Comandos para el Cifrado Asimétrico de Clave Pública en Linux

🔑 Escenario

Supongamos que:

- Usuario **Alice** quiere enviar un mensaje secreto a **Bob**.
- Alice cifra el mensaje con la **clave pública de Bob**.
- Bob lo descifra con su **clave privada**.

📌 Pasos y comandos

1. Bob genera su par de claves

```bash
gpg --gen-key
```

👉 Se te pedirá: nombre, correo, contraseña de la clave, etc.

Esto genera dos claves:

- **Clave pública** (para compartir).
- **Clave privada** (secreta, solo para Bob).

---

2. Bob exporta su clave pública y se la da a Alice

```bash
gpg --armor --export bob@example.com > bob_public.key
```

👉 El archivo `bob_public.key` contiene la clave pública de Bob.

Alice recibe ese archivo.

---

3. Alice importa la clave pública de Bob

```bash
gpg --import bob_public.key
```

---

4. Alice cifra un archivo con la clave pública de Bob

Supongamos que Alice quiere enviar `mensaje.txt`.

```bash
gpg --encrypt --recipient bob@example.com mensaje.txt
```

👉 Esto genera el archivo `mensaje.txt.gpg`, que está cifrado.
Solo Bob podrá descifrarlo con su clave privada.

---

5. Bob descifra el archivo

```bash
gpg --output mensaje_descifrado.txt --decrypt mensaje.txt.gpg
```

👉 Ahora Bob obtiene el contenido original en `mensaje_descifrado.txt`.

✅ Resultado final

- Alice nunca usó ni necesitó la clave privada de Bob.
- Nadie que intercepte el archivo cifrado podrá leerlo, solo Bob (con su clave privada).
