# Introducción

El objetivo de este trabajo es practicar y dominar la herramienta de cifrado GnuPG (GPG), usando como medio el programa Kleopatra.

GnuPG una herramienta que permite cifrar y firmar tus datos y comunicaciones, ofreciendo seguridad y privacidad. GnuPG utiliza un sistema de criptografía de clave pública, donde los usuarios generan un par de claves (una clave pública y otra privada). La clave pública puede ser compartida con otros para cifrar mensajes hacia el poseedor de la clave, mientras que la clave privada se usa para descifrar esos mensajes o para firmar mensajes, permitiendo la autenticación de la identidad del remitente. Cabe destacar que tales actividades serán realizadas en la tarea de hoy.

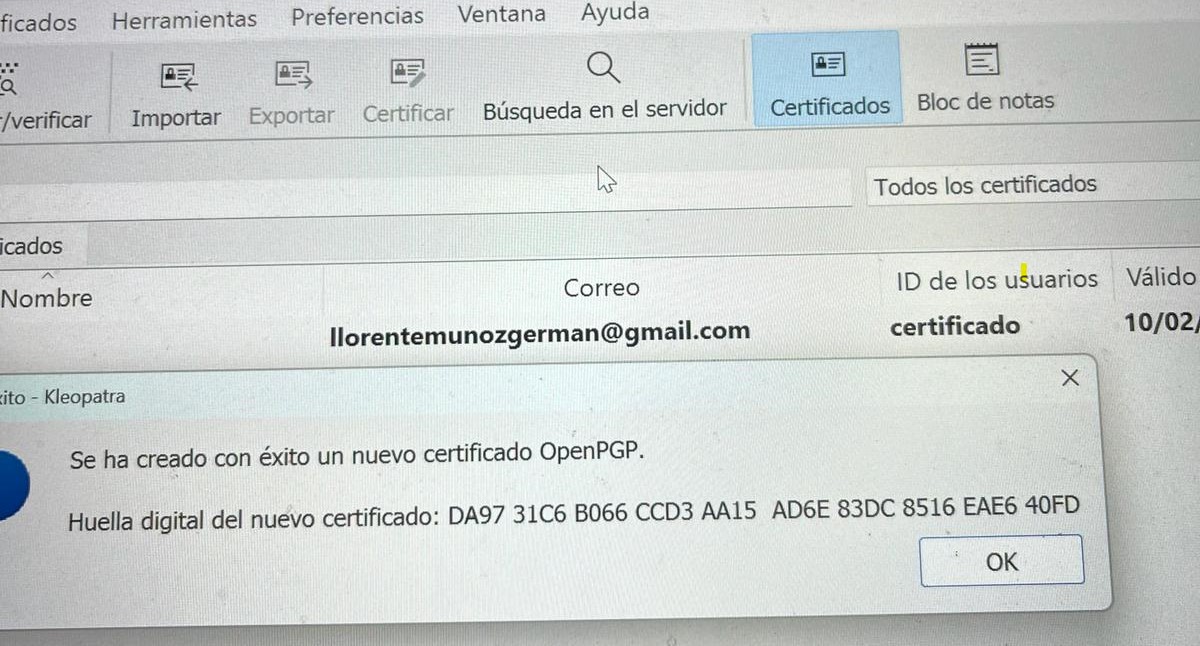
Por otro lado, Kleopatra es una interfaz gráfica de usuario (GUI) para la gestión de certificados y claves de criptografía, incluyendo las de GnuPG y otros estándares como X.509. Verdaderamente, es una forma de facilitar el uso de GnuPG, haciéndola más accesible para usuarios que se sienten más cómodos empleando una interfaz visual.

# Realización de la tarea

Este es un trabajo cooperativo en el que dos usuarios trabajas con datos cifrados del otro. Al abrir el programa, lo primero que se debe hacer es certificar a tu compañero. De esta forma se podrán compartir los datos y que este pueda realizar el descifrado. Aquellos usuarios que no estén certificados no tendrán permitido el descifrado de datos aunque sigan los pasos adecuados para este.

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente



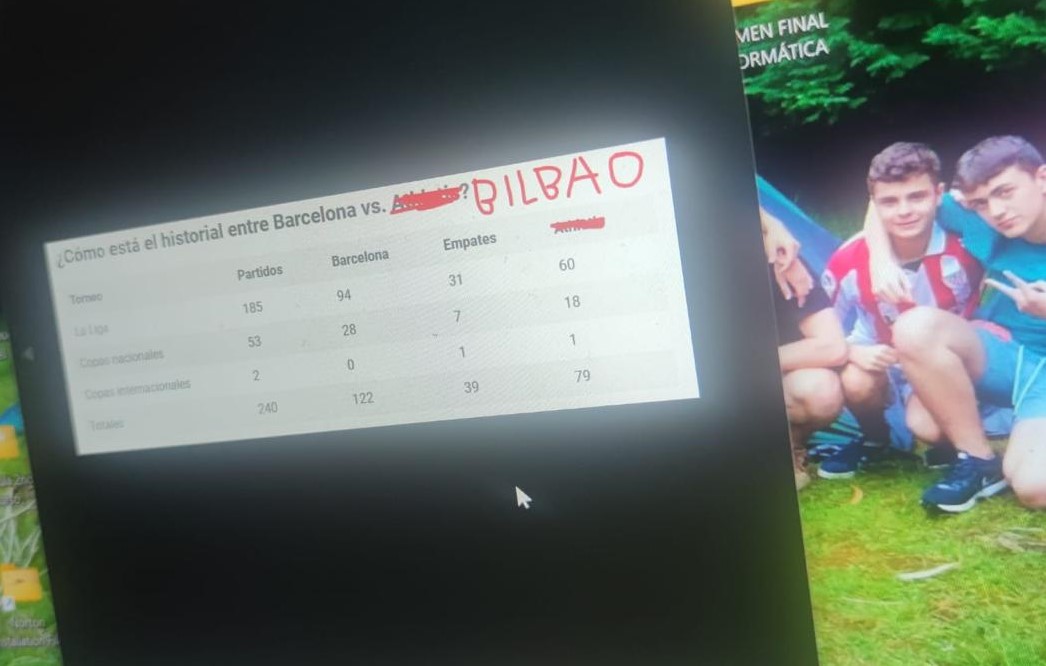
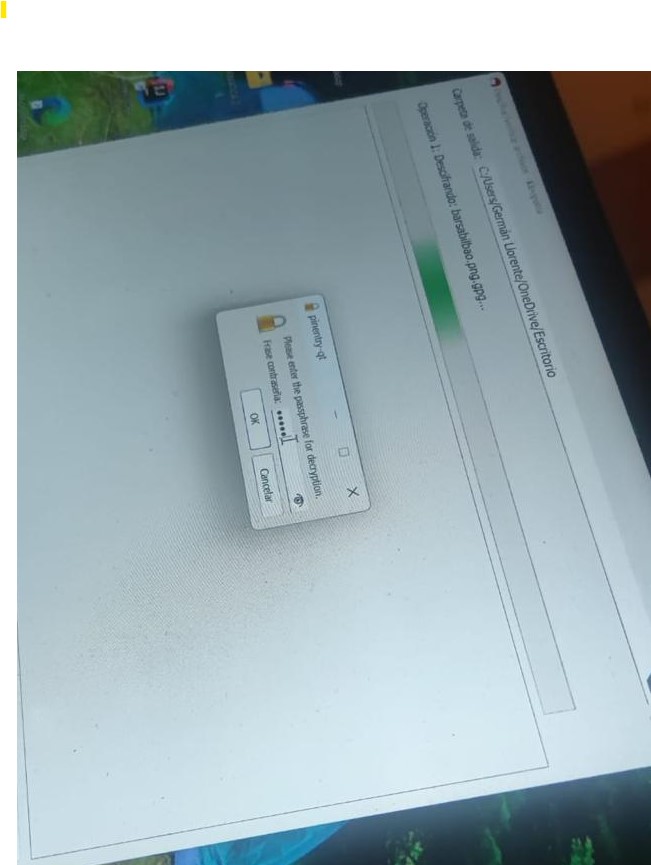
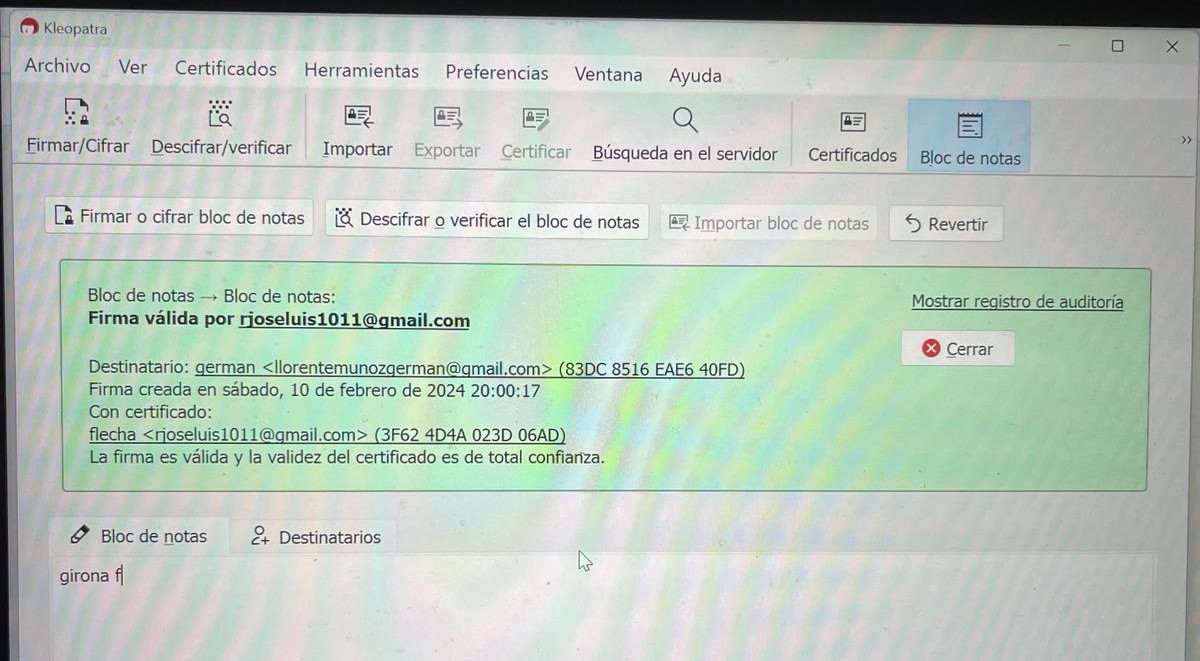
Para ello, hemos creado un par de llaves para el cifrado asimetrico y nos la hemos compartido,exportandola previamente.

Tras esto, podemos proceder a realizar los cifrados. Vamos a realizar el cifrado de un archivo.png .

Para ello exportaremos el archivo.png y con click derecho cifraremos y firmaremos la imagen, el cifrado sirve para que solo las personas que hayas añadido a destinatarios del archivo(solo tendrás opción de compartirlas con personas que ya hayas certificado dentro de Kleopatra gracias a su clave pública) podrán ver el contenido del archivo(Cabe destacar que cuanto más larga y compleja sea la contraseña, más segura será la protección del archivo) y la firma sirve para cerciorarse del emisor del archivo.

Una vez hecho este paso, el siguiente es compartir el archivo y una vez que lo tengas, descifrarlo y ver el contenido.

Texto

Descripción generada automáticamente

Cabe destacar que hemos probado a compartir el archivo a Carlos, no tiene nuestras clave publicas ni nosotros las suyas ni tampoco compartimos con él desde kleopatra el archivo, y no tuvo acceso al contenido del archivo).

Finalmente hemos compartido y visualizado el contenido poniendo la contraseña y hemos comprobando su funcionamiento.