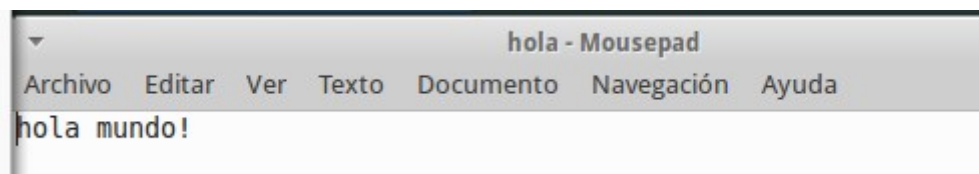


Ejercicio: Cifrado simétrico de un documento.

1. Crea un documento de texto con cualquier editor o utiliza uno del que dispongas.
He creado un documento llamado hola y dentro contenía hola mundo

1.



2. Cifra este documento con alguna contraseña acordada con el compañero de al lado.

```
usuario@servidorsmm:~/Escritorio$ gpg -c hola
```

Ejecutamos el anterior comando y nos pedirá una contraseña, yo he puesto hola.



3. Haz llegar por algún medio al compañero de al lado el documento que acabas de cifrar.

Yo he usado el comando scp

```
usuario@servidorsmm:~/Escritorio$ scp hola.gpg usuario@192.168.122.150:/home/usuario/Escritorio/hola.gpg
The authenticity of host '192.168.122.150 (192.168.122.150)' can't be established.
ECDSA key fingerprint is 24:d8:9f:65:dd:1c:a7:aa:d4:25:5e:5f:05:12:7a:9e.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.122.150' (ECDSA) to the list of known hosts.
usuario@192.168.122.150's password:
hola.gpg                                100% 52      0.1KB/s   00:00
usuario@servidorsmm:~/Escritorio$
```

4. Descifra el documento que te ha hecho llegar tu compañero de al lado.

Y cuando ha llegado lo he descifrado con el siguiente comando.

-gpg hola.gpg, nos pide la contraseña y nos lo descifra.

```
usuario@servidorsmm:~/Escritorio$ gpg hola.gpg
gpg: datos cifrados CAST5
gpg: cifrado con 1 contraseña
gpg: AVISO: la integridad del mensaje no está protegida
usuario@servidorsmm:~/Escritorio$
```

5. Repite el proceso anterior, pero añadiendo la opción -a. Observa el contenido del archivo generado con un editor de textos o con la orden cat.

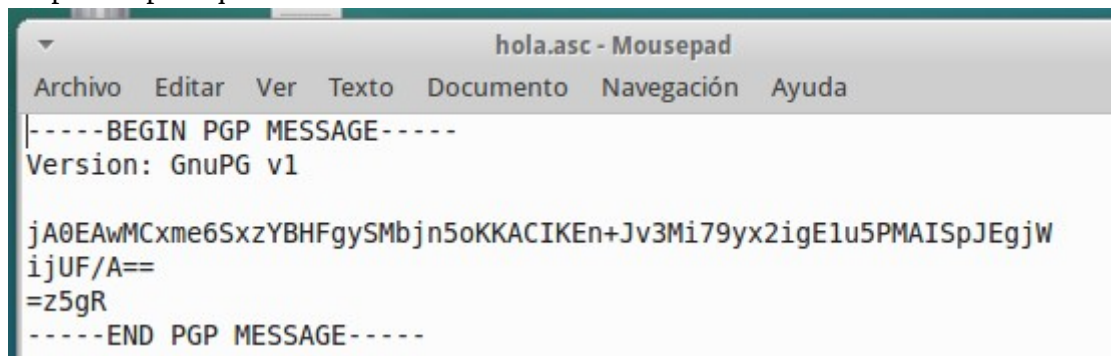
Ponemos el mismo comando con la opción -a y lo visualizamos con cat.

Observamos que ahora nos lo cifra con caracteres ASCII.

```
usuario@servidorsmm:~/Escritorio$ gpg -ca hola
usuario@servidorsmm:~/Escritorio$ cat hola
hola      hola.asc hola.gpg
usuario@servidorsmm:~/Escritorio$ cat hola
hola      hola.asc hola.gpg
usuario@servidorsmm:~/Escritorio$ cat hola.asc
-----BEGIN PGP MESSAGE-----
Version: GnuPG v1

jA0EAwMCxme6SxzYBHFgySmbjn5oKKACIKEn+Jv3Mi79yx2igE1u5PMAISpJEgjW
ijUF/A==
=z5gR
-----END PGP MESSAGE-----
usuario@servidorsmm:~/Escritorio$
```

6. Copia y pega el contenido del archivo cifrado anteriormente y envíalo por mail a tu compañero para que lo descifre.



```
hola.asc - Mousepad
Archivo  Editar  Ver  Texto  Documento  Navegación  Ayuda
|-----BEGIN PGP MESSAGE-----
|Version: GnuPG v1
|
|jA0EAwMCxme6SxzYBHFgySmbjn5oKKACIKEn+Jv3Mi79yx2igE1u5PMAISpJEgjW
|ijUF/A==
|=z5gR
|-----END PGP MESSAGE-----
```

7. Una vez has recibido el mensaje de tu compañero en tu mail, copialo en un archivo de texto para obtener el mensaje original.

Lo he descifrado igual que antes con gpg hola.asc

```
usuario@servidorsmm:~/Escritorio$ gpg hola.asc
gpg: datos cifrados CAST5
gpg: cifrado con 1 contraseña
El archivo «hola» ya existe. ¿Sobreescribir? (s/N) s
gpg: AVISO: la integridad del mensaje no está protegida
usuario@servidorsmm:~/Escritorio$
```

Creación de la pareja de claves pública-privada

1. Siguiendo las indicaciones de este epígrafe, crea tu par de claves pública y privada. La clave que vas a crear tendrá una validez de 1 mes.

Cuando ejecutamos el comando nos dice que seleccionemos uno, seleccionamos la primera.

```
usuario@usuario-VirtualBox:~$ gpg --gen-key
gpg (GnuPG) 1.4.16; Copyright (C) 2013 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.

gpg: /home/usuario/.gnupg: directorio creado
gpg: creado un nuevo archivo de configuración '/home/usuario/.gnupg/gpg.conf'
gpg: ATENCIÓN: aún no se han activado en esta ejecución las opciones en '/home/usuario/.gnupg/gpg.conf'
gpg: anillo «/home/usuario/.gnupg/secring.gpg» creado
gpg: anillo «/home/usuario/.gnupg/pubring.gpg» creado
Seleccione el tipo de clave deseado:
  (1) RSA y RSA (por defecto)
  (2) DSA y ElGamal (por defecto)
  (3) DSA (sólo firmar)
  (4) RSA (sólo firmar)
¿Su elección? 1
```

Después nos preguntará que de que longitud en bits queremos la clave, yo lo he puesto por defecto.

```
las claves RSA pueden tener entre 1024 y 4096 bits de longitud.
¿De qué tamaño quiere la clave? (2048)
```

Luego nos pedirá cuanto queremos que dure nuestra clave, yo he puesto como se ve en la imagen 1 mes.

```
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
```

Luego nos pedirá información personal como nombre y apellido, correo, etc.

```
¿Validez de la clave (0)? 1m
La clave caduca vie 07 abr 2017 00:49:35 CEST
¿Es correcto? (s/n) s

Necesita un identificador de usuario para identificar su clave. El programa
construye el identificador a partir del Nombre Real, Comentario y Dirección
de Correo electrónico de esta forma:
  "Heinrich Heine (Der Dichter) <heinrichh@duesseldorf.de>"

Nombre y apellidos: sergio
```

Después con pedirá una contraseña para nuestra clave, la ponemos

```
Nombre y apellidos: sergio
Dirección de correo electrónico:
Comentario:
Ha seleccionado este ID de usuario:
    «sergio»

¿Cambia (N)ombre, (C)omentario, (D)irección o (V)ale/(S)alir? v
Necesita una contraseña para proteger su clave secreta.
Introduzca contraseña: █
```

Y por último que generemos bits la crear nuestra clave, abrir y cerrar cosas o crear ficheros es una buena forma de crear estos bits.

```
Es necesario generar muchos bytes aleatorios. Es una buena idea realizar
alguna otra tarea (trabajar en otra ventana/consola, 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.

No hay suficientes bytes aleatorios disponibles. Haga algún
otro trabajo para que el sistema pueda recolectar más entropía
(se necesitan 219 bytes más).
█
```

Y una vez creada ya nos saldrá algo como la siguiente imagen.

```
gpg: /home/usuario/.gnupg/trustdb.gpg: se ha creado base de datos de confianza
gpg: clave 344B8223 marcada como de confianza absoluta
claves pública y secreta creadas y firmadas.

gpg: comprobando base de datos de confianza
gpg: 3 dudosa(s) necesaria(s), 1 completa(s) necesaria(s),
modelo de confianza PGP
gpg: nivel: 0 validez: 1 firmada: 0 confianza: 0-, 0q, 0n, 0m, 0f, 1u
gpg: siguiente comprobación de base de datos de confianza el: 2017-04-06
pub 2048R/344B8223 2017-03-07 [[caduca: 2017-04-06]]
    Huella de clave = C18D C0AA 8247 1794 B611 9FB8 7EDC 1277 344B 8223
uid          sergio
sub 2048R/967D1126 2017-03-07 [[caduca: 2017-04-06]]
usuario@usuario-VirtualBox:~$ █
```

2. Recuerda el ID de usuario de tu clave y la contraseña de paso utilizada. Anótala en un lugar seguro si lo consideras necesario.

Ejercicio: Exportar e importar claves públicas.

Exporta tu clave pública en formato ASCII y guárdalo en un archivo nombre_apellido.asc y envíalo a un compañero/a.

Primero ponemos `gpg -a --export nuestra_clavepublica` y así veo mi clave pública mi clave pública.

```
usuario@usuario-VirtualBox:~$ gpg -a --export 344B8223
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1

mQENBfi/0VABCACHk7P0b+FivrPdFS0clXKR3sYVeUkcauglw3cnNgHztb2i0l8y
WpISKC200BoXQPLY2hYpeaVrhC7K4KdLXA0M2d0Kw0jVON/6d4S7vzjbv01h+wqs
ESE3bxv0dHgB25lq7LXI3CzCEgs+dkatHGxfioXpR77g17HLDp0zNGhZ+XoKFyXl
z2dfwlCdV+jRSAuvFLAPx5ypkcHt4U3X91BsLFtqrx6jwgA+YgEwxVtGcL0rxPBP
5u/nFp8VdlF9AdRgYpeF3j/bcaoAzSeg/eemqn/Pix3sBskwuSnBt0NjiVHgTay3
K80LtCxpitiXQAbGjvscI0TP8hR9NTEGL4BfABEBAAG0BnNlcmdpb4kBPgQTAQIA
KAUCWL85UAIbAwUJACeNAAYLCQgHAWIGFQgCCQoLBbYCAwECHgECF4AACgkQftwS
dzRLgiPaagf/bt3aEdCJ0a7bBMxCM5GLrYknHWY05nWfSdktEHGHh3mAxWxyUKJ0
EzHGRw7ANokwiXajyaN6gvEZmrApYdplhlTZQzrna4dWKEF70iINuU/xM9mUj+MX
iFdnVqlvC0voTRehiBqm7EqBckkYaDVn7AbMJo1/Na/CrhHU/ommcYKx6GWqnQpQ
e6LxArJZ3gU35p4BippZp6rJl0kkMv3Bs/q2tZaQxRv37nIRDDwhjBiQQ7XuZ/0H
vXK2d/+sqVlnhxebXygkjiX7tea7ys6EBT4YbRbT7QWW80v9csGQB+ZB0jK1/+pu
n504SsvYa/MjyH9PdbcYz+S4b6g5ina3A7kBDQRYvzlQAQgAtjROTJG+OMLgqGy/
MnwuNWUXGNkSndZnLX0dxK/P40L+/kU/LI4KBpL0hn+HCE6Xa1Q2xQo/bUcuHb/d
Nyixhji77rfod7Q2bwZSvtvc0l0KdoJRxnDVRrLHTko+gd36CwmVqNMkLWQ0wc5R
c0Ei2C+XNnAoF+hp18vWvY6I8TF9P18tSJHxu2PIAhvxeaIWbmZhqzKsDCn/8FZX
QpwWQBjHzyCrLaS5GbnODL4onlwMM4EPz0lV3DTW0cY6vMNF/xoZCwYMD/is7R8H
SrK7zZPVVd3jpnYrTupRR4Iu+c5KJzzXI2UH2mrmi/hlxvqjimS28tGPQs4Ums9
Lt06BQARAQABiQElBBgBAGAPBQJYvzlQAhsMBQkAJ40AAAJEH7cEnc0S4Ij+okH
+gPlWY3Qjz5jQ1ldsUo54FGXq0n0qudAUZ68RaqsCDiuI50fzy8Micj5goEHdCWN
PkCHaC+6oicQplQ37azNm4nHrVyukvFV7AHqQvLzv+fse3HpZQKbh7WFABE7QvoA
TR4bj7dTFuG12agjARxI61rJcU4KqB/YrlBeqkciQEsPa6KgTGdPpNLQX3xPpoFe
D2+y1306tk6NtAKNKCel3D3Z+43f4e6Bhxr8eM+7VTXpfiMmexASFfhJWuM1L4ax
D/kKvS+tyMQD8SVSiZesQ8BwHKY/DWGHfXwNURM/ySpCHH552bSSN8r4uLjGgH/
eMoGVlZErp6FYu2or6Wbw2k=
=HBWK
-----END PGP PUBLIC KEY BLOCK-----
usuario@usuario-VirtualBox:~$
```

La exportamos a ascii con el siguiente comando:

```
usuario@usuario-VirtualBox:~$ gpg -a --export --output sergio_martínez.asc 344B8223
usuario@usuario-VirtualBox:~$
```

Importamos las claves públicas recibidas de vuestros/as compañeros/as con el comando `gpg --import clave_a_importar`

**Nota: dado que mi compañero, Juanma no estaba y a los que he preguntado no habían llegado aquí, he hecho la practica solo con dos maquinas.*

```
usuario@usuario-VirtualBox:~$ gpg --import Escritorio/sergio_martínez.asc
gpg: clave 344B8223: clave pública "sergio" importada
gpg: Cantidad total procesada: 1
gpg:      importadas: 1 (RSA: 1)
usuario@usuario-VirtualBox:~$
```

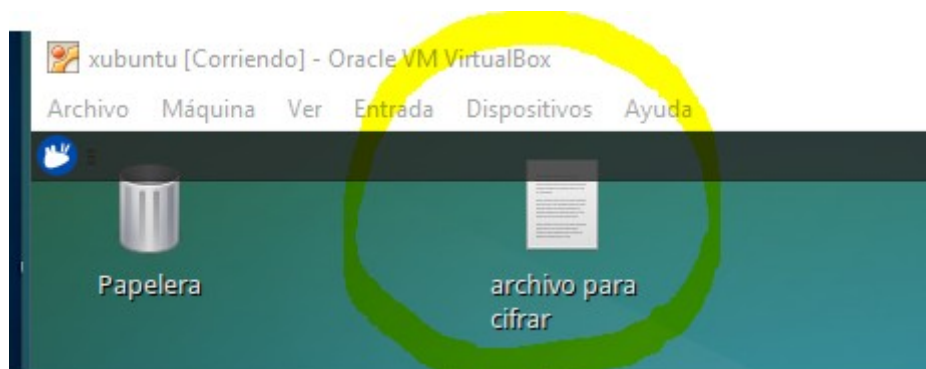
Comprueba que las claves se han incluido correctamente en vuestro keyring. Con `gpg -kv`.

```
usuario@usuario-VirtualBox:~$ gpg -kv
/home/usuario/.gnupg/pubring.gpg
-----
pub   2048R/344B8223  2017-03-07 [[caduca: 2017-04-06]]
uid           sergio
sub   2048R/967D1126  2017-03-07 [[caduca: 2017-04-06]]
usuario@usuario-VirtualBox:~$
```

Ejercicio: Cifrado y descifrado de un documento.

Cifraremos un archivo cualquiera y lo remitiremos por email a uno de nuestros compañeros que nos proporcionó su clave pública.

Yo he creado este archivo que por evitarme lios después le cambie el nombre a archivo.



Con el comando `gpg -a -r clave_publica --encrypt archivo_encryptar` encriptaremos nuestro archivo con la clave publica seleccionada.

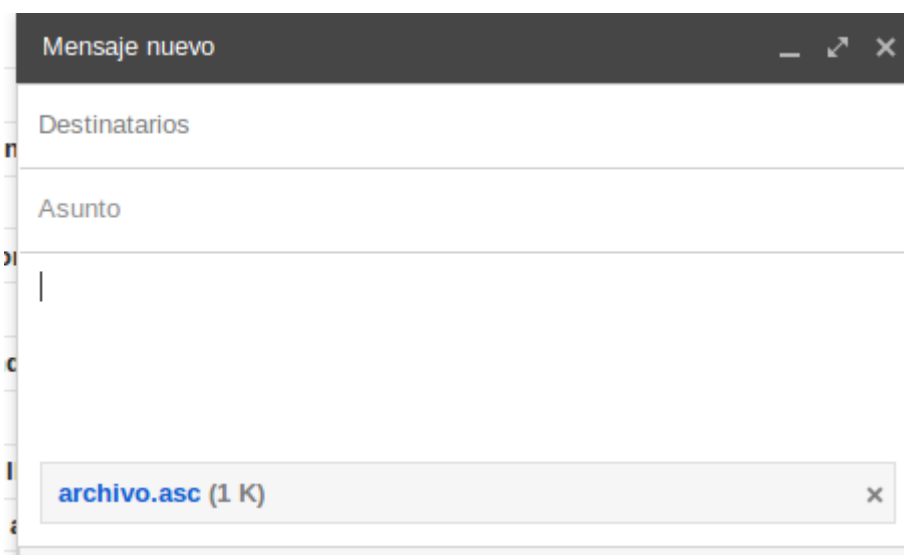
```
usuario@usuario-VirtualBox:~$ gpg -a -r sergio --encrypt Escritorio/archivo
gpg: 967D1126: No hay seguridad de que esta clave pertenezca realmente
al usuario que se nombra

pub 2048R/967D1126 2017-03-07 sergio
Huella de clave primaria: C18D C0AA 8247 1794 B611 9FB8 7EDC 1277 344B 8223
Huella de subclave: BFEE 9679 DC35 5483 4AA7 1059 6C84 B2A1 967D 1126

No es seguro que la clave pertenezca a la persona que se nombra en el
identificador de usuario. Si *realmente* sabe lo que está haciendo,
puede contestar sí a la siguiente pregunta.

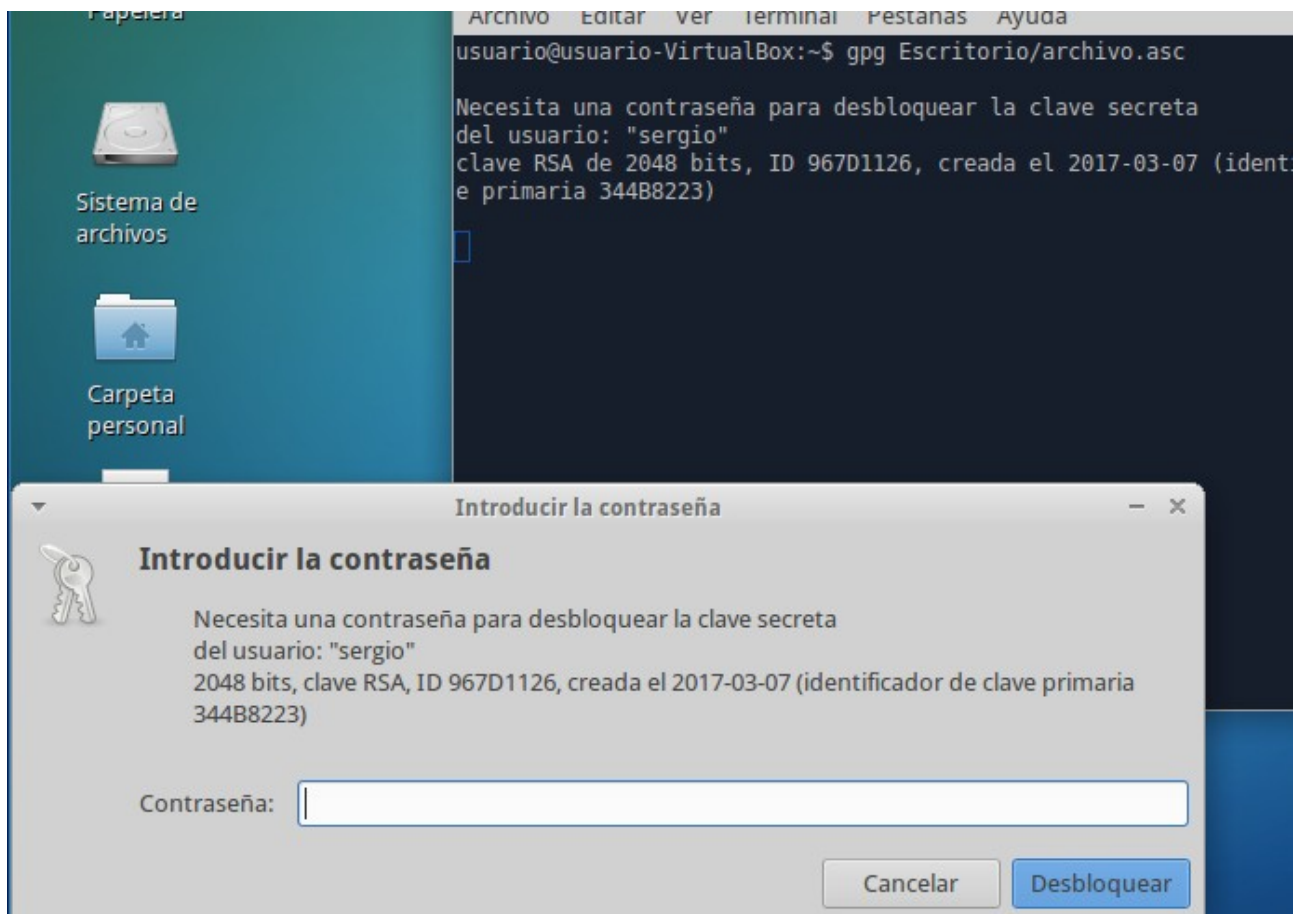
¿Usar esta clave de todas formas? (s/N) █
```

Y luego se lo paso por email a nuestro compañero, pero como yo lo estoy haciendo solo pues me lo he pasado a mi y lo he abierto con otra maquina.

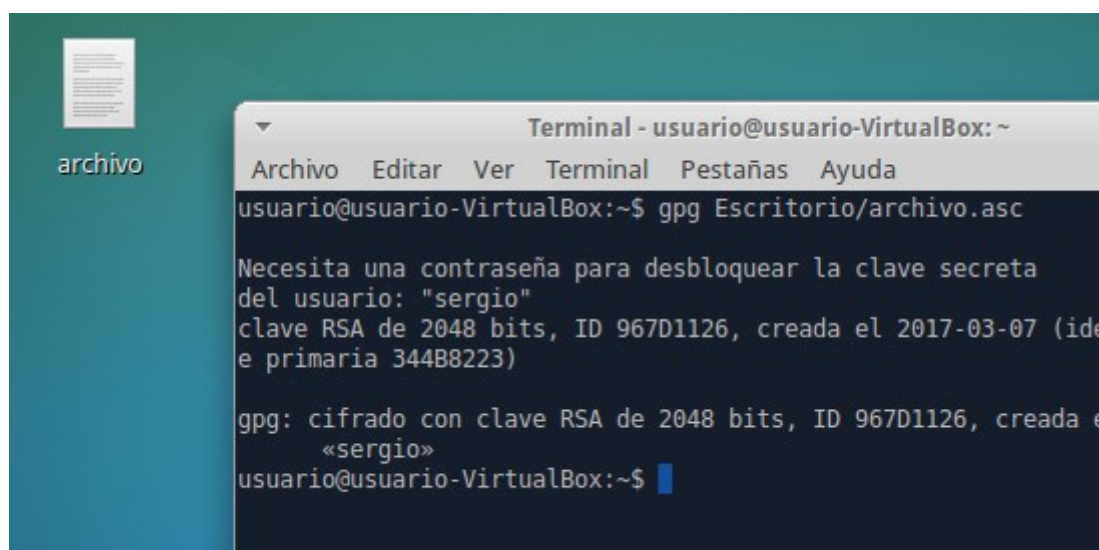


Tanto nosotros como nuestro compañero comprobaremos que hemos podido descifrar los mensajes recibidos respectivamente.

Descifremos el archivo con gpg archivo.asc y nos pedirá una contraseña.



Y por ultimo comprobamos que el archivo ha sido descifrado con éxito.



Por último, enviaremos el documento cifrado a alguien que no estaba en la lista de destinatarios y comprobaremos que este usuario no podrá descifrar este archivo.

Nos sale este error si alguien que no tiene nuestra clave publica intenta descifrarlo.


```
usuario@servidoresmm:~/Escritorio$ gpg Probando_clave
gpg: no se han encontrado datos OpenPGP válidos
gpg: processing message failed: eof
```

Ejercicio: Firma digital de un documento.

Crea la firma digital de un archivo de texto cualquiera y envíale éste junto al documento con la firma a un compañero.

Primero firmaremos un archivo con el comando `gpg -sb -a archivo`

```
usuario@servidoresmm:~/Escritorio$ gpg -sb -a hola
Necesita una contraseña para desbloquear la clave secreta
del usuario: "sergio"
clave RSA de 2048 bits, ID 8186F51B, creada el 2017-03-08
usuario@servidoresmm:~/Escritorio$
```

Verifica que la firma recibida del documento es correcta.

Luego se lo pasaremos a un compañero junto a nuestra firma del archivo y utilizaremos el comando `gpg --verify archivo.asc` para comprobar si es el mismo archivo

```
usuario@servidoresmm:~/Escritorio$ gpg --verify hola.asc
gpg: Firmado el mié 08 mar 2017 18:41:23 CET usando clave RSA ID 8186F51B
gpg: Firma correcta de «sergio»
gpg: AVISO: ¡Esta clave no está certificada por una firma de confianza!
gpg: No hay indicios de que la firma pertenezca al propietario.
Huellas digitales de la clave primaria: 36F0 6A3B 6601 AA97 1C10 8D85 AC13 9DCB
8186 F51B
usuario@servidoresmm:~/Escritorio$
```

Modifica el archivo ligeramente, insertando un carácter o un espacio en blanco, y vuelve a comprobar si la firma se verifica.

Por ultimo haremos lo mismo pero antes modificando el fichero para ver que error nos sale.

```
usuario@servidoresmm:~/Escritorio$ gpg --verify hola.asc
gpg: Firmado el mié 08 mar 2017 18:41:23 CET usando clave RSA ID 8186F51B
gpg: Firma INCORRECTA de «sergio»
usuario@servidoresmm:~/Escritorio$
```

Como podemos observar nos dice que la firma no es correcta es decir que el fichero no corresponde a la firma, ha sido modificado.