



Pràctica : Cygwin



Cygwin és un entorn Unix i una interfície de línia d'ordres per a Microsoft Windows

Des de Windows.....

1. Baixar i instal·lar Cygwin. Afegir el mòdul gnupg2, i el mòdul vim
2. Entrar en la terminal de Cygwin i preparar les claus
 - Explora l'entorn de Cygwin
 - Generar claus (full-generate). Utilitza Rsa4096 i data expiració 6 mesos
 - Exporta la teua clau pública
 - Des de Windows, on estan les claus ?
 - Envia a tots els companys de classe (i tu rebràs les claus públiques dels teus companys)
 - Importa les claus públiques dels teus companys
3. Xifrat simètric

Crea un fitxer de text amb l'editor **vi** i Xifra'l amb una clau simètrica.

 - Quina extensió té l'arxiu xifrat?
 - On es guarda?
4. 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
5. Canvia la passphrase de la clau privada. Canvia la data de caducitat.

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 <==