

Práctica de Criptografía



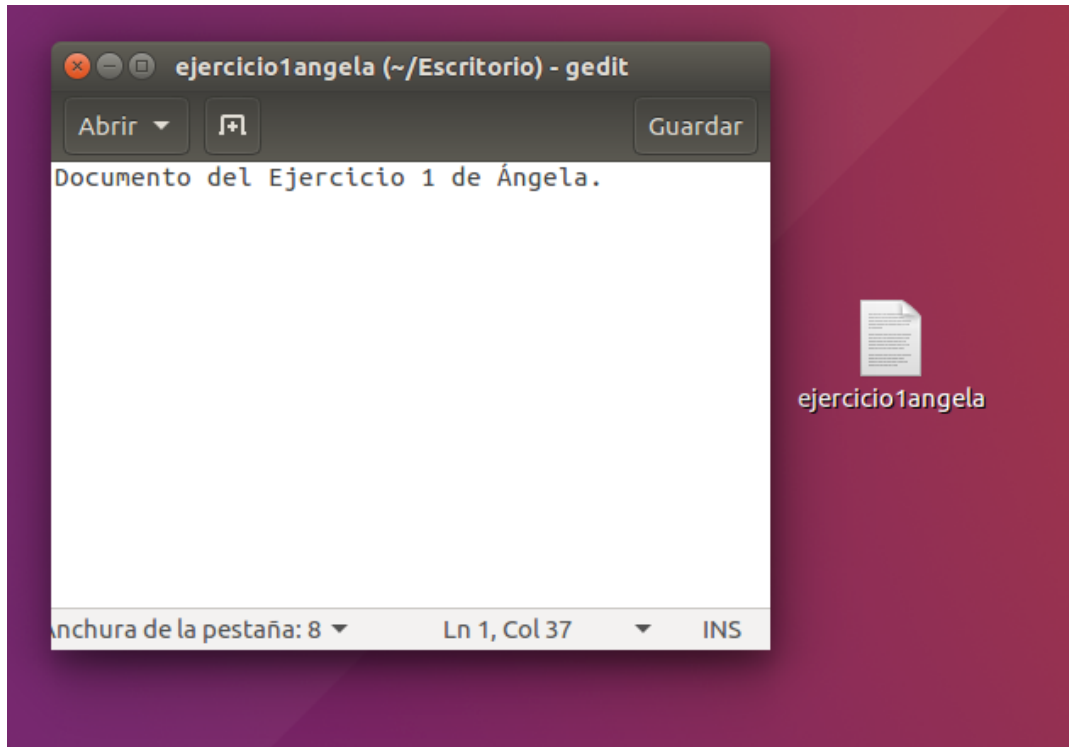
Ángela Pérez Pérez
2ºG SMR

Índice

Ejercicio 1: Cifrado simétrico de un documento.....	3
Ejercicio 2: Creación de nuestro par de claves pública-privada.....	7
Ejercicio 3: Exportar e importar claves públicas.....	11
Ejercicio 4: Cifrado y descifrado de un documento.....	14
Ejercicio 5: Firma digital de un documento.....	16

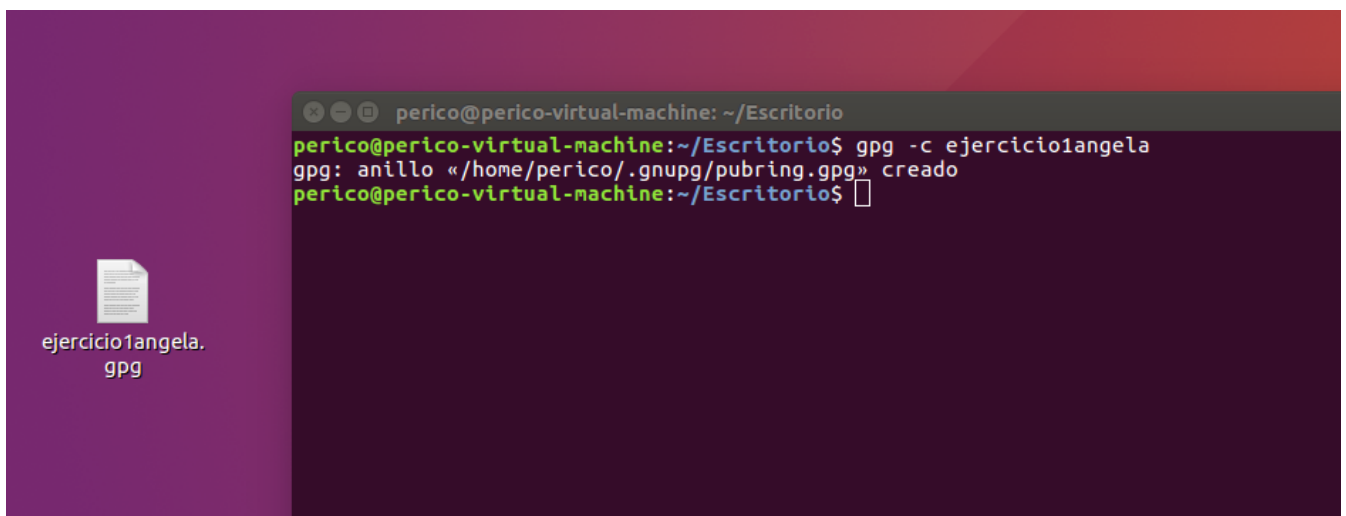
1.- Ejercicio 1: Cifrado simétrico de un documento.

1.- Crea un documento de texto con cualquier editor o utiliza uno del que dispongas.

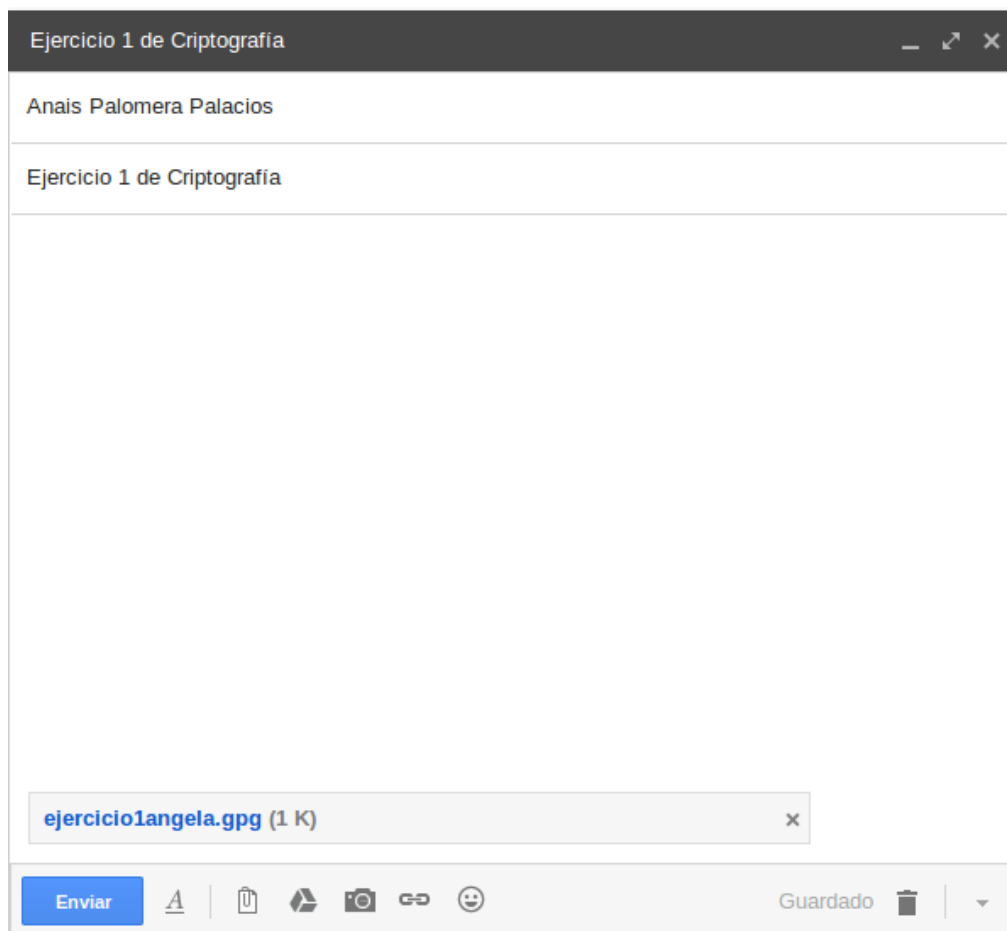


2.- Cifra este documento con alguna contraseña acordada con el compañero de al lado.

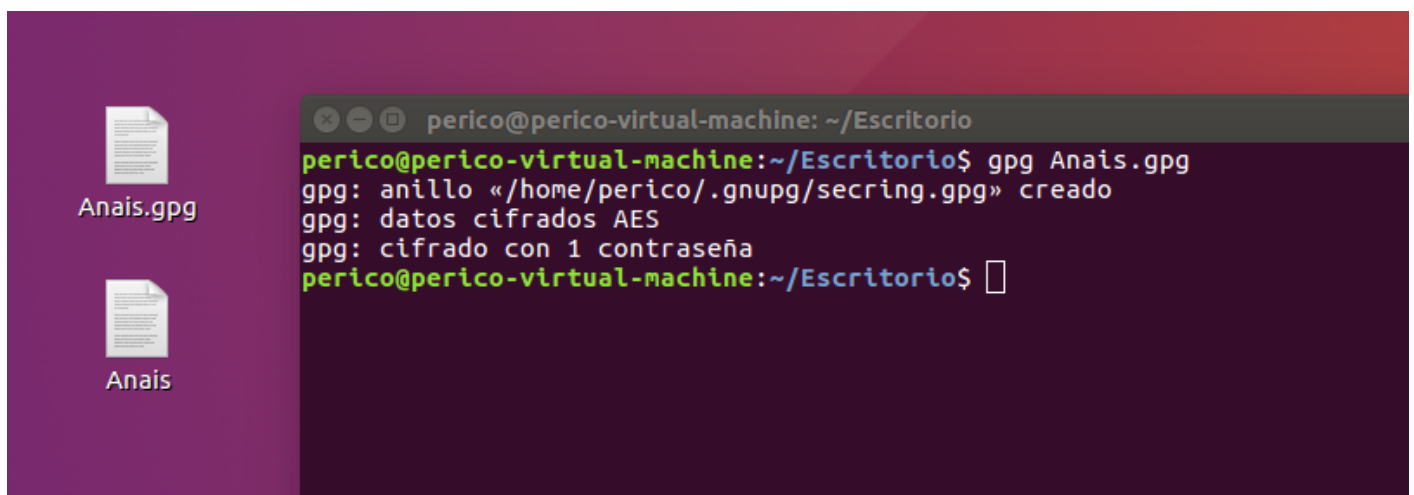
La contraseña en este caso es: 1234



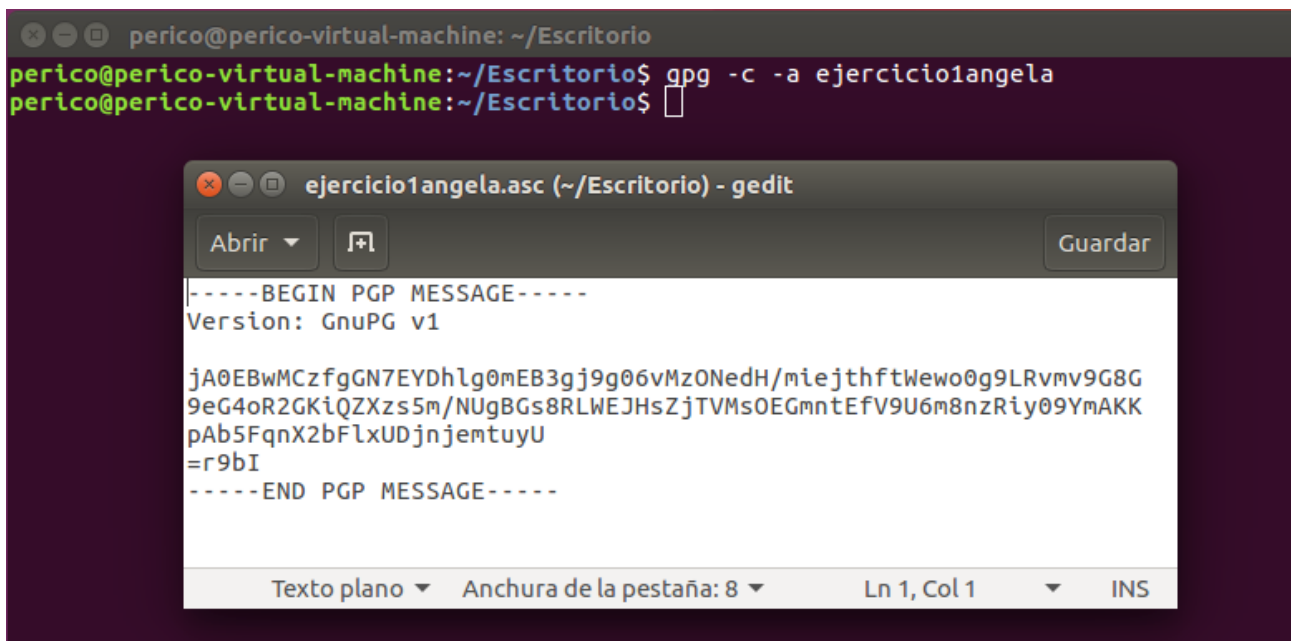
3.- Haz llegar por algún medio al compañero de al lado el documento que acabas de cifrar.



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



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.



The screenshot shows a terminal window with the command `gpg -c -a ejercicio1angela` being executed. Below the terminal, a text editor window titled "ejercicio1angela.asc (~/Escritorio) - gedit" is open, displaying the content of the generated PGP message. The message is a plain text representation of a PGP-encrypted file, starting with "-----BEGIN PGP MESSAGE-----" and ending with "-----END PGP MESSAGE-----". The body of the message is a long string of base64-encoded data.

```
perico@perico-virtual-machine: ~/Escritorio
perico@perico-virtual-machine:~/Escritorio$ gpg -c -a ejercicio1angela
perico@perico-virtual-machine:~/Escritorio$

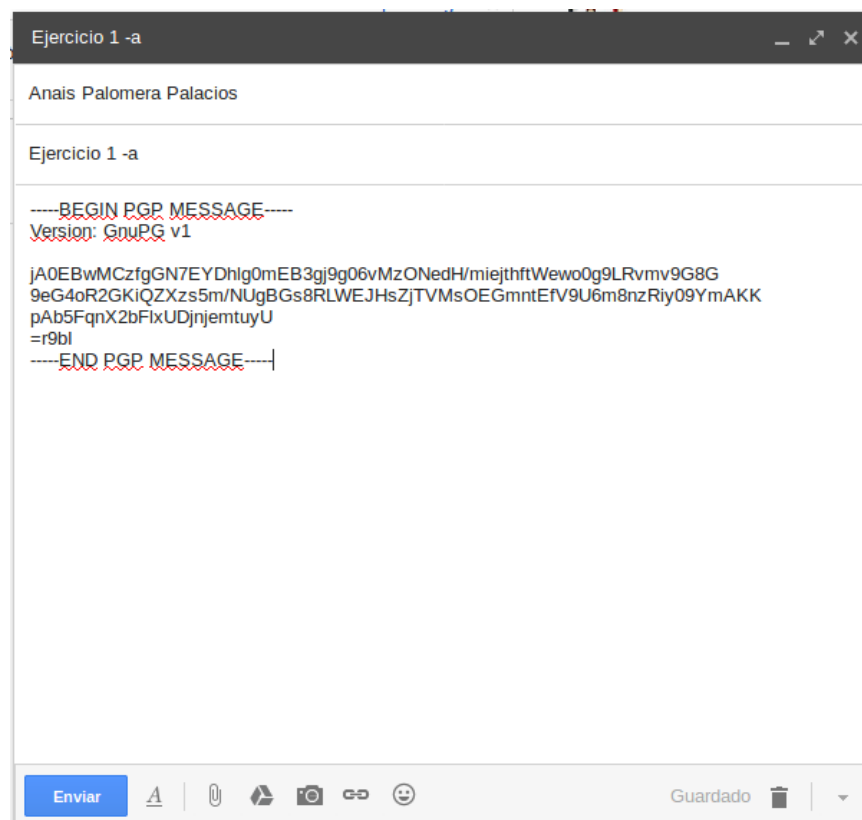
ejercicio1angela.asc (~/Escritorio) - gedit

-----BEGIN PGP MESSAGE-----
Version: GnuPG v1

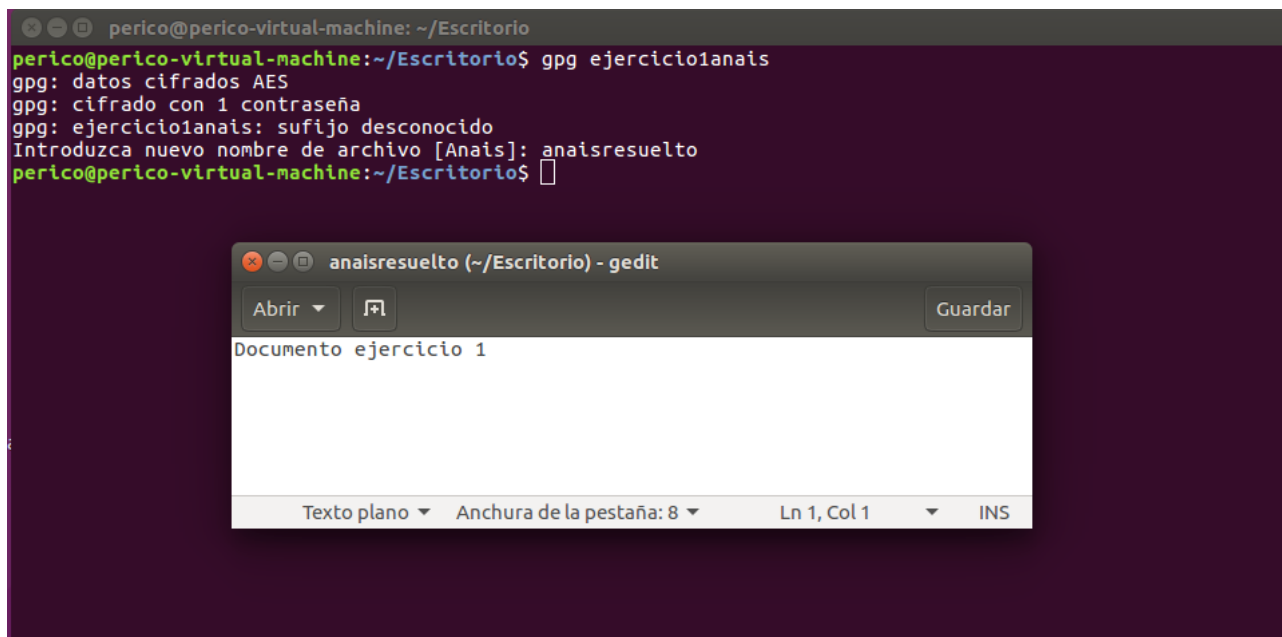
jA0EBwMCzfgGN7EYDhlg0mEB3gj9g06vMzONedH/miejthftWewo0g9LRvmv9G8G
9eG4oR2GKiQZXzs5m/NUgBGs8RLWEJHsZjTVMsOEGmntEfV9U6m8nzRiy09YmAKK
pAb5FqnX2bFlxUDjnjemtuyU
=r9bI
-----END PGP MESSAGE-----

Texto plano ▾  Anchura de la pestaña: 8 ▾  Ln 1, Col 1 ▾  INS
```

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



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



The image shows a terminal window and a gedit editor window on a virtual machine. The terminal window has a title bar that reads "perico@perico-virtual-machine: ~/Escritorio". The command prompt shows the user running "gpg ejercicio1anais". The output of the command is as follows:

```
perico@perico-virtual-machine:~/Escritorio$ gpg ejercicio1anais
gpg: datos cifrados AES
gpg: cifrado con 1 contraseña
gpg: ejercicio1anais: sufixo desconocido
Introduzca nuevo nombre de archivo [Anais]: anaisresuelto
perico@perico-virtual-machine:~/Escritorio$
```

The gedit editor window has a title bar that reads "anaisresuelto (~/Escritorio) - gedit". It contains a single line of text: "Documento ejercicio 1". The status bar at the bottom of the gedit window shows "Texto plano", "Anchura de la pestaña: 8", "Ln 1, Col 1", and "INS".

Ejercicio 2: Creación de nuestro par 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.

```
perico@perico-virtual-machine:~/Escritorio$ gpg --gen-key
gpg (GnuPG) 1.4.20; Copyright (C) 2015 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)? 1m
La clave caduca mié 05 abr 2017 23:50:28 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: Ángela Pérez Pérez
Dirección de correo electrónico: angelaperezperezfp@gmail.com
Comentario:
Está usando el juego de caracteres 'utf-8'.
Ha seleccionado este ID de usuario:
  «Ángela Pérez Pérez <angelaperezperezfp@gmail.com>»

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

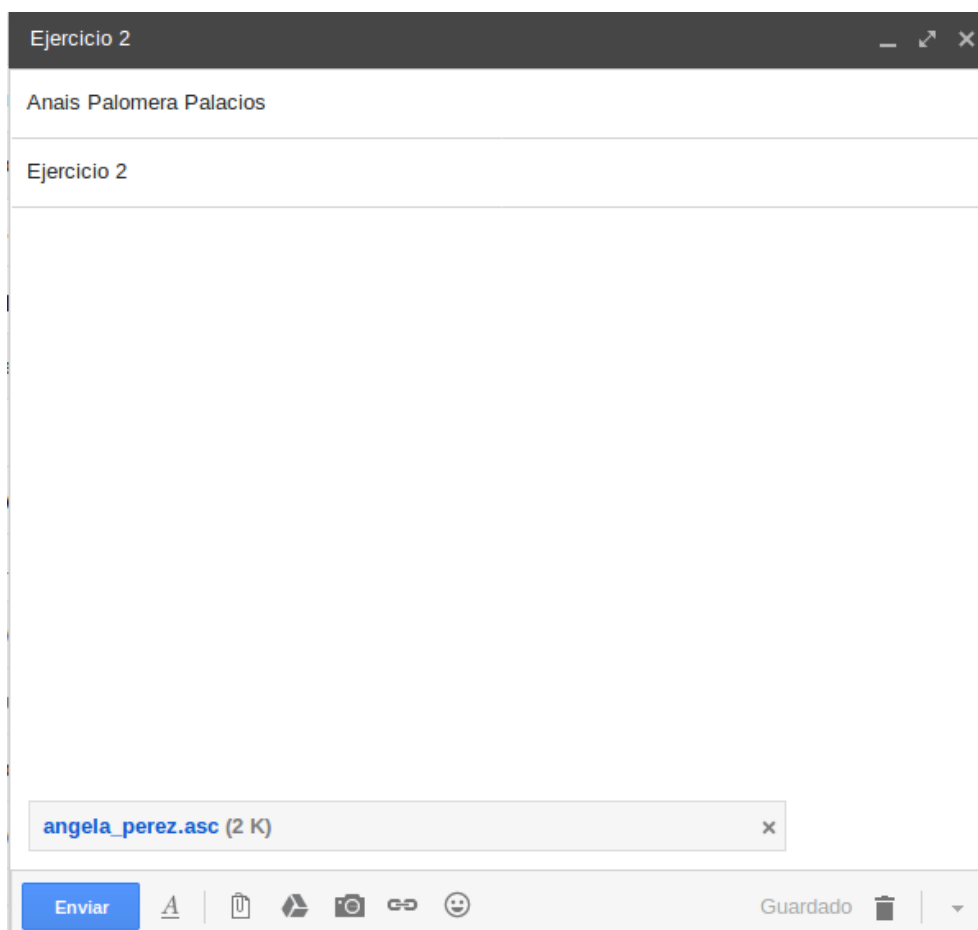
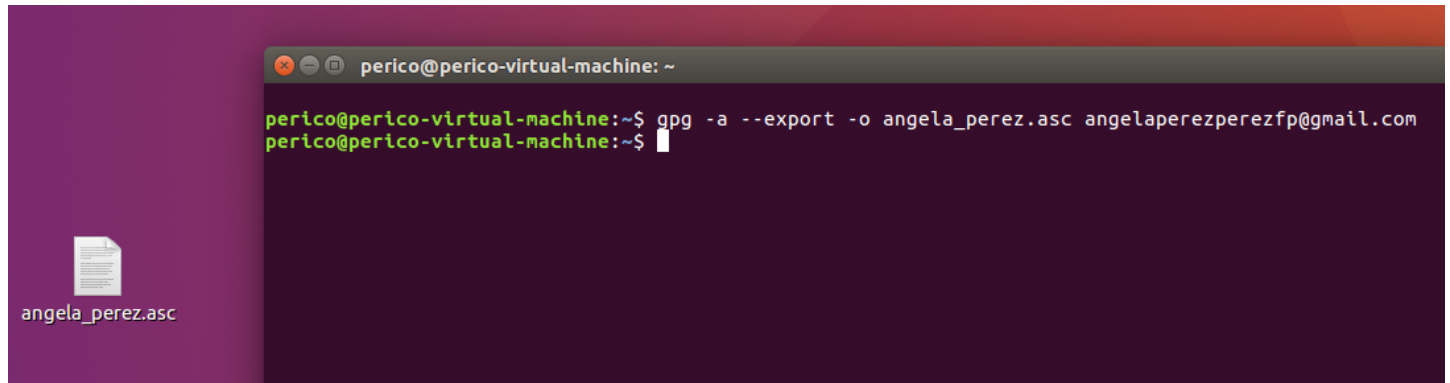
Es necesario generar muchos bytes aleatorios. Es una buena idea realizar
alguna otra tarea (trabajar en otra ventana/consola, mover el ratón, usar
la red y los discos) durante la generación de números primos. Esto da al
generador de números aleatorios mayor oportunidad de recoger suficiente
entropía.
.+++++
.....+++++
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 70 bytes más).
.....+++++
...+++++
gpg: /home/perico/.gnupg/trustdb.gpg: se ha creado base de datos de confianza
gpg: clave 36A23798 marcada como de confianza absoluta
claves pública y secreta creadas y firmadas.

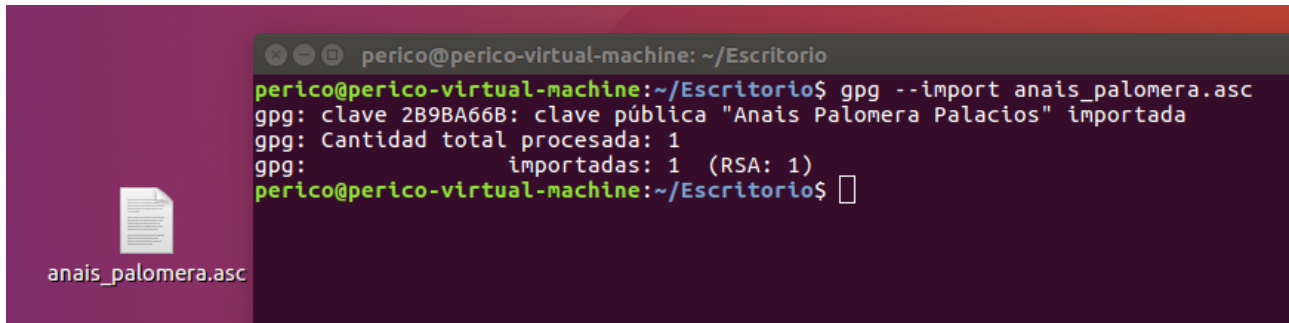
gpg: comprobando base de datos de confianza
gpg: 3 dudosa(s) necesaria(s), 1 completa(s) necesaria(s),
modelo de confianza PGP
gpg: nivel: 0 validez: 1 firmada: 0 confianza: 0-, 0q, 0n, 0m, 0f, 1u
gpg: siguiente comprobación de base de datos de confianza el: 2017-04-05
pub 2048R/36A23798 2017-03-06 [[caduca: 2017-04-05]]
    Huella de clave = 28C3 25A8 58CD E28C 7DDE CC5D D69D 13C8 36A2 3798
uid                               Ángela Pérez Pérez <angelaperezperezfp@gmail.com>
sub 2048R/D68D7F9A 2017-03-06 [[caduca: 2017-04-05]]
```


Ejercicio 3: Exportar e importar claves públicas.

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



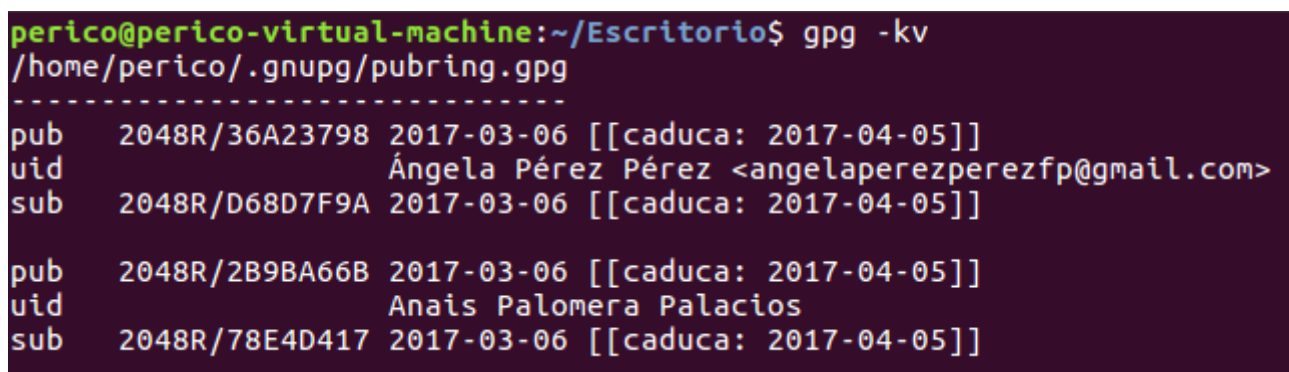
2.- Importa las claves públicas recibidas de vuestros/as compañeros/as.



The screenshot shows a terminal window titled "perico@perico-virtual-machine: ~/Escritorio". On the desktop, there is a file icon labeled "anais_palomera.asc". The terminal output shows the command "gpg --import anais_palomera.asc" being executed, followed by the messages: "gpg: clave 2B9BA66B: clave pública "Anais Palomera Palacios" importada", "gpg: Cantidad total procesada: 1", and "gpg: importadas: 1 (RSA: 1)". The prompt returns to "perico@perico-virtual-machine:~/Escritorio\$".

```
perico@perico-virtual-machine: ~/Escritorio
perico@perico-virtual-machine:~/Escritorio$ gpg --import anais_palomera.asc
gpg: clave 2B9BA66B: clave pública "Anais Palomera Palacios" importada
gpg: Cantidad total procesada: 1
gpg: importadas: 1 (RSA: 1)
perico@perico-virtual-machine:~/Escritorio$
```

3.- Comprueba que las claves se han incluido correctamente en vuestro keyring.



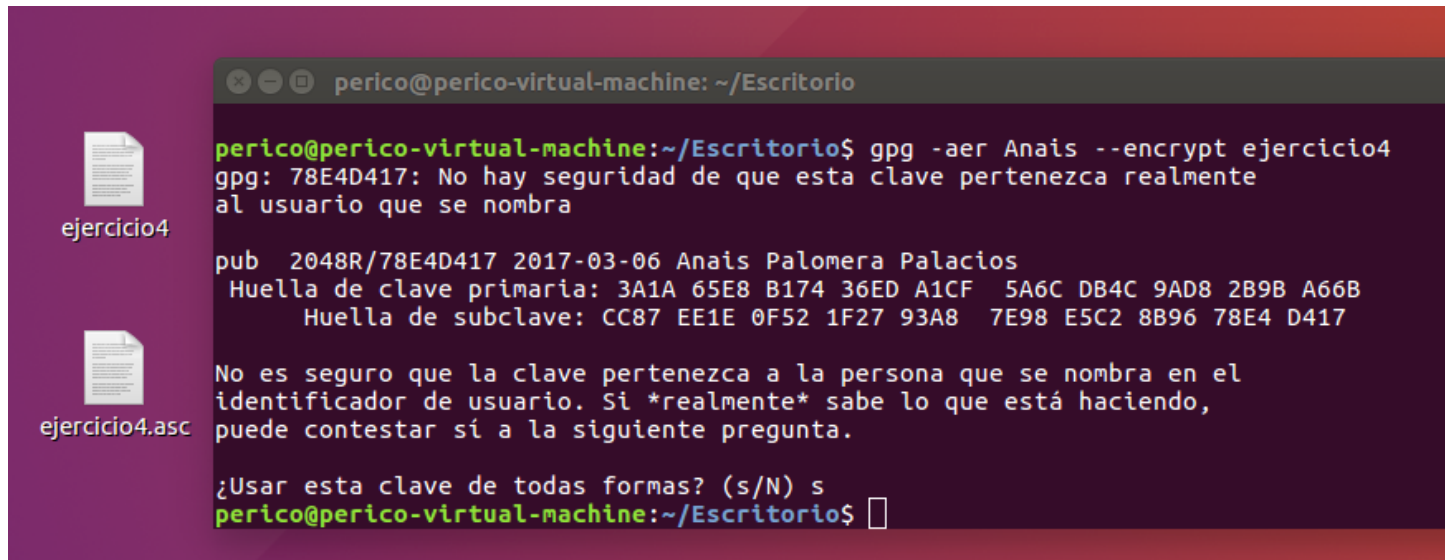
The screenshot shows a terminal window with the command "gpg -kv /home/perico/.gnupg/pubring.gpg" being executed. The output lists the keys in the keyring, including their fingerprints, creation dates, expiration dates, and names. The keys are: 2048R/36A23798 (Ángela Pérez Pérez), 2048R/D68D7F9A, 2048R/2B9BA66B (Anais Palomera Palacios), and 2048R/78E4D417.

```
perico@perico-virtual-machine:~/Escritorio$ gpg -kv
/home/perico/.gnupg/pubring.gpg
-----
pub   2048R/36A23798 2017-03-06 [[caduca: 2017-04-05]]
uid           Ángela Pérez Pérez <angelaperezperezfp@gmail.com>
sub   2048R/D68D7F9A 2017-03-06 [[caduca: 2017-04-05]]

pub   2048R/2B9BA66B 2017-03-06 [[caduca: 2017-04-05]]
uid           Anais Palomera Palacios
sub   2048R/78E4D417 2017-03-06 [[caduca: 2017-04-05]]
```

Ejercicio 4: Cifrado y descifrado de un documento.

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



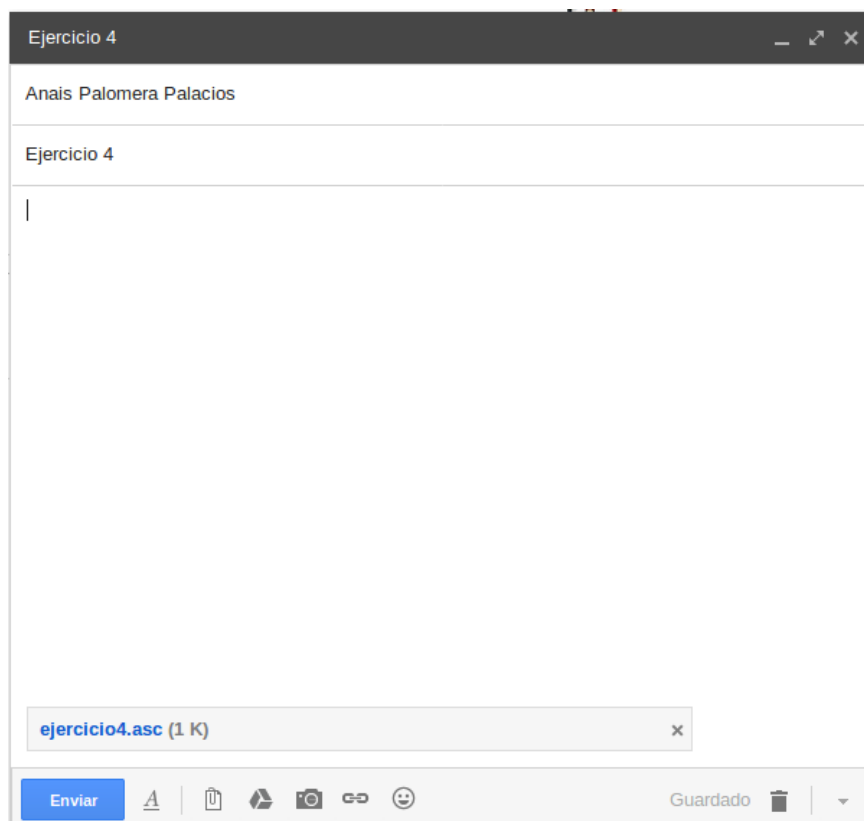
The image shows a purple desktop environment. On the left, there are two file icons: 'ejercicio4' and 'ejercicio4.asc'. To the right, a terminal window is open with the title 'perico@perico-virtual-machine: ~/Escritorio'. The terminal shows the execution of the command 'gpg -aer Anais --encrypt ejercicio4'. The output displays the GPG key ID '78E4D417' and a warning about the security of the key. It then shows the public key for 'Anais Palomera Palacios' with its primary and subkey fingerprints. A warning message follows, stating that the key's ownership is not guaranteed. Finally, it asks '¿Usar esta clave de todas formas? (s/N) s' and the user responds with 's'.

```
perico@perico-virtual-machine: ~/Escritorio
perico@perico-virtual-machine:~/Escritorio$ gpg -aer Anais --encrypt ejercicio4
gpg: 78E4D417: No hay seguridad de que esta clave pertenezca realmente
al usuario que se nombra

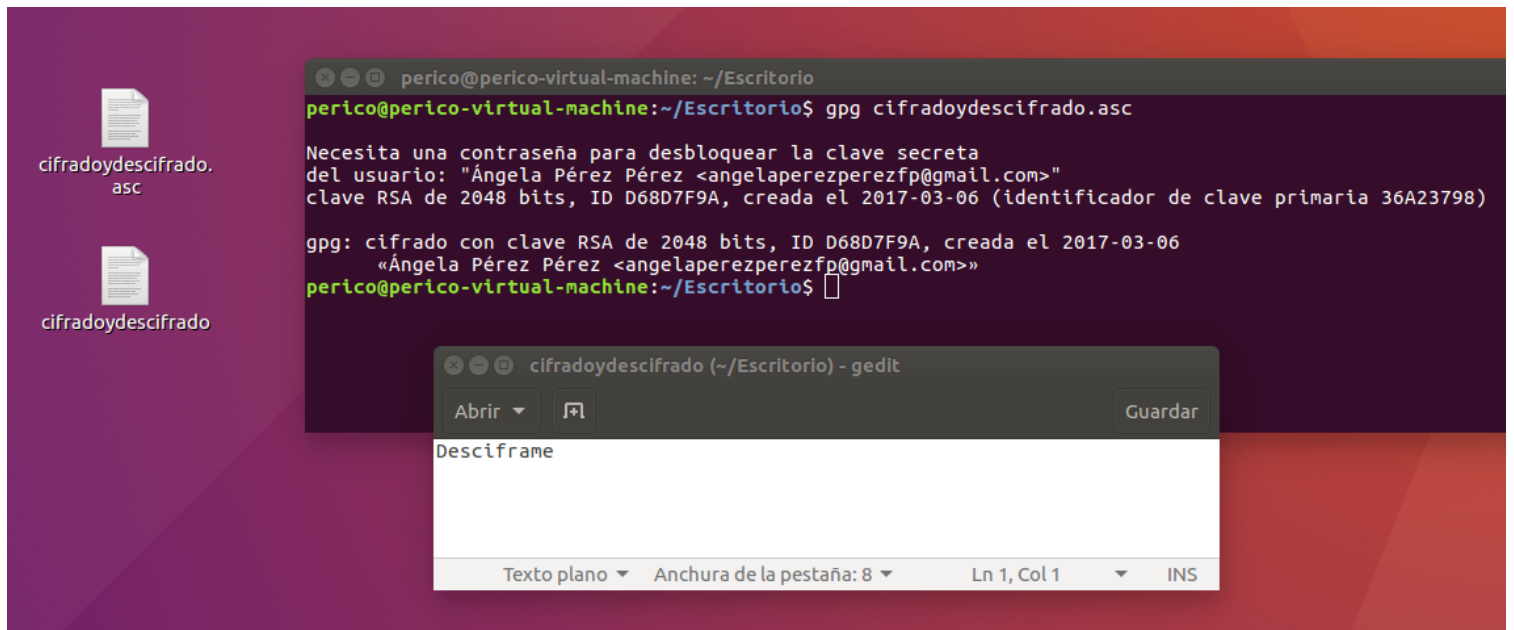
pub 2048R/78E4D417 2017-03-06 Anais Palomera Palacios
Huella de clave primaria: 3A1A 65E8 B174 36ED A1CF 5A6C DB4C 9AD8 2B9B A66B
Huella de subclave: CC87 EE1E 0F52 1F27 93A8 7E98 E5C2 8B96 78E4 D417

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) s
perico@perico-virtual-machine:~/Escritorio$
```

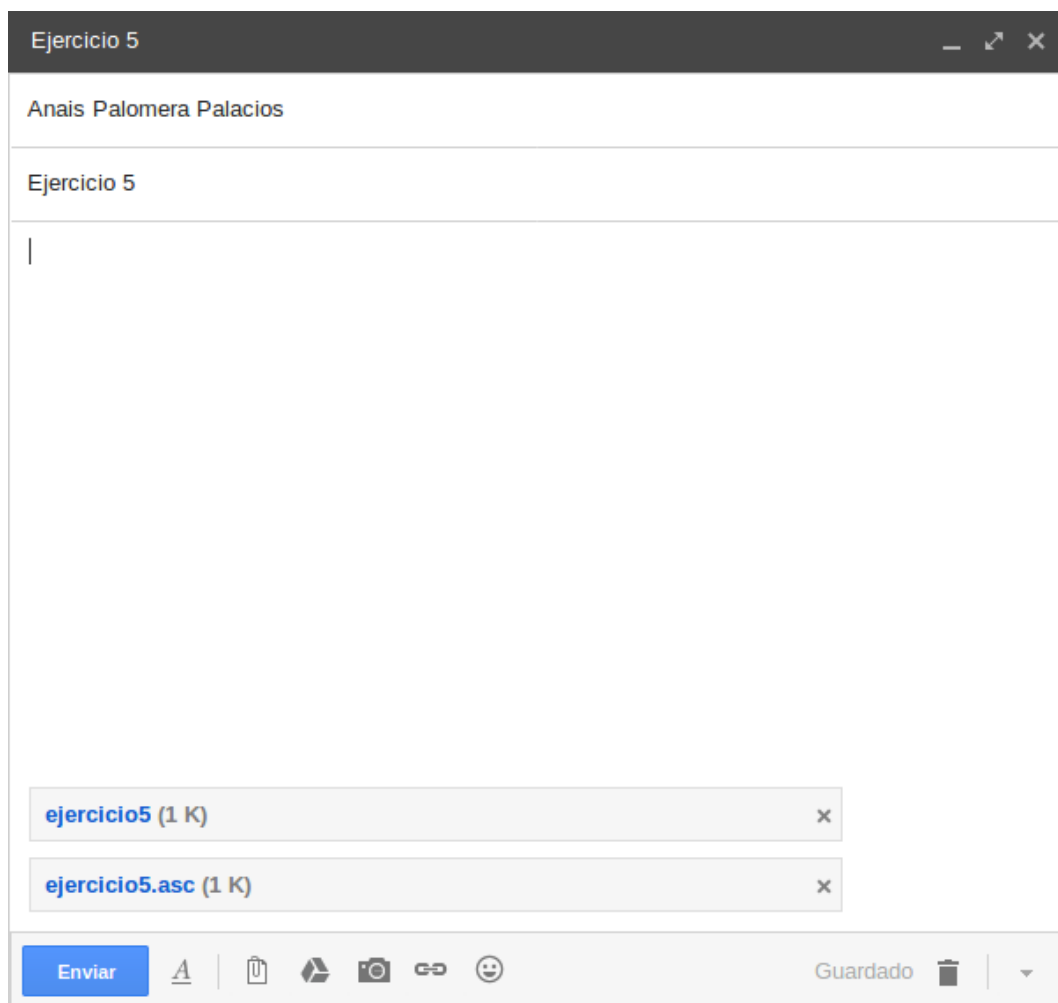
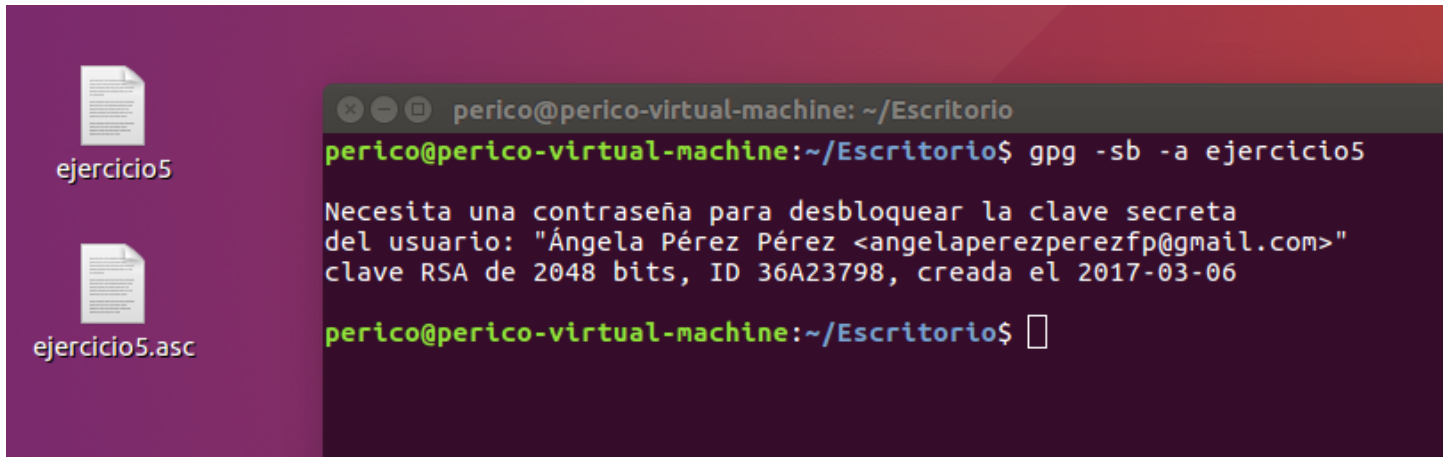


3.- Tanto nosotros como nuestro compañero comprobaremos que hemos podido descifrar los mensajes recibidos respectivamente.



Ejercicio 5: Firma digital de un documento.

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



2.- Verifica que la firma del documento es correcta.

```
perico@perico-virtual-machine: ~/Escritorio
perico@perico-virtual-machine:~/Escritorio$ gpg --verify Anais.asc
gpg: asumiendo que hay datos firmados en «Anais»
gpg: Firmado el lun 06 mar 2017 23:54:55 CET usando clave RSA ID 2B9BA66B
gpg: Firma correcta de «Anais Palomera Palacios»
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: 3A1A 65E8 B174 36ED A1CF 5A6C DB4C 9AD8 2B9B A66B
perico@perico-virtual-machine:~/Escritorio$
```

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

```
perico@perico-virtual-machine:~/Escritorio$ gpg --verify Anais.asc
gpg: asumiendo que hay datos firmados en «Anais»
gpg: Firmado el lun 06 mar 2017 23:54:55 CET usando clave RSA ID 2B9BA66B
gpg: Firma INCORRECTA de «Anais Palomera Palacios»
perico@perico-virtual-machine:~/Escritorio$
```