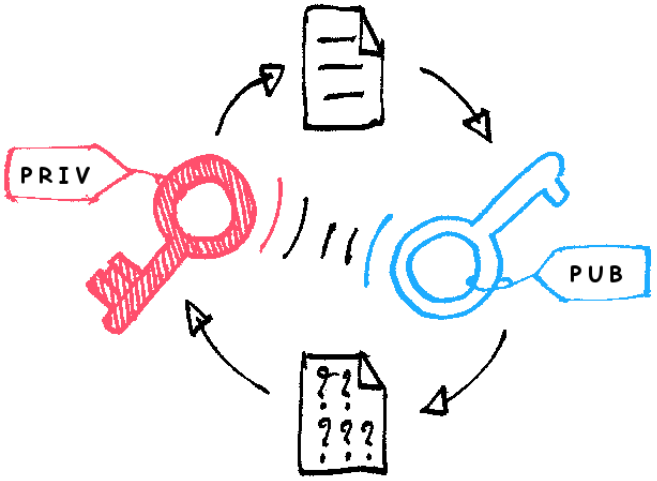
Cifrado y descifrado de archivos con GPG



computo@ciencias.unam.mx

COORDINACIÓN DE LOS SERVICIOS DE CÓMPUTO

FACULTAD DE CIENCIAS
UNAM

Elaborado por:
Omar Martínez Olivares
Paulo Contreras Flores
Yeudiel Hernández Torres

COORDINACIÓN DE LOS SERVICIOS DE CÓMPUTO
FACULTAD DE CIENCIAS

Contenido

Introducción

En el año 1991, Phil Zimmerman creó un sistema de cifrado de llave pública conocido como Pretty Good Privacy (PGP, por sus siglas en inglés), para que cualquier persona pudiera utilizar un sistema de cifrado confiable. En noviembre de 2007 se publicó el RFC 4880 con la especificación del estándar libre OpenPGP, el cuál está basado en el creado por Zimmerman. Posteriormente, surgió una implementación completa y libre de OpenPGP conocida como GnuPG o simplemente GPG, la cuál es ampliamente utilizada en los esquemas de cifrado de llave pública.

Una de las técnicas empleadas para cumplir con la confidencialidad en una comunicación, consiste en cifrar la información para que sólo sea accesible a aquellos que cuenten con autorización, esto se logra a través de una contraseña. Por ejemplo, un archivo se cifra con una contraseña y sólo aquel que cuenta con ésta podrá descifrar el archivo y acceder a su contenido. Si se usa la misma contraseña para cifrar y descifrar, entonces, se está trabajando con un sistema de llave secreta, a lo que también se conoce como criptografía simétrica. En cambio, si se usan contraseñas diferentes, pero relacionadas, para cifrar y descifrar, se está trabajando con un sistema de llave pública, también conocido como criptografía asimétrica.

OpenPGP, particularmente GPG, a grandes rasgos, utiliza una llave de sesión única para cifrar un archivo usando criptografía simétrica. Posteriormente, cifra esta llave de sesión con la llave pública del receptor del archivo, usando criptografía asimétrica. De esta forma, al enviar este archivo por un medio inseguro, como puede ser la Internet, si son interceptados tanto el archivo como la llave, ambos cifrados, quien los tenga en su poder no podrá descifrarlos, ya que no cuenta con llave privada asociada a la llave pública que se utilizó para cifrar la llave de sesión, únicamente el dueño de esas llaves, la pública y la privada, podrá descifrar la llave de sesión usando su llave privada; una vez realizado ésto, podrá descifrar el archivo con esa llave de sesión.

La Coordinación de los Servicios de Cómputo de la Facultad de Ciencias ha desarrollado este manual para que la transmisión de información reservada o confidencial, entre sus pares, se lleve a cabo de una forma sencilla y lo más segura posible. En éste, se indican los pasos a seguir para generar las llaves pública y privada, asociadas a una dirección de correo electrónico, utilizando el estándar OpenPGP. También se indica cómo cifrar y descifrar un archivo siguiendo el mismo estándar.

Sistemas Windows

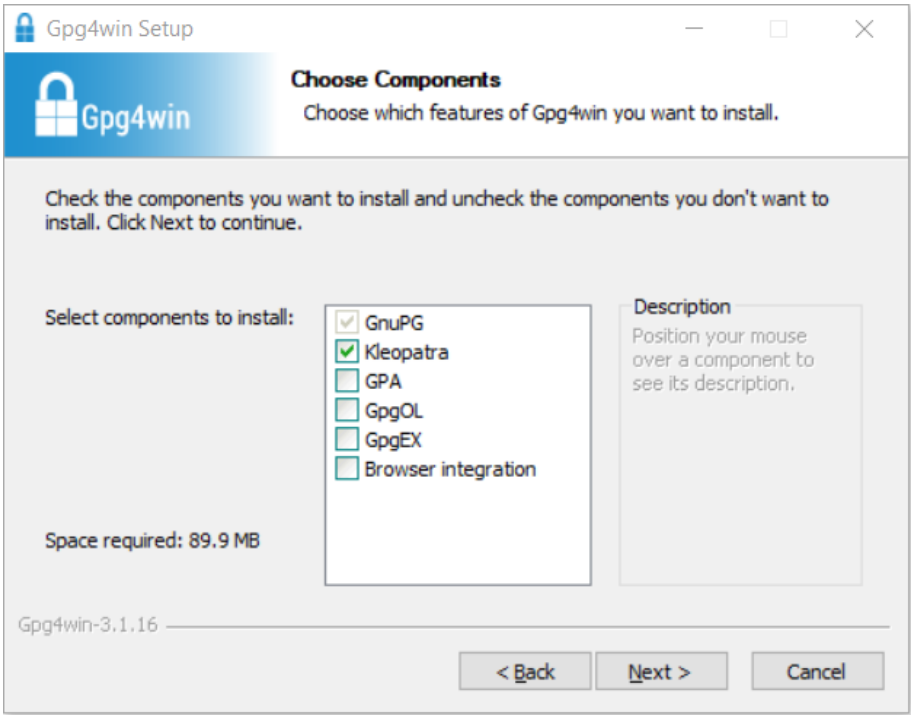
Instalación

Esta instalación es válida para sistemas Windows 7 o superior de 32 y 64 bits, de acuerdo con los requerimientos de Gpg4win. (https://www.gpg4win.org/system-requirements.html)

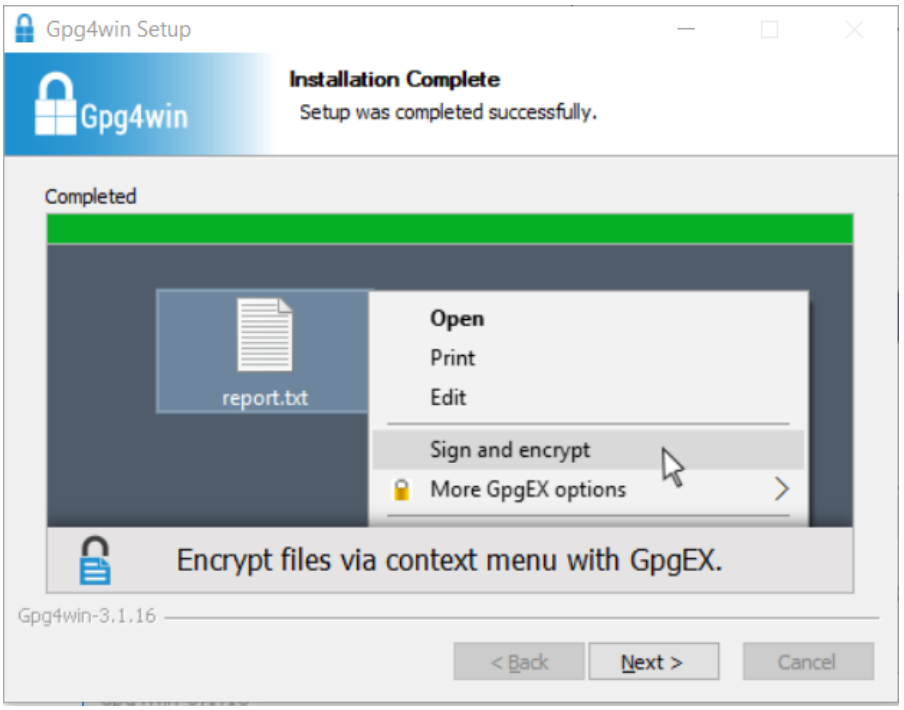
Se debe descargar el instalador de la Suite Gpg4win del siguiente enlace https://www.gpg4win.org

Ejecutar el archivo .exe que se descargó desde el sitio oficial de Gpg4win y se da clic en el botón **next**.

Seleccionar Kleopatra y dar clic en el botón **next** para comenzar la instalación.



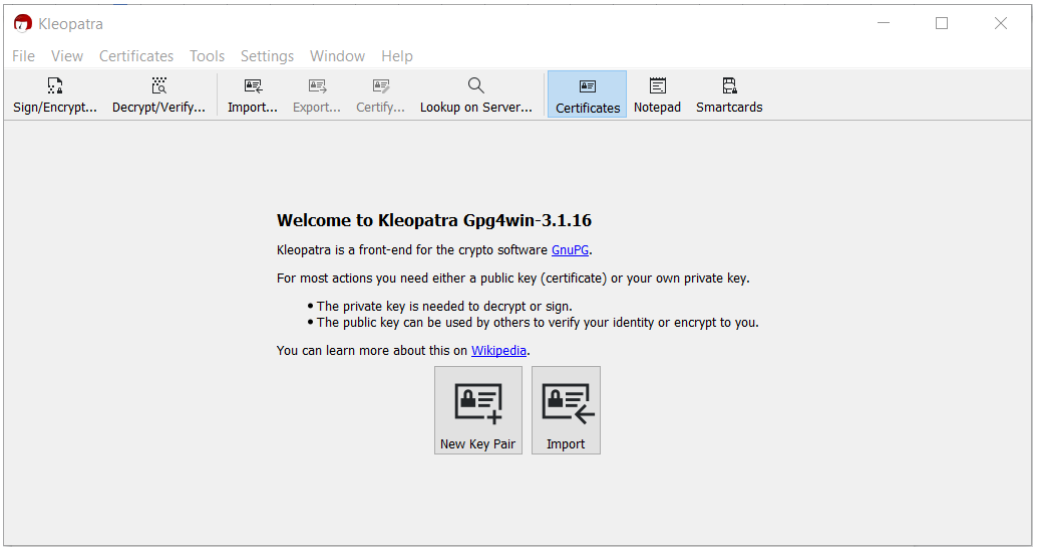
Al finalizar la instalación aparece la siguiente pantalla. Dar clic en **next**.



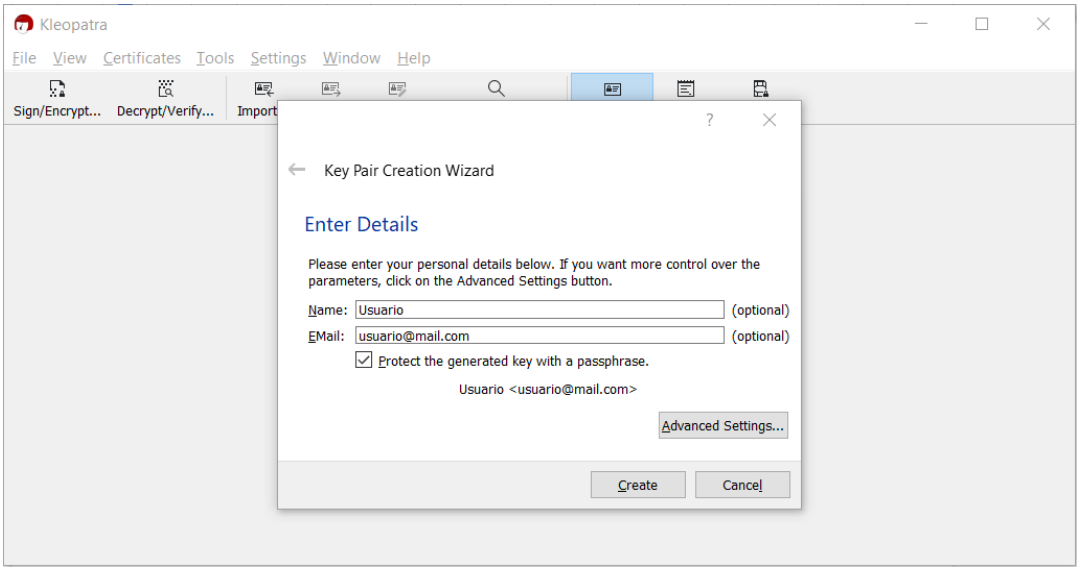
Seleccionar *Run Kleopatra* y dar clic en **Finish**.

Generación de Llaves GPG

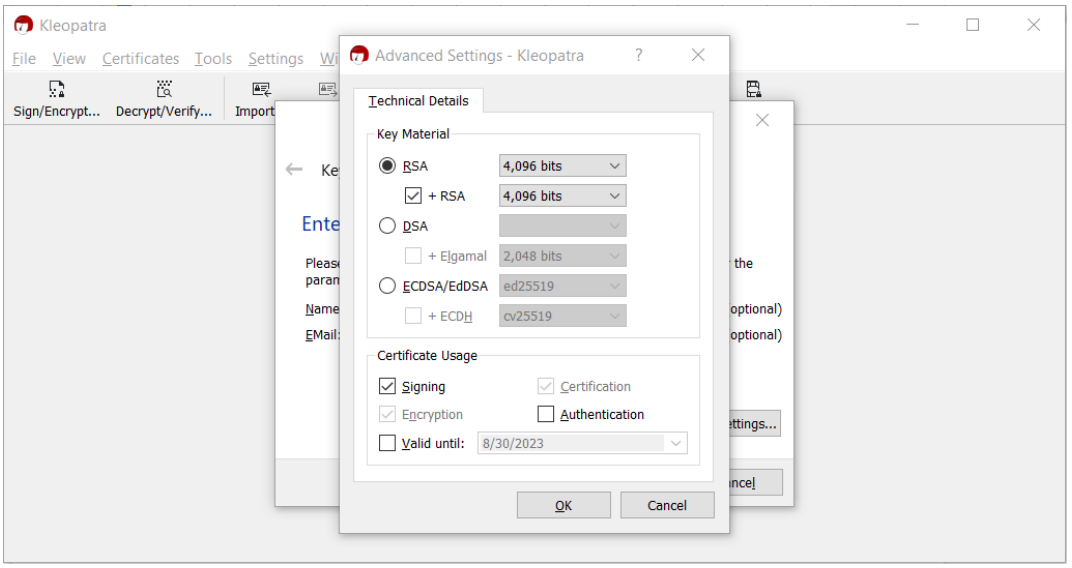
De esta forma se generan las llaves pública y privada, además de otros archivos necesarios, que se usarán para el cifrado y descifrado de archivos. Dar clic en **New Key Pair**.



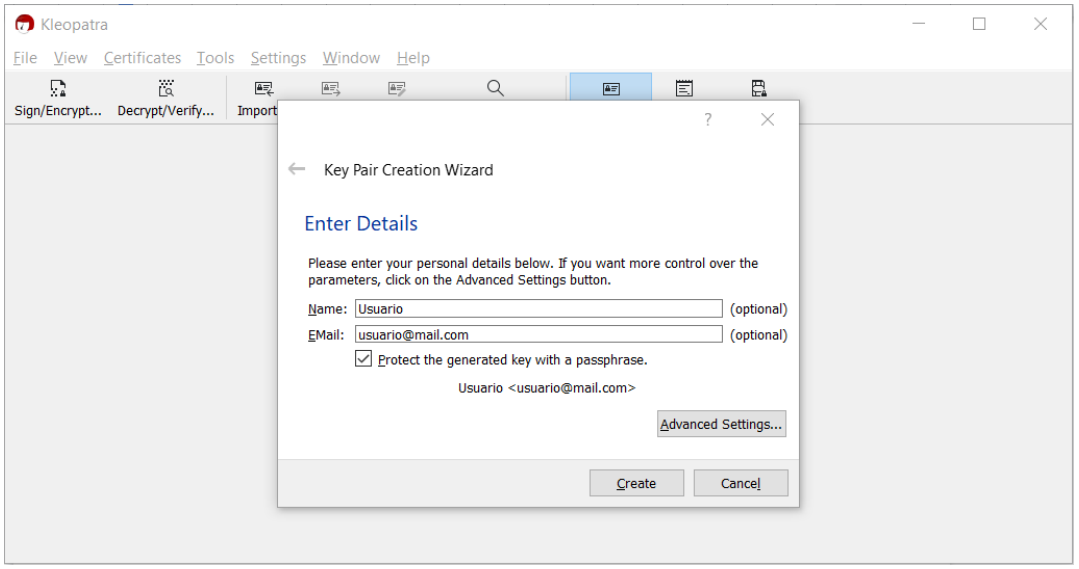
Ingresar nombre completo, correo electrónico y seleccionar la casilla **Proteger la llave generada con contraseña**. Antes de crear el par de llaves dar clic en **Advance Settings**.



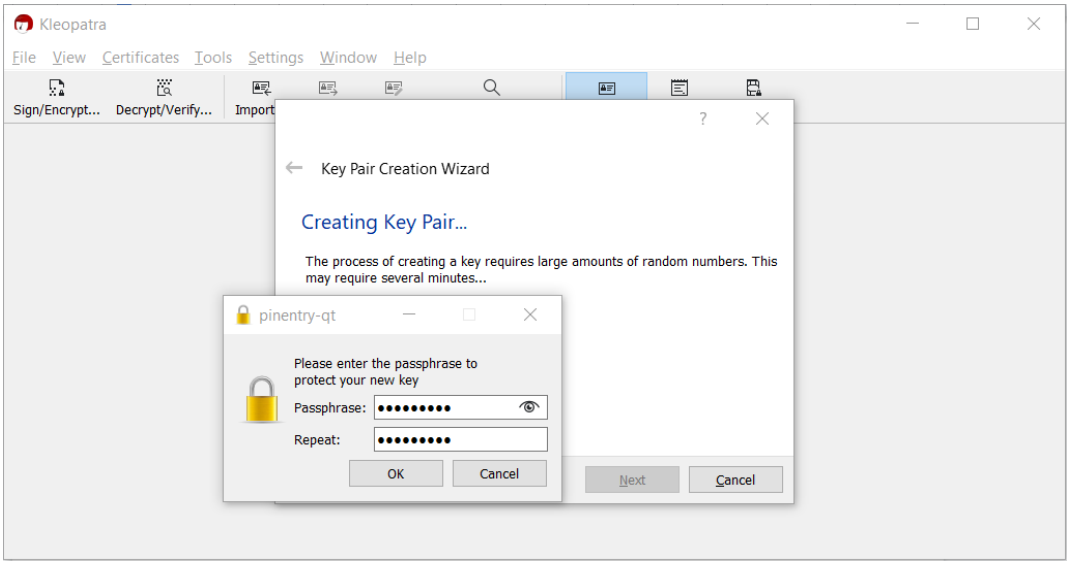
Se recomienda usar la opción **RSA + RSA** con valores de **4,096 bits**.



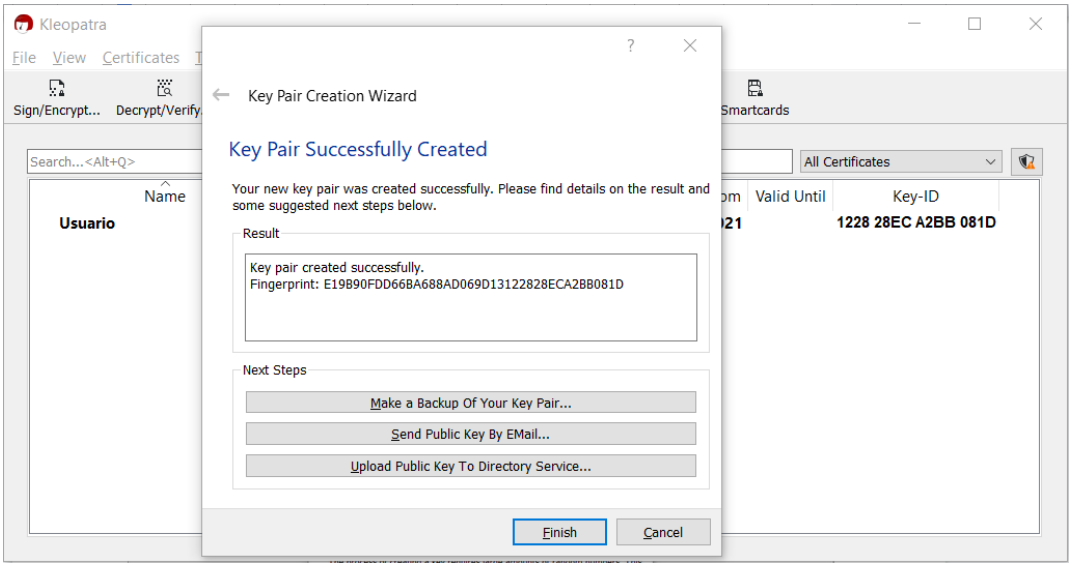
Ya con los datos y **configuraciones avanzadas** recomendadas, dar clic en **Create.**



Ahora, solicitará una contraseña para salvaguardar las llaves GPG.



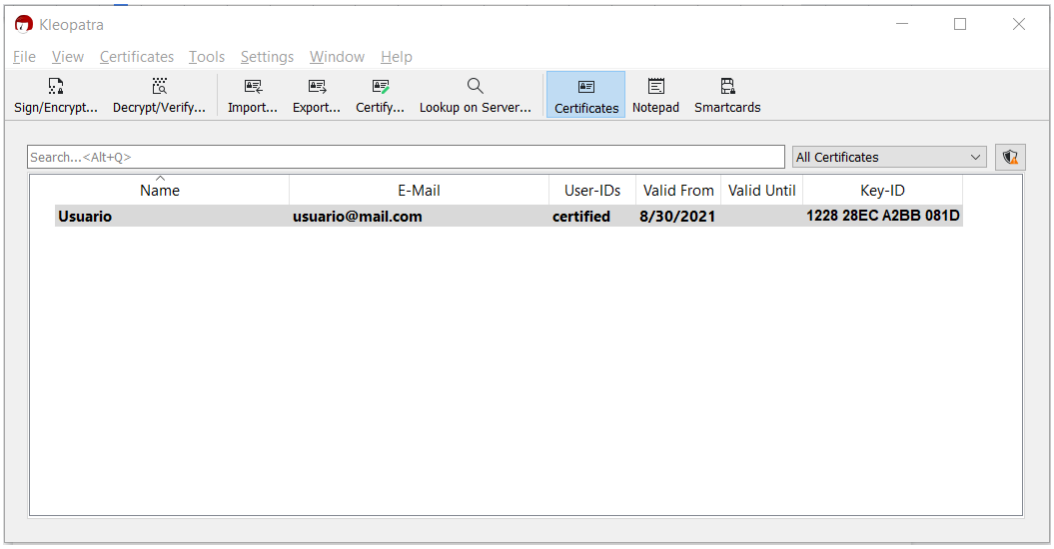
Al generar las llaves se muestra la siguiente ventana. Dar clic en **Finish**.



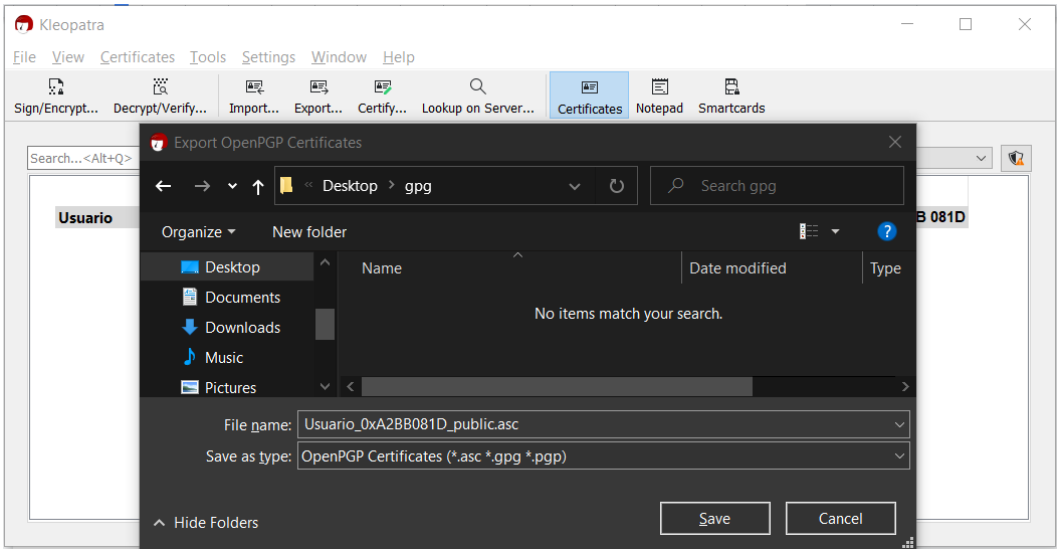
Envío de Llave Pública

Exportar la llave pública creada previamente a un archivo de texto, para así poder enviarla por correo electrónico o para subirla a un repositorio de llaves públicas. El correo electrónico será el mismo que se usó al generar las llaves.

Dar clic en **Export.**



Seleccionar la ubicación donde se guardará la llave pública.

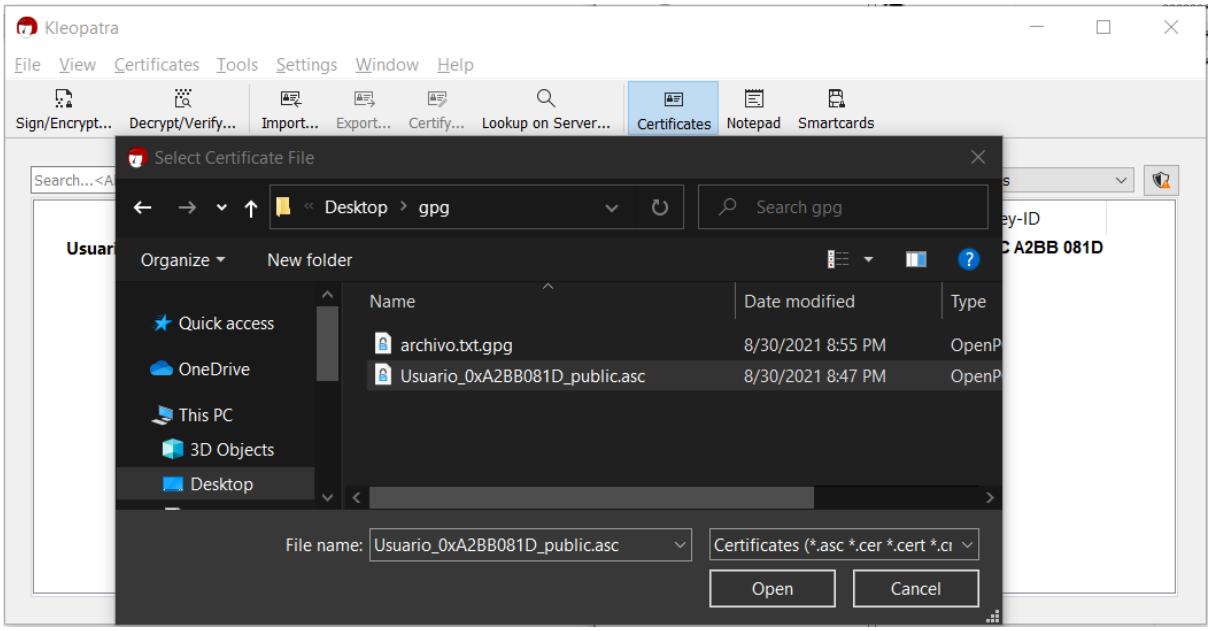


Se creará el archivo con extensión .asc que contendrá la llave pública

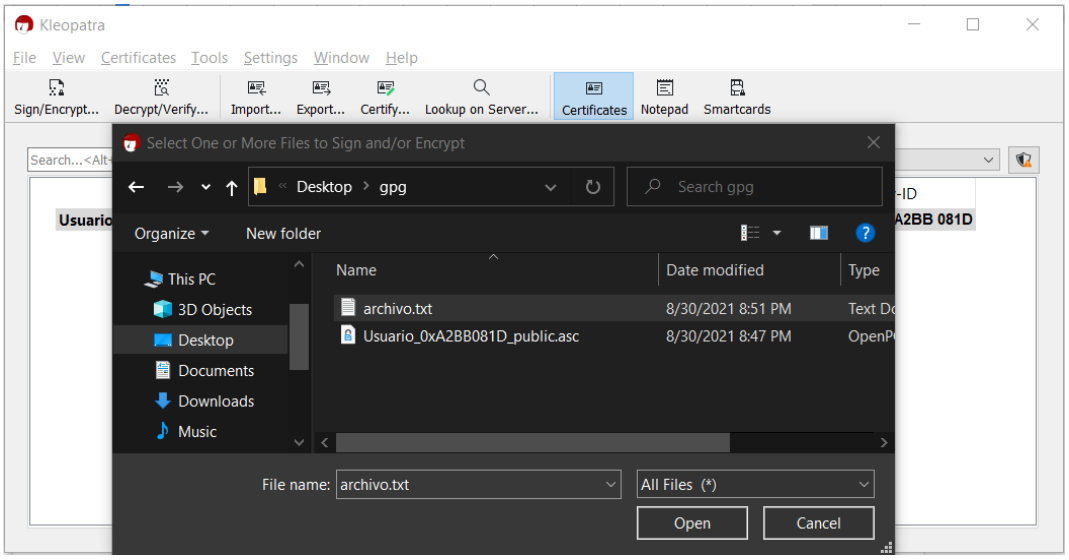
Cifrado de archivos

Obtener la llave pública legítima del ente que tendrá autorización para acceder al archivo, es decir, la persona que podrá descifrar el archivo.

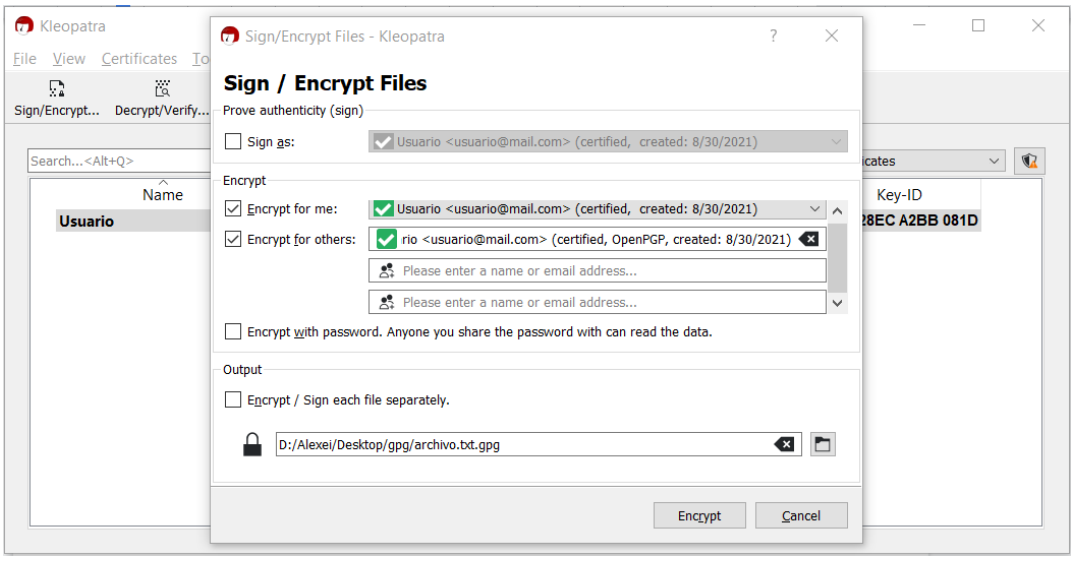
Dar clic en **Import** y seleccionar el archivo de la llave pública.



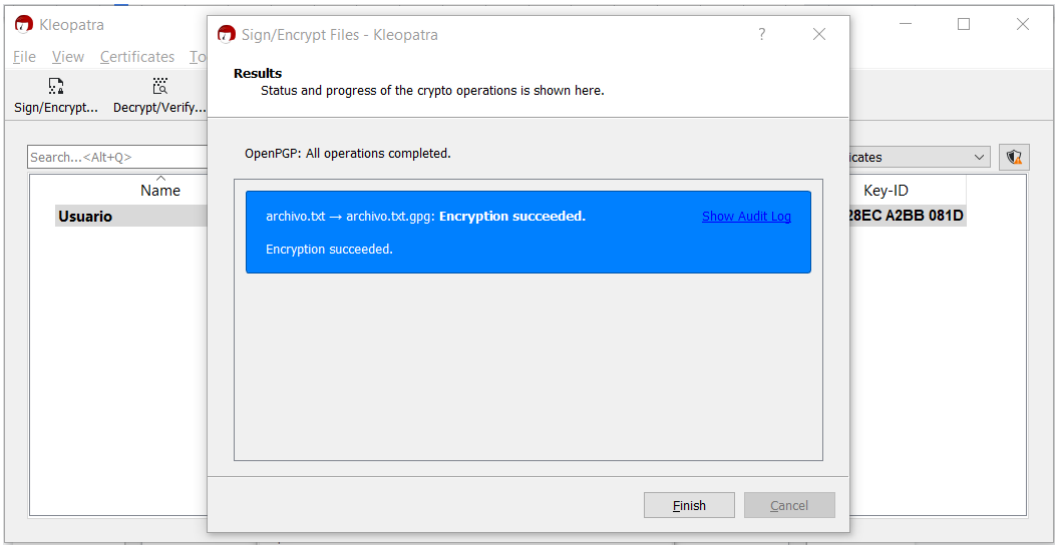
Dar clic en **Sign/Encrypt** y seleccionar el archivo que se quiere cifrar.

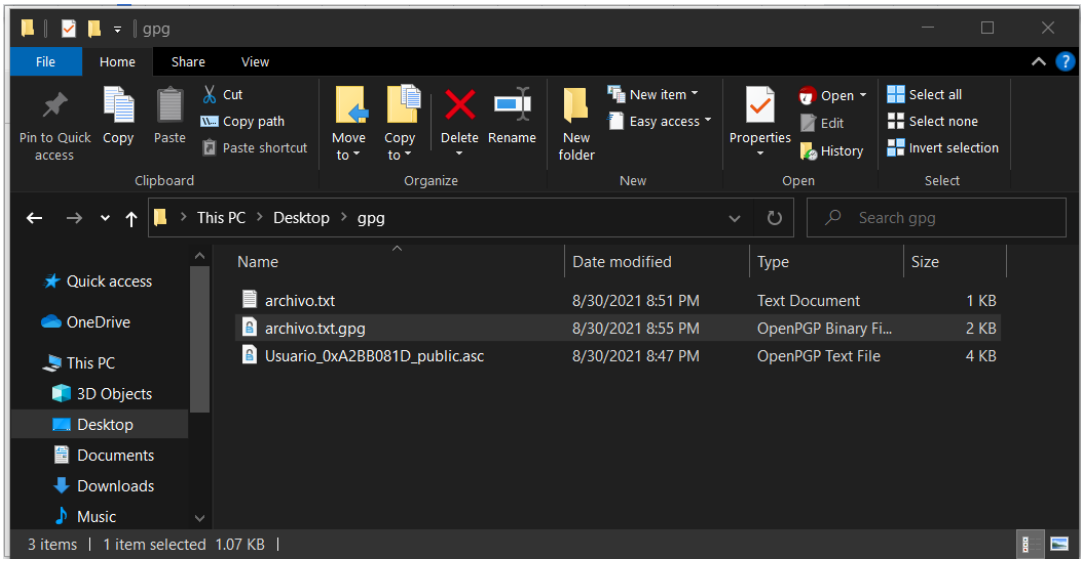


Seleccionar la casilla **Encrypt for others** y elegir la llave pública que se acaba de importar. Dar clic en **Encrypt**.



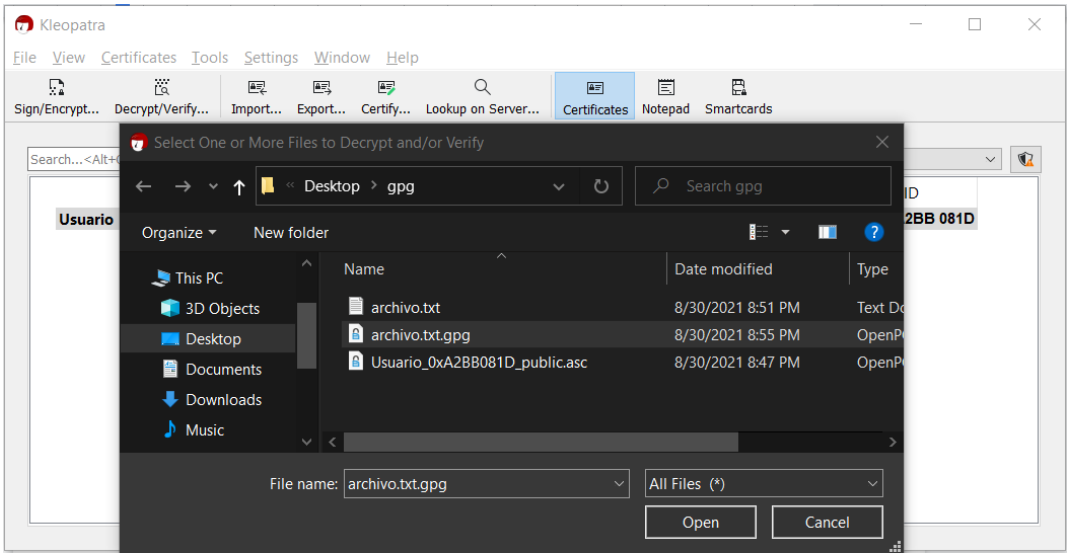
Al dar clic en **Finish** se creará un nuevo archivo con extensión gpg en la ruta seleccionada.



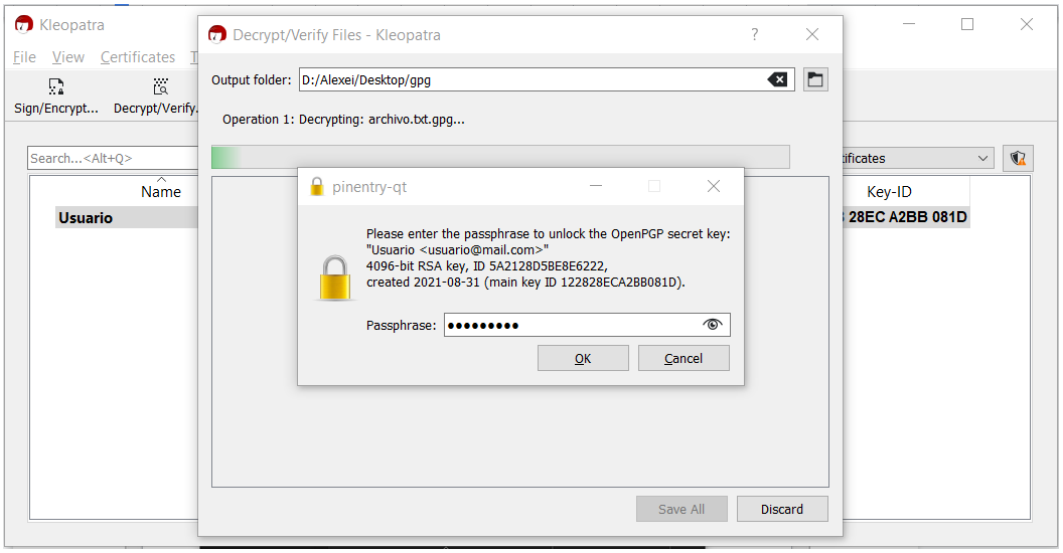


Descifrado de archivos

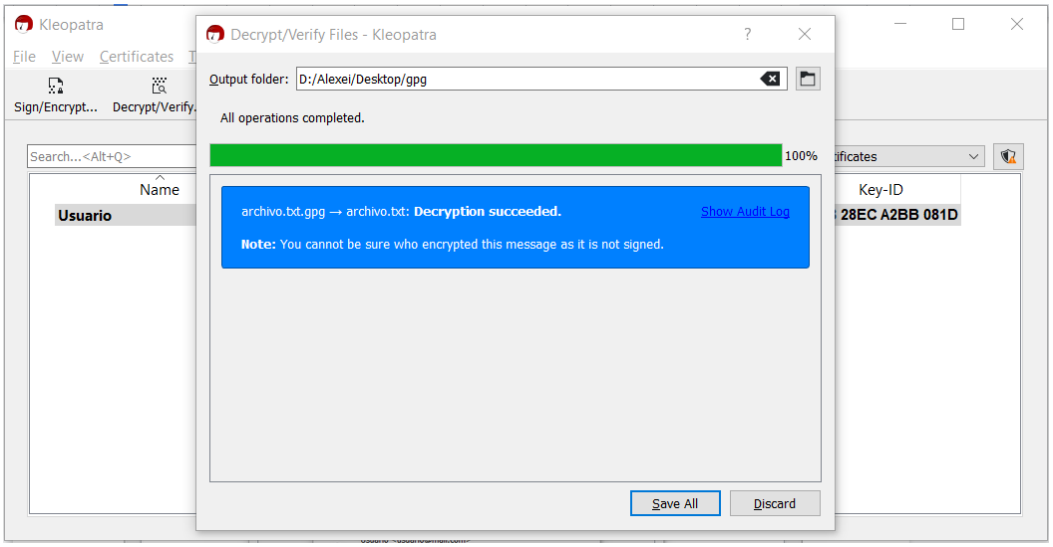
Descargar el archivo cifrado que se recibió en el correo electrónico. Este archivo fue cifrado con la llave pública que se envió previamente. Dar clic en el botón **Decrypt/Verify** y seleccionar el archivo cifrado



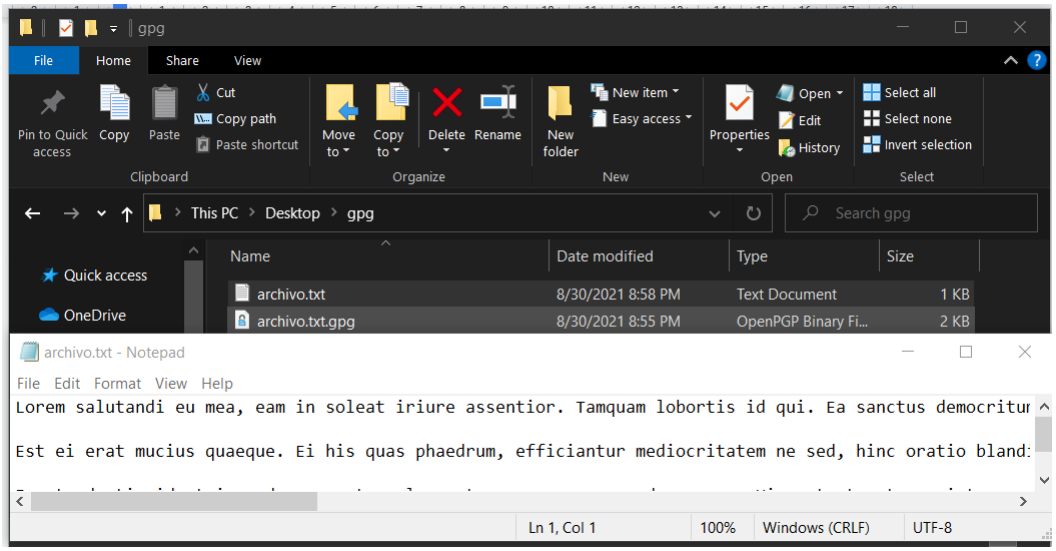
Ingresar la contraseña que resguarda las llaves.



Es necesario dar clic en **Save all** para que el archivo descifrado se almacene.



Así, el archivo ha sido descifrado y almacenado en la misma ruta que el archivo original y es legible.

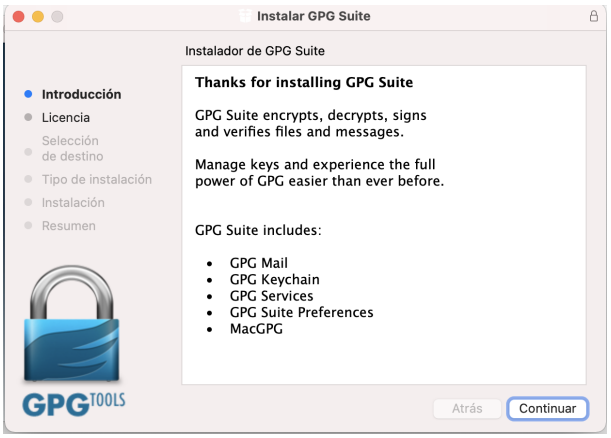


Sistemas Mac OS

Usando una aplicación

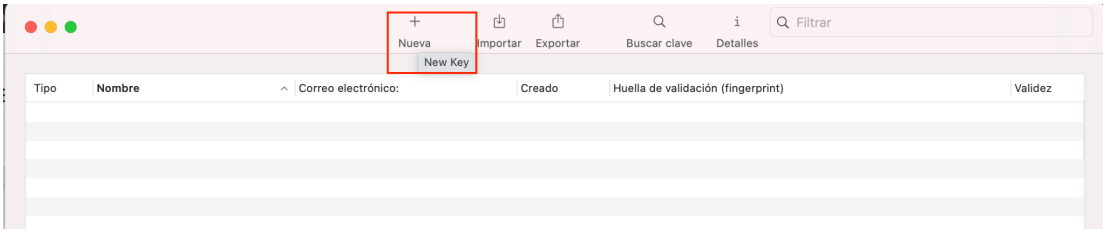
Instalación

Se puede utilizar la aplicación GPGTOOLS, para ello es necesario descargar e instalar la versión gratuita a través de su sitio oficial en en siguiente enlace https://gpgtools.org/



Generación de llaves GPG

Una vez instalada, ingresar la palabra “GPG KeyChain” en el Spotlight  del equipo Mac, lo cual abrirá el programa para la gestión de claves GPG. A través de esta aplicación, se va a generar tanto la llave pública como la privada, para ello damos clic en el símbolo de “+”.

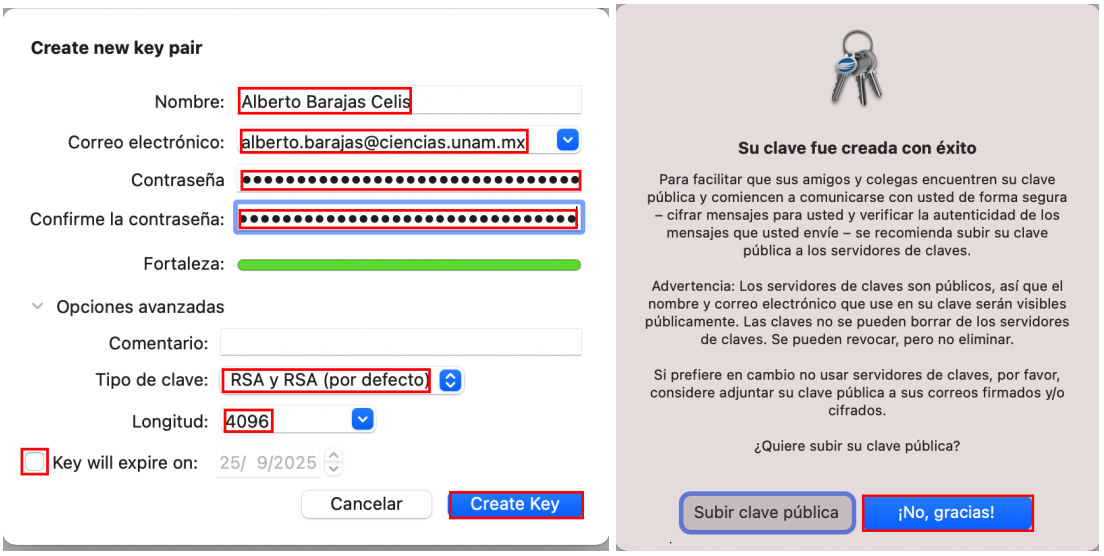


En la nueva ventana, configurar los campos con los valores que correspondan a cada campo.

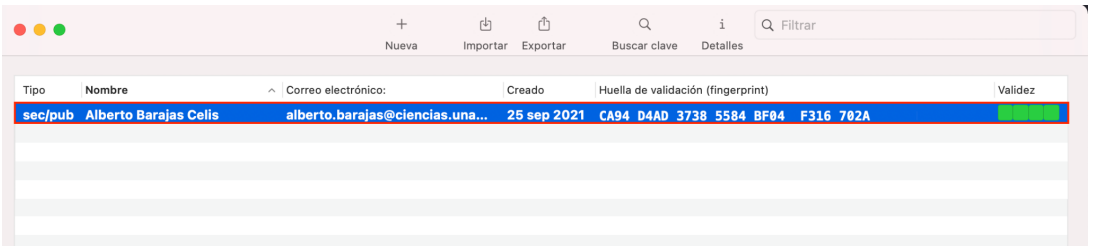
- En los campos **Nombre y Correo electrónico** ingresar el valor que corresponda para su caso.

- En el campo **Contraseña** y **Confirmar la contraseña**, ingresar la contraseña que se usará para salvaguardar las llaves GPG.
- Desplegar la sección de "**Opciones Avanzadas**"
    - En el campo **Tipo de Clave** se recomienda utilizar "**RSA y RSA (por defecto)**"
    - En el campo **Longitud** se recomienda utilizar una longitud de clave de **4096.**
    - Desmarcar la casilla de "Key will expire on", para indicar que la clave no caduca.

Por último, dar clic en el botón **"Create Key",** para crear las llaves, al finalizar se mostrará el mensaje de que las claves fueron creadas.



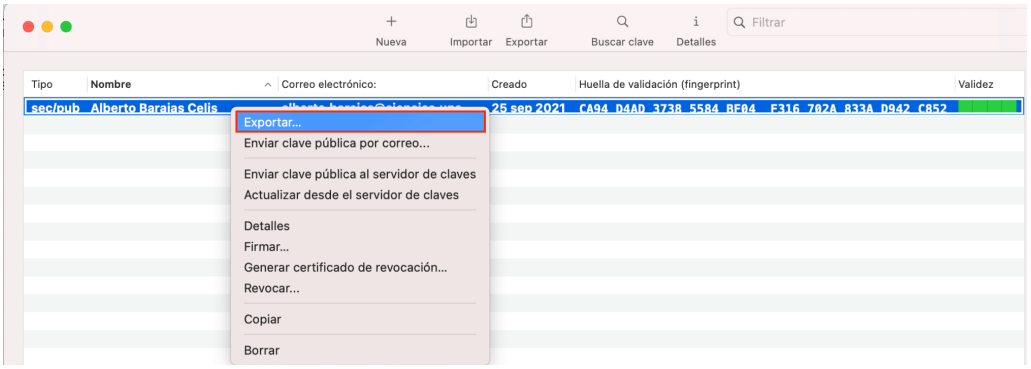
Una vez terminado el proceso de generación de claves, se visualizarán las claves creadas en el listado de la aplicación.



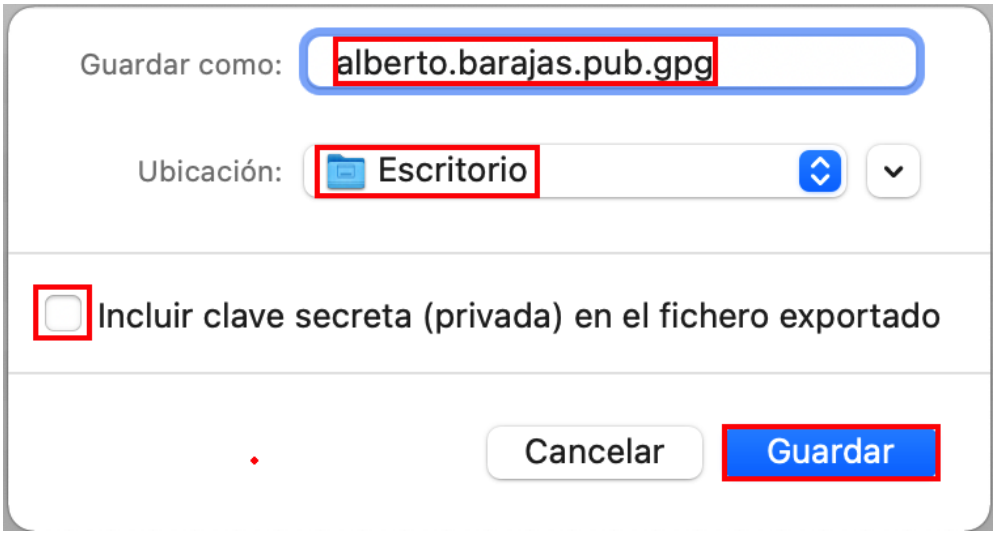
Envío de llave pública

Exportar la llave pública creada previamente a un archivo de texto, para así poder enviarla por correo electrónico o para subirla a un repositorio de llaves públicas.

Desde la aplicación de gestión de llaves GPG, seleccionar la llave pública creada con el mismo correo del paso anterior, dar clic derecho sobre la misma y seleccionar la opción "**Exportar**",



A continuación, asignar un nombre al archivo exportado, seleccionar la ubicación donde se guardará la llave pública y desmarcar la casilla de Incluir clave secreta. Dar clic en guardar

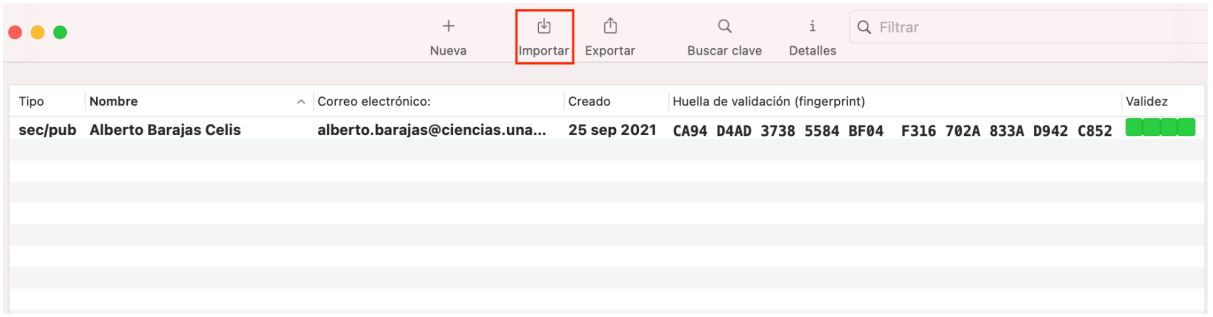


Enviar la llave pública exportada o el enlace al repositorio de llaves públicas, al correo computo@ciencias.unam.mx.

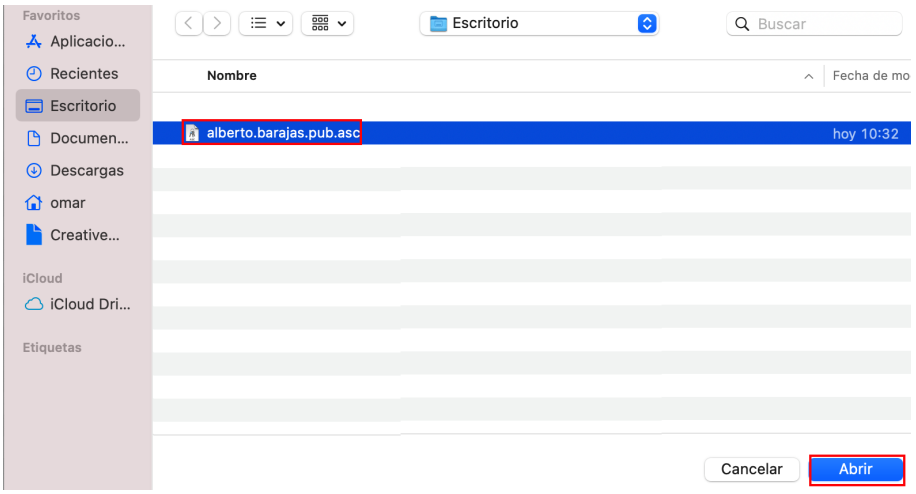
Cifrado de archivos

Obtener la llave pública legítima del ente que tendrá autorización para acceder al archivo, es decir, la persona que podrá descifrar el archivo.

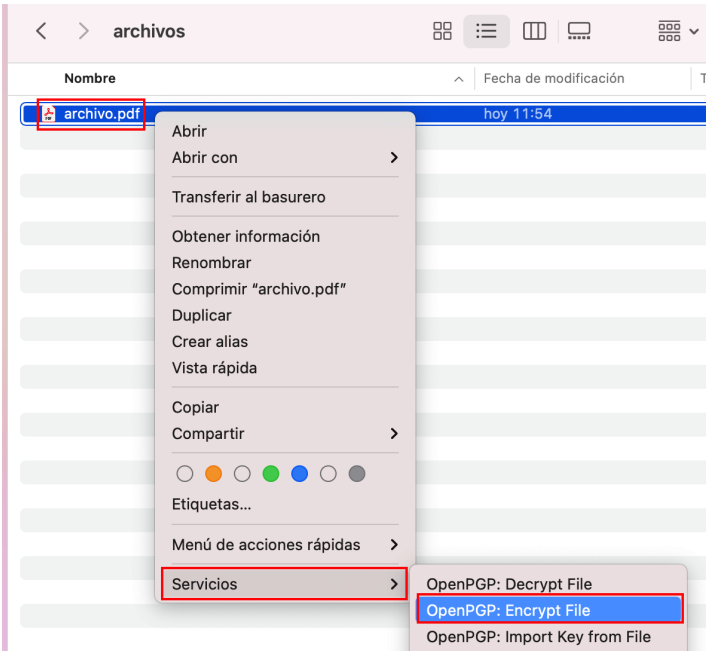
Importar dicha llave pública al llavero (o keyring), a través de la aplicación de gestión de llaves GPG, dar clic en el icono de “**Importar**”.



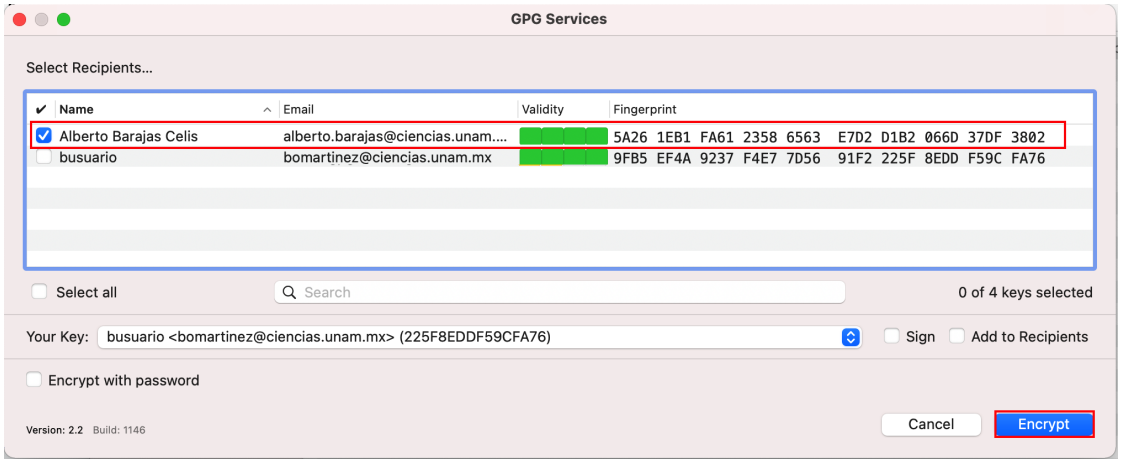
Indicar la ubicación de la llave pública, dar clic en el botón “**Abrir**”. Para que la aplicación reconozca que se trata de un archivo que puede importar, la extensión del archivo tiene que ser “.asc”.



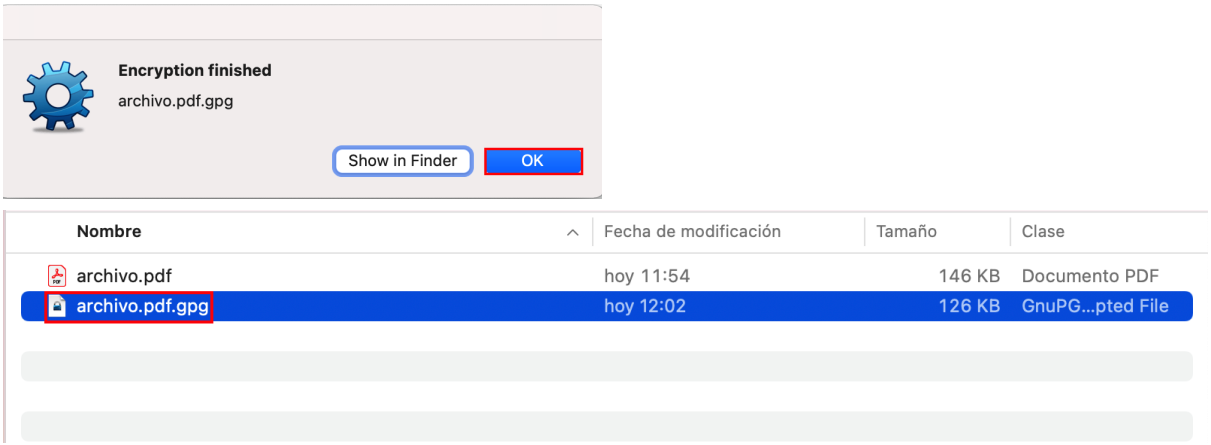
Para cifrar un archivo, dar clic derecho sobre el mismo y seleccionar del menú emergente las opciones **Servicios>OpenPGP>Encrypt File**



Seleccionar la llave pública a usar para cifrar el archivo, recordar que sólo quien tenga la llave privada asociada a esta llave podrá descifrarlo. Dar clic en el botón “**Encrypt**”



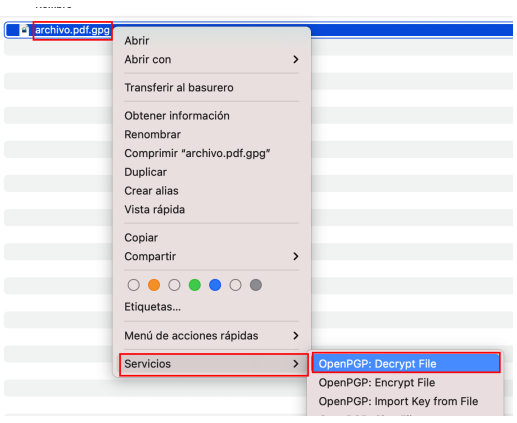
Una vez terminado el proceso de cifrado, se generará un nuevo archivo con la extensión GPG.



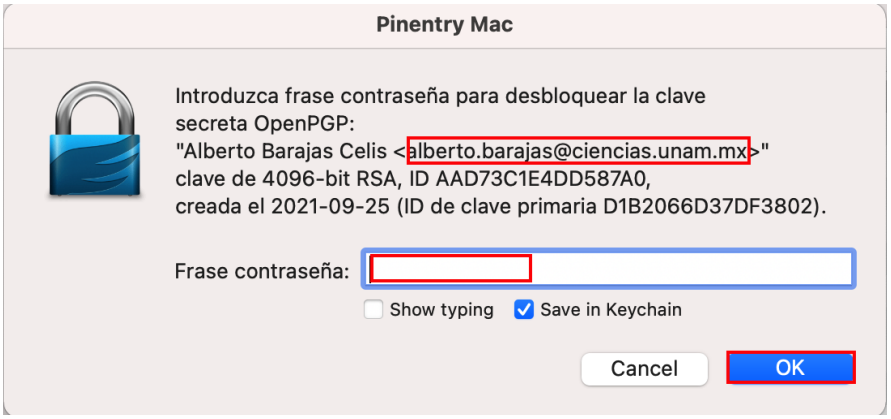
Descifrado de archivos

Descargar el archivo cifrado que se recibió en el correo electrónico. Este archivo fue cifrado con la llave pública que se envió previamente.

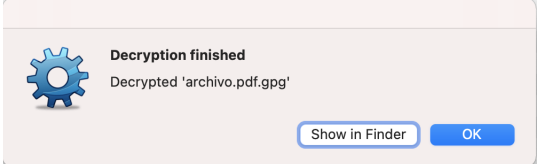
Para descifrar un archivo, dar clic derecho sobre el mismo y seleccionar del menú emergente las opciones **Servicios>OpenPGP>Decrypt File**

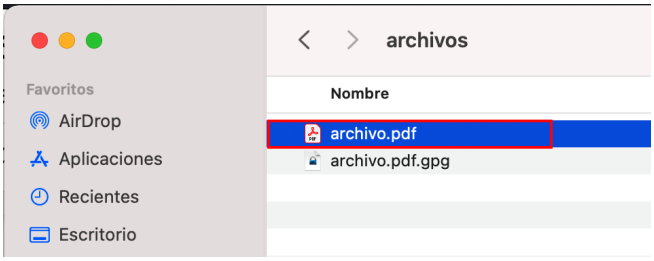


Solicitará la contraseña que resguarda las llaves, ingresar la contraseña correspondiente.



Una vez terminado el proceso de descifrado, se mostrará el contenido legible del archivo.





Usando una terminal de comandos

Requisitos previos

Para instalar algunos programas desde la línea de comandos, es necesario descargar e instalar un gestor de paquetes como MacPorts (https://www.macports.org) o Homebrew (https://brew.sh/) .

Generación de llaves GPG

Desde una terminal de Mac OS, instalar el paquete gnupg y gnupg2, con el gestor de paquetes que se cuente, como ejemplo se muestra la instalación con Homebrew. Para abrir la terminal, ingresar la palabra “Terminal” en el Spotlight  del equipo Mac .

```
$ brew install gnupg gnupg2
```

Generar tanto la llave pública como la privada.

```
$ gpg --full-generate-key
```

Antes de que se generen, configurar las siguientes opciones.

```
Por favor seleccione tipo de clave deseado:
   (1) RSA and RSA
   (2) DSA and Elgamal
   (3) DSA (sign only)
   (4) RSA (sign only)
   (9) ECC (sign and encrypt) *default*
  (10) ECC (sólo firmar)
  (14) Existing key from card
Su elección: 1
```

Se recomienda el valor 1, aunque también se puede poner el 2.

```
las claves RSA pueden tener entre 1024 y 4096 bits de longitud.
¿De qué tamaño quiere la clave? (3072) 4096
```

Se recomienda el valor de 4096, por considerarlo más seguro.

```
Por favor, 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)? 0
```

Se recomienda el valor de 0, lo cual significa que la llave nunca caduca, más adelante se creará automáticamente un archivo de revocación de llaves, en caso de que se requiera que ya no sean válidas por algún motivo.

```
La clave nunca caduca
¿Es correcto? (s/n) s
```

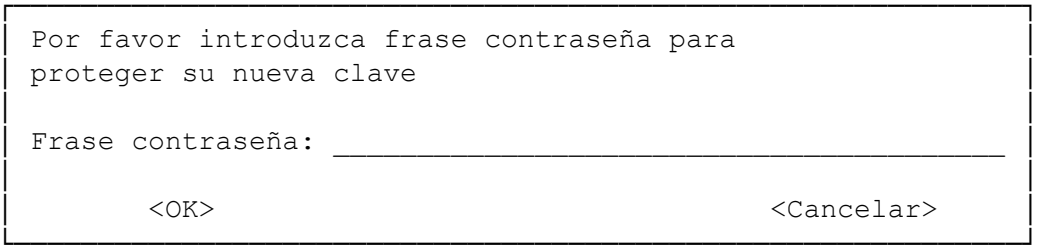
Colocar la opción s, que significa sí.

A continuación, solicitará una serie de valores personales, llenar según corresponda.

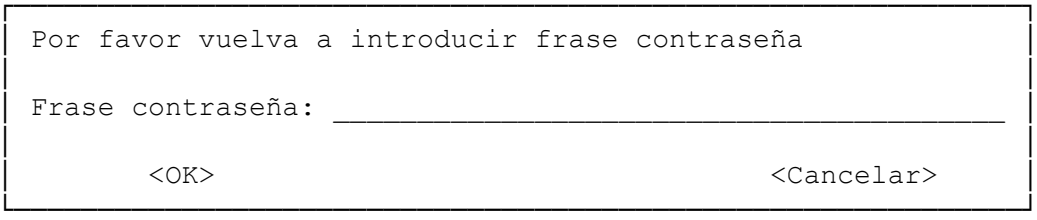
```
Nombre y apellidos: Alberto Barajas Celis
Dirección de correo electrónico: alberto.barajas@ciencias.unam.mx
Comentario: Llave GPG para el cifrado de archivos
Ha seleccionado este ID de usuario:
    "Alberto Barajas Celis (Llave GPG para el cifrado de archivos)
<alberto.barajas@ciencias.unam.mx>"

¿Cambia (N)ombre, (C)omentario, (D)irección o (V)ale/(S)alir? V
```

Ahora, solicitará una contraseña para salvaguardar las llaves GPG.



Y volverá a solicitar la misma contraseña.



Ya con los datos de configuración, el sistema procederá a crear la llave.

```
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.
gpg: clave 176E8FD123453EAB marcada como de confianza absoluta
gpg: creado el directorio '/Users/carlos/.gnupg/openpgp-revocs.d'
gpg: certificado de revocación guardado como
'/Users/carlos/.gnupg/openpgp-revocs.d/13214EABFECBA2124A1341CA176E8FD1
23453EAB.rev'
claves pública y secreta creadas y firmadas.

pub   rsa4096 2021-09-24 [SC]
      13214EABFECBA2124A1341CAB0E8CE22B43C3CEFA
uid                      Alberto Barajas Celis (Llave GPG para el
cifrado de archivos) <alberto.barajas@ciencias.unam.mx>
sub   rsa4096 2021-09-24 [E]
```

Envío de llave pública

Exportar la llave pública creada previamente a un archivo de texto, para así poder enviarla por correo electrónico o para subirla a un repositorio de llaves públicas. El correo electrónico será el mismo que se usó al generar las llaves.

```
$ gpg --export --armor alberto.barajas@ciencias.unam.mx >
alberto.barajas.pub.gpg
```

Enviar la llave pública o el enlace al repositorio de llaves públicas, al correo **computo@ciencias.unam.mx**.

Cifrado de archivos

Obtener la llave pública legítima del ente que tendrá autorización para acceder al archivo, es decir, la persona que podrá descifrar el archivo.

Importar dicha llave pública al llavero (o keyring), con el comando.

```
$ gpg --import sotero.prieto.pub.gpg
```

Cifrar el archivo, con el siguiente comando, recordar que sólo quien tenga la llave privada asociada podrá descifrarlo.

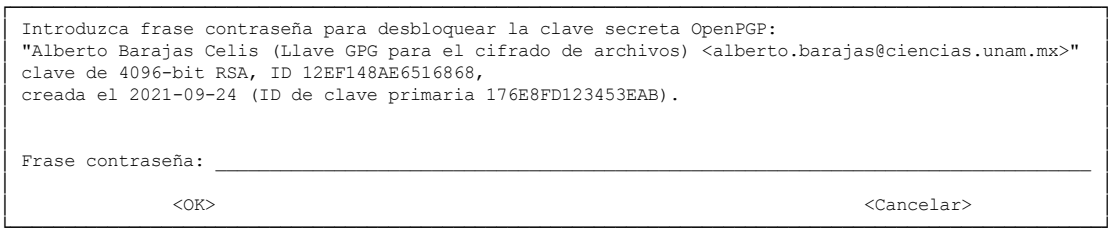
```
$ gpg --encrypt --armor --recipient sotero.prieto@ciencias.unam.mx
archivo.pdf
```

Descifrado de archivos

Descargar el archivo cifrado que se recibió en el correo electrónico. Este archivo fue cifrado con la llave pública que se envió previamente. Ejecutar el siguiente comando para descifrarlo.

```
$ gpg --output archivo.pdf --decrypt archivo.pdf.asc
```

Ingresar la contraseña que resguarda las llaves.



Así, el archivo ha sido descifrado y es legible.

Sistemas basados en Linux

Generación de llaves GPG

Instalar el paquete rng-tool, con el cual se genera la entropía necesaria utilizada en la generación de las llaves GPG.

```
$ sudo apt-get install rng-tools
```

Generar entropía y enviarla al dispositivo generador de números pseudoaleatorios /dev/urandom, gpg usará esta fuente para la generación de las llaves GPG.

```
$ sudo rngd -r /dev/urandom
```

Generar tanto la llave pública como la privada.

```
$ gpg --full-generate-key
```

Antes de que se generen, configurar las siguientes opciones.

```
Por favor seleccione tipo de clave deseado:
   (1) RSA y RSA (por defecto)
   (2) DSA y ElGamal
   (3) DSA (sólo firmar)
   (4) RSA (sólo firmar)
Su elección: 1
```

Se recomienda el valor 1, aunque también se puede poner el 2.

```
las claves RSA pueden tener entre 1024 y 4096 bits de longitud.
¿De qué tamaño quiere la clave? (3072) 4096
```

Se recomienda el valor de 4096, por considerarlo más seguro.

```
Por favor, 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)? 0
```

Se recomienda el valor de 0, lo cual significa que la llave nunca caduca, más adelante se creará automáticamente un archivo de revocación de llaves, en caso de que se requiera que ya no sean válidas por algún motivo.

```
La clave nunca caduca
¿Es correcto? (s/n) s
```

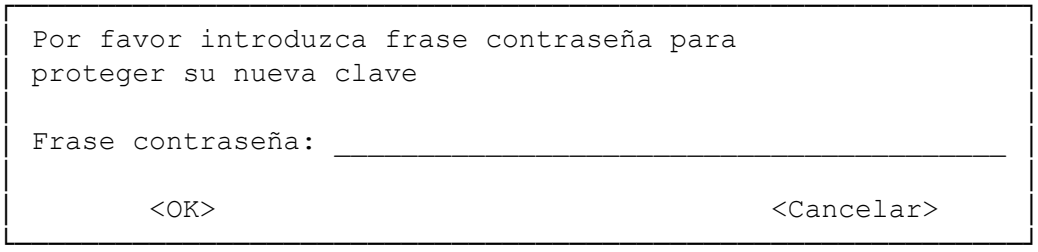
Colocar la opción s, que significa sí.

A continuación, solicitará una serie de valores personales, llenar según corresponda.

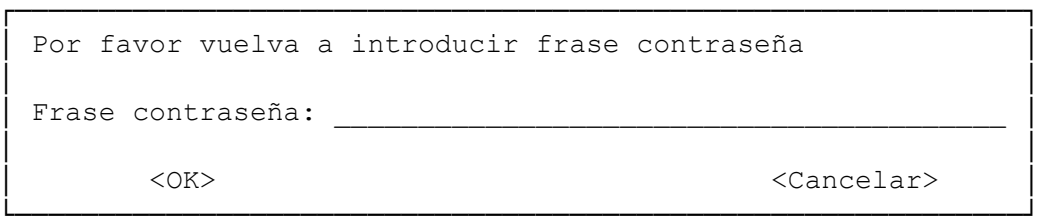
```
Nombre y apellidos: Alberto Barajas Celis
Dirección de correo electrónico: alberto.barajas@ciencias.unam.mx
Comentario: Llave GPG para el cifrado de archivos
Ha seleccionado este ID de usuario:
    "Alberto Barajas Celis (Llave GPG para el cifrado de archivos)
<alberto.barajas@ciencias.unam.mx>"

¿Cambia (N)ombre, (C)omentario, (D)irección o (V)ale/(S)alir? V
```

Ahora, solicitará una contraseña para salvaguardar las llaves GPG.



Y volverá a solicitar la misma contraseña.



Ya con los datos de configuración, el sistema procederá a crear la llave. Como previamente se generó entropía, el proceso será más rápido.

```
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.
gpg: clave 186D8FD879323EAE marcada como de confianza absoluta
gpg: creado el directorio '/home/alberto/.gnupg/openpgp-revocs.d'
gpg: certificado de revocación guardado como
'/home/alberto/.gnupg/openpgp-revocs.d/863FE089D72798857F4C843C186D8FD8
79323EAE.rev'
claves pública y secreta creadas y firmadas.

pub   rsa4096 2020-05-29 [SC]
      863FE089D72798857F4C843C186D8FD879323EAE
uid                      Alberto Barajas Celis (Llave GPG para el
cifrado de archivos) <alberto.barajas@ciencias.unam.mx>
sub   rsa4096 2020-05-29 [E]
```

Detener el proceso de la generación de entropía:

```
$ sudo killall rngd
```

De esta forma se han generado las llaves pública y privada, además de otros archivos necesarios, que se usarán para el cifrado y descifrado de archivos.

Envío de llave pública

Exportar la llave pública creada previamente a un archivo de texto, para así poder enviarla por correo electrónico o para subirla a un repositorio de llaves públicas. El correo electrónico será el mismo que se usó al generar las llaves.

```
$ gpg --export --armor alberto.barajas@ciencias.unam.mx >
alberto.barajas.pub.gpg
```

Enviar la llave pública o el enlace al repositorio de llaves públicas, al correo **computo@ciencias.unam.mx**.

Cifrado de archivos

Obtener la llave pública legítima del ente que tendrá autorización para acceder al archivo, es decir, la persona que podrá descifrar el archivo.

Importar dicha llave pública al llavero (o keyring), con el comando.

```
$ gpg --import sotero.prieto.pub.gpg
```

Cifrar el archivo, con el siguiente comando, recordar que sólo quien tenga la llave privada asociada podrá descifrarlo.

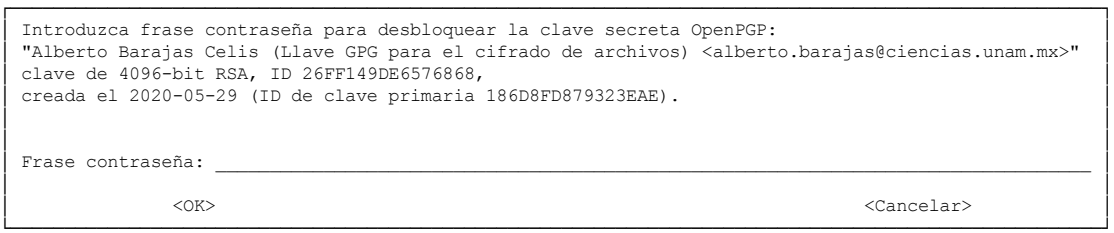
```
$ gpg --encrypt --armor --recipient sotero.prieto@ciencias.unam.mx
archivo.pdf
```

Descifrado de archivos

Descargar el archivo cifrado que se recibió en el correo electrónico. Este archivo fue cifrado con la llave pública que se envió previamente. Ejecutar el siguiente comando para descifrarlo.

```
$ gpg --output archivo.pdf --decrypt archivo.pdf.asc
```

Ingresar la contraseña que resguarda las llaves.



Así, el archivo ha sido descifrado y es legible.

Hoja de control documental

Título	**MAN01 - Cifrado y descifrado de archivos con GPG**
Resumen	Manual que indica cómo generar llaves GPG, para el cifrado y descifrado de archivos, con el fin de preservar su confidencialidad durante su transmisión en medios inseguros.
Autor(es)	Omar Martínez Olivares (omartinez@ciencias.unam.mx), Paulo Contreras Flores (paulo.contreras.flores@ciencias.unam.mx), Yeudiel Hernández Torres (yeudiel@ciencias.unam.mx)
Revisor(es)	
Organización	Universidad Nacional Autónoma de México, Facultad de Ciencias
Área solicitante	Coordinación de los servicios de Cómputo, Facultad de Ciencias
Categoría	Documentación técnica
Clasificación	Documento público
Versión	1.2
Última actualización	24 de septiembre de 2021
Edición	1a

Control de Versiones

Autor(es)	Fecha de Actualización	Revisor	Aprobación	Notas	Versión
Paulo Contreras Flores Yeudiel Hernández Torres	29 de mayo de 2020				1.0
Paulo Contreras Flores Yeudiel Hernández Torres	31 de agosto de 2021				1.1
Omar Martínez Olivares Paulo Contreras Flores Yeudiel Hernández Torres	24 de septiembre de 2021				1.2