



Pràctica : gpg4win



Amb l'aplicació de xifratge asimètric per a Windows **gpg4win**

1. Baixar i instal·lar gpg4win

- Generar claus .Desplegar opcions avançades. Utilitza Rsa4096 i data expiració 6 mesos
- Exporta la clau pública
- Envia a tots els companys de classe (i tu rebràs les claus públiques dels teus companys)
- Importa les claus públiques dels teus companys

2. Xifrat simètric

Crea un fitxer de text amb notepad i Xifra'l amb una clau simètrica.

- Quina extensió té l'arxiu xifrat?
- On es guarda?

3. Xifrat asimètric

Ja tenim les nostres claus i les claus públiques dels companys/es

- Xifrar fitxer amb clau pública de company/a i enviar-la
- Rebre fitxer-xifrat destinat a nosaltres i desxifrar-lo amb la nostra clau privada
- Signar un fitxer amb la nostra clau privada i enviar-lo als companys
- Rebre fitxers signats per cada company. Verificar la seua autenticitat.

4. Canvia la passphrase de la teua parella de claus, la data de caducitat, el nom i el email.

Documentar el procés. I no oblidis seguir les indicacions del document de Aules "Com fer un treball". Documentar els errors o dificultats trobades i documentar-les explicant la solució adoptada . ==> Entregar el document en format PDF <==