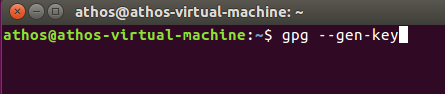
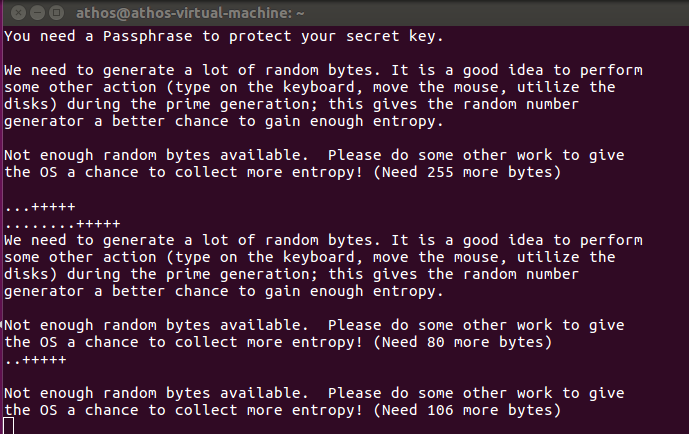
# Práctica 5.5: Cifrado asimético

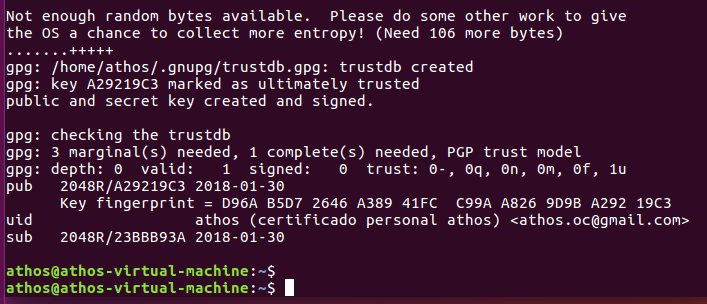
Lo primero que tenemos que hacer es crear la pareja de clave publica / clave privada. Esto lo haremos con el comando gpg –gen-key



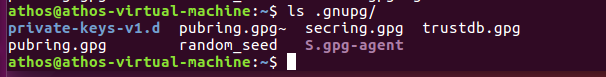
Nos pedirá el tipo de clave que queremos utilizar, en este caso vamos a seleccionar rsa

Mas tarde, después de poner los datos para nuestra clave, como nombre, email y descripción nos pedirá que abramos programas para que se generen bytes de forma aleatoria y generar una clave mas segura



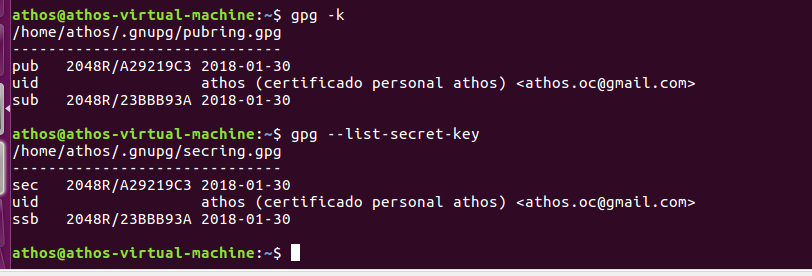
Luego veremos que nos ha creado nuestra clave 

Las claves se por defecto se crean el el directorio .gnupg con el nombre pubring.gpg y secring.gpg



## Ver claves generadas

Para ver las claves generadas lo haremos con gpg –k para ver la publica y con gpg –list-secret-key para ver la privada.



## Distribuir nuestra clave publica:

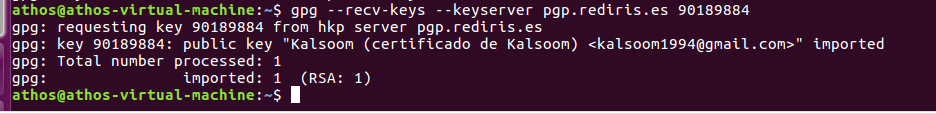
Ahora, una vez generada nuestra pareja de claves, deberíamos guardar nuestra clave privada a buen recaudo y distribuir nuestra clave publica. Para esto ultimo, podríamos enviar la clave por email, subirla a un servidor propio u otras muchas formas, pero en este caso, vamos a utilizar un servidor de claves de rediris.

Para enviar las claves utilizaremos el comando que se ve en la siguiente imagen, donde tendremos que especificar el servidor (pgp.rediris.es en este caso) y el identificador de nuestra clave.

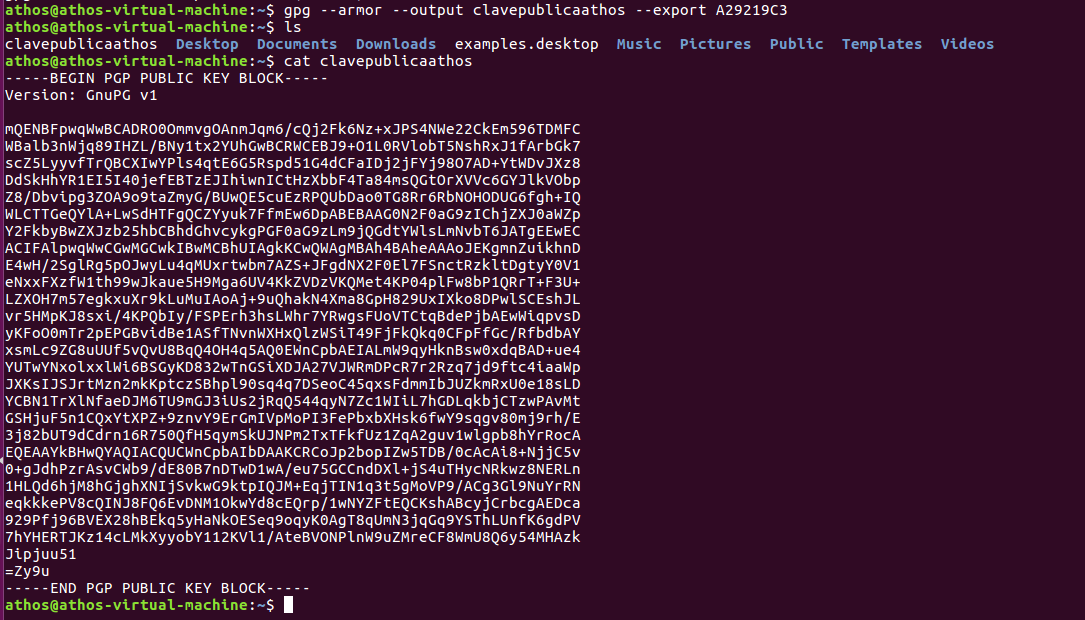


## Recibir claves:

Si queremos descargar la clave publica de alguna persona, tendremos que utilizar el comando como se muestra en la siguiente imagen, vemos que es igual que enviar las claves, sólo que cambiando el parámetro –send-keys por –recv-keys. Tendremos que especificar el id de la clave publica de la persona que queremos descargar su clave.

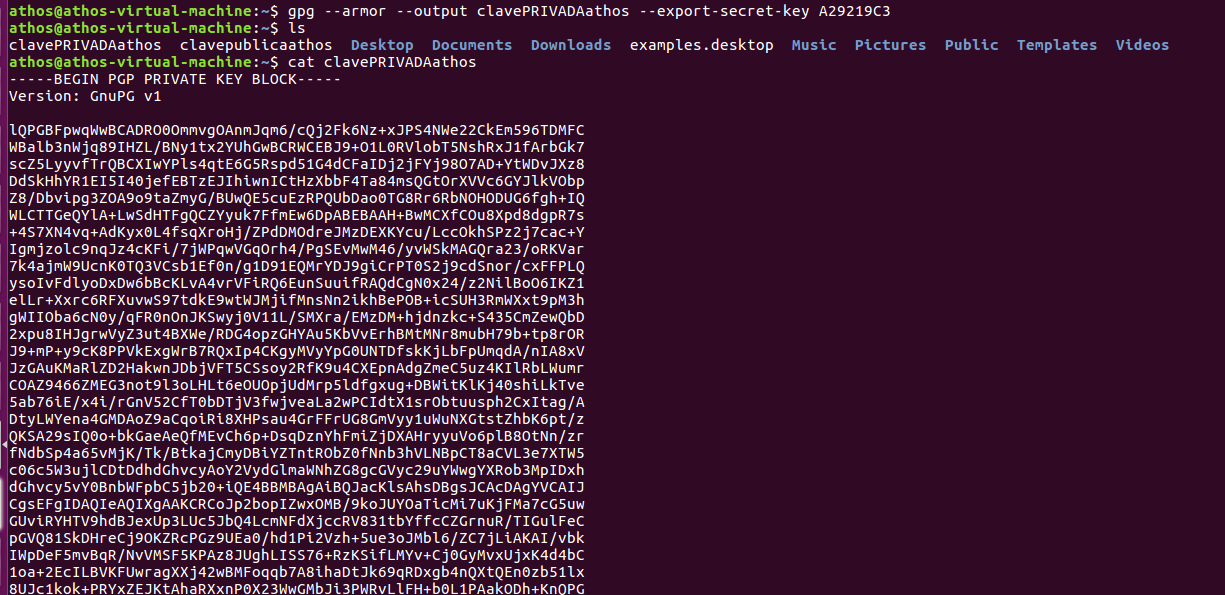


Si quisiéramos enviar nuestra clave publica por correo electrónico por ejemplo, primero deberíamos exportar nuestra clave como se puede ver en la siguiente imagen.



## Exportar nuestra clave privada:

Para poder exportar nuestra clave privada y guardarla en algún otro sitio como puede ser un pendrive o un cd, tendremos que hacerlo como se ve a continuación



Si hubiésemos recibido la clave por correo electrónico, deberíamos importarlo de forma manual a nuestro “llavero” de claves, esto lo hacemos de la siguiente forma.



Por si en algún momento quisiéramos revocar nuestro certificado, tendríamos que crear certificado de revocación ( lo utilizaremos en una de las siguientes practicas ).

Esto se hace como se ve en la siguiente imagen.

