Apartado 1: GPG en GNU/Linux

Usando la herramienta GPG para GNU/Linux, lleva a cabo las siguientes acciones relacionadas con la criptografía asimétrica:

1. Crea en una máquina virtual con GNU/Linux dos usuarios distintos llamados *user1* y *user2*, estableciendo para cada uno de ellos una contraseña segura.
2. Para el usuario *user1*, crea una pareja de claves pública/privada y publícala en uno de los servidores públicos usados para tal fin, por ejemplo, https://keyserver.ubuntu.com/.
3. Realiza una copia de seguridad de la pareja de claves que has generado.
4. Cambia al usuario *user2*. Crea una pareja de claves pública/privada y publícala en uno de los servidores públicos usados para tal fin, por ejemplo, https://keyserver.ubuntu.com/.
5. Realiza una copia de seguridad de la pareja de claves que has generado.
6. Importa desde el servidor de claves al anillo de claves del usuario *user2* la clave pública de *user1*. Muestra el anillo de claves resultante de *user2*.
7. Genera un documento de texto y llámalo *cifradoLinux_user2.txt*. Cífralo con la clave pública de *user1*. Envía por algún medio, el documento cifrado al usuario *user1*.
8. Descifra usando tu clave privada de *user1*, el documento *cifradoLinux_user2.txt*.

Enlace de interés:

https://www.genbeta.com/desarrollo/manual-de-gpg-cifra-y-envia-datos-de-forma-segura

Servidores de claves alternativos:

https://pgp.mit.edu/

https://www.rediris.es/keyserver/index.html.es

Apartado 2: Certificado Digital

Explica los pasos que deberías seguir para obtener un certificado de ciudadano o de usuario. Busca en la página web de CERES (Certificación Española), perteneciente a la Fábrica Nacional de Moneda y Timbre, www.cert.fnmt.es, información sobre dónde podemos utilizar el certificado digital. Si no posees un certificado digital, solicítalo en la página web citada en la actividad anterior siguiendo los pasos que allí te indican.

Indicaciones de entrega de la práctica

Deberás elaborar una memoria de la práctica que contenga los enunciados y sus soluciones. Para ello, deberás añadir capturas de pantalla que muestren todo el proceso seguido en la resolución de la práctica. Cada captura de pantalla debe ir acompañada del comentario o explicación correspondiente.

Deberás entregar un documento en formato pdf cuyo nombre contenga tus apellidos y nombre de la siguiente manera:

Apellido1_Apellido2_Nombre_UD5_Práctica1.pdf