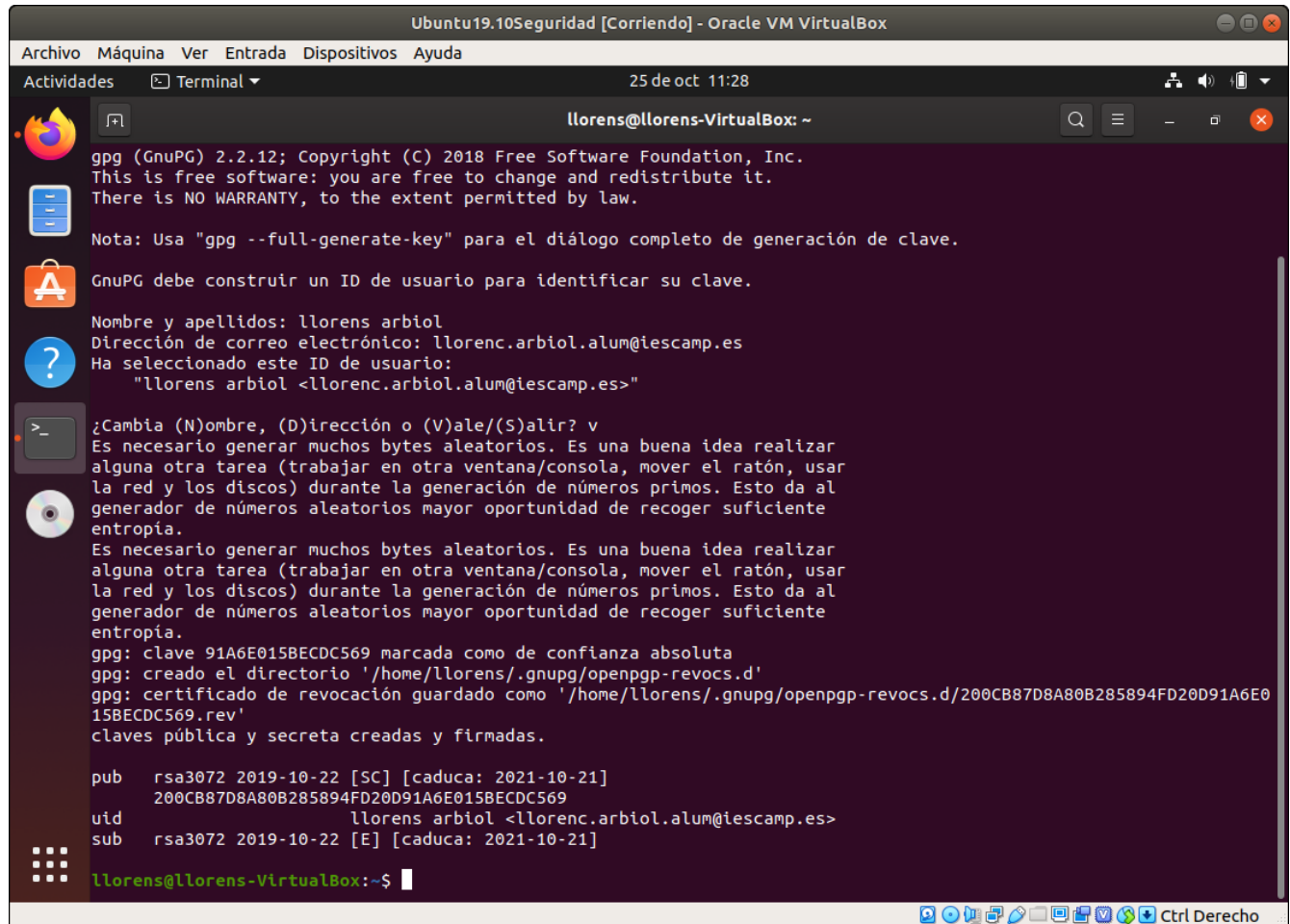


Cifrado asimétrico

Primeramente vamos a generar una clave con mi nombre



```
Ubuntu19.10Seguridad [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
Actividades  Terminal  25 de oct 11:28
llorens@llorens-VirtualBox: ~
gpg (GnuPG) 2.2.12; Copyright (C) 2018 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.

Nota: Usa "gpg --full-generate-key" para el diálogo completo de generación de clave.

GnuPG debe construir un ID de usuario para identificar su clave.

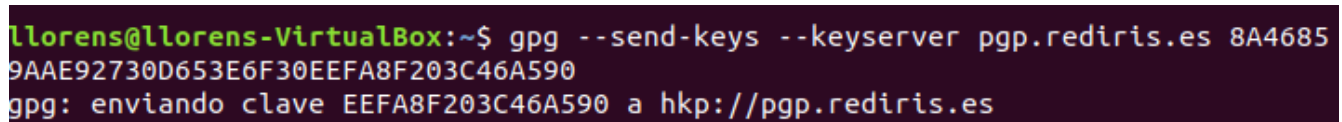
Nombre y apellidos: llorens arbiol
Dirección de correo electrónico: llorenc.arbiol.alum@iescamp.es
Ha seleccionado este ID de usuario:
"llorens arbiol <llorenc.arbiol.alum@iescamp.es>"

¿Cambia (N)ombre, (D)irección o (V)ale/(S)alir? v
Es necesario 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.
Es necesario 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 91A6E015BECDC569 marcada como de confianza absoluta
gpg: creado el directorio '/home/llorens/.gnupg/openpgp-revocs.d'
gpg: certificado de revocación guardado como '/home/llorens/.gnupg/openpgp-revocs.d/200CB87D8A80B285894FD20D91A6E015BECDC569.rev'
claves pública y secreta creadas y firmadas.

pub  rsa3072 2019-10-22 [SC] [caduca: 2021-10-21]
    200CB87D8A80B285894FD20D91A6E015BECDC569
uid                               llorens arbiol <llorenc.arbiol.alum@iescamp.es>
sub  rsa3072 2019-10-22 [E] [caduca: 2021-10-21]

llorens@llorens-VirtualBox:~$
```

Una vez creadas vamos a subirla a un servidor publico de claves



```
llorens@llorens-VirtualBox:~$ gpg --send-keys --keyserver pgp.rediris.es 8A4685
9AAE92730D653E6F30EEFA8F203C46A590
gpg: enviando clave EEFA8F203C46A590 a hkp://pgp.rediris.es
```

Cifrado asimétrico

Después verificaremos



Type	bits/keyID	cr. time	exp time	key expir
pub	3072R/BECDC569	2019-10-22		
uid	llorens arbiol <llorenc.arbiol.alum@iescamp.es>			
sig	sig3 BECDC569	2019-10-22		2021-10-21 [selfsig]
sub	3072R/D21C80DD	2019-10-22		
sig	sbind BECDC569	2019-10-22		2021-10-21 []

Vamos a tener ahora una copia a parte por seguridad

```
llorens@llorens-VirtualBox:~$ gpg --armor --output /home/llorens/claves/llorens  
--export 8A46859AAE92730D653E6F30EEFA8F203C46A590
```

Cifrado asimétrico

REVOCAR CLAVE

```
llorens@llorens-VirtualBox:~$ gpg -o revocacion.asc --gen-revoke 8A46859AAE9273
0D653E6F30EEFA8F203C46A590

sec  rsa3072/EEFA8F203C46A590 2019-10-25 llorenc.arbiol.alum@iescamp.es

¿Crear un certificado de revocación para esta clave? (s/N) s
Por favor elija una razón para la revocación:
Terminal
0 = No se dio ninguna razón
1 = La clave ha sido comprometida
2 = La clave ha sido reemplazada
3 = La clave ya no está en uso
Q = Cancelar
(Probablemente quería seleccionar 1 aquí)
¿Su decisión? 1
Introduzca una descripción opcional; acábela con una línea vacía:
>
Razón para la revocación: La clave ha sido comprometida
(No se dio descripción)
¿Es correcto? (s/N) s
se fuerza salida con armadura ASCII.
Certificado de revocación creado.

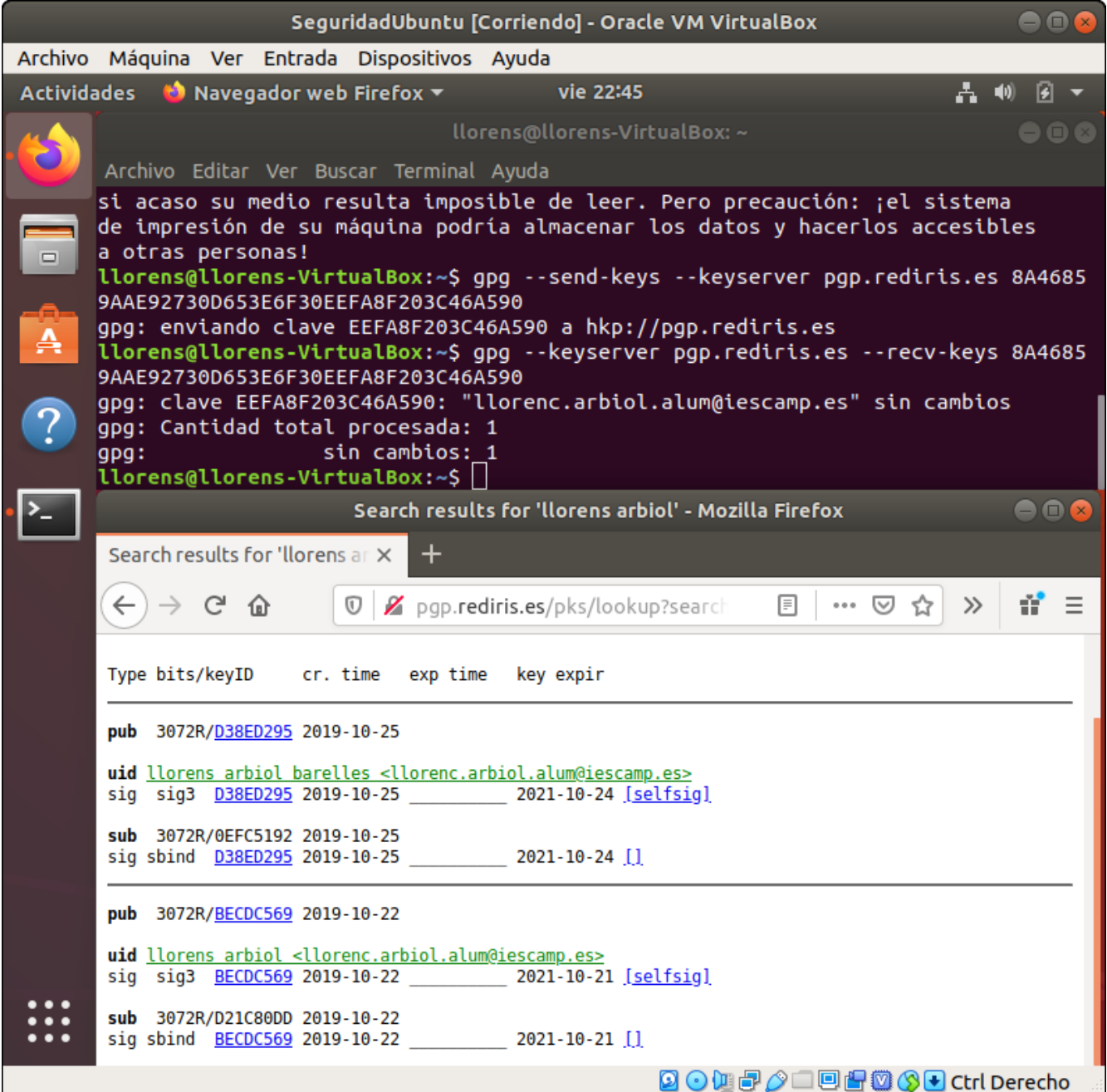
Por favor consérvelo en un medio que pueda esconder; si alguien consigue
acceso a este certificado puede usarlo para inutilizar su clave.
Es inteligente imprimir este certificado y guardarlo en otro lugar, por
si acaso su medio resulta imposible de leer. Pero precaución: ¡el sistema
de impresión de su máquina podría almacenar los datos y hacerlos accesibles
a otras personas!
llorens@llorens-VirtualBox:~$
```

Comunicamos a los servidores la revocación

```
llorens@llorens-VirtualBox:~$ gpg --send-keys --keyserver pgp.rediris.es 8A4685
9AAE92730D653E6F30EEFA8F203C46A590
gpg: enviando clave EEFA8F203C46A590 a hkp://pgp.rediris.es
llorens@llorens-VirtualBox:~$ 6~
```

Cifrado asimétrico

De momento no se actualiza en los servidores...



The screenshot shows a VirtualBox window titled "SeguridadUbuntu [Corriendo] - Oracle VM VirtualBox". Inside the VM, there is a terminal window and a Firefox browser window.

Terminal Window:

```
llorens@llorens-VirtualBox: ~  
Archivo Editar Ver Buscar Terminal Ayuda  
si acaso su medio resulta imposible de leer. Pero precaución: ¡el sistema  
de impresión de su máquina podría almacenar los datos y hacerlos accesibles  
a otras personas!  
llorens@llorens-VirtualBox:~$ gpg --send-keys --keyserver pgp.rediris.es 8A4685  
9AAE92730D653E6F30EEFA8F203C46A590  
gpg: enviando clave EEFA8F203C46A590 a hkp://pgp.rediris.es  
llorens@llorens-VirtualBox:~$ gpg --keyserver pgp.rediris.es --recv-keys 8A4685  
9AAE92730D653E6F30EEFA8F203C46A590  
gpg: clave EEFA8F203C46A590: "llorenc.arbiol.alum@iescamp.es" sin cambios  
gpg: Cantidad total procesada: 1  
gpg: sin cambios: 1  
llorens@llorens-VirtualBox:~$
```

Firefox Browser Window:

Search results for 'llorens arbiol' - Mozilla Firefox

Search results for 'llorens arbiol' X +

pgp.rediris.es/pks/lookup?search

Type	bits/keyID	cr. time	exp time	key expir
pub	3072R/D38ED295	2019-10-25		
uid	llorens arbiol barelles <llorenc.arbiol.alum@iescamp.es>			
sig	sig3 D38ED295	2019-10-25		2021-10-24 [selfsig]
sub	3072R/0EFC5192	2019-10-25		
sig	sbind D38ED295	2019-10-25		2021-10-24 [.]
pub	3072R/BECDC569	2019-10-22		
uid	llorens arbiol <llorenc.arbiol.alum@iescamp.es>			
sig	sig3 BECDC569	2019-10-22		2021-10-21 [selfsig]
sub	3072R/D21C80DD	2019-10-22		
sig	sbind BECDC569	2019-10-22		2021-10-21 [.]

Cifrado asimétrico

Esta practica ha sido un tanto rara, primero lo realice con Ubuntu 19.10 dado que a veces al ser versiones muy recientes suelen hacer cosas raras. Y con esta ni tan si quiera apareció en la web de pgp.rediris.es.

La que te enseñado esta hecha con Ubuntu 18.... LTS. Que teóricamente es mas estables y no suele hacer cosas raras. Ahora entiendo que las distribuciones de Debian aun utiliza paqueteria mas vieja aun en su versión estable. Pero bueno aun que no esta acabada, los pasos son los correctos o creo yo que los he dado.