**Cómo funcionan las llaves públicas y privadas**

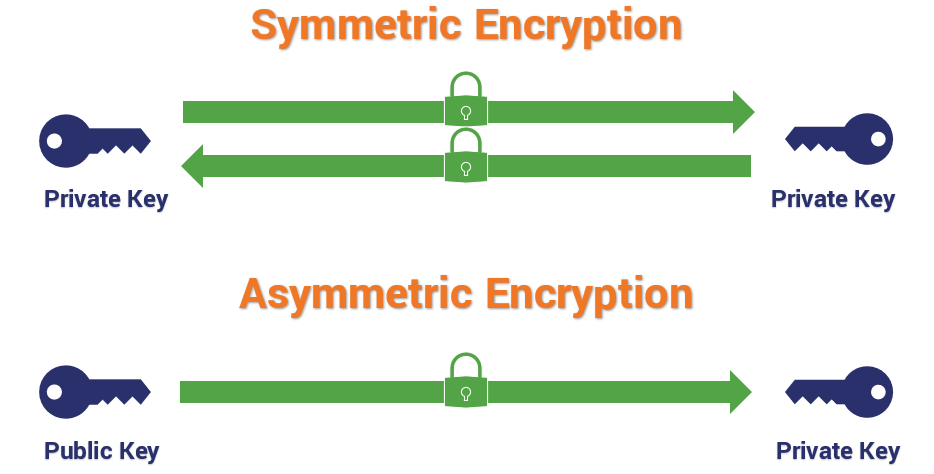
Las llaves públicas y privadas nos ayudan a cifrar y descifrar nuestros archivos de forma que los podamos compartir sin correr el riesgo de que sean interceptados por personas con malas intenciones.

La forma de hacerlo es la siguiente:

1. Ambas personas deben crear su llave pública y privada.
2. Ambas personas pueden compartir su llave pública a las otras partes (recuerda que esta llave es pública, no hay problema si la “interceptan”).
3. La persona que quiere compartir un mensaje puede usar la llave pública de la otra persona para cifrar los archivos y asegurarse que solo puedan ser descifrados con la llave privada de la persona con la que queremos compartir el mensaje.
4. El mensaje está cifrado y puede ser enviado a la otra persona sin problemas en caso de que los archivos sean interceptados.
5. La persona a la que enviamos el mensaje cifrado puede usar su llave privada para descifrar el mensaje y ver los archivos.

Puedes compartir tu llave pública pero nunca tu llave privada.

En la siguiente clase vamos a crear nuestras llaves para compartir archivos con GitHub sin correr el riesgo de que sean interceptados.

**Encriptación simétrica vs asimétrica**  
  
.  
**Encriptación simétrica:**

* Una sola llave es usada para encriptar y desencriptar.
* Es un método simple de encriptado.
* Requiere menos poder computacional.  
  .  
  .  
  **Encriptación asimétrica**
* Usa dos llaves: pública y privada.
* Es un proceso más complejo.
* Requiere más capacidad computacional por su complejidad.