

La clau privada, es una clau que pertany únicament a l'usuari i que s'utilitza per desenscriptar la informació xifrada amb la clau pública.

La clau pública es comparteix amb altres usuaris i es la que s'utilitza per xifrar la informació que després es desenscripta fent servir la clau privada

Per compartir arxius de manera segura, els usuaris han de generar una clau privada i una pública. La clau pública es comparteix amb els usuaris que volem intercanviar informació . Quan vulguem enviar un arxiu xifrat a un altre usuari, xifrem l'arxiu que volem enviar amb la clau pública del destinatari i aquest farà ús de la seva clau privada per desenscriptar la informació.