

E2: PRUEBA PRÁCTICA

Cifrado con GnuPG

Denominación del curso	IFCT0109. Seguridad Informática	Código curso:	23-38/002065
Denominación del MF/UF	MF0489_3 Sistemas seguros de acceso y transmisión de datos	Fecha:	21/10/2024
		Duración:	60 minutos
Nombre Docente Examinador	Benito Manuel González Rodríguez	Firma Docente	
Nombre y apellido del alumno/a DNI		Firma Alumno	
		Nota Obtenida	

INTRUCCIONES PARA EL/LA ALUMNO/A

⇒ DESCRIPCIÓN GENERAL DE LA PRÁCTICA:

GnuPG es una implementación completa, gratuita y abierta de **OpenPGP**. Es un estándar para el cifrado en muchas distribuciones de Linux y se usa principalmente a través de la línea de comandos.

GnuPG no es una herramienta sofisticada de ninguna manera, y no podrá usarla para cifrar un disco duro completo o configurar una caja de seguridad. Aun así, si tiene algunos datos por ahí, o tal vez un mensaje para enviar, esta aplicación es imprescindible en Linux.

Características notables

- El cifrado de **GnuPG** admite múltiples algoritmos, como **RSA, ECDH, ECDSA, EdDSA, Elgamal, DSA, AES, Camellia, 3DES, Twofish, SHA2** y más.
- Es multiplataforma y se ejecuta en **Mac, Windows** y todos los sistemas similares a Unix como **Linux y BSD**.
- Se puede utilizar para encriptar comunicaciones o archivos de datos.



⇒ INSTRUCCIONES ESPECÍFICAS:

TAREA 1.- Descargar e instalar GnuPG en 2 equipos. Cifrar un archivo en un equipo. Descifrar archivo en otro equipo.

TAREA 2.- Desarrollar una memoria en procesador de textos en la que se desarrollen los apartados solicitados.

TAREA 3.- Subir la memoria a la plataforma

⇒ EQUIPO Y MATERIAL:

Ordenador con conexión a Internet, navegador y procesador de textos.

⇒ DURACIÓN DE LA PRUEBA:

El tiempo estimado de la prueba es de 60 minutos