

Abrimos nuestra maquina virtual
Creamos nuestra clave publica , mi clave de paso es Elpepazo1

```
usuario@usuario-VirtualBox:~$ gpg --full-generate-key
gpg (GnuPG) 2.2.19; Copyright (C) 2019 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Por favor seleccione tipo de clave deseado:
(1) RSA y RSA (por defecto)
(2) DSA y ElGamal
(3) DSA (sólo firmar)
(4) RSA (sólo firmar)
(14) Existing key from card
Su elección: 1
Las claves RSA pueden tener entre 1024 y 4096 bits de longitud.
¿De qué tamaño quiere la clave? (3072) 4096
El tamaño requerido es de 4096 bits
Por favor, especifique el período de validez de la clave.
  0 = la clave nunca caduca
  <n> = la clave caduca en n días
  <n>w = la clave caduca en n semanas
  <n>m = la clave caduca en n meses
  <n>y = la clave caduca en n años
¿Validez de la clave (0)? 1m
```

```
¿Es correcto? (y/n) y
GnuPG debe construir un ID de usuario para identificar su clave.
Nombre y apellidos: Francisco Usuario
Dirección de correo electrónico: usuario.sanchez.f@gmail.com
Comentarios:
No seleccionado este ID de usuario:
  "Francisco Usuario <usuario.sanchez.f@gmail.com>"
¿Cambia (N)ombre, (C)omentario, (D)irección o (V)ale/(S)alt? v
Si necesita generar muchos bytes aleatorios. Es una buena idea realizar
alguna otra tarea (trabajar en otra ventana/console, mover el ratón, usar
la red y los discos) durante la generación de números primos. Esto da al
generador de números aleatorios mayor oportunidad de recoger suficiente
entropía.
Si necesita generar muchos bytes aleatorios. Es una buena idea realizar
alguna otra tarea (trabajar en otra ventana/console, mover el ratón, usar
la red y los discos) durante la generación de números primos. Esto da al
generador de números aleatorios mayor oportunidad de recoger suficiente
entropía.
gpg: clave 1AA4E94A8C909775 marcada como de confianza absoluta
gpg: creado el directorio /home/usuario/.gnupg/openpgp-revocs.d
gpg: certificado de revocación guardado como /home/usuario/.gnupg/openpgp-revocs.d/719F5A5A50E712F600F74231AA4E94A8C909775.rev
Claves pública y secreta creadas y firmadas.
pub  rsa4096 2022-11-30 [SC] [caduca: 2022-12-30]
uid 719F5A5A50E712F600F74231AA4E94A8C909775
     Francisco Usuario <usuario.sanchez.f@gmail.com>
sub  rsa4096 2022-11-30 [S] [caduca: 2022-12-30]
```

Exportamos mi clave publica

```
usuario@usuario-VirtualBox:~/Descargas$ gpg -a -o usuario publica.asc --export usuario.sanchez.f@gmail.com
```

La subo al drive compartido

Compartido conmigo > SMR02 > franciscouser0 >			
Nombre	Propietario	Abierto última ve...	Tamaño de archivo
usuario publica.asc	Usuario	11-30-22 at 07:54 AM 8:53	3 kB

Descargamos la clave publica de otro
La importamos al llavero

```
usuario@usuario-VirtualBox:~/Descargas$ gpg --import daniel publica.asc
gpg: clave 8C17E663BA5A5999: clave pública "Daniel Cuadrado (patata) <jcuavor0110@g.educaand.es>" importada
gpg: Cantidad total procesada: 1
gpg: importadas: 1
```

Firmamos su clave , después nos pedirá nuestra clave de paso

```
usuario@usuario-VirtualBox:~/Descargas$ gpg --sign-key jcuavor0110@g.educaand.es
```

Frase de paso:

Introduzca frase contraseña para desbloquear la clave secreta OpenPGP:
"Francisco Usuario <usuario.sanchez.f@gmail.com>"
clave de 4096-bit RSA, ID 1AA4E94A8C909775, creada el 2022-11-30.

●●●●●●●●

☐ Guardar en gestor de contraseñas

Usuario 11-30-22 at 08:00 AM

CancelarOK

Encriptamos nuestra foto con su clave publica

```
usuario@usuario-VirtualBox:~/Descargas$ gpg -o usuario_para_dani.gpg -r jcuavor0110@g.educaand.es -e usuario.jpg
```

Se la subimos

Compartido conmigo > SMR02 > dani

Nombre	Propietario	Abierto última ve...	Tamaño de archivo
usuario_para_dani.gpg	yo	9:04	1,1 MB
dani publica.asc	Usuario 11-30-22 at 08:05 AM		3 kB

Listamos las claves publicas

```
usuario@usuario-VirtualBox:~/Descargas$ gpg --list-key
/home/usuario/.gnupg/pubring.kbx
-----
pub   rsa4096 2022-11-30 [SC] [caduca: 2022-12-30]
uid   [ absoluta ] Francisco Usuario <usuario.sanchez.f@gmail.com>
sub   rsa4096 2022-11-30 [E] [caduca: 2022-12-30]

pub   rsa4096 2022-11-24 [SC] [caduco: 2022-12-01]
uid   [ total ] Sergey Tereshkov (sergey) <sergey.simplente@gmail.com>
sub   rsa4096 2022-11-30 [E] [caduca: 2022-12-30]

pub   rsa4096 2022-11-30 [SC] [caduca: 2023-11-30]
uid   [desconocida] Adrian Castilla Lopez (hola) <adriex234@gmail.com>
sub   rsa4096 2022-11-30 [E] [caduca: 2023-11-30]

pub   rsa4096 2022-11-29 [SC] [caduca: 2022-12-29]
uid   [ total ] Francisco Fernández Carmona (Seguridad Cifrada Asimetrica) <franciscofdezcarmona0@gmail.com>
sub   rsa4096 2022-11-29 [E] [caduca: 2022-12-29]

pub   rsa4096 2022-11-30 [SC] [caduca: 2023-11-30]
uid   [ total ] CHENHAO (sluuu) <chenhao3090102@gmail.com>
sub   rsa4096 2022-11-30 [E] [caduca: 2023-11-30]

pub   rsa4096 2022-11-30 [SC] [caduca: 2023-11-30]
uid   [ total ] Gonzalo <gonzalogomez@gmail.com>
sub   rsa4096 2022-11-30 [E] [caduca: 2023-11-30]

pub   rsa4096 2022-11-29 [SC] [caduca: 2023-11-29]
uid   [ total ] Adrian Gutierrez villegas <agutierrezvillegas326@gmail.com>
sub   rsa4096 2022-11-29 [E] [caduca: 2023-11-29]

pub   rsa4096 2022-11-29 [SC] [caduca: 2023-11-29]
uid   [desconocida] Adrian Gutierrez <agutierrezvillegas326@gmail.com>
sub   rsa4096 2022-11-29 [E] [caduca: 2023-11-29]

pub   rsa4096 2022-11-30 [SC] [caduca: 2023-11-30]
uid   [desconocida] Adrian Gutierrez Villegas <agutierrezvillegas326@gmail.com>
sub   rsa4096 2022-11-30 [E] [caduca: 2023-11-30]

pub   rsa4096 2022-11-30 [SC] [caduca: 2023-11-30]
uid   [desconocida] Adrian <agutierrezvillegas326@gmail.com>
sub   rsa4096 2022-11-30 [E] [caduca: 2023-11-30]

pub   rsa4096 2022-11-29 [SC] [caduca: 2023-11-29]
uid   [ total ] online ezzokary (estudiante) <online@gmail.com>
sub   rsa4096 2022-11-29 [E] [caduca: 2023-11-29]

pub   rsa4096 2022-11-30 [SC] [caduca: 2023-11-30]
uid   [ total ] paco requena (francisco Requena) <franreke506@gmail.com>
sub   rsa4096 2022-11-30 [E] [caduca: 2023-11-30]

pub   rsa4096 2022-12-01 [SC] [caduca: 2023-12-01]
uid   [ total ] cristian (s4) <cristianlang@gmail.com>
sub   rsa4096 2022-12-01 [E] [caduca: 2023-12-01]

pub   rsa4096 2022-12-01 [SC] [caduca: 2027-11-30]
uid   [desconocida] online ezzokary (estudiante) <ezzokaryonline.snr1@gmail.com>
sub   rsa4096 2022-12-01 [E] [caduca: 2027-11-30]

pub   rsa4096 2022-11-30 [SC] [caduca: 2023-11-30]
uid   [ total ] IvánSaavedra <lvansaared@gmail.com>
sub   rsa4096 2022-11-30 [E] [caduca: 2023-11-30]

pub   rsa4096 2022-11-30 [SC] [caduca: 2023-11-30]
uid   [desconocida] IvánSaavedra <lvansaared@gmail.com>
sub   rsa4096 2022-11-30 [E] [caduca: 2023-11-30]

pub   rsa4096 2022-12-01 [SC] [caduca: 2023-12-01]
uid   [ total ] JoseFernandez <empirexont@gmail.com>
sub   rsa4096 2022-12-01 [E] [caduca: 2023-12-01]

pub   rsa4096 2022-12-01 [SC] [caduca: 2023-12-01]
uid   [desconocida] Jose Fernandez <empirexont@gmail.com>
sub   rsa4096 2022-12-01 [E] [caduca: 2023-12-01]
```

Vemos las claves privada

```
usuario@usuario-VirtualBox:~/Descargas$ gpg --list-secret-keys
/home/usuario/.gnupg/pubring.kbx
-----
sec   rsa4096 2022-11-30 [SC] [caduca: 2022-12-30]
uid   [ absoluta ] Francisco Usuario <usuario.sanchez.f@gmail.com>
ssb   rsa4096 2022-11-30 [E] [caduca: 2022-12-30]
```

Des-encryptamos las fotos de los demas

```
usuario@usuario-VirtualBox:~$ cd Descargas/
usuario@usuario-VirtualBox:~/Descargas$ gpg -o fotoguti --decrypt adrianparausero.gpg
gpg: cifrado con clave de 4096 bits RSA, ID 9E2A23E8B802F354, creada el 2022-11-30
"Francisco Usero <usero.sanchez.f@gmail.com>"
usuario@usuario-VirtualBox:~/Descargas$
```

Escribimos la clave de paso si nos lo pide



Aquí esta des-encryptada



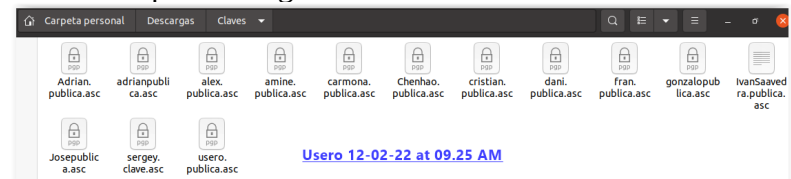
Las fotos que hemos des-encryptado de los demás



Esta es mi foto



Las claves que descargamos de los demás incluida la mía



Las encriptadas para los demás



Las encriptadas para mi

