UF1 00 PR1.1 Encriptació en JAVA

Enllaç al github: https://github.com/achivaq01/Encriptacion

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.

Les Claus públiques i privades, són components són dos claus generats matemàticament que estan relacionades entre elles per ser utilitzades en criptografia.
Les claus privades tenen la funció de desxifrar la informació xifrada amb la seva clau pública. És recomanable mantenir-les secretes per evitar filtracions d'informació. En contraposició, les claus públiques tenen la funció de xifrar informació, la qual només pot ser desxifrada fent servir la seva clau privada.

Es considera que aquestes claus són segures, ja que encara que estan matemàticament relacionades, és molt difícil derivar una de les claus a partir de l'altre.

Aquesta eina s'utilitza seguint el següent procediment:

1. Generar claus públiques i privada.
2. Fer servir la clau pública per encriptar la informació desitjada.
3. Enviar la informació xifrada juntament amb la clau privada a qui es vulgui compartir la informació
4. Fer servir la clau privada per desxifrar la informació