Práctica 3: Autenticación de mensajes

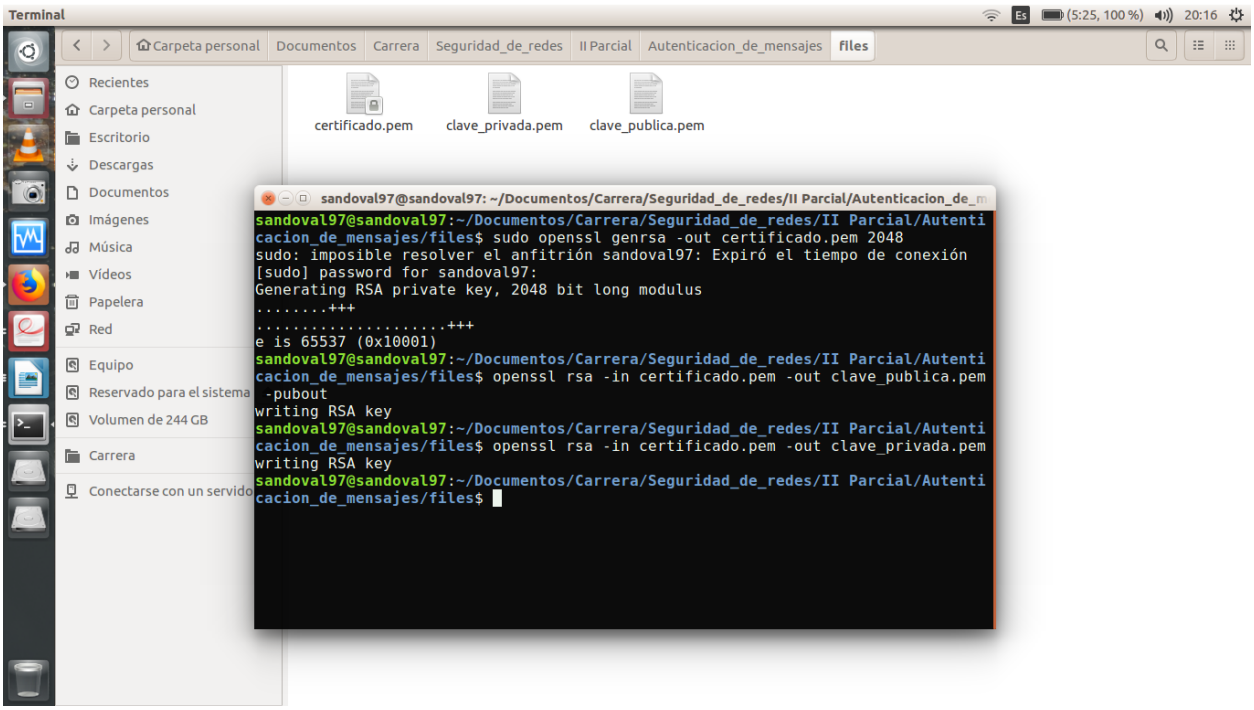
1.1 Crear una clave pública y una privada con OpenSSL

Lo primero que deberemos de hacer es crear una clave pública y una privada para nuestro uso. Para ello las crearemos en un solo archivo haciendo uso del comando:

$ sudo openssl genrsa -out certificado.pem 2048

A continuación podemos utilizar el comando rsa para extraer en otro fichero .pem sólo la clave pública y sólo la clave privada.

openssl rsa -in certificado.pem -out clave_publica.pem -pubout
openssl rsa -in certificado.pem -out clave_privada.pem



2. Conceptos básicos de cifrado asimétrico

Crear un texto corto (una línea) en un archivo de texto

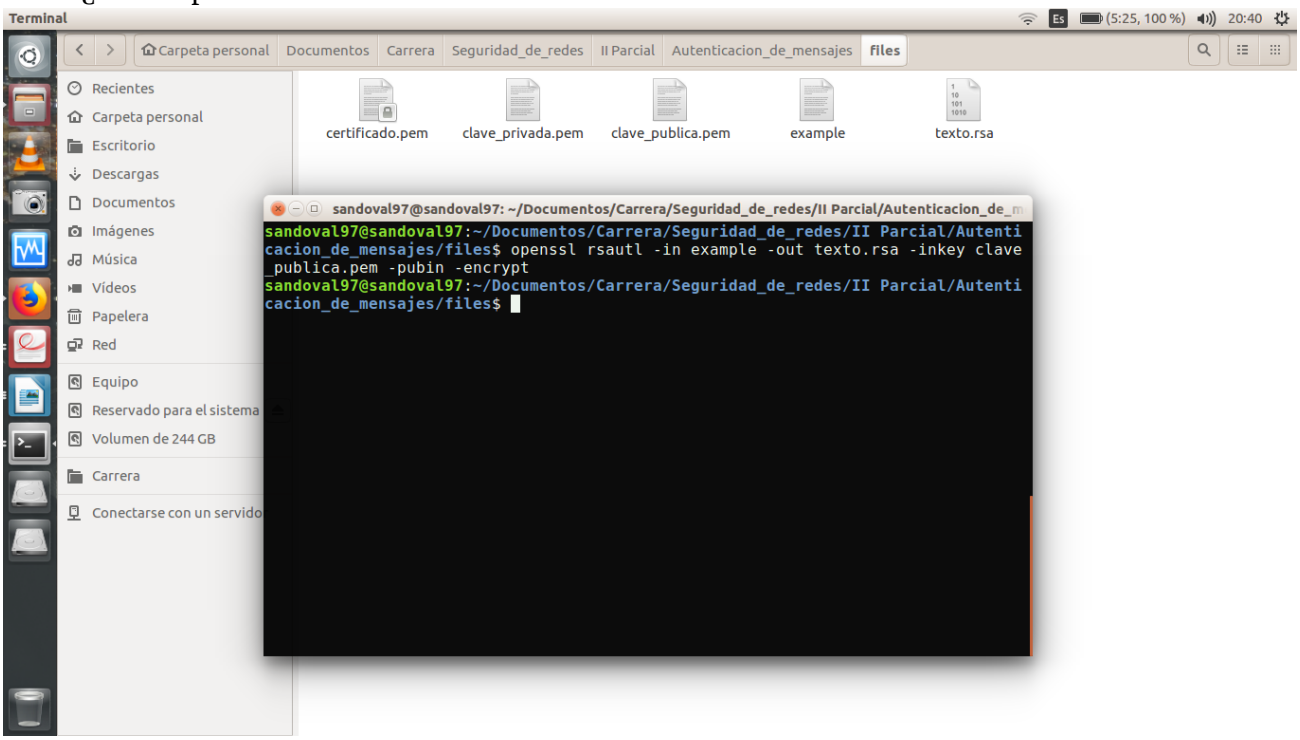
2.1 Para cifrar con la clave pública:

openssl rsautl -in texto.txt -out texto.rsa -inkey clave_publica.pem -pubin -encrypt

- ¿qué significa cada opción?

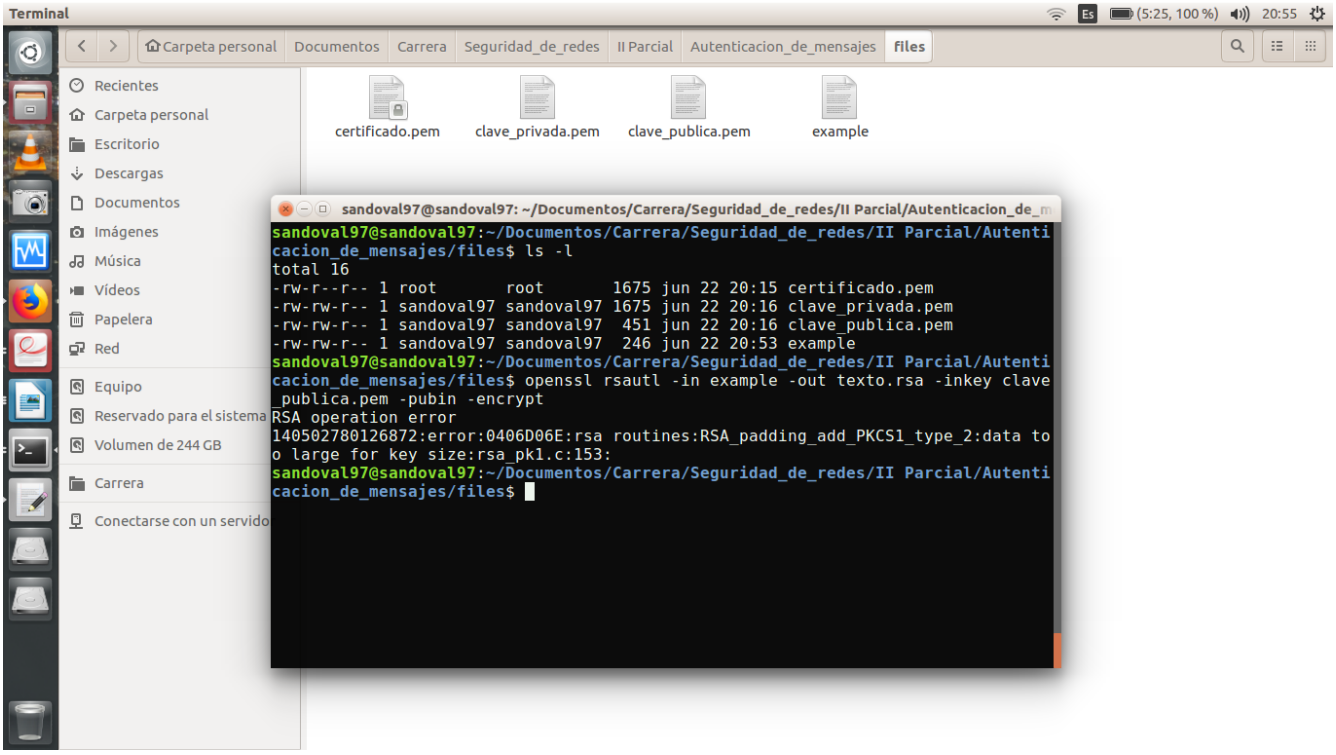
R: El comando rsautl se puede usar para firmar, verificar, cifrar y descifrar datos usando el algoritmo RSA, con el parametro -in especificamos el archivo de entrada a cifrar, -out es para especificar el nombre del archivo resultante despues del cifrado, -inkey es para especificar la clave publica con la que queremos cifrar el mensaje, -pubin indica que el archivo de entrada es una clave publica y -encrypt es para cifrar los datos de entrada utilizando una clave pública RSA.

- ¿Pide el password?



R: Como podemos observar en la imagen el comando efectuado no pide una contraseña

- ¿Cuál es la longitud máxima de fichero que se puede cifrar por este método?



R: el máximo de los datos que se pueden cifrar con RSA es de 245 bytes.

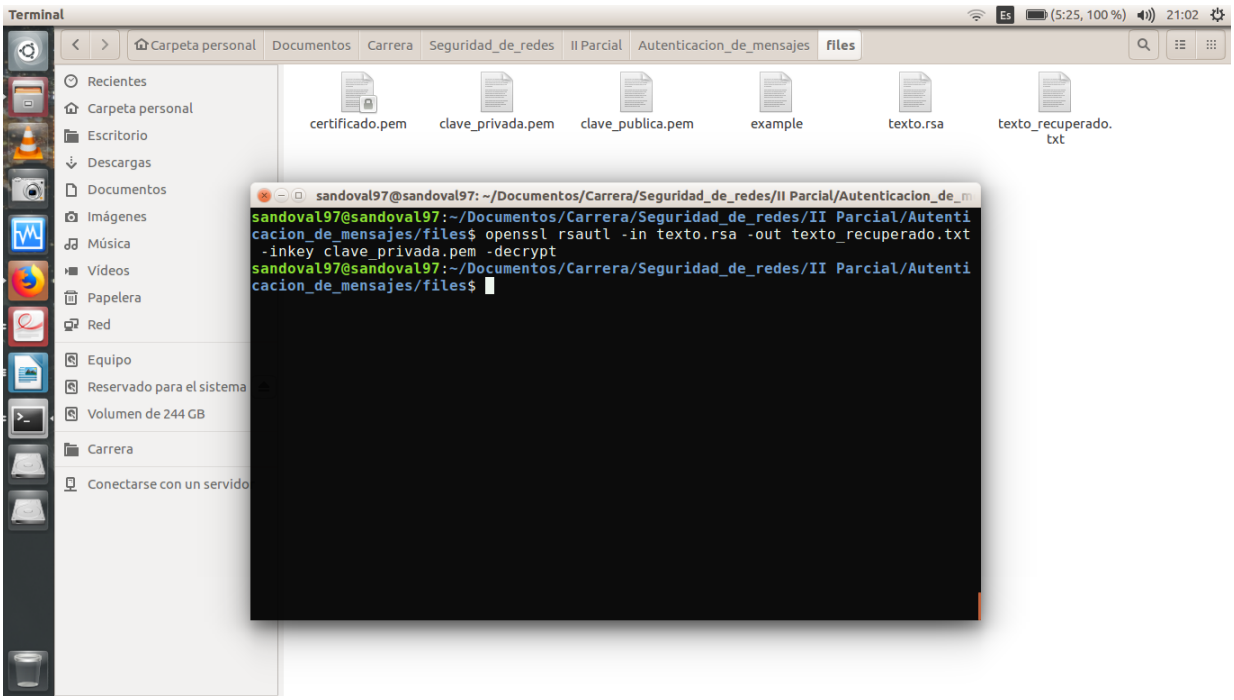
2.2 Para descifrar con la clave privada:

openssl rsautl -in texto.rsa -out texto_recuperado.txt -inkey clave_privada.pem -decrypt
openssl rsautl -in texto.rsa -out texto_recuperado.txt -inkey certificado.pem -decrypt

- ¿qué significa cada opción?

R: al igual que en la prueba anterior algunos parametros son los que cambian como lo es el parametro -decrypt esto es descifrar los datos de entrada utilizando una clave privada RSA.

- ¿Pide el password?



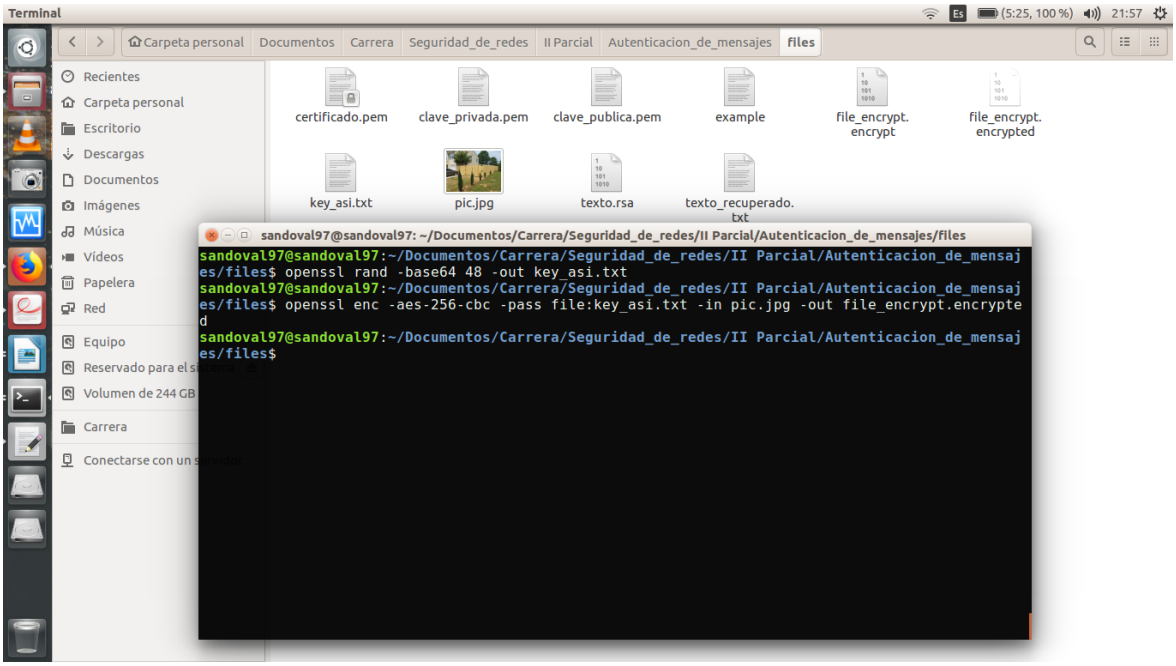
R: como podemos ver tampoco en esta opcion pide una contraseña.

3. Envío de un mensaje cifrado a un compañero

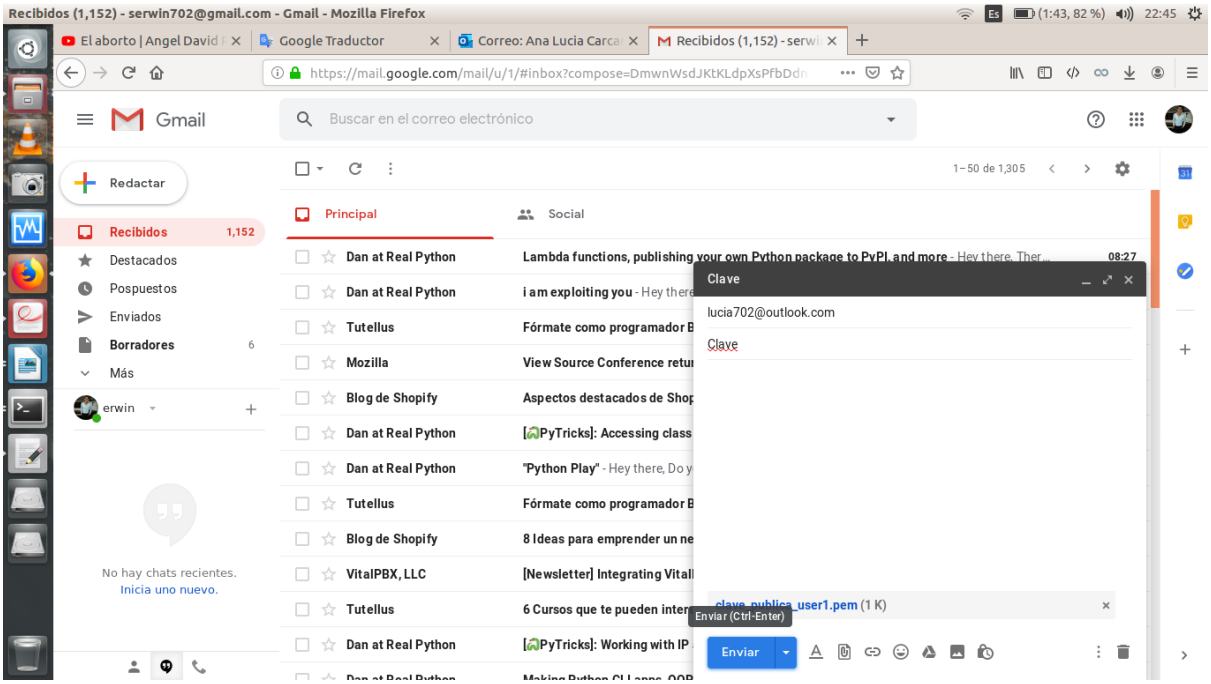
Para cifrar ficheros grandes se suelen combinar algoritmos simétricos con asimétricos. Realizar con openssl los siguientes pasos para poder enviar por correo electrónico un archivo grande.

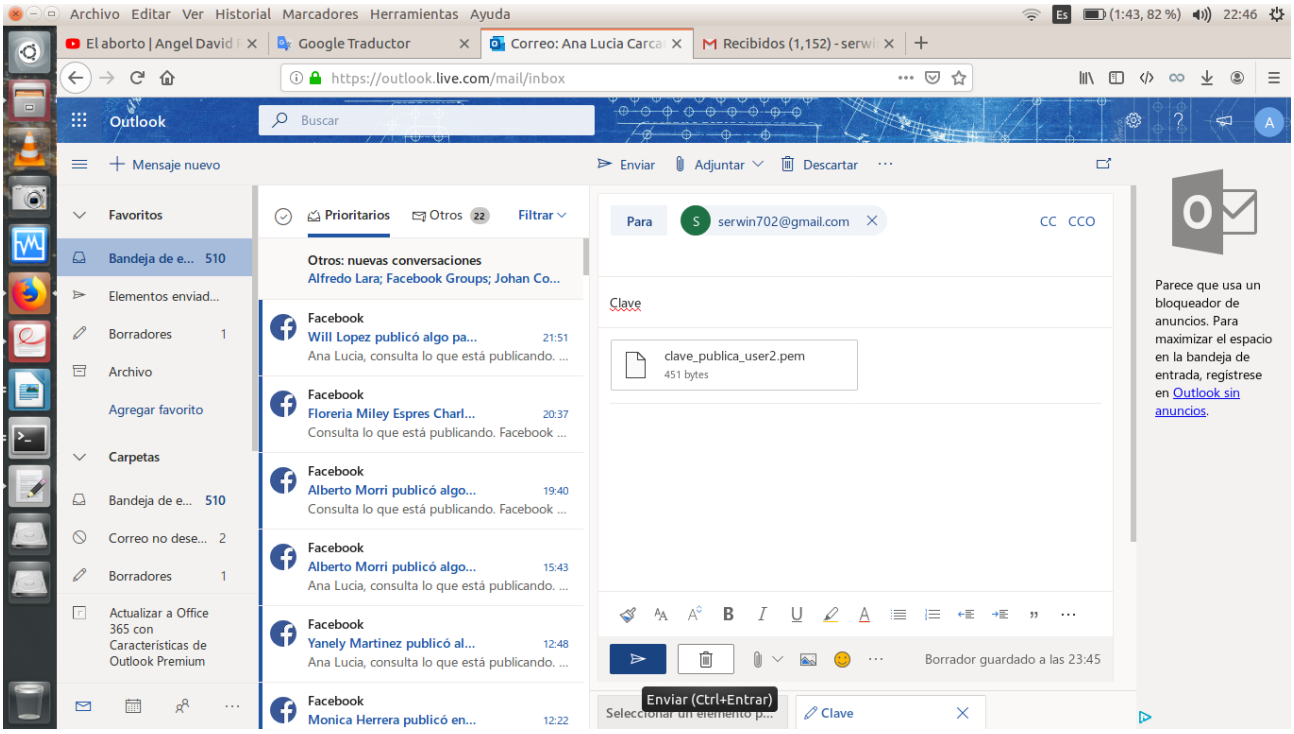
1. Preparar un fichero grande, por ejemplo una foto.
2. Cifrar el fichero utilizando un algoritmo simétrico.

Creamos la clave con la que vamos a cifrar el fichero y luego lo ciframos



3. Por correo electrónico, intercambiar con un compañero las claves públicas.



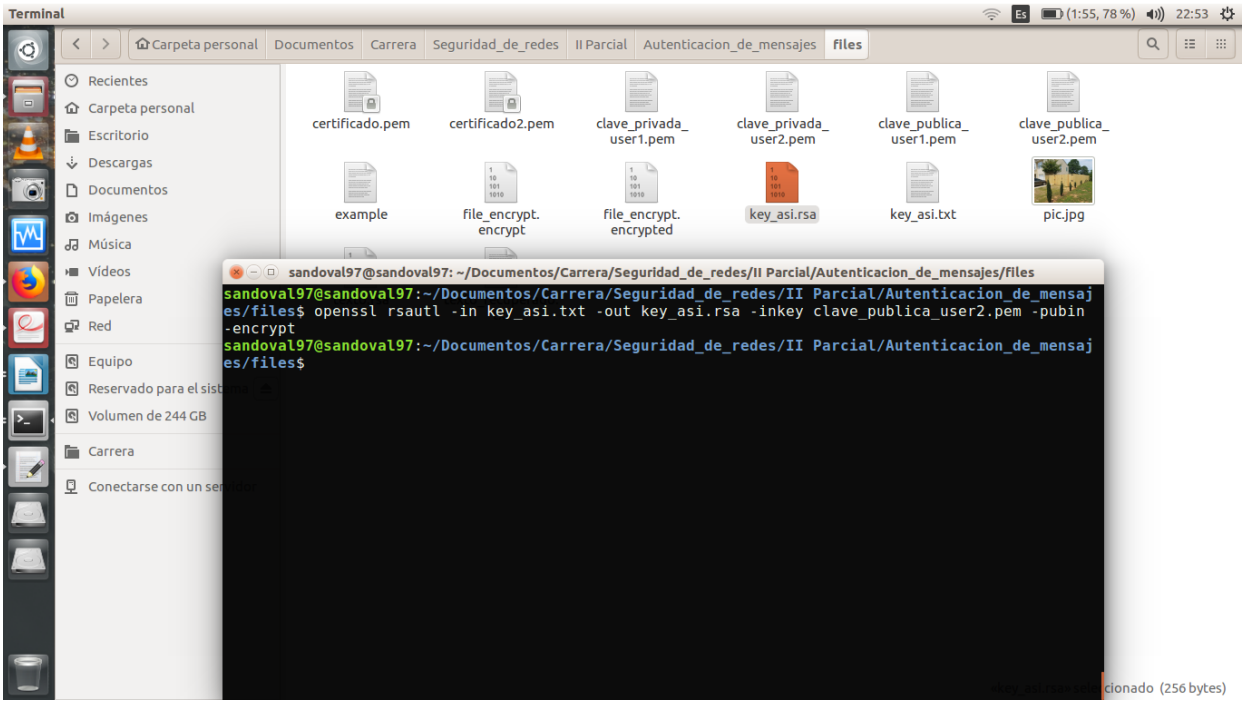


4. Cifrar con RSA la clave utiliza para el cifrado simétrico.

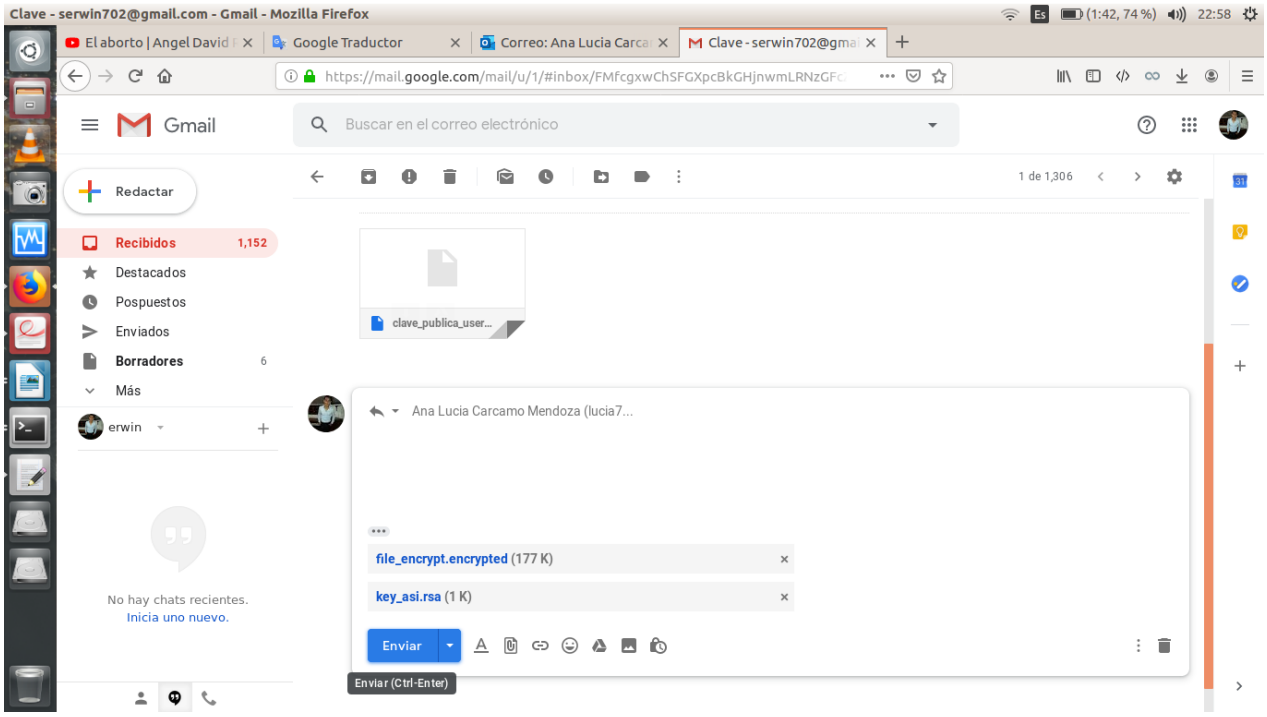
- La clave utilizada para el cifrado simétrico debe guardarse en un fichero de texto para poder cifrarla con RSA
- ¿qué clave habrá que utilizar para cifrar con RSA?

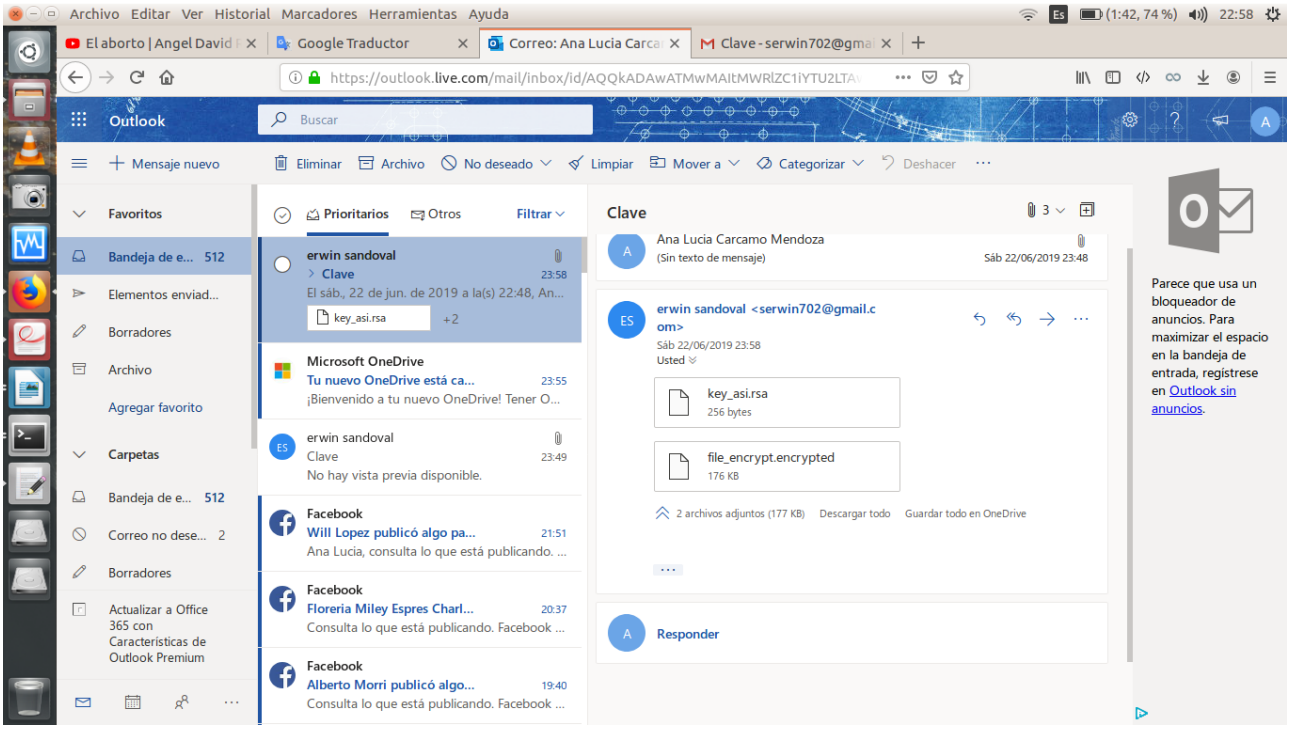
R: el usuario 1 usara la clave publica del usuario 2 para que el descifre con su clave privada y vice versa de esa forma tendran una comunicación segura

- Al realizar este cifrado RSA, openssl no debe pedir ninguna clave.

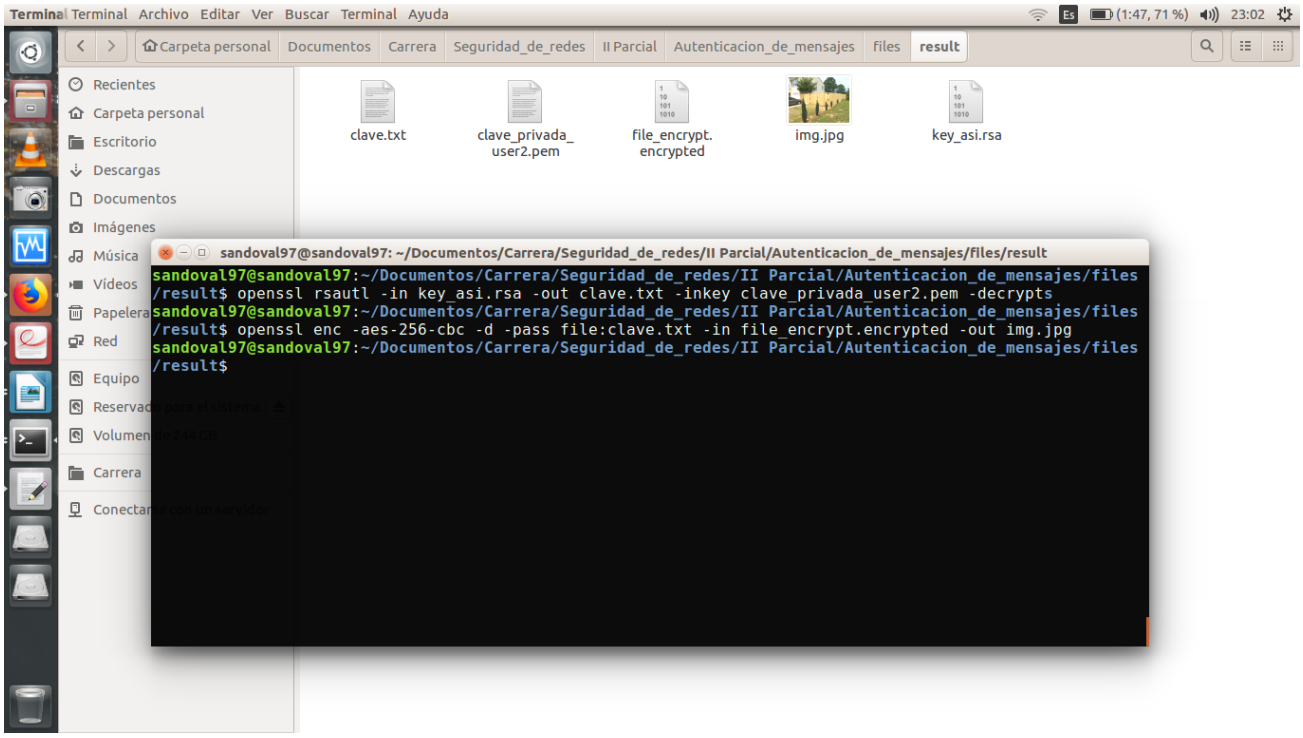


5. Enviar al compañero el archivo cifrado (simétrico) junto con la clave cifrada (en asimétrico).





6. Deshacer los cifrados para obtener el archivo original. Para obtener la clave simétrica, deberíamos utilizar nuestra clave privada.

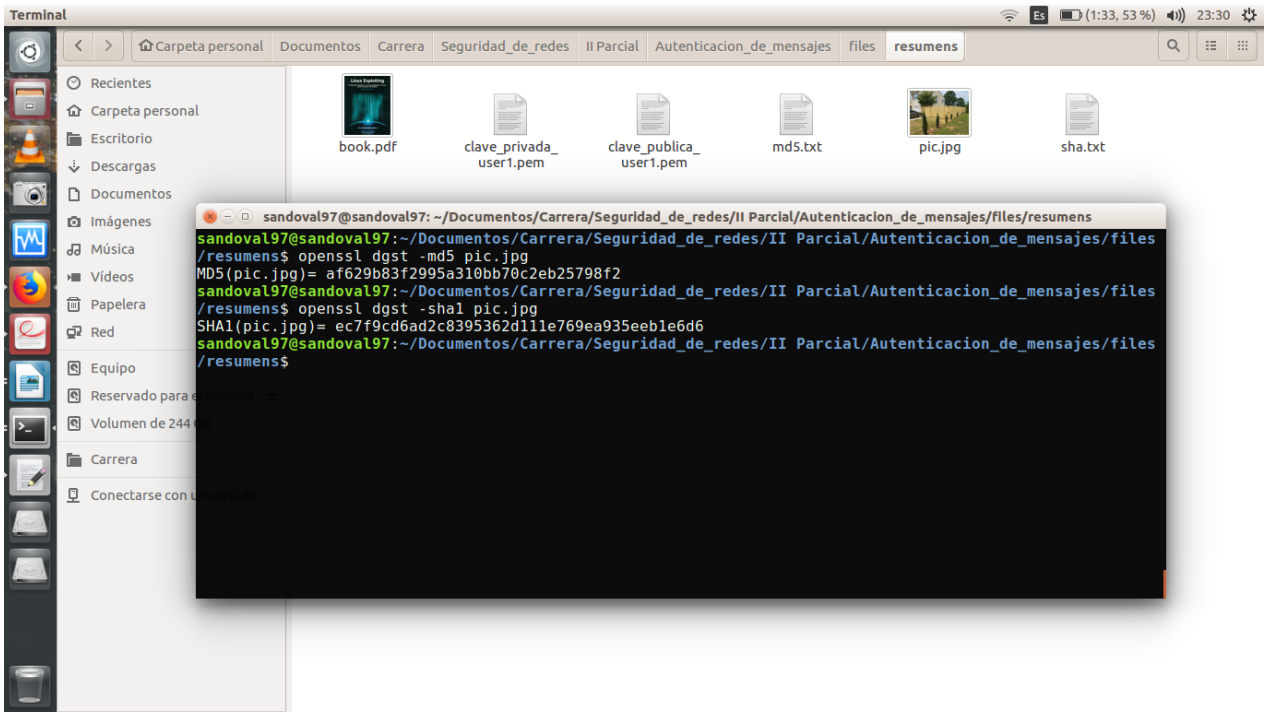


4. Envío de un mensaje firmado

4.1 Obtener el resumen de un documento

Utilizar el comando dgst de openssl para generar el resumen del documentos

- openssl dgst –md5 fichero.doc
- openssl dgst –sha1 fichero.doc



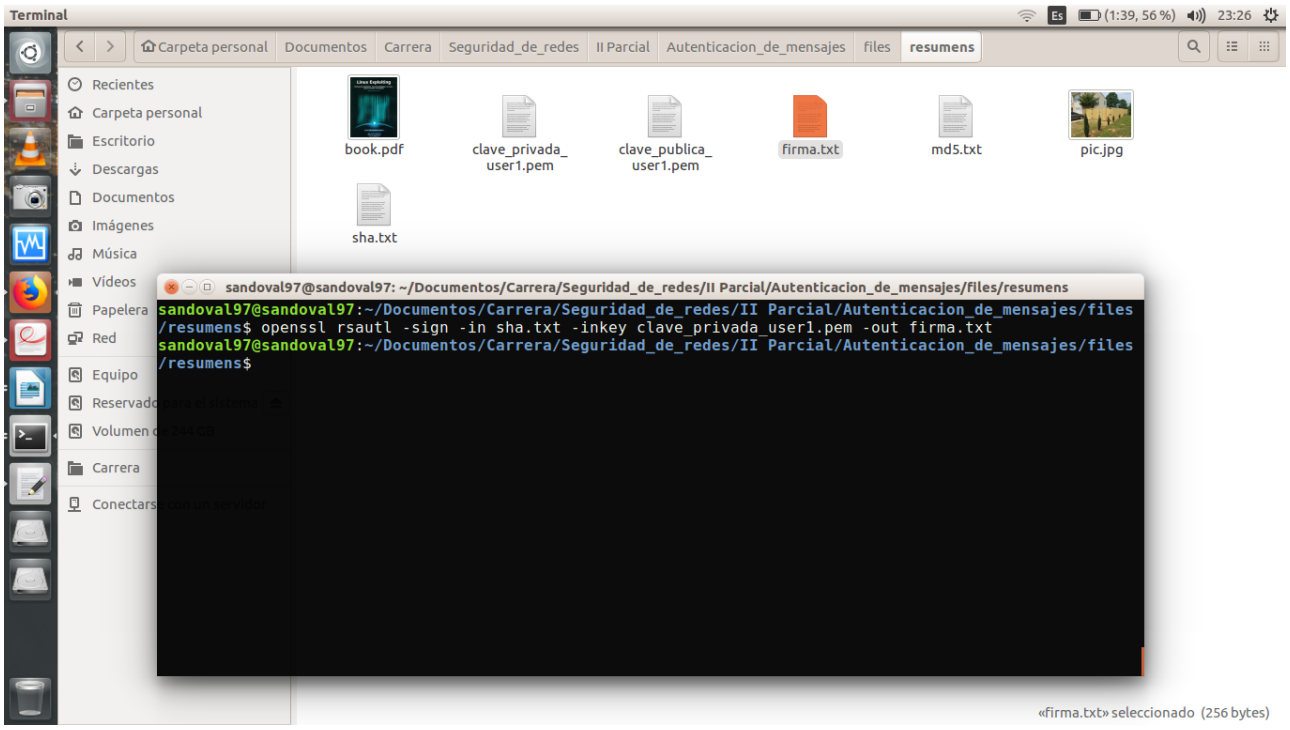
4.2 Cifrar el resumen

Realizar los siguientes pasos:

- Guardar el código de resumen en un fichero de texto
- ¿Qué clave hay que utilizar para el cifrado RSA?

R: para firmar nuestro documento ciframos el resumen con la clave privada del emisor

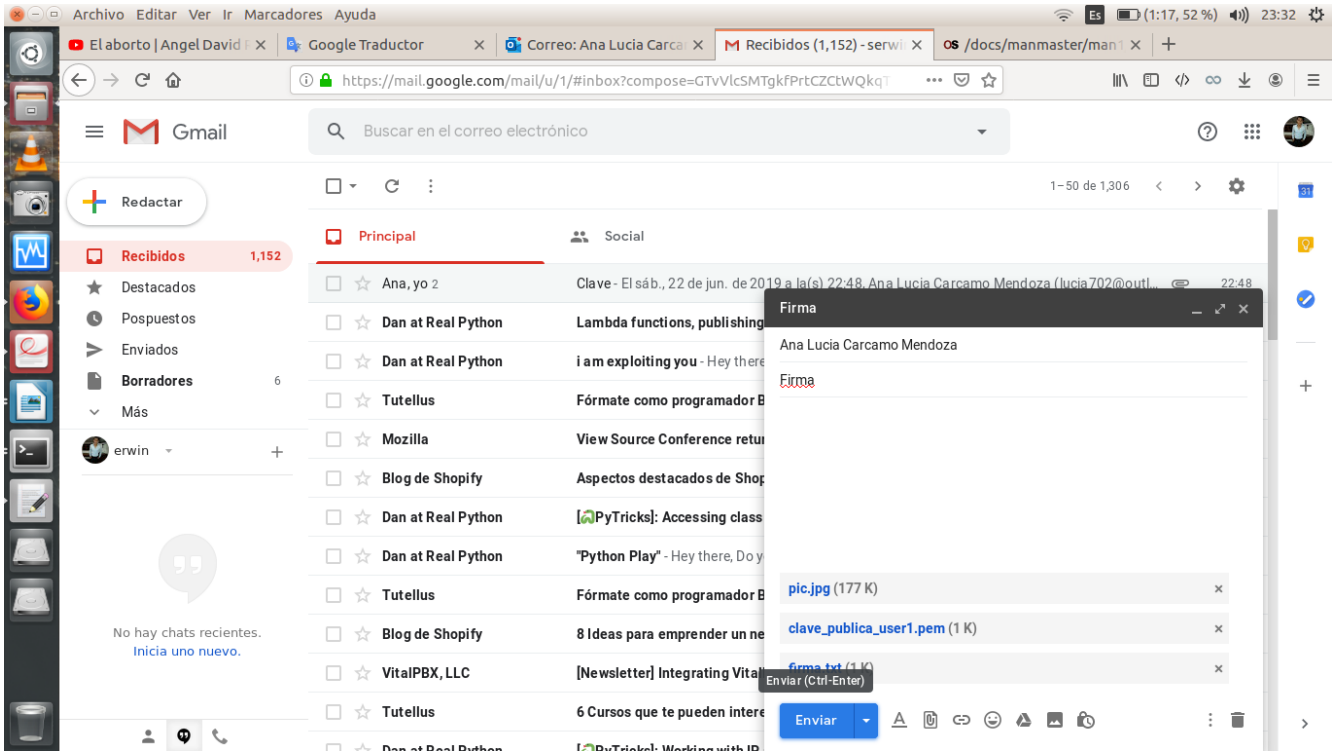
- Cifrar dicho fichero de manera asimétrica con la clave privada, mediante el comando:
  openssl rsautl -sign -in sha.txt -inkey prikey.pem -out firma.txt

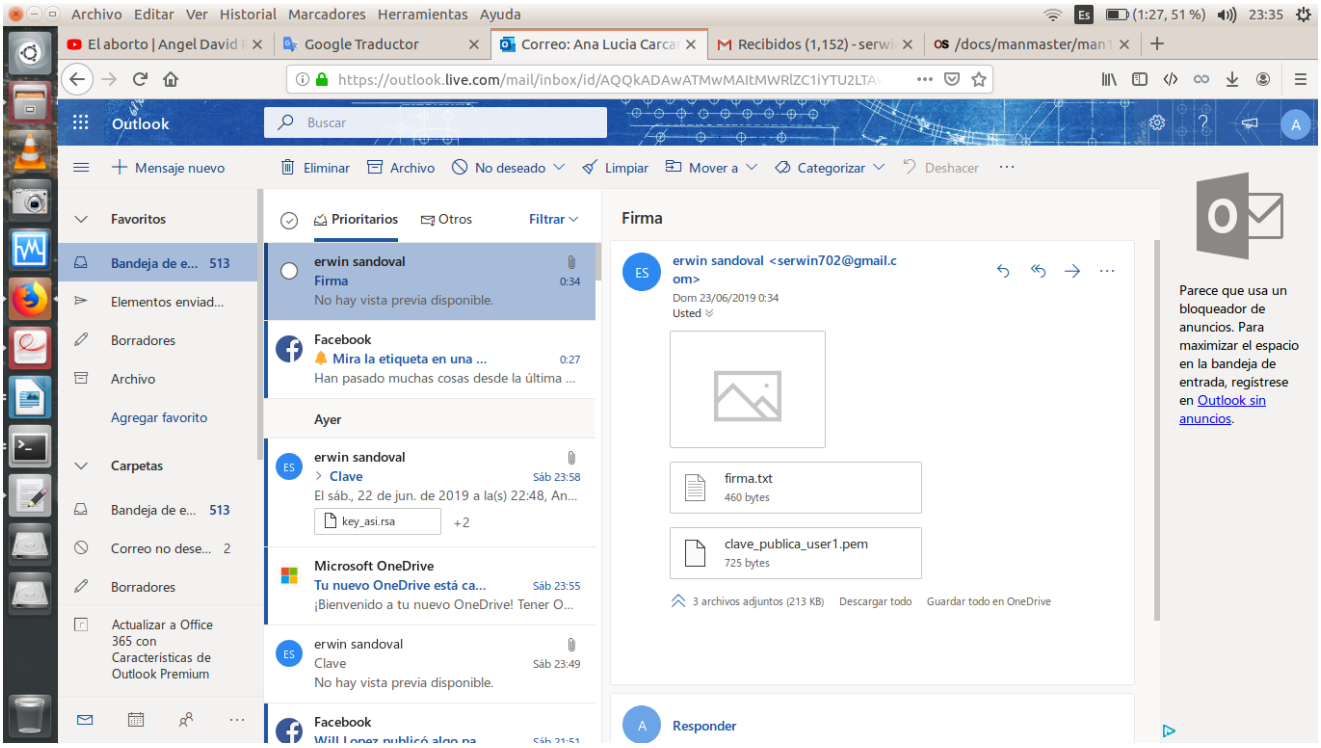


4.3 Enviar por correo electrónico

Enviar a un compañero los siguientes elementos:

- Documento original, sin cifrar
- La firma electrónica (código de resumen cifrado con la clave privada: firma.txt)
- La clave pública


Archivo Editar Ver Ir Marcadores Ayuda
El aborto | Angel David
Google Traductor
Correo: Ana Lucia Carca
Recibidos (1,152) - serwi
/docs/manmaster/man1
https://mail.google.com/mail/u/1/#inbox?compose=GTvVlcSMTgkfPrtCZCtWQkq
Gmail
Buscar en el correo electrónico
Redactar
Recibidos 1,152
Destacados
Pospuestos
Enviados
Borradores 6
Más
erwin
No hay chats recientes.
Inicia uno nuevo.
1–50 de 1,306
Principal
Social
Ana, yo 2
Clave - El sáb., 22 de jun. de 2019 a la(s) 22:48, Ana Lucia Carcamo Mendoza (lucia702@outl...
22:48
Dan at Real Python
Lambda functions, publishing
Dan at Real Python
i am exploiting you - Hey there
Tutellus
Fórmate como programador B
Mozilla
View Source Conference retur
Blog de Shopify
Aspectos destacados de Shop
Dan at Real Python
[PyTricks]: Accessing class
Dan at Real Python
"Python Play" - Hey there, Do y
Tutellus
Fórmate como programador B
Blog de Shopify
8 Ideas para emprender un ne
VitalPBX, LLC
[Newsletter] Integrating Vita
Tutellus
6 Cursos que te pueden intere
Firma
Ana Lucia Carcamo Mendoza
Firma
pic.jpg (177 K)
clave_publica_user1.pem (1 K)
Enviar (Ctrl-Enter)
Enviar


Archivo Editar Ver Historial Marcadores Herramientas Ayuda
El aborto | Angel David
Google Traductor
Correo: Ana Lucia Carca
Recibidos (1,152) - serwi
/docs/manmaster/man1
https://outlook.live.com/mail/inbox/id/AQQkADAwATMwMAItMWRlZC1iYTU2LTA
Outlook
Buscar
Mensaje nuevo
Eliminar
Archivo
No deseado
Limpiar
Mover a
Categorizar
Deshacer
Favoritos
Bandeja de e... 513
Elementos enviad...
Borradores
Archivo
Agregar favorito
Carpetas
Bandeja de e... 513
Correo no dese... 2
Borradores
Actualizar a Office 365 con Características de Outlook Premium
Prioritarios
Otros
Filtrar
erwin sandoval
Firma
No hay vista previa disponible.
0:34
Facebook
Mira la etiqueta en una ...
Han pasado muchas cosas desde la última ...
0:27
Ayer
erwin sandoval
Clave
El sáb., 22 de jun. de 2019 a la(s) 22:48, An...
key_asi.rsa
+2
Sáb 23:58
Microsoft OneDrive
Tu nuevo OneDrive está ca...
¡Bienvenido a tu nuevo OneDrive! Tener O...
Sáb 23:55
erwin sandoval
Clave
No hay vista previa disponible.
Sáb 23:49
Facebook
Will Lopez publicó algo na...
Sáb 21:51
Firma
erwin sandoval <serwin702@gmail.com>
Dom 23/06/2019 0:34
Usted
firma.txt
460 bytes
clave_publica_user1.pem
725 bytes
3 archivos adjuntos (213 KB)
Descargar todo
Guardar todo en OneDrive
Responder
Parece que usa un bloqueador de anuncios. Para maximizar el espacio en la bandeja de entrada, regístrese en Outlook sin anuncios.

4.4 Verificar la firma

Realizar los siguientes pasos para verificar la integridad del documento recibido:

- Obtener el resumen del documento (mediante MD5 o SHA)
- Comparar con el resultado de extraer el resumen de firma.txt:

openssl rsautl -verify -in firma.txt -inkey clave_publica_user1.pem –pubin –raw

el parametro -raw es para aplicar relleno