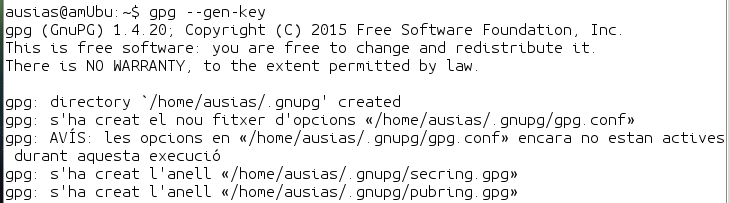
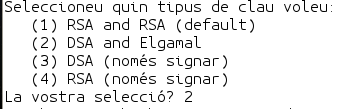
| Nom i cognoms: Òscar Rodríguez |  |
| --- | --- |
| Data:7/12/2022 |  |
| Nom de l’activitat/pràctica: ACT424 |  |

**Objectiu: xifrar fitxers amb algoritmes asimètrics mitjançant l'eina gpg.**

**Desenvolupament:**

**a) El primer pas serà generar un parell de claus de criptografia asimètrica, la nostra pròpia clau pública i clau privada. Quina comanda usaràs?**  Utilitzare la comanda gpg –gen-key

**b) Durant el procés de generació de claus ens preguntarà diversos detalls. El primer és el tipus de clau. Els noms corresponen amb el tipus d'algoritme asimètric associat, és a dir, una clau de tipus DSA s'utilitza en un algoritme DSA, per exemple. Per què les dues primeres opcions ens ofereixen dos algoritmes? Ara tria la segona opció, què té algoritmes diferents, i així veurem clarament quan s'utilitza cada clau.** Seleccionem l’opció 2

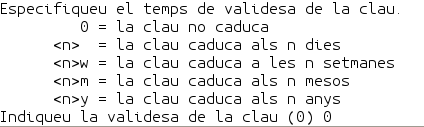
****

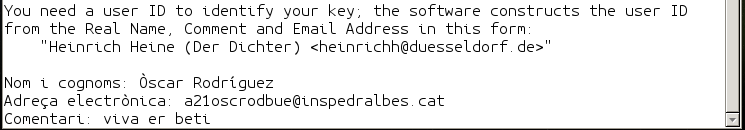
**c) A continuació ens preguntarà la grandària de la clau de l'algoritme DSA. Indica que la faci de 1024(perquè trigarà menys en generar-la que una de 2048...).**

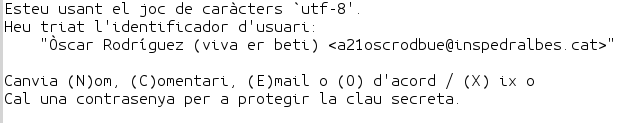
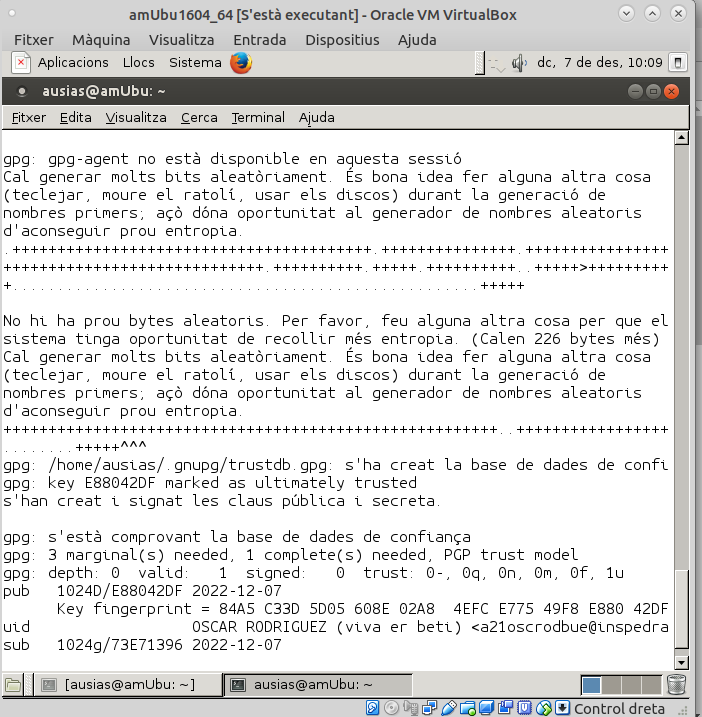
Indiquem el volum

****

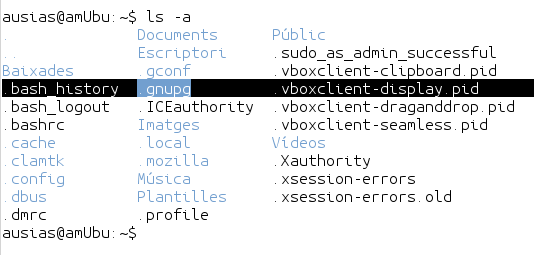
**d) La següent pregunta és el període de validesa de la clau. Li trobes sentit a que una clau caduqui? Per què? Ara tria que mai caduqui.** Si, per protegir el nostre equip.

****

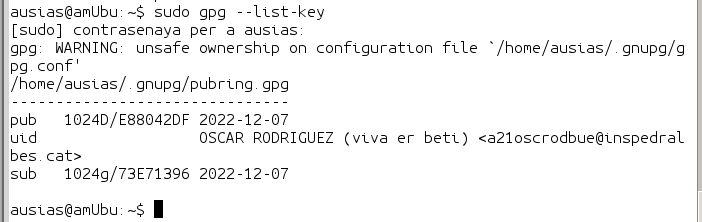
**e) Ens demanarà algunes dades per identificar la clau. Per què creus que cal identificar-la? A continuació segueix els passos, fins que et generi les dues claus: veuràs que et crearà una clau primària de tipus DSA amb mida de clau 1024 (pub) i una clau subordinada de tipus Elgamal amb mida de clau 1024 (sub).** 

****

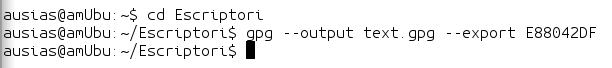
**f) Al directori home s'haurà creat un directori ocult .gnupg, on estan els fitxers interns que utilitza l'eina gpg. El fitxer pubring.gpg conté les claus públiques i el fitxer secring.gpg, les claus privades. Intenta veure el ontingut d'aquestos fitxers, què passa?**

****

**g) Per mostrar o llistar les claus que tenim utilitzem el paràmetre list-keys (man gpg), llista-les.**

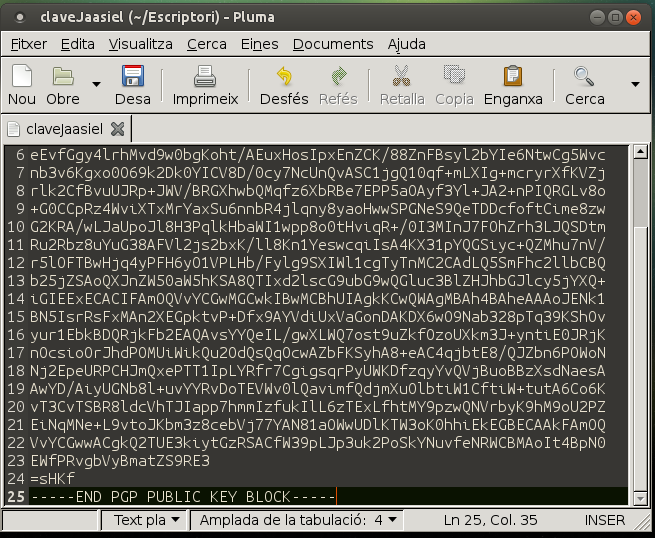
****

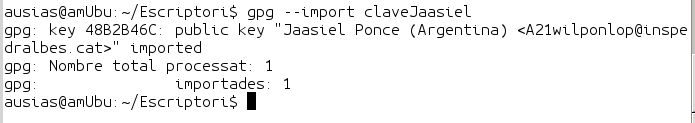
**h) Ara haurem de comunicar la nostra clau pública a qui estigui interessat en enviar-nos un missatge xifrat (algun company). Primer hem d'exportar-la amb el paràmetre export (man gpg), fes-ho. Passa la clau a algun company.**

****



**i) Ara importa la clau que t'ha passat algun company a tu. Utilitza el paràmetre import i després llista les claus disponibles amb el paràmetre list-keys.**

****

****

****

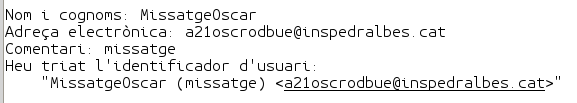
**j) Seguidament crea un fitxer anomenat missatgeNomTeu i xifra'l per enviar-lo al company, usant la clau pública que ell t'havia passat prèviament. Els paràmetres que hauràs d'usar són: -v, -a, -o, --encrypt i --recipient. Explica què és cada paràmetre.**

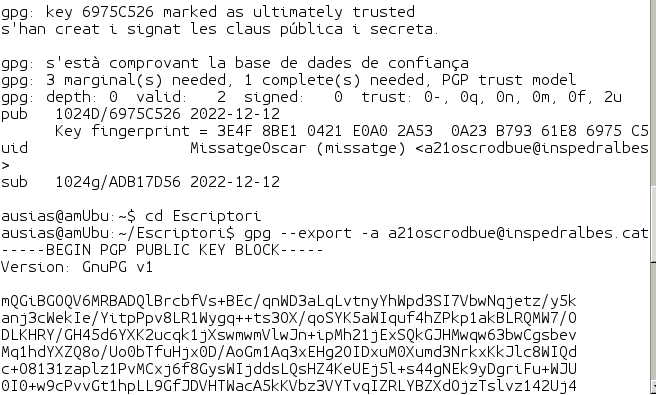
-v: mostra els detalls específics

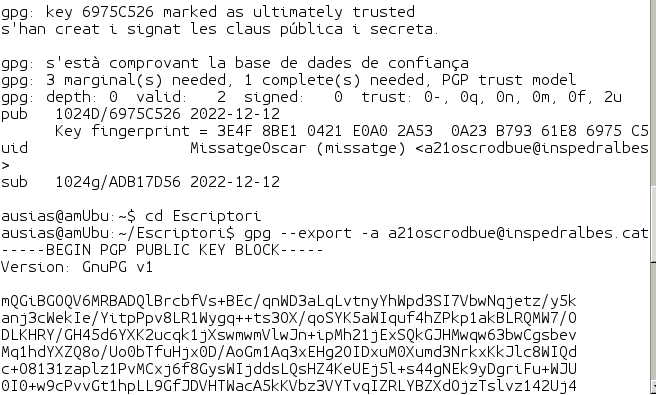
-a: crea la sortida amb ascii

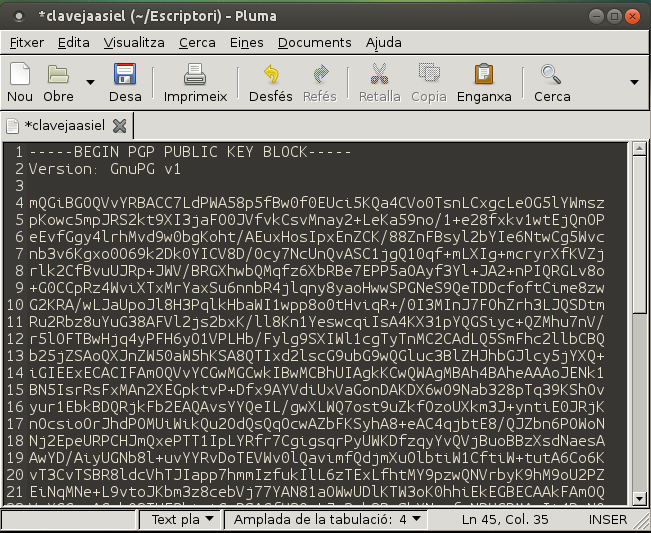
-o: arxiu de sortida

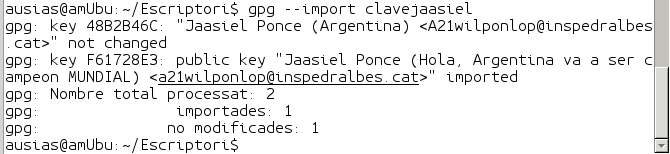
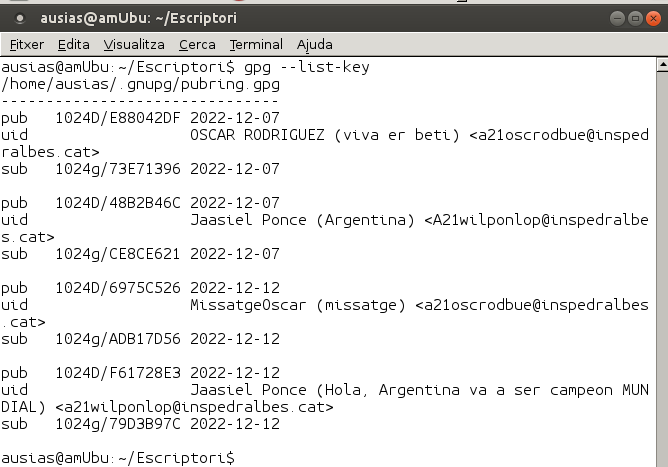
–encrypt: comanda que encripta un missatge, necessita la clau pública del destinatari.

–recipient: comanda que es fa servir una vegada per a cada destinatari, especifica la clau pública amb què serà xifrat el document.





**k) A continuació, envia el missatge anterior al company i que ell t'enviï el seu. Intenta desxifrar-lo. Que es vegi bé la comanda que uses. Si has introduït bé la contrasenya apareixerà el missatge que t'ha enviat el company xifrat amb la teva clau pública**



**l) Comprova què passa si modifiques el fitxer encriptat original i després intentes desxifrar-lo. Quin error et dona?**