Claus privades i claus publiques

1. Diferencia claus privades i claus publiques:

- **Claus privades**: Les claus privades son un tipus de clau secreta que únicament pertany al seu propietari. Generalment aquestes no han de ser compartides amb altres persones.

Son utilitzades per desencriptar missatges o arxius que han estat encriptats fent ús de la clau publica corresponent. Generalment aquest tipus de claus son utilitzades per propostes d'autentificació, ja que si un arxiu es encriptat utilitzant una clau privada, qualsevol persona amb una clau publica corresponent a aquesta, pot verificar que l'arxiu ha estat encriptat per el propietari corresponent de la clau privada.

- **Claus publiques**: Les claus publiques són compartides de forma oberta i distribuïdes àmpliament. Són utilitzades per encriptar missatges que únicament el propietari amb la corresponent clau privada pot desencriptar. Això fa que tot i que la clau publica la tingui un gran nombre de gent, la clau privada es manté igualment en secret només per el seu propietari.

Les claus publiques son utilitzades generalment per establir canals de comunicació, firmes digitals o verificar qui ha enviat un arxiu encriptat.

2. Seguretat amb claus publiques i privades:

- **Confidencialitat**: Les claus publiques i privades generalment es fan servir entre elles per proporcionar confidencialitat. Una persona que vol enviar a un altre un missatge o arxiu, utilitzaria la clau publica de la persona a la que vol enviar aquest missatge i el receptor es l'únic que pot desencriptar-ho fent ús de la seva clau privada.

- **Autentificació**: Les claus privades permeten l'autentificació d'un usuari ja que funcionen com a firma digital degut a que es troben connectades al seu propietari. D'aquesta forma un arxiu encriptat amb una clau privada, permet a una persona amb la corresponent clau publica verificar que ha estat enviat per el propietari de la clau privada.

- **Integritat**: Les firmes digitals per part de les claus privades permeten assegurar certa integritat per als missatges ja que si el contingut es modificat, la verificació fallarà fent saber al receptor que un extern ha interactuat amb el contingut.

3. Ús de les claus privades i publiques en la encriptació

Per tal de fer-ne ús d'aquestes claus en el moment de realitzar la encriptació corresponent haurem de seguir unes passes sense les quals la comunicació seria impossible:

1. **Generació de claus**: Inicialment, les dos (o més) persones que volen formar part de la comunicació generaren el seu propi parell de claus (publica i privada). Les claus publiques es compartiren amb les altres persones que pertanyen a l'intercanvi mentre que la privada, com el seu nom s'indica, no ha de ser compartida.

2. **Encriptació de fitxer**: L'emissor agafarà la clau publica del receptor a qui vol enviar el missatge. Encriptarà l'arxiu fent ús d'aquesta assegurant-se que només el receptor corresponent podrà desencriptar-ho fent ús de la seva clau privada.
3. **Enviament del missatge**: L'emissor enviarà el missatge al receptor a través d'un medi segur que sigui convenient. Alguns exemples d'això poden ser un email a través de gmail, un missatge de text a través de plataformes com Whatsapp o Telegram, etc.
4. **Desencriptació del missatge**: El receptor en fa ús de la seva clau privada per desencriptar el missatge i accedir al seu contingut. Com la clau publica correspon a la seva clau privada, ell es l'únic amb la capacitat de realitzar aquesta acció.

Tot aquest procés, tot i que no sembla tant habitual sol realitzar-se a tots llocs on a través d'internet hi ha comunicació entre dos persones, únicament que el procés es realitza de forma automàtica per el sistema/aplicació ja que connecta una clau privada o publica al nostre perfil/usuari.