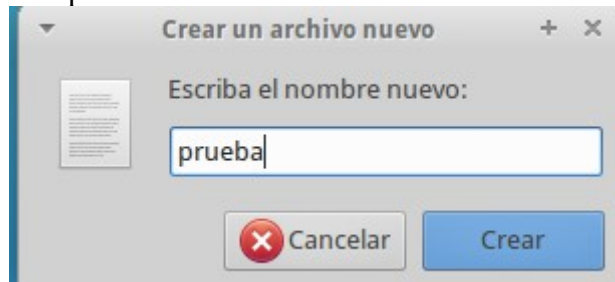


Ejercicio: Cifrado simétrico de un documento.

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

Volvemos a repetir el proceso pero añadiendo -a

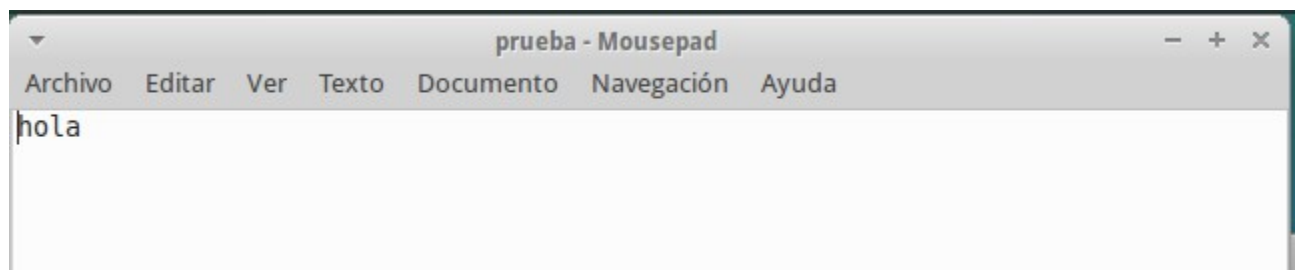
```
root@servidorrhp:/home/usuario# pgp -ca /home/usuario/Escritorio/prueba
```

Se verá así el archivo

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

jA0EAwMCJube0y0GLFBgySCRl+Uqdf0nEQrxxMk3UfkG1Zg46+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

```
Archivo  Editar  Ver  Terminal  Pestañas  Ayuda
root@servidorrhp:/home/usuario# 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.

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
las claves RSA pueden tener entre 1024 y 4096 bits de longitud.
¿De qué tamaño quiere la clave? (2048)
El tamaño requerido es de 2048 bits
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
La clave caduca mié 05 abr 2017 21:26:39 CEST
¿Es correcto? (s/n) s
```

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

```
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: Señor prueba
Dirección de correo electrónico: señorprueba@ejercicio.com
Comentario: nada
Está usando el juego de caracteres `utf-8'.
Ha seleccionado este ID de usuario:
  «Señor prueba (nada) <señorprueba@ejercicio.com>»

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

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/Escritorio/rubenhidalgo.asc
```

Importamos la clave

```
root@servidorrhp:/home/usuario# gpg --import /home/usuario/Escritorio/rubenhidalgo.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# gpg -ca /home/usuario/Escritorio/paracompartir
```

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

```
root@servidorrhp:/home/usuario/Escritorio# gpg -sb -a /home/usuario/Escritorio/informacion

Necesita una contraseña para desbloquear la clave secreta del usuario: "yoyayo <yo@hotmail.com>"
```

Verificamos que el archivo sea el original

```
root@servidorrhp:/home/usuario/Escritorio# gpg --verify informacion.asc
gpg: Firmado el mar 07 mar 2017 20:42:54 CET usando clave RSA ID ACF7B10B
gpg: Firma correcta de «yoyayo <yo@hotmail.com>»
root@servidorrhp:/home/usuario/Escritorio#
```

Si el archivo es modificado, nos mostraría este mensaje

```
root@servidorrhp:/home/usuario/Escritorio# gpg --verify informacion.asc
gpg: error de redundancia cíclica: 4F91B0 - B2DEF8
gpg: [don't know]: invalid packet (ctb=69)
gpg: no se ha encontrado ninguna firma
gpg: la firma no se pudo verificar.
Por favor recuerde que el archivo de firma (.sig o .asc) debería ser el primero que se da en la línea de órdenes.
```