ACTIVITAT
Objectius: - Aprendre a generar claus privades en Linux
Instruccions: - Es tracta d'un treball en grups de dos - Responeu a l'espai de cada pregunta, si ho feu amb diapositives enganxeu la diapositiva en aquest mateix espai. - Es valorarà la cura en la presentació del document i que segueixi l'estructura indicada.
Criteris d'avaluació: - Cada pregunta té el mateix pes - Es valorarà la presentació i els comentaris al codi
Entrega: - Aquest document anomenat **memoria.pdf** amb les explicacions i captures necessàries, i també els arxius adjunts necessaris del codi que es demana dins d'un .zip anomenat: **PR32-NomCognomNomCognom.zip**

Noms i Cognoms: Joel Berzal Álamo

Materials:

Aquest és un treball d'investigació al web, feu servir els recursos que cregueu convenients.

Feu servir Google per buscar els tutorials que us serveixin millor.

Tasca:

- Exercici 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.

Juntament amb el codi, entrega un "exercici1.pdf" on hi hagin les explicacions d'aquest exercici.

Tant les claus privades i com les públiques són components essencials en la criptografia de clau asimètrica, un mètode criptogràfic que fa servir dues claus per dur a terme diverses funcions de seguretat, com per exemple el xiframent i la signatura digital.

Malgrat que ambdues tenen aquest àmbit en comú, aquestes claus tenen una diferència clara: la distribució de les seves dades. Mentre que les claus privades es mantenen i mai són compartides amb altres persones, ja que la seguretat del sistema depèn en gran mesura de la confidencialitat d'aquest tipus de clau, les clau públiques poden distribuïr-se àmpliament sense comprometre la seguretat del sistema.

Aquestes claus també es poden fer servir per compartir arxius de manera segura, sempre i quan es segueixi el procediment següent:

1) Cadascun dels usuaris ha de generar dues claus (una privada i una pública). La clau privada ha de mantenir-se en secret, mentre que la pública es comparteix lliurament.

2) Cadascun dels usuaris comparteix la seva clau pública als demés a través d'un servidor de claus, d'un correu electrònic o d'uns altres mitjans segurs.

3) Quan un usuari desitgi compartir un arxiu de manera segura amb algú, ha de fer servir la clau pública del destinatari per xifrar l'arxiu. Això garantitza que només el posseïdor de la clau privada corresponent pot desxifrar l'arxiu.

4) L'usuari envia l'arxiu xifrat al destinatari.

5) El destinatari fa servir la seva clau privada per desxifrar l'arxiu. Donat que només el destinatari té la clau privada corresponent, es garantitza que només ell/a pot accedir al contingut original de l'arxiu.