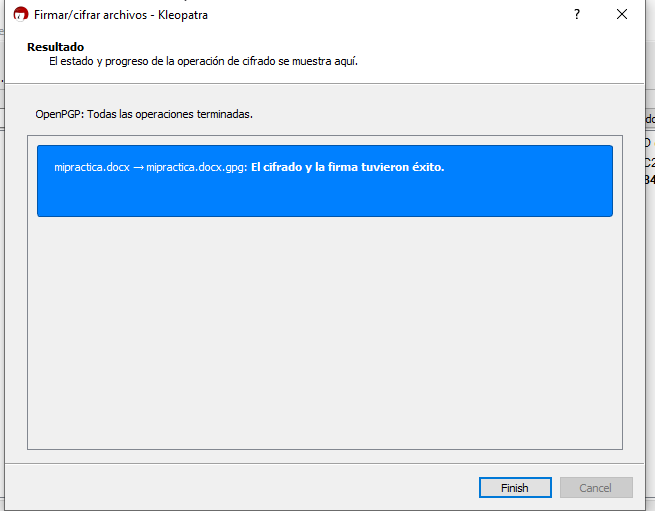


A continuación voy a encriptar el contenido de mi fichero. En este ejemplo lo realice con un archivo llamado “mipractica.doc”.

Lo encripto desde “Kleopatra” con la opción de “cifrar” y elijo como clave de cifrado la clave pública del profesor.



En la ventana que nos sale podemos también elegir como clave de firmado la nuestra, pero esto es opcional.



Sólo me quedaría enviar ese fichero. Como he publicado mi clave pública, si he firmado el documento el profesor podrá comprobar mi identidad. En cualquier caso, solamente el profesor con su clave privada podrá acceder descifrar el fichero que le he enviado y visualizar su contenido.

