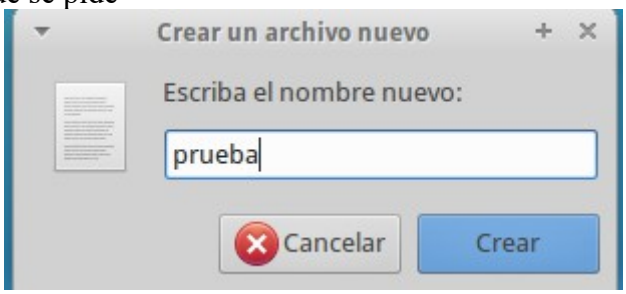
Ejercicio: Cifrado simétrico de un documento.

Creamos el documento que se pide



Ciframos el archivo

```
root@servidorrhp:/home/usuario# pgp -c /home/usuario/Escritorio/prueba
```

Desciframos el archivo

```
root@servidorrhp:/home/usuario# gpg /home/usuario/Escritorio/prueba.pgp
gpg: datos cifrados CAST5
gpg: el agente gpg no esta disponible en esta sesión
gpg: cifrado con 1 contraseña
```

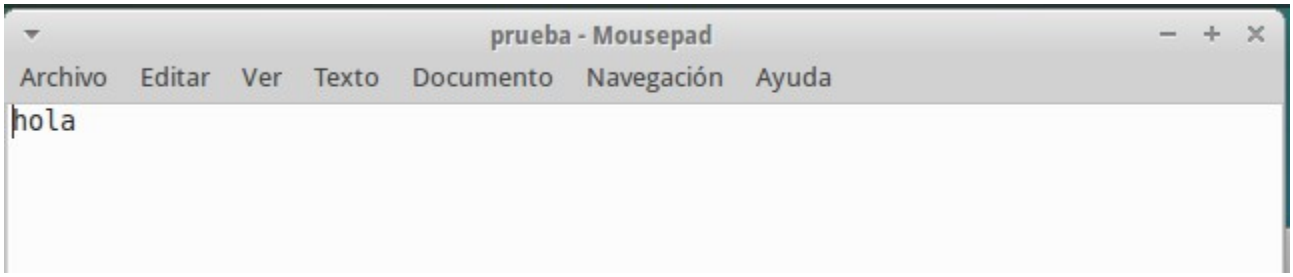
Volvemos a repetir el proceso pero añadiendo -a

```
root@servidorrhp:/home/usuario# pgp -ca /home/usuario/Escritorio/prueba
```

Se verá así el archivo

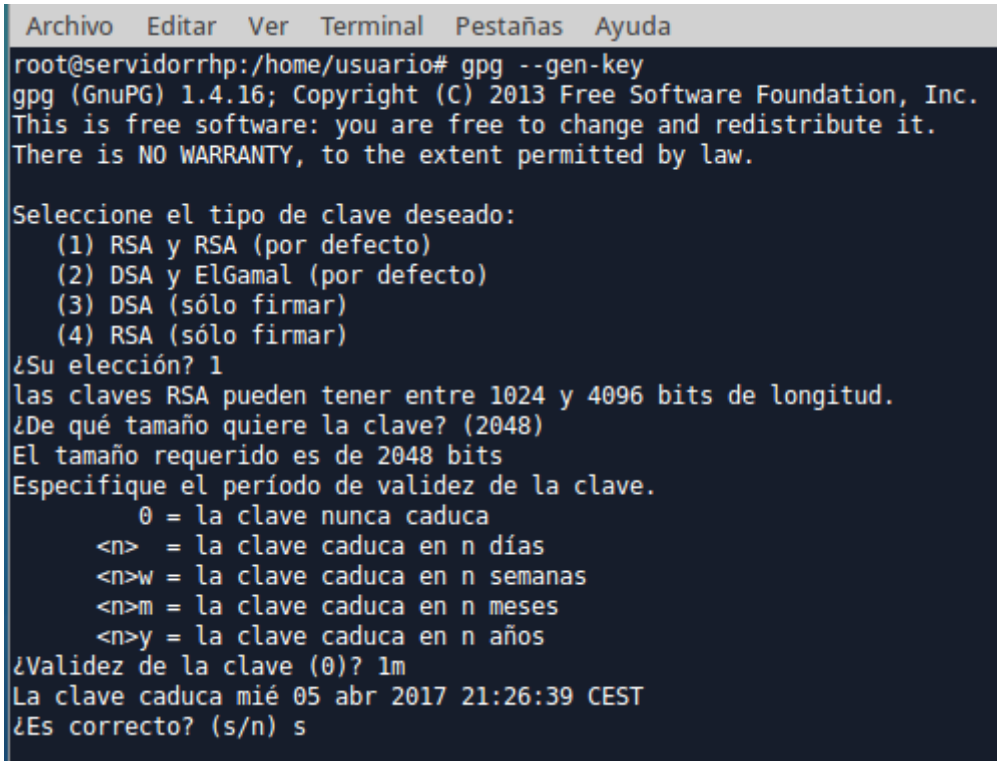
```
root@servidorrhp:/home/usuario# cat /home/usuario/Escritorio/prueba.asc
-----BEGIN PGP MESSAGE-----
Version: GnuPG v1

jA0EAwMCJubeOyOGLFBgySCRl+UqdfOnEQrxxMk3UfkGlZg46+i9h+6gsq7x4xfb
zg==
=bZ/K
-----END PGP MESSAGE-----
```

El mensaje original es este:

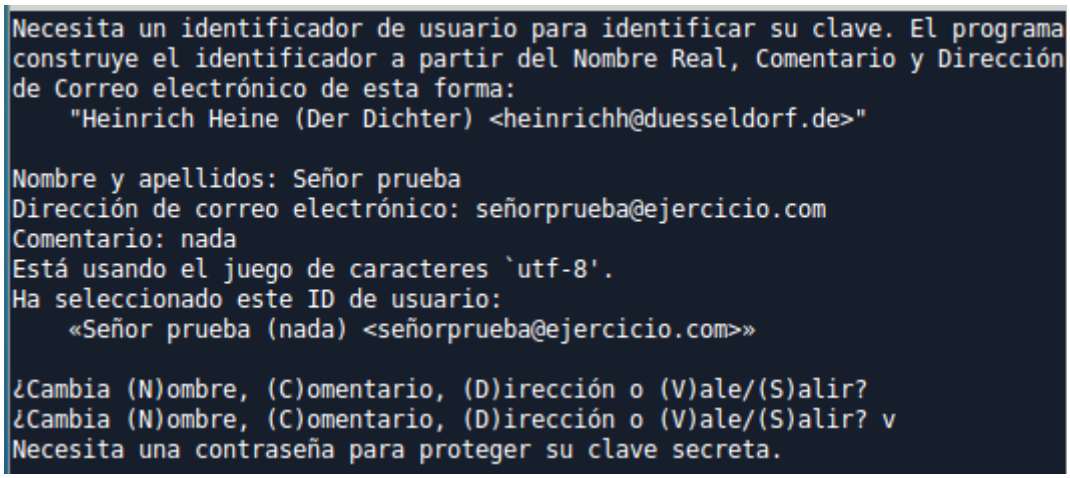


Ejercicio: Creación de nuestro par de claves pública-privada.

Para crear las claves usamos el comando gpg –gen-key, el tipo de clave y tamaño lo vamos a dejar por defecto, solo elegiré el periodo de validez a 1 mes porque es lo que pide el ejercicio



La identificación de usuario y el correo me lo he inventado, y la contraseña es *yo*



Ejercicio: Exportar e importar claves públicas.

Exporto mi clave pública en el archivo rubenhidalgo.asc

```
root@servidorrhp:/home/usuario# gpg -a --export 1D27FD08 >/home/usuario/Esc
ritorio/rubenhidalgo.asc
```

Importamos la clave

```
root@servidorrhp:/home/usuario# gpg --import /home/usuario/Escritorio/ruben
hidalgo.asc
```

Comprobamos nuestro keyring

```
root@servidorrhp:/home/usuario# gpg -kv
/root/.gnupg/pubring.gpg
------------------------
pub   1024D/11F63C51 2002-02-28
uid                  Jamie Cameron <jcameron@webmin.com>
sub   1024g/1B24BE83 2002-02-28

pub   2048R/1D27FD08 2017-03-06 [[caduca: 2017-04-05]]
uid                  Señor prueba (nada) <señorprueba@ejercicio.com>
sub   2048R/0EB52A73 2017-03-06 [[caduca: 2017-04-05]]
```

Ejercicio: Cifrado y descifrado de un documento.

Archivo a entregar

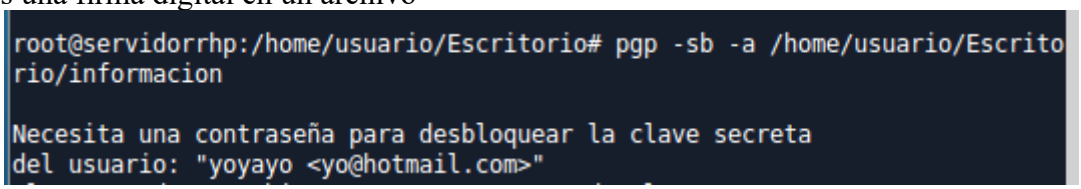
```
root@servidorrhp:/home/usuario# pgp -ca /home/usuario/Escritorio/paracompar
tir
```

Archivo a recibir para descifrar

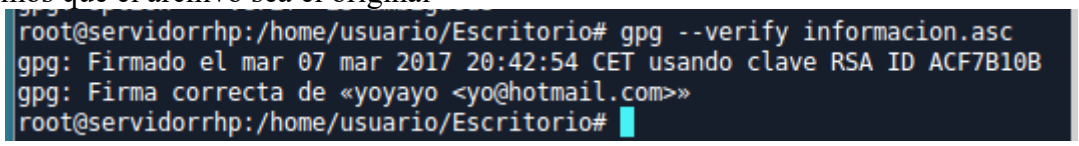
```
root@servidorrhp:/home/usuario# gpg /home/usuario/Escritorio/arecibir.asc
gpg: datos cifrados CAST5
gpg: el agente gpg no esta disponible en esta sesión
gpg: cifrado con 1 contraseña
```

Ejercicio: Firma digital de un documento.

Creamos una firma digital en un archivo



Verificamos que el archivo sea el original



Si el archivo es modificado, nos mostraría este mensaje