Cifrado Asimétrico y Seguridad de Claves

1. ¿Qué ventajas tiene el cifrado asimétrico?

- Permite compartir información de forma segura sin necesidad de intercambiar claves previamente.
- Se utiliza una pareja de claves: una pública para cifrar y una privada para descifrar.
- Aporta autenticación (firma digital) y confidencialidad.
- Facilita el establecimiento de canales seguros (como HTTPS).
- Escalable y práctico en redes abiertas y ambientes distribuidos.

2. ¿Qué posibles fallas de seguridad pueden existir?

- Si un atacante accede a la clave privada, puede descifrar toda la información cifrada.
- Vulnerabilidades en el software o implementación (como algoritmos débiles o errores de codificación).
- Suplantación de identidad si se falsifica una clave pública.
- Ataques de intermediario (man-in-the-middle) si no se verifica la autenticidad de las claves públicas.

3. ¿Qué sucede si pierdo mi clave privada? ¿Qué sucede si la comparto?

- Si pierdes tu clave privada, no podrás descifrar mensajes cifrados para ti ni firmar digitalmente documentos.
- Si compartes tu clave privada, cualquier persona podrá hacerse pasar por ti, firmar documentos en tu nombre o leer tus mensajes cifrados.
- La clave privada debe mantenerse en absoluto secreto y respaldarse adecuadamente en un entorno seguro.

Conclusión:

El cifrado asimétrico es poderoso y útil, pero su seguridad depende totalmente de la protección de

la clave privada.