

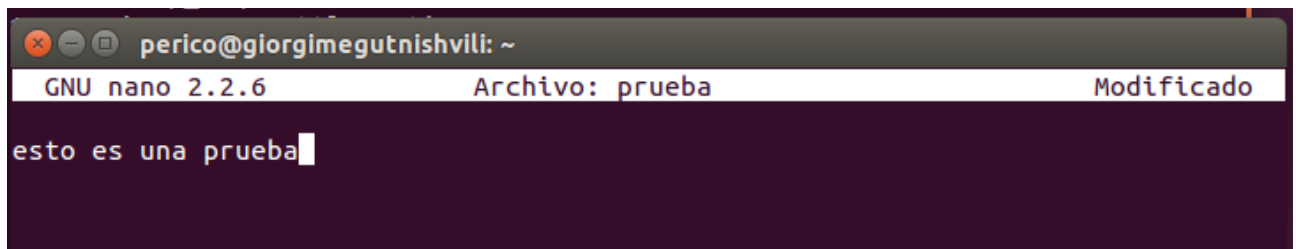
Encriptación



Giorgi Megutnishvili
16 de Marzo 2017
IES Severo Ochoa 2-SMRG

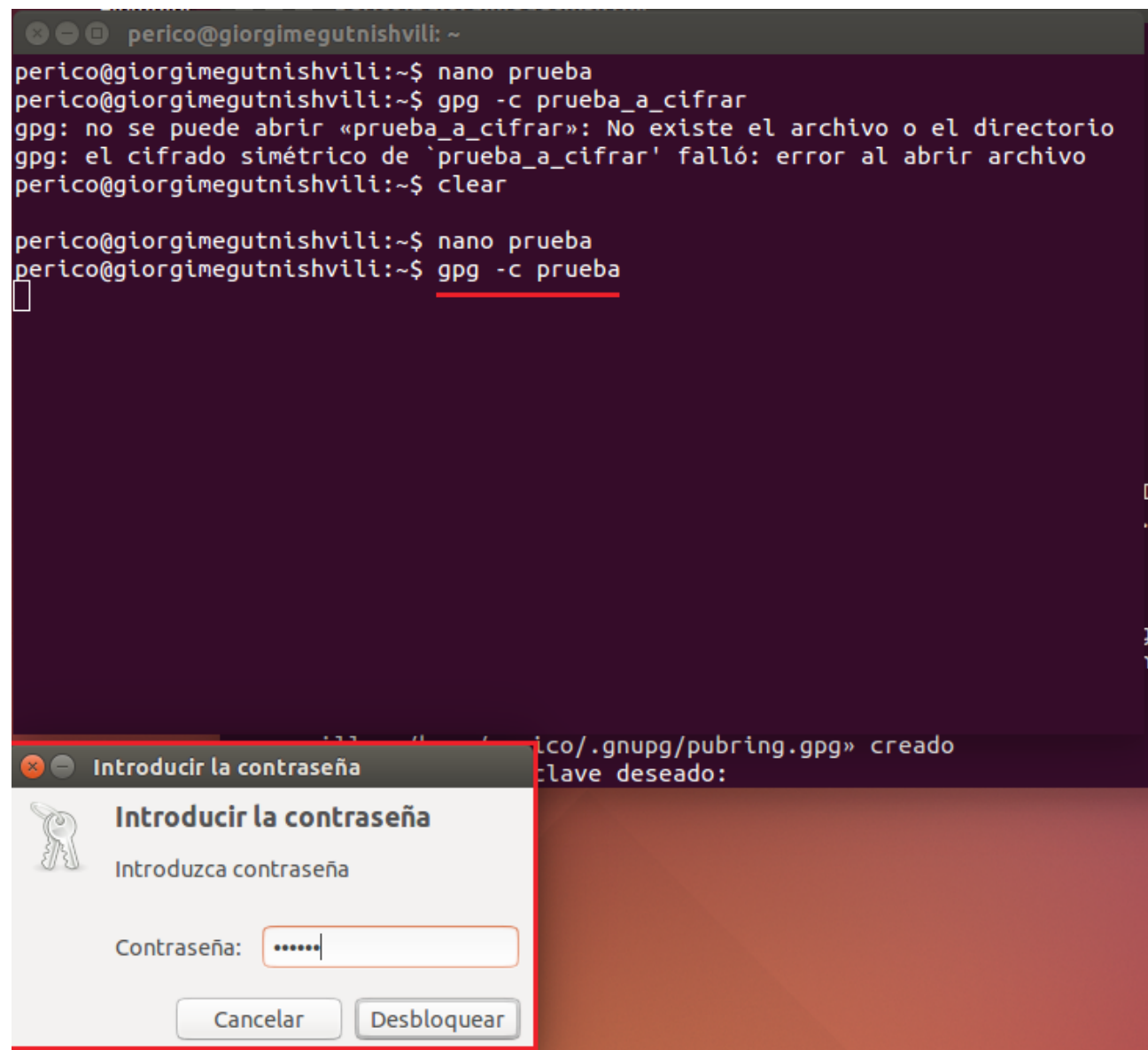
Ejercicio: Cifrado simétrico de un documento.

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



```
perico@giorgimegutnishvili: ~  
GNU nano 2.2.6 Archivo: prueba Modificado  
esto es una prueba
```

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



```
perico@giorgimegutnishvili:~$ nano prueba  
perico@giorgimegutnishvili:~$ gpg -c prueba_a_cifrar  
gpg: no se puede abrir «prueba_a_cifrar»: No existe el archivo o el directorio  
gpg: el cifrado simétrico de 'prueba_a_cifrar' falló: error al abrir archivo  
perico@giorgimegutnishvili:~$ clear  
  
perico@giorgimegutnishvili:~$ nano prueba  
perico@giorgimegutnishvili:~$ gpg -c prueba
```

Introducir la contraseña

Introduzca contraseña

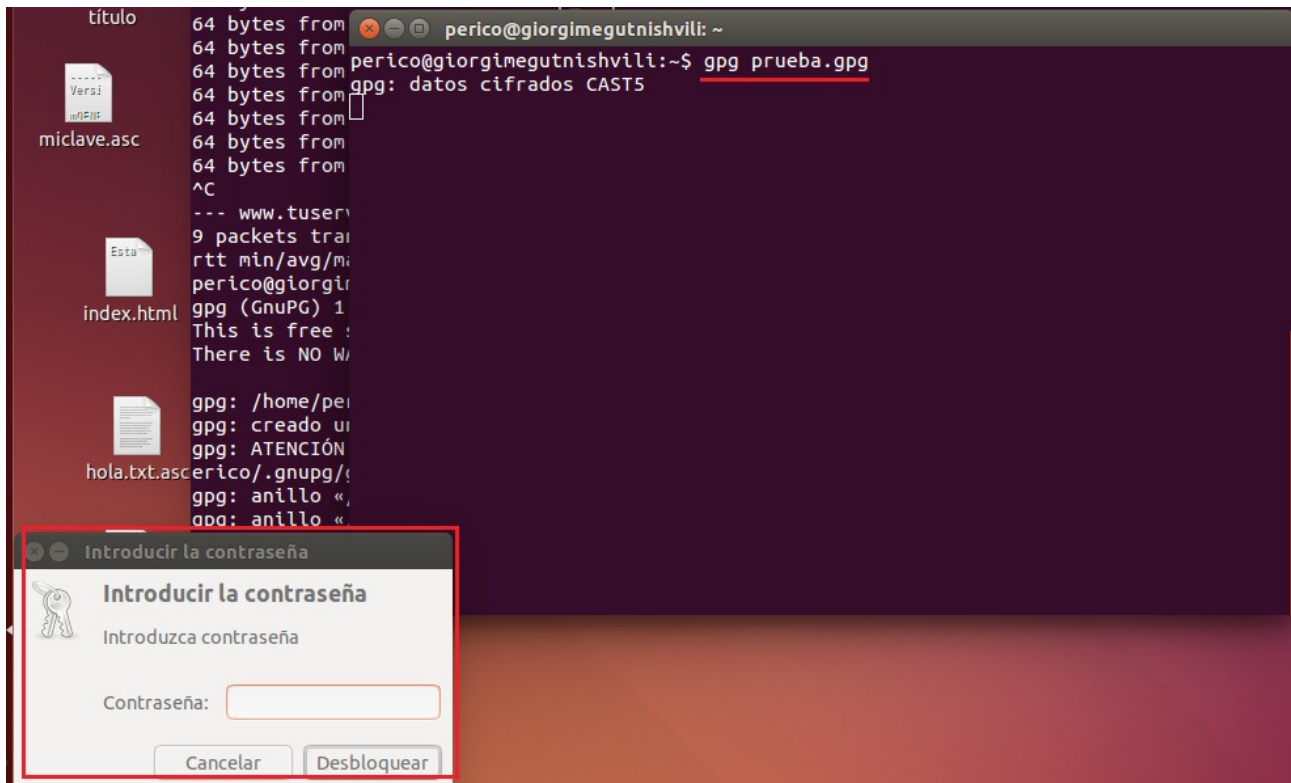
Contraseña:

Cancelar Desbloquear

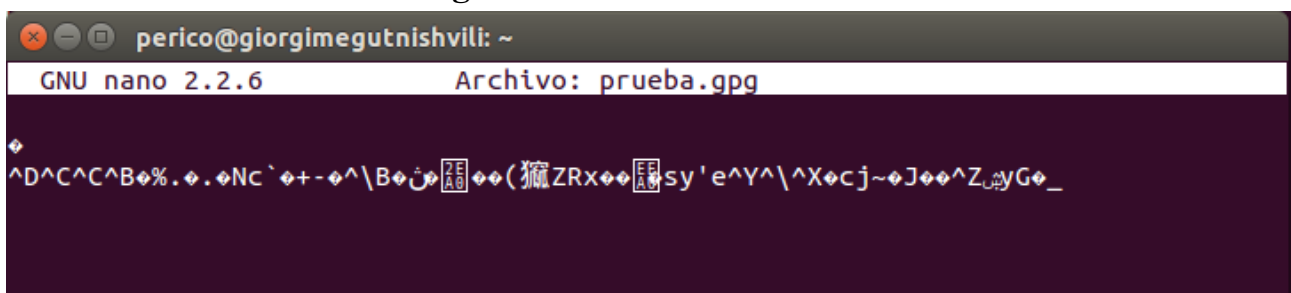
3. Haz llegar por algún medio al compañero de al lado el documento que acabas de cifrar.

(lo hare yo mismo)

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

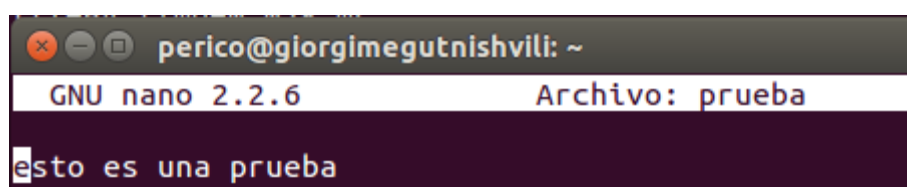


5. Repite el proceso anterior, pero añadiendo la opción -a. Observa el contenido del archivo generado con un editor de textos o con la orden cat.



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.



Ejercicio: 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@giorgimegutnishvili:~$ 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/perico/.gnupg: directorio creado
gpg: creado un nuevo archivo de configuración `/home/perico/.gnupg/gpg.conf'
gpg: ATENCIÓN: aún no se han activado en esta ejecución las opciones en `/home/p
erico/.gnupg/gpg.conf'
gpg: anillo «/home/perico/.gnupg/secring.gpg» creado
gpg: anillo «/home/perico/.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
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 jue 13 abr 2017 06:47:42 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: giorgimegut
Dirección de correo electrónico: giorgimegut@gmail.com
Comentario:
Ha seleccionado este ID de usuario:
  «giorgimegut <giorgimegut@gmail.com>»
```

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



Ejercicio: 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.

```
perico@giorgimegutnishvili:~$ gpg --import ramon
gpg: clave A9230619: clave pública "Ramón Botella Alfonso (Hola) <ramon.botell.a@gmail.com>" importada
gpg: Cantidad total procesada: 1
gpg:             importadas: 1 (RSA: 1)
perico@giorgimegutnishvili:~$ gpg -a -r ramon --encrypt cifradogio.txt
gpg: 0B863318: No hay seguridad de que esta clave pertenezca realmente
al usuario que se nombra

pub 2048R/0B863318 2017-03-14 Ramón Botella Alfonso (Hola) <ramon.botell.a@gmail.com>
Huella de clave primaria: EAA6 F53C 0A2A 39CA 05C6 C392 83CF D869 A923 0619
Huella de subclave: EA0D 7175 D1D7 6B16 1EE1 70E0 129E 7553 0B86 3318

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
```

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

```
perico@giorgimegutnishvili:~$ gpg -kv
/home/perico/.gnupg/pubring.gpg
-----
pub      2048R/465AEA40 2017-03-14 [[caduca: 2017-04-13]]
uid                               giorgimegut (Soy giorgi) <giorgimegut@gmail.com>
sub      2048R/3A082AA1 2017-03-14 [[caduca: 2017-04-13]]
-----
pub      2048R/A9230619 2017-03-14 [[caduca: 2017-04-13]]
uid                               Ramón Botella Alfonso (Hola) <ramon.botell.a@gmail.com>
sub      2048R/0B863318 2017-03-14 [[caduca: 2017-04-13]]
-----
perico@giorgimegutnishvili:~$
```

Ejercicio: 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.

```
perico@giorgimegutnishvili:~$ gpg -a -r ramon --encrypt cifradogio.txt
gpg: 0B863318: No hay seguridad de que esta clave pertenezca realmente
al usuario que se nombra

pub 2048R/0B863318 2017-03-14 Ramón Botella Alfonso (Hola) <ramon.botella@gmail
.com>
Huella de clave primaria: EAA6 F53C 0A2A 39CA 05C6 C392 83CF D869 A923 0619
Huella de subclave: EA0D 7175 D1D7 6B16 1EE1 70E0 129E 7553 0B86 3318

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
```

2. Nuestro compañero, a su vez, nos remitirá un archivo cifrado para que nosotros lo descifremos.

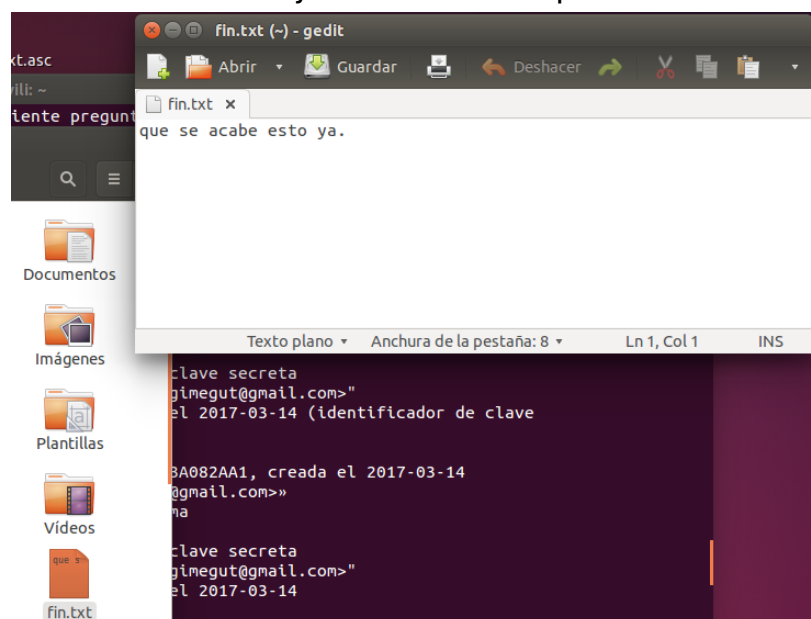
```
perico@giorgimegutnishvili:~$ gpg fin.txt.asc

Necesita una contraseña para desbloquear la clave secreta
del usuario: "giorgimegut (Soy giorgi) <giorgimegut@gmail.com>"
clave RSA de 2048 bits, ID 3A082AA1, creada el 2017-03-14 (identificador de clave
primaria 465AEA40)

gpg: cifrado con clave RSA de 2048 bits, ID 3A082AA1, creada el 2017-03-14
«giorgimegut (Soy giorgi) <giorgimegut@gmail.com>»
perico@giorgimegutnishvili:~$ gpg -sb -a firma

Necesita una contraseña para desbloquear la clave secreta
del usuario: "giorgimegut (Soy giorgi) <giorgimegut@gmail.com>"
clave RSA de 2048 bits, ID 465AEA40, creada el 2017-03-14
```

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



4. 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.

No le he podido mandarle a nadie pero he hecho yo mismo la prueba esto me salía antes de tener la clave de ramón

```
perico@giorgimegutnishvili:~$ gpg texto.txt.asc
gpg: cifrado con clave RSA, ID 0B863318
gpg: descifrado fallido: clave secreta no disponible
```

Ejercicio: 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.

```
perico@giorgimegutnishvili:~$ gpg -sb -a firmaramon.txt

Necesita una contraseña para desbloquear la clave secreta
del usuario: "giorgimegut (Soy giorgi) <giorgimegut@gmail.com>"
clave RSA de 2048 bits, ID 465AEA40, creada el 2017-03-14
```

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

No se cual se refería así que puse las 2 el de ramón y el abajo es el mio.

```
perico@giorgimegutnishvili:~$ gpg firmar.txt.asc
gpg: Firmado el mié 15 mar 2017 00:00:26 CET usando clave RSA ID A9230619
gpg: Firma correcta de «Ramón Botella Alfonso (Hola) <ramon.botell.a@gmail.com>»
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: EAA6 F53C 0A2A 39CA 05C6 C392 83CF D869 A
923 0619
```

No se porque era pero al enviarle el archivo a Ramón le aparecia como si alguien hubiese modificado el archivo no se si era culpa de filezilla o que, así que lo hare en mi propia maquina para que se vea la firma.

```
perico@giorgimegutnishvili:~$ gpg --verify firmaramon.txt.asc
gpg: Firmado el mié 15 mar 2017 00:19:09 CET usando clave RSA ID 465AEA40
gpg: Firma correcta de «giorgimegut (Soy giorgi) <giorgimegut@gmail.com>»
perico@giorgimegutnishvili:~$
```

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

```
perico@giorgimegutnishvili:~$ gpg firmar.txt.asc
gpg: Firmado el mié 15 mar 2017 00:00:26 CET usando clave RSA ID A9230619
gpg: Firma INCORRECTA de «Ramón Botella Alfonso (Hola) <ramon.botell.a@gmail.com>»
```