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: **Pablo Mejías Torvisco**

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

Tasques:

- Exercici 0 - Us caldrà una llibreria per fer servir una llibreria GPG en Java, configureu 'maven' per tal que funcioni.

- 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.

Cada usuari té una clau de cada tipus, la pública que utilitza per poder xifrar i la privada que només té ell i serveix per poder desxifrar missatges xifrats per la seva mateixa clau.
Un exemple seria una comunicació xifrada, en la que l'usuari A envia la seva clau publica al B i viceversa, ara si l'usuari A vol enviar un missatge al B, codificarà el seu missatge amb la clau pública del B. Després el receptor descodificarà el missatge amb la seva clau privada, evitant així que si algú interceptés el missatge durant l'enviament el puguis desxifrar.

- Exercici 2 - Fes un programa JAVAFX amb la següent estructura:

- 1a pantalla, demana si es vol encriptar o desencriptar un arxiu

- 2a pantalla:
  Permet escollir l'arxiu a encriptar/desencriptar
  Permet escollir la clau pública/privada (segons correspon)
  En cas de desencriptar cal també un camp per posar la contrasenya
  Permet definir el nom d'arxiu on es guarda el resultat
  Permet tornar a la pantalla anterior

- 3a pantalla, executa l'acció i mostra el resultat (OK o Error)
  Permet tornar a l'inici