

UF1. [PAC02] CERTIFICADOS

Para la realización de las siguientes actividades deberéis ayudaros del libro de texto, capítulo 5, y consultar, si lo creéis necesario, internet.

Debéis subir un único archivo comprimido que contenga **UN ÚNICO DOCUMENTO PDF** con las respuestas teóricas, y las capturas de pantalla que expliquen los pasos realizados para la parte práctica.

Recordad que la fecha límite para la entrega de la PAC es el día 7 de JUNIO.

Actividades

Parte teórica

1. Explicar las diferencias entre los algoritmos de cifrado de clave pública y de clave privada. ¿Qué ventajas e inconvenientes tiene cada uno de ellos?
2. Explica para qué sirve firmar un correo.

Parte práctica

3. Crear un par de claves (pública y privada) con el programa GPG4win que lo podéis descargar de <https://www.gpg4win.org/download.html>, y después:
 - a. Mandar un correo a la siguiente dirección: agonzalez@ilernaonline.com con vuestra clave pública adjuntada, y el asunto: Clave Pública Nombre Apellido1 Apellido2.
 - b. Mandar un mensaje cifrado a agonzalez@ilernaonline.com con el asunto: Mensaje Cifrado Nombre Apellido1 Apellido2.

Entrega: Entregar la solución en una carpeta comprimida con el nombre nombre_apellido1_apellido2_NúmeroUF_NumeroPAC donde se incluya todos los archivos y documentos generados necesarios para la solución de estos ejercicios.