

Exercici 1

Nombre	Alejandro León	Curs	AMS2
--------	----------------	------	------

-
1. Explica la diferència entre les claus privades i les claus públiques i descriu quin paper juguen en la seguretat (amb les vostres paraules). Explica també com pots fer servir aquesta eina per compartir arxius de manera segura.

Claus privades:

-Aquestes claus són cadenes de dígit que s'han de mantenir en secret. Amb aquestes es pretén desxifrar la informació que s'ha xifrat prèviament amb una clau pública. Només el propietari de la clau privada ha de ser capaç de fer això.

Claus públiques:

-Aquestes claus són cadenes de dígit que es poden compartir amb altres usuaris. Amb aquestes es pretén xifrar informació que després haurà de ser desxifrada amb la seva clau privada corresponent.

Per compartir arxius de manera segura amb claus privades i claus públiques, l'usuari haurà de generar una clau pública i una clau privada. La clau pública podrà ser compartida amb més usuaris i, d'aquesta manera, podrà rebre arxius xifrats i desxifrar-los amb la seva clau privada. D'aquesta manera, es garanteix la privadesa i seguretat de la informació.