

PRÁCTICA DE CRIPTOGRAFÍA (GPG)



Rubén Irles Esclapez

IES SEVERO OCHOA

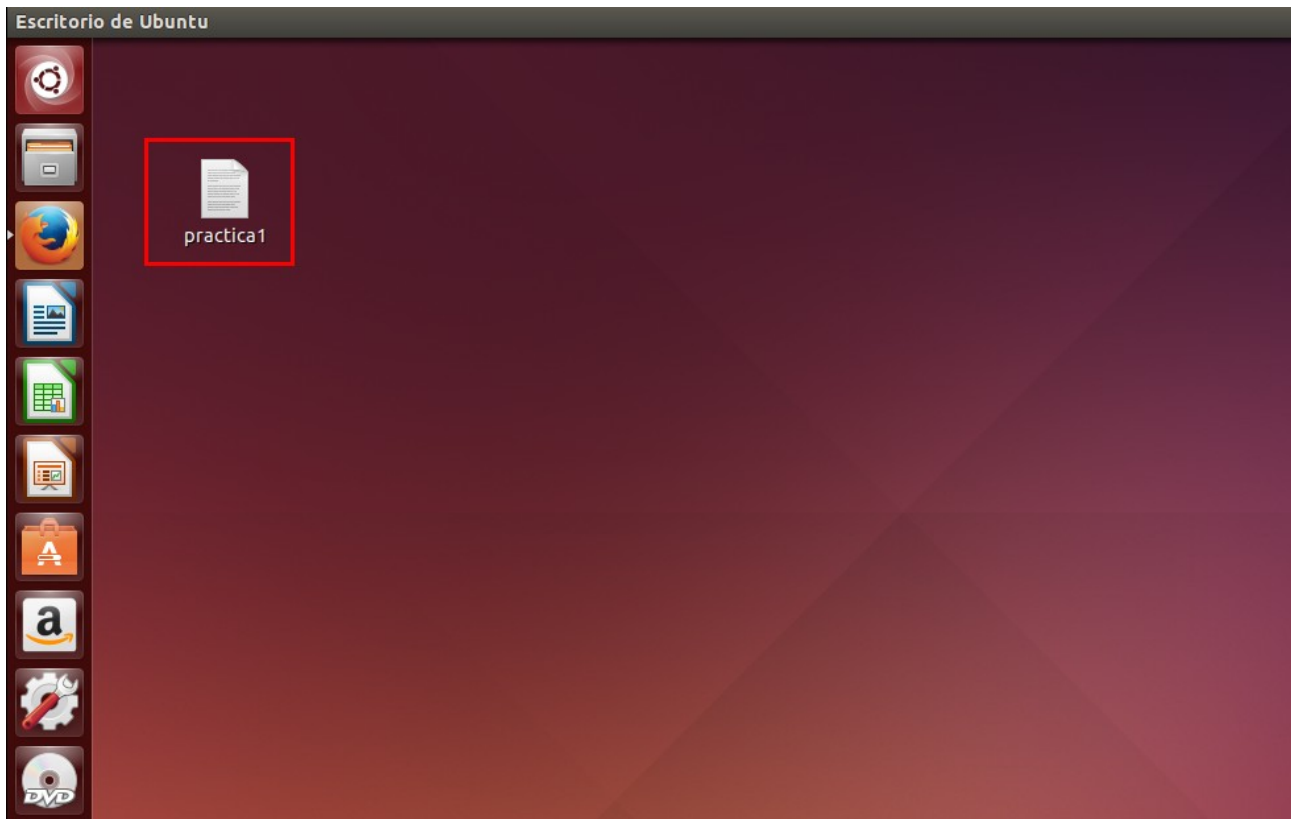
2ºG SMR 2016-2017

ÍNDICE

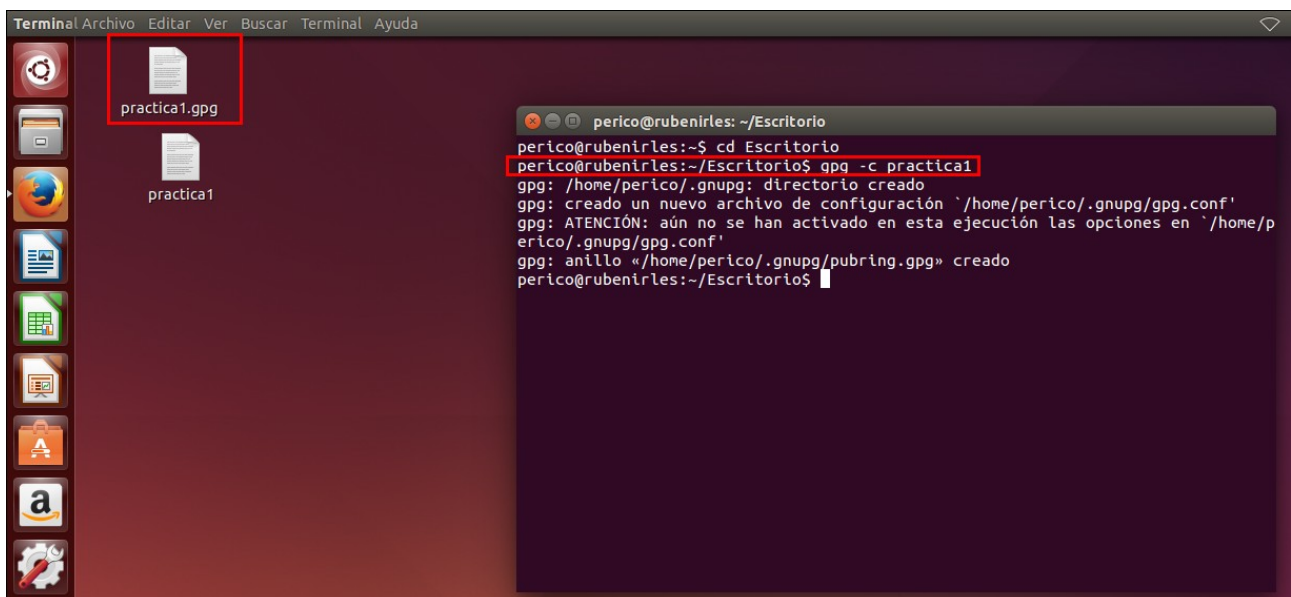
| | |
|---|---|
| Cifrado simétrico de un documento..... | 3 |
| Creación de la pareja de claves: pública – privada..... | 5 |
| Creación de nuestro par de claves: pública – privada..... | 7 |
| Exportar e importar claves públicas..... | 7 |
| Cifrado y descifrado de un archivo..... | 8 |
| Firma digital de un documento..... | 9 |

CIFRADO SIMÉTRICO DE UN DOCUMENTO:

- Crear un documento de texto:

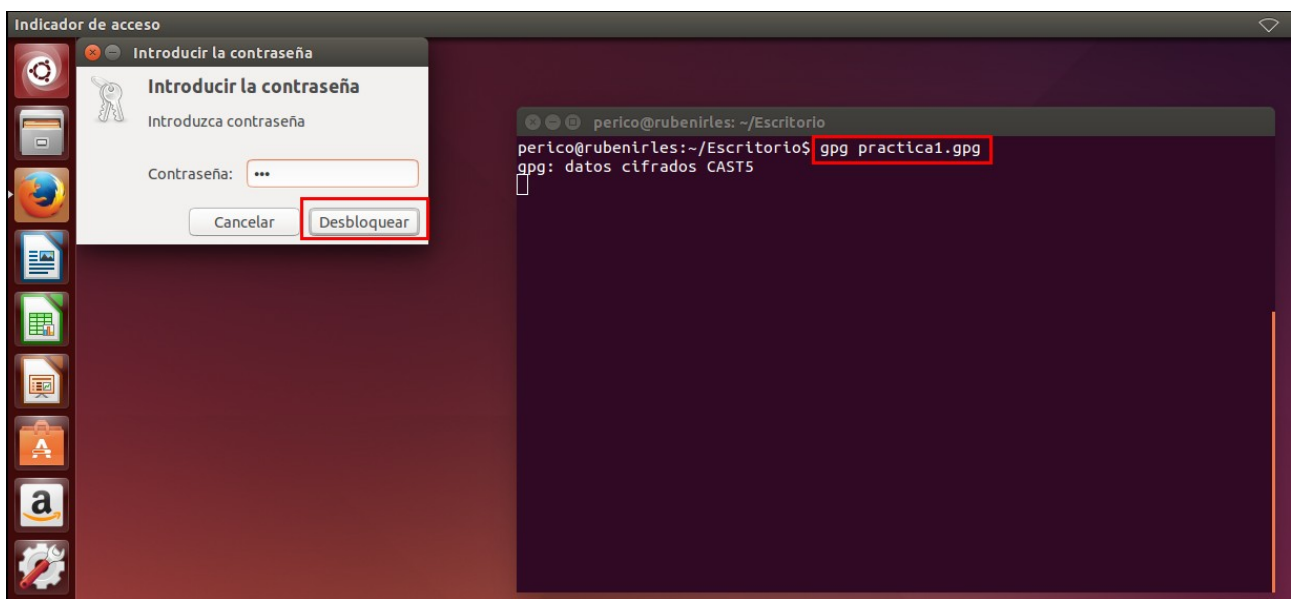


- Cifrarlo con el comando: **gpg -c "nombre_de_archivo"**

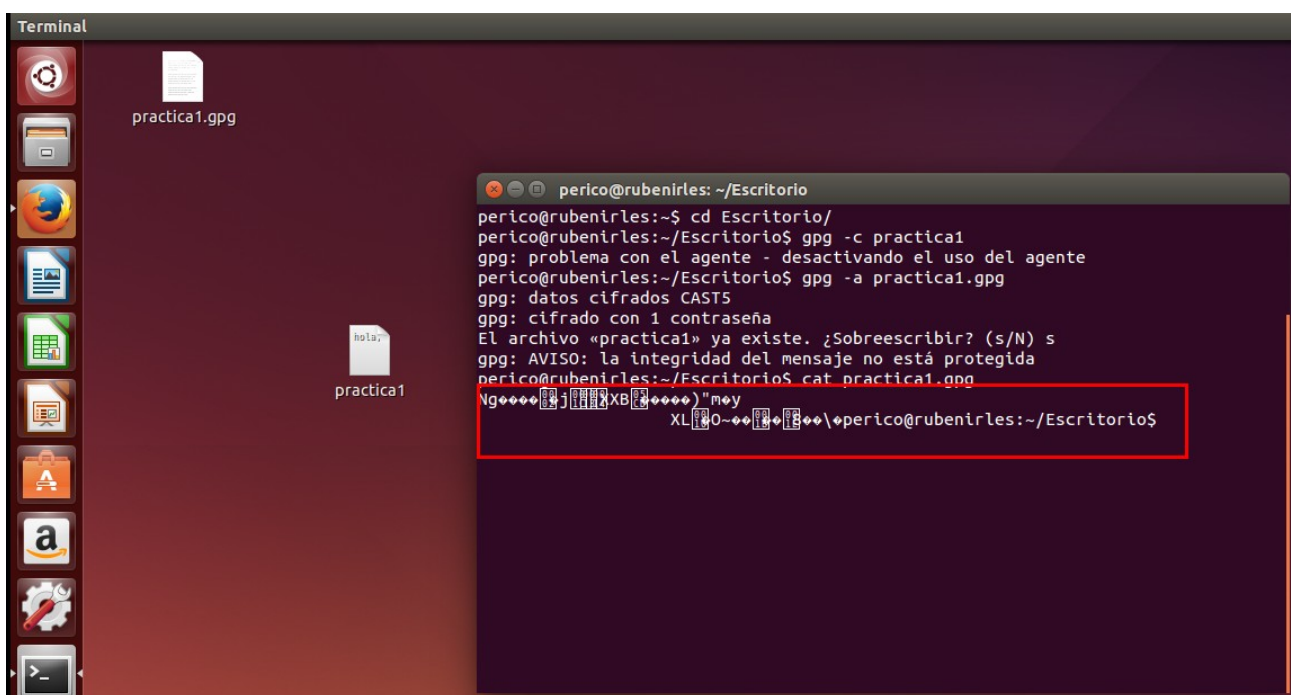


- Descifrar el archivo:

Para descifrar el archivo tenemos que usar el comando gpg “nombre_de_archivo” y introducir la contraseña que se le haya puesto a ese archivo



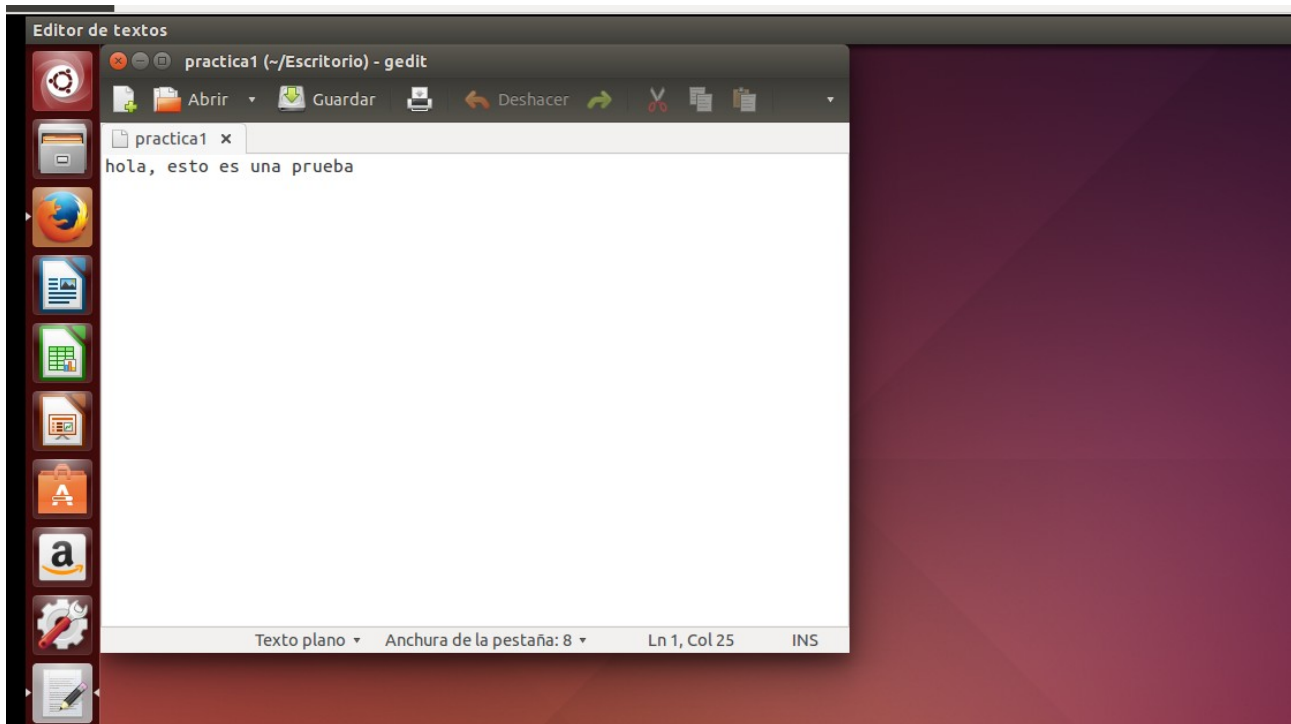
- Repetir el proceso pero con la opción -a:



Ahora si mostramos el contenido del archivo con un cat, vemos que el contenido está cifrado y no podemos leer que pone.

- Enviar mensaje por mail y descifrarlo:

He descargado el fichero que me ha enviado mi compañero y al descifrarlo, puedo ver el contenido:



CREACIÓN DE LA PAREJA DE CLAVES PÚBLICA – PRIVADA:

- Usamos el comando **gpg --gen-key**

- En el tipo de clave, seleccionamos 1
- En la longitud, seleccionamos la que viene por defecto, 2048
- En el periodo de validez podemos poner hasta cuando es válida la clave, si ponemos 0 es que nunca caduca
- Después podemos poner un identificador para nuestra clave, como nombre y apellidos, correo, comentario, etc.
- Por último, ponemos una contraseña y entonces nos pedirá que trabajemos con el ordenador para recopilar bytes aleatorios

```
perico@rubenirles:~$ 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) 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)?
La clave nunca caduca
¿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: ruben irles
Dirección de correo electrónico: ruben@correo.es
Comentario: hola
Ha seleccionado este ID de usuario:
  «ruben irles (hola) <ruben@correo.es>»

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

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
```

```
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.

No hay suficientes bytes aleatorios disponibles. Haga algún
otro trabajo para que el sistema pueda recolectar más entropía
(se necesitan 181 bytes más).
```

Después de éste último mensaje, nos ponemos a trabajar con el ordenador, abrimos carpetas, archivos, le mandamos tareas etc.

Y cuando recopile la información que necesita, aparecerá esto:

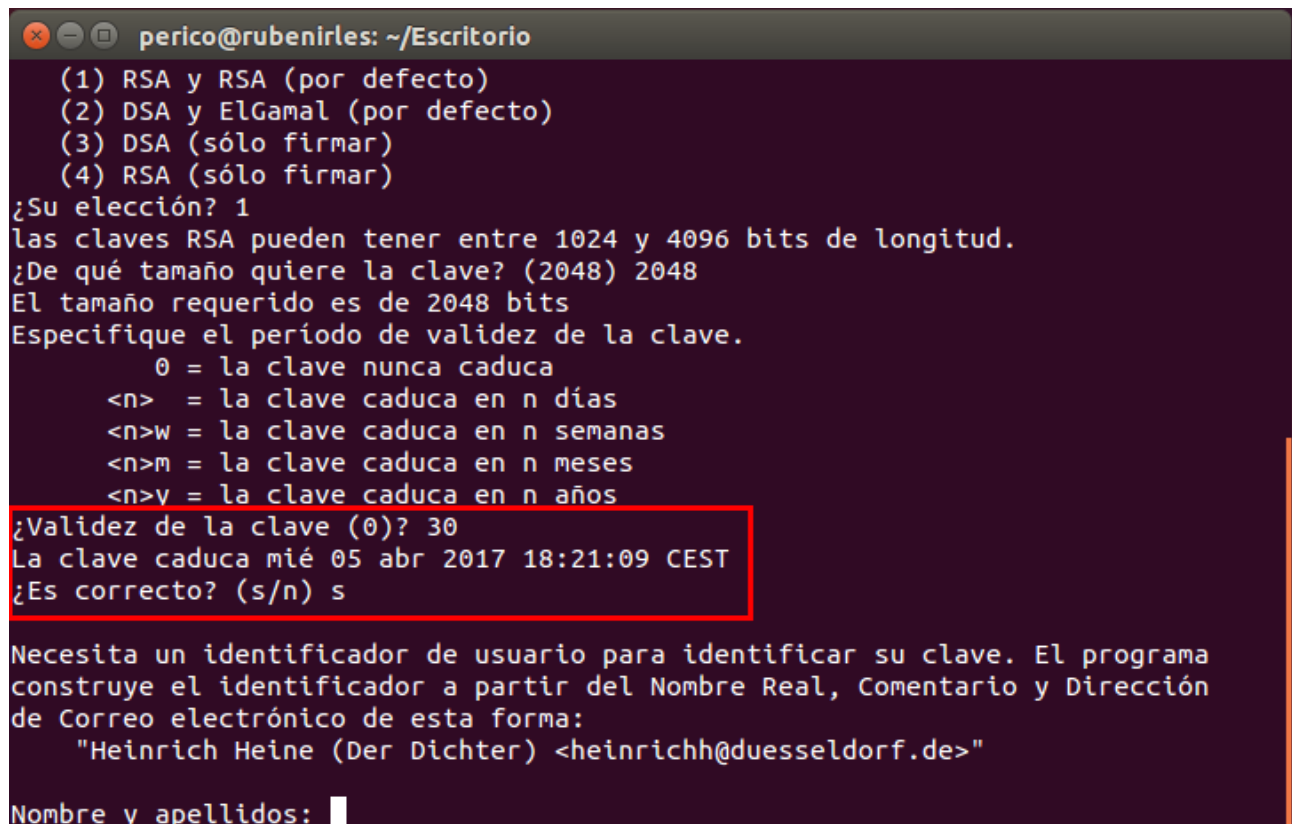
```
gpg: /home/perico/.gnupg/trustdb.gpg: se ha creado base de datos de confianza
gpg: clave 3574D5B1 marcada como de confianza absoluta
claves pública y secreta creadas y firmadas.

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
pub 2048R/3574D5B1 2017-03-06
Huella de clave = 4E5E 6521 D73F 5BF5 E08D B9CE 56F0 C528 3574 D5B1
uid ruben irles (hola) <ruben@correo.es>
sub 2048R/896319BB 2017-03-06

perico@rubenirles:~$
```

CREACIÓN NUESTRO PAR DE CLAVES PÚBLICA – PRIVADA:

- Creación de una clave con 1 mes de validez:



```
perico@rubenirles: ~/Escritorio
(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) 2048
El tamaño requerido es de 2048 bits
Especifique el periodo 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)? 30
La clave caduca mié 05 abr 2017 18:21:09 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: 
```

Después de hacerlo es importante anotar la clave que hemos utilizado.

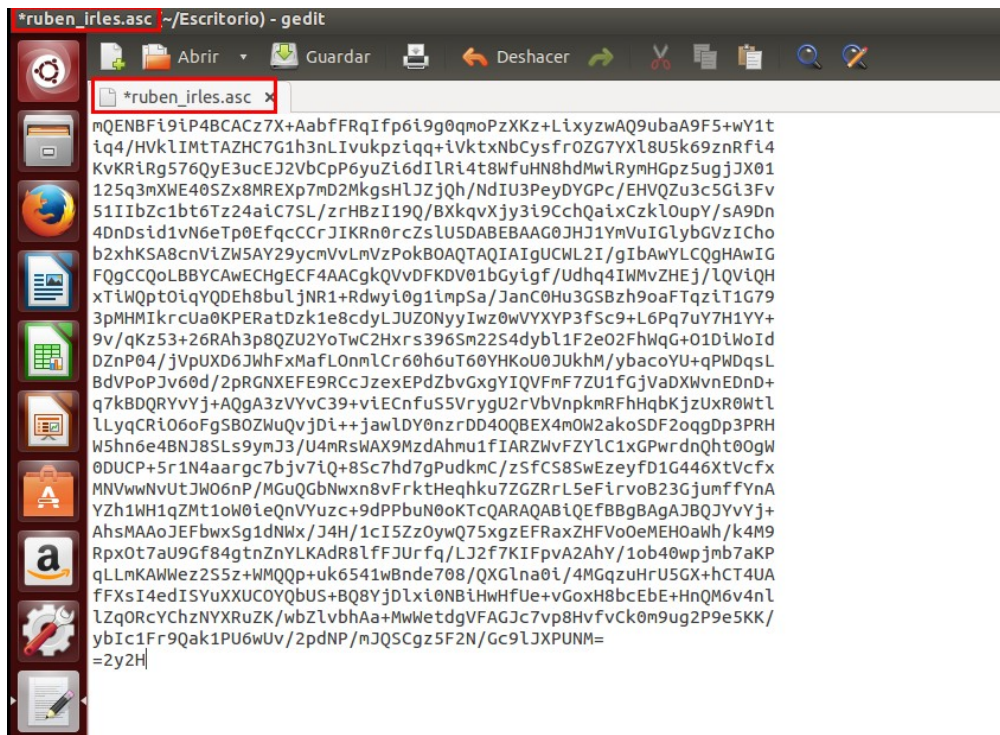
Yo la he apuntado para que no se olvide para usarla en los ejercicios siguientes

EXPORTAR E IMPORTAR CLAVES PÚBLICAS:

- Exportar mi clave pública y mandarla

He exportado mi clave pública en formato ASCII y la he exportado en un fichero .asc

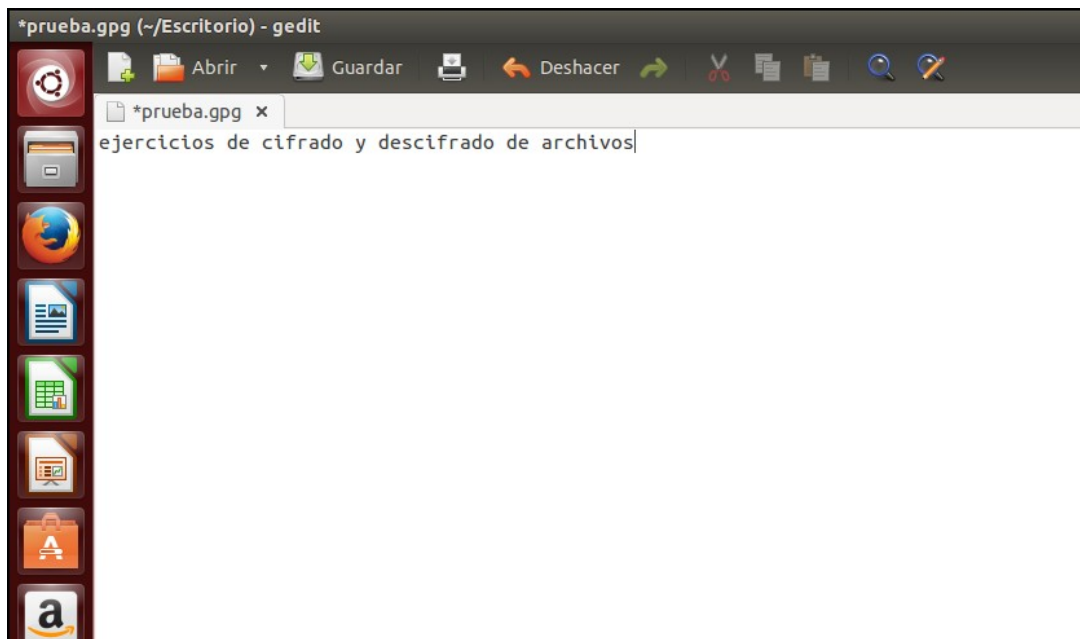
Como se puede ver en la imagen de la siguiente página:



CIFRADO Y DESCIFRADO DE UN ARCHIVO

- Vamos a cifrar y descifrar un archivo cualquiera y enviárselo a un compañero. El compañero hará lo mismo pero nos enviará el suyo a nosotros.

He recibido el archivo del compañero y lo he descifrado con la clave que me ha dado y he podido ver el contenido:

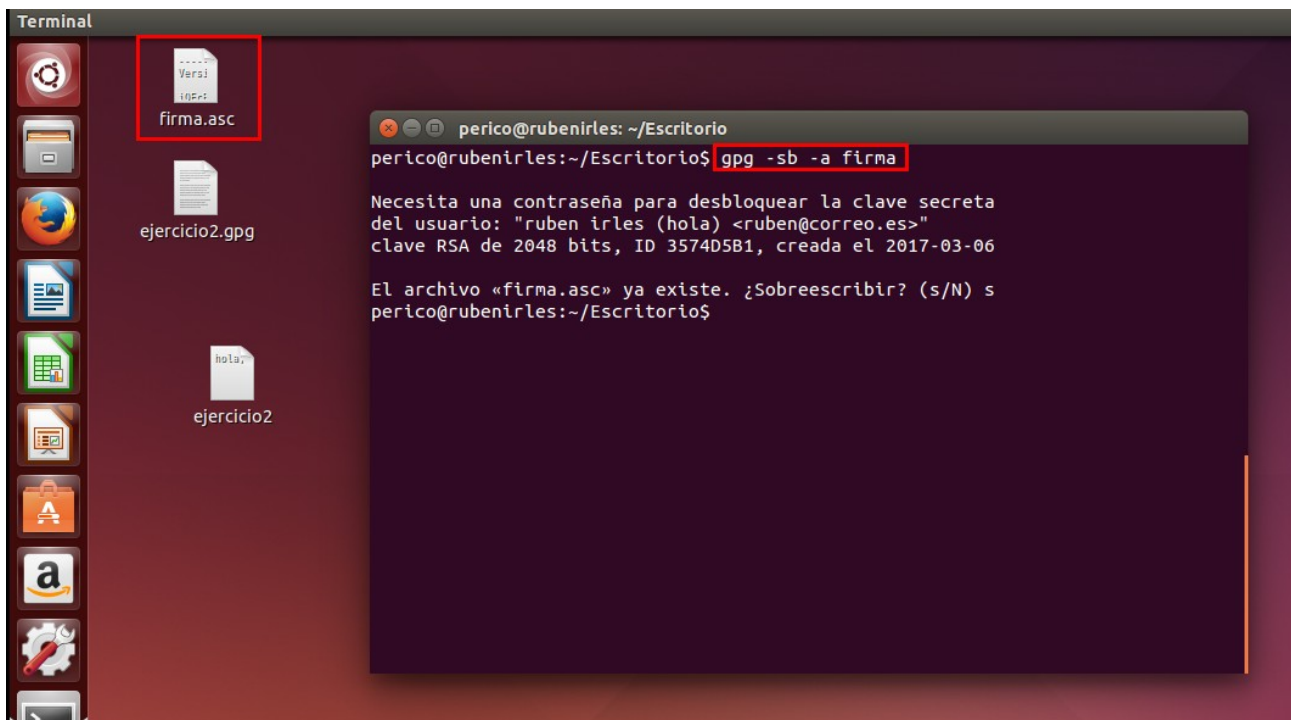


Y después comprobamos que los que no estaban en la lista de destinatarios no pueden abrirlo

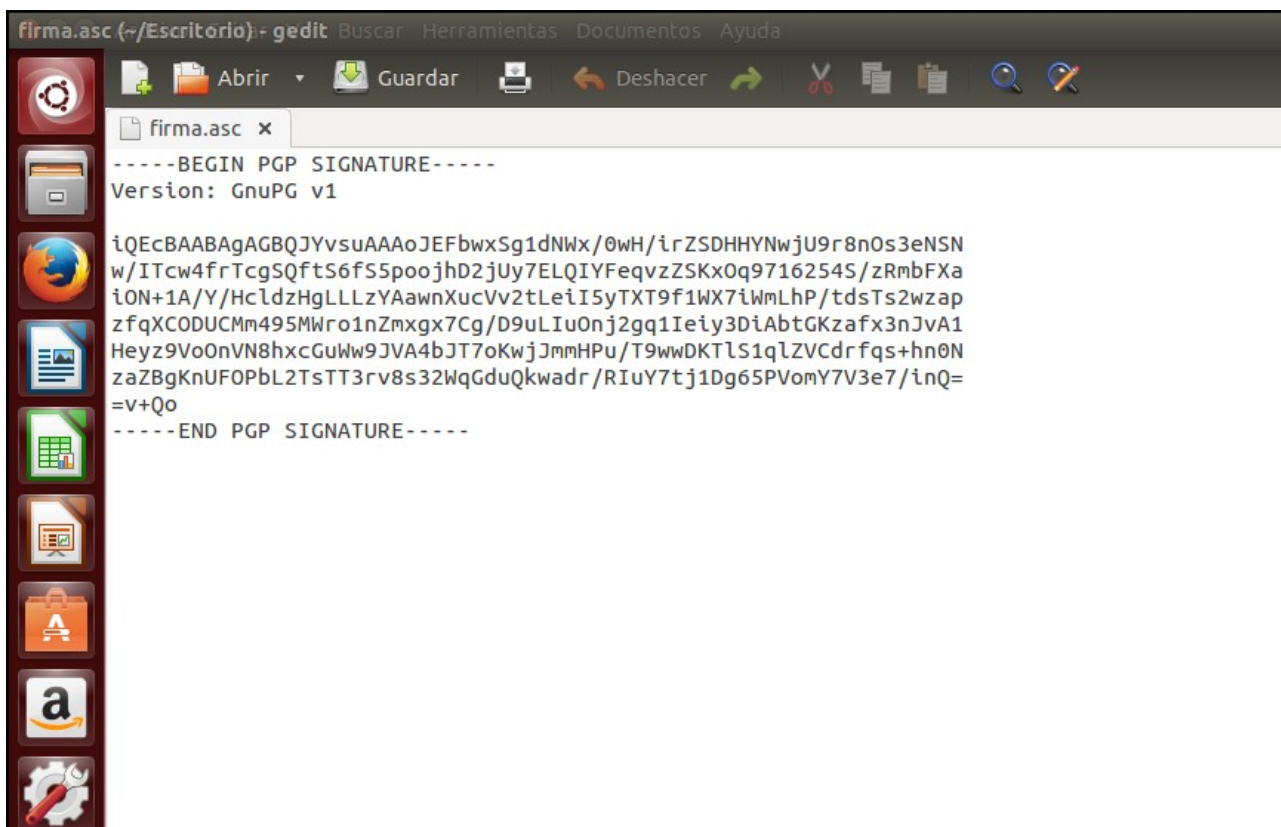
FIRMA DIGITAL DE UN DOCUMENTO:

- Vamos a firmar digitalmente un documento

Para ello tenemos que usar el comando `gpg -sb -a "nombre_de_archivo"`

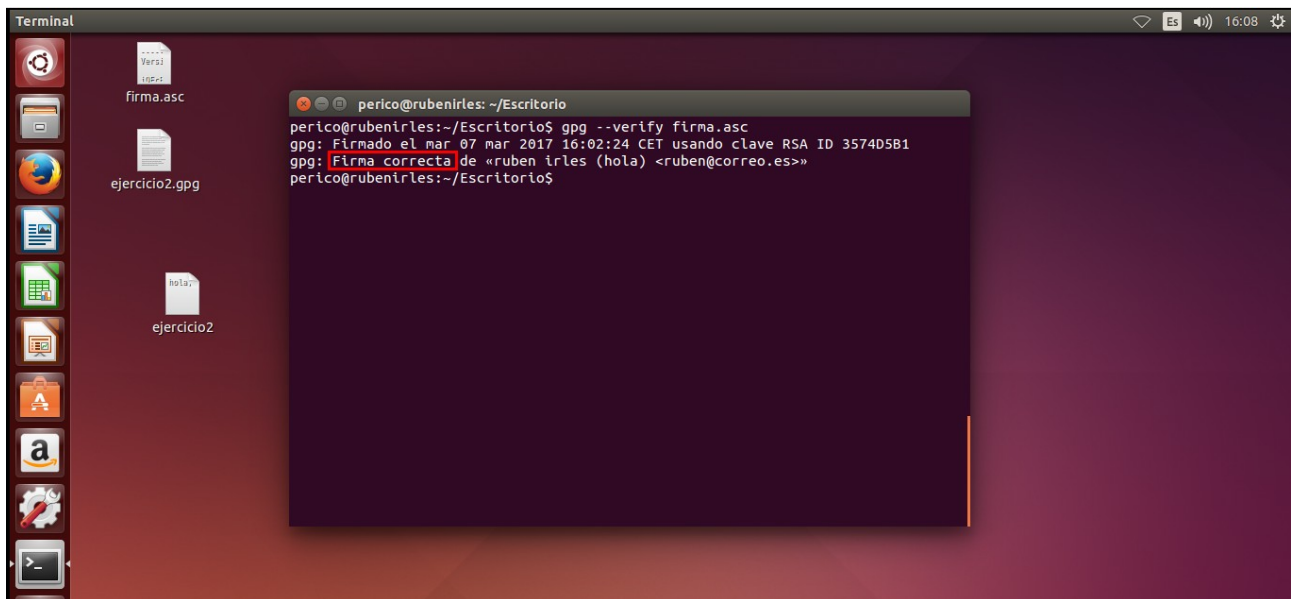


Y al ejecutar ese comando se nos creará un archivo con la extensión `.asc`, que será la firma



- Ahora comprobamos que la firma del documento es correcta:

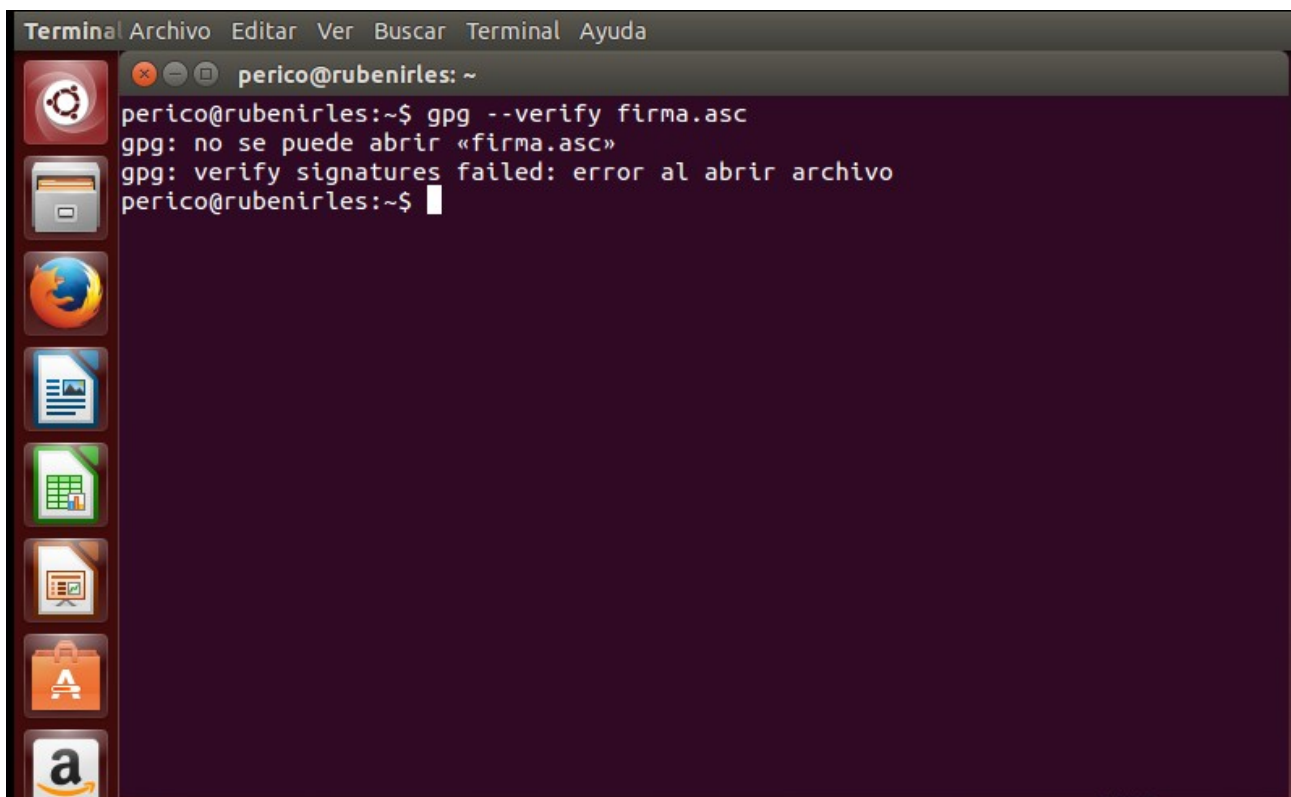
Para comprobar que la firma sea correcta, tenemos que usar el comando `gpg --verify documento`

A terminal window titled "Terminal" is open on a Linux desktop. The desktop has a dark purple background and a sidebar with icons for various applications. On the desktop, there are three files: "firma.asc", "ejercicio2.gpg", and "hola.". The terminal window shows the following commands and output:

```
perico@rubenirles: ~/Escritorio
perico@rubenirles:~/Escritorio$ gpg --verify firma.asc
gpg: Firmado el mar 07 mar 2017 16:02:24 CET usando clave RSA ID 3574D5B1
gpg: [Firma correcta] de «ruben irles (hola) <ruben@correo.es>»
perico@rubenirles:~/Escritorio$
```

Ahora vamos a modificar el archivo y poner cualquier espacio o carácter.

Una vez modificado, comprobamos la firma otra vez con el comando `gpg --verify.asc`

A terminal window titled "Terminal" is open on the same Linux desktop. The terminal window shows the following commands and output:

```
perico@rubenirles: ~
perico@rubenirles:~$ gpg --verify firma.asc
gpg: no se puede abrir «firma.asc»
gpg: verify signatures failed: error al abrir archivo
perico@rubenirles:~$
```