# Instrucciones y aclaraciones

* Utiliza GPG para llevar a cabo la práctica.
* Para realizar este ejercicio, trabajaremos en parejas.

**Tarea 1 - Creación del par de claves**

Utilizando GNU PrivacyGuard, realiza las siguientes tareas:

1. Crea un par de claves pública-privada.
   1. Usa tu nombre y apellidos.
   2. Pon tu dirección de correo electrónico.
2. Exporta la clave. Nombre: [tu\_nombre.pub] (*naroa.pub*, por ejemplo).
3. Envía a tu pareja la clave pública .
4. Recoge el documento cifrado que te mande tu pareja, descífralo.
5. Manda a tu pareja el texto que aparece en el documento , demostrándole que has descifrado el mensaje.

**Tarea 2 - Envío de documento firmado**

1. Recoge la clave pública de tu pareja.
2. Crea un fichero de nombre tunombre\_prac (naroa\_prac, por ejemplo); escribe algo con sentido en él.
3. Cifra el fichero.
4. Firma el fichero tunombre\_prac.
5. Envía el fichero y el hash cifrados a tu pareja.