# Guía Completa de GPG: Cifrado Asimétrico, Firmas Digitales e Intercambio de Claves Públicas


**¿Qué es GPG?:** GPG, o GNU Privacy Guard, es una herramienta de cifrado que permite asegurar la confidencialidad, integridad y autenticidad de los datos mediante el uso de criptografía asimétrica. Este tipo de criptografía utiliza dos claves: una clave pública, que puede ser compartida libremente, y una clave privada, que debe mantenerse en secreto.

GPG es compatible con el estándar OpenPGP y se utiliza ampliamente no solo para cifrar mensajes y archivos, sino también para firmar digitalmente documentos, verificar la autenticidad de firmas, gestionar certificados, y más.

**Funciones Clave de GPG y Escenarios de Uso**

1. Cifrado de Mensajes y Archivos: GPG permite cifrar mensajes y archivos para protegerlos de accesos no autorizados. Solo el destinatario, que posee la clave privada correspondiente, puede descifrar el contenido.

2. Firmas Digitales: GPG se utiliza para crear firmas digitales que verifican la autenticidad y la integridad de un mensaje o archivo. Esto es crucial en entornos donde la confianza en la procedencia del mensaje es fundamental.

3. Verificación de Firmas: Permite verificar si un mensaje o archivo ha sido firmado digitalmente por una clave específica, lo que asegura que el contenido no ha sido alterado y proviene de la fuente legítima.

4. Gestión de Claves Públicas y Privadas: GPG facilita la generación, exportación, importación y revocación de claves, lo que permite a los usuarios administrar sus credenciales de cifrado de manera efectiva.

5. Autenticación de Identidad: En entornos de colaboración, como en el desarrollo de software, GPG se usa para autenticar identidades, garantizando que los cambios en el código provienen de fuentes confiables.

# Ejercicio: Cifrado Asimétrico, Firmas Digitales e Intercambio de Claves Públicas

**Paso 1: Crear un Par de Claves (Pública/Privada)**

Comienza por generar tu par de claves, que utilizarás para cifrar documentos, firmar digitalmente y verificar la autenticidad de mensajes o archivos.

- gpg --gen-key

Descripción:Inicia el proceso de generación de un par de claves GPG.
Se te pedirá que elijas las características de la clave, como tipo, tamaño y fecha de expiración.

1. Asocia tu nombre y correo electrónico con las claves.
2. Define una contraseña para proteger tu clave privada.

**Paso 2: Verificar las Claves Generadas**

Puedes listar todas las claves generadas y almacenadas en tu sistema utilizando:

gpg -k

**Descripción:** Lista todas las claves públicas y privadas disponibles en tu llavero.
Es útil para verificar que tus claves se han generado correctamente.

**Paso 3: Crear y Exportar la Clave Pública para Compartir**

Para que otros puedan enviarte mensajes cifrados o verificar tu firma, debes exportar y compartir tu clave pública.

- gpg -a --export -o <Nombre_Archivo> <Identificador>

**Descripción:**

1. Genera un archivo en formato ASCII que contiene tu clave pública.
2. Puedes compartir este archivo con otras personas para que puedan cifrar mensajes que solo tú podrás descifrar.

**Paso 4: Importar Claves Públicas de Otros**

Para cifrar un mensaje o archivo para otra persona, primero necesitas importar su clave pública.

- gpg --import <archivoclavepublica>

**Descripción:** Este comando agrega la clave pública del archivo especificado a tu llavero, permitiéndote utilizar para cifrar mensajes dirigidos a esa persona.

**Paso 5: Cifrar un Documento con la Clave Pública**

Una vez que tienes la clave pública del destinatario, puedes cifrar un archivo para que solo esa persona pueda descifrarlo.

- gpg --encrypt --recipient <uid o email> <archivo_texto_claro>

**Descripción:** Cifra el archivo especificado para que solo el destinatario pueda descifrarlo con su clave privada.

**Paso 6: Descifrar un Documento Cifrado**

Si recibes un archivo cifrado, puedes descifrarlo usando tu clave privada.

- gpg --output <salida_archivo_texto_claro> --decrypt <archivo_cifrado>

**Descripción:** Descifra el archivo y guarda el contenido en un archivo de salida especificado.

**Paso 7: Firmar un Documento Digitalmente**

Firmar un documento asegura al receptor que proviene de ti y no ha sido alterado.

- gpg --sign <archivo>

**Descripción:** Crea una firma digital del archivo, asociando tu identidad con el documento.
Esto es útil para verificar la autenticidad y la integridad del documento.

**Paso 8: Verificar la Firma de un Documento**

Puedes verificar la firma digital de un documento para confirmar su autenticidad y origen.

- gpg --verify <archivo_firmado>

**Descripción:** Verifica la firma digital en el archivo, confirmando que fue firmado por la clave privada correspondiente y que no ha sido modificado desde la firma.

**Paso 9: Revocar una Clave (Opcional)**

Si tu clave privada se ve comprometida o ya no la necesitas, puedes revocar.

- gpg --gen-revoke <uid>

**Descripción:** Genera un certificado de revocación que deshabilita tu clave, evitando su uso futuro.