# 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





# Contenido

Contenido	2
Introducción	3
Sistemas Windows	4
Instalación	4
Generación de Llaves GPG	6
Envío de Llave Pública	9
Cifrado de archivos	10
Descifrado de archivos	13
Sistemas Mac OS	15
Usando una aplicación	15
Instalación	15
Generación de llaves GPG	15
Envío de llave pública	17
Cifrado de archivos	18
Descifrado de archivos	20
Usando una terminal de comandos	22
Requisitos previos	22
Generación de llaves GPG	22
Envío de llave pública	24
Cifrado de archivos	24
Descifrado de archivos	25
Sistemas basados en Linux	26
Generación de llaves GPG	26
Envío de llave pública	28
Cifrado de archivos	29
Descifrado de archivos	29
Hoja de control documental	30



### 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 <u>https://www.gpg4win.org</u>

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.

Gpg4win Setup		- 🗆 X
Gpg4win	Choose Components Choose which features of Gpg4wi	n you want to install.
Check the components yo install. Click Next to contin	ou want to install and uncheck the com nue.	ponents you don't want to
Select components to inst	tall: GnuPG Kleopatra GPA GpgOL GpgEX Browser integration	Description Position your mouse over a component to see its description,
Space required: 89.9 MB		
Gpg4win-3,1,16 ————	< <u>B</u> ack	Next > Cancel

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

Gpg4win Setup	Installation ( Setup was co	Complete mpleted successfully.	_		
Completed					
геро	ort.txt	<b>Open</b> Print Edit			
		Sign and encrypt More GpgEX options	R	>	
Encryp	t files via co	ntext menu with G	ogEX.		
Gpg4win-3.1.16 ————		< <u>B</u> ack <u>N</u> ex	t >	Cano	el



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**.

🔊 Kleopatra	_	$\times$
File View Certificates Tools Settings Window Help		
Image: Construction of the second s		
Welcome to Kleopatra Gpg4win-3.1.16		
Kleopatra is a front-end for the crypto software GnuPG.		
For most actions you need either a public key (certificate) or your own private key.		
<ul> <li>The private key is needed to decrypt or sign.</li> <li>The public key can be used by others to verify your identity or encrypt to you.</li> </ul>		
You can learn more about this on Wikipedia.		
New Key Pair Import		



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.

👦 Kleopatra								_	$\times$
<u>File View Certificates T</u>	ools <u>S</u> ettings <u>W</u>	indow <u>H</u> elp							
Sign/Encrypt Decrypt/Verify.	Import		Q	<b>A</b> 77	<b>E</b> ?	×	-		
	← K Ent Plea para <u>N</u> am EMa	ey Pair Creation V er Details se enter your perso meters, click on the e: <u>Usuario</u> II: usuario@mail.c	Nizard nal details below Advanced Sett	w. If you want mor ings button.	e control ove	er the (optional) (optional)			
		✓ Protect the g	generated key w Usuario <usua< td=""><td>vith a passphrase. ario@mail.com&gt; <u>C</u>reate</td><td>Advanced S</td><td>Settings</td><td></td><td></td><td></td></usua<>	vith a passphrase. ario@mail.com> <u>C</u> reate	Advanced S	Settings			

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

7 Kleopatra		×
<u>File View Certificates Tools Settings Wi</u>	🗇 Advanced Settings - Kleopatra 🦳 🗧 🗙	
Sign/Encrypt Decrypt/Verify Import	Technical Details	
	Key Material	
— Ке	● <u>R</u> SA 4,096 bits ∨	
	✓ + RSA 4,096 bits ∨	
Ente	◯ <u>D</u> SA ∨	
Please	+ E <u>lg</u> amal 2,048 bits $\vee$	the
paran	◯ <u>E</u> CDSA/EdDSA ed25519 ∨	
Name	+ ECD <u>H</u> cv25519 V	optional)
Email:	Certificate Usage	optional)
	Signing	
	Encryption	attings
	□ <u>V</u> alid until: 8/30/2023 ∨	stelligs
		incel
	<u>Q</u> K Cancel	



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

<u>File View C</u> ertificates <u>T</u> oo	ls <u>S</u> ettings <u>\</u>	<u>W</u> indow <u>H</u> elp							
Sign/Encrypt Decrypt/Verify	lmport ⊡		Q	<u>*</u> =	2	×	-		
	← +	Key Pair Creation	Wizard						
	En	ter Details							
	Plea	ase enter your perso ameters, click on th	onal details belo e Advanced Sett	w. If you want mo tings button.	ore control ov	er the			
	Nar	ne: Usuario				(optional)			
	Em	Protect the	generated key v	with a passphrase.		(optional)			
			Usuario <usu< td=""><td>ario@mail.com&gt;</td><td></td><td></td><td></td><td></td><td></td></usu<>	ario@mail.com>					
					<u>A</u> dvanced	Settings			
						l			

Ahora, solicitará una contraseña para salvaguardar las llaves GPG.

👦 Kleopatra		_	×
<u>File View Certificates Too</u>	ls <u>S</u> ettings <u>W</u> indow <u>H</u> elp		
Sign/Encrypt Decrypt/Verify			
	Key Pair Creation Wizard     Creating Key Pair     The process of creating a key requires large amounts of random numbers. This     may require several minutes		
	Please enter the passphrase to protect your new key Passphrase: ••••••• • Repeat: •••••••		
	OK Cancel <u>Next</u> <u>Cancel</u>		



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

<b>F</b> ile <u>V</u> iew <u>C</u> ertificates <u>I</u>	? ×	×
Sign/Encrypt Decrypt/Verify.	← Key Pair Creation Wizard	E Smartcards
Search <alt+q></alt+q>	Key Pair Successfully Created	All Certificates
Name Usuario	Your new key pair was created successfully. Please find details on the result and some suggested next steps below. Result	Dm         Valid Until         Key-ID           121         1228 28EC A2BB 081D
	Key pair created successfully. Fingerprint: E19B90FDD66BA688AD069D13122828ECA2BB081D	
	Next Steps	
	Make a Backup Of Your Key Pair	
	Send Public Key By EMail	
	<u>Einish</u>	

# 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.

👦 Kleopatra										_		×
<u>F</u> ile <u>V</u> iew <u>C</u> erti	ificates <u>T</u> ool	s <u>S</u> etting	s <u>W</u> indo	w <u>H</u> elp								
Sign/Encrypt De	દ્વ crypt/Verify	Import	ा Export	E Certify	Q Lookup on S	Server	Certificates	E. Notepad	E Smartcards			
Search <alt+q></alt+q>	>									All Certificates	~	
	Name			E-	Mail		User-IDs	Valid Fr	om Valid Until	Key-ID		
Usuario			usuario@	mail.cor	n		certified	8/30/20	21	1228 28EC A2BB 0	81D	



Seleccionar la ubicación donde se guardará la llave pública.

👩 Kleonatra				- 🗆 X
File View Certificates Table Cettion	- Mőzeleve Hele			
File View Certificates Tools Settings	s <u>window H</u> eip		-	
い こ に に に い に に に に い に に い に に い に に い に い に い い に い い に い	Export Certify Lookup on Server	Certificates Notepad	Smartcards	
Search <alt+0></alt+0>	Certificates			× 🕡
$\leftarrow \rightarrow \checkmark \uparrow$	≪ Desktop ≯ gpg	<b>~ ບ</b> ຸ ∕		
Usuario Organize ▼ Ne	w folder			() B 081D
🥅 Desktop	^ Name ^		Date modified	Туре
🗎 Documents				
		No items match your se	earch.	
Music				
E Pictures	~ <			>
File en en er	Haussia 0xA300001D publicass			
File <u>n</u> ame:	Usuano_0xA2BB08TD_public.asc			
Save as <u>t</u> ype:	OpenPGP Certificates (*.asc *.gpg *.	.pgp)		~
∧ Hide Folders			<u>S</u> ave Cance	

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.

👩 Kleopatr	a				_			_	
<u>F</u> ile <u>V</u> iew	<u>C</u> ertificates <u>T</u> ools	<u>S</u> ettings	<u>W</u> indow <u>H</u> elp						
Sign/Encrypt	لم Decrypt/Verify	Import Exp	ert Certify	Q Lookup on Server	Certificates	Notepad Smartca	ards	_	
	👦 Select Certific							×	a la
Search </th <th>← → ~ ↑</th> <th>📙 « Desl</th> <th>ttop → gpg</th> <th></th> <th>U</th> <th>, О Search gpg</th> <th></th> <th>ey-ID</th> <th></th>	← → ~ ↑	📙 « Desl	ttop → gpg		U	, О Search gpg		ey-ID	
Usua	ri Organize <del>▼</del>	New folder					- 🔳	C A2BB 081	D
	📌 Quick acce	ss	Name			Date modified	д Тур	e	
		- 11	archivo.tx	t.gpg		8/30/2021 8:5	5 PM Op	enP	
	OneDrive	- 11	🔒 Usuario_0	xA2BB081D_public.	asc	8/30/2021 8:4	7 PM Op	enP	
	🔳 This PC								
	🧊 3D Objec	ts							
	💻 Desktop					_		>	
	_	File name	: Usuario_0xA2	BB081D_public.asc	~ [	Certificates (*.asc	*.cer *.cert *.cr ~ Cancel		



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

👦 Kleopatra		- 🗆 X
<u>File View Certificates Tools</u>	<u>S</u> ettings <u>W</u> indow <u>H</u> elp	
Sign/Encrypt Decrypt/Verify In	Image:	
Search <alt-< th=""><th>More Files to Sign and/or Encrypt</th><th>×</th></alt-<>	More Files to Sign and/or Encrypt	×
← → • ↑	Search gpg	
Usuario Organize <del>-</del>	New folder	A2BB 081D
🧢 This PC	^ Name ^ Date modified	Туре
🧊 3D Objec	ts 📄 archivo.txt 8/30/2021 8:51 PM	M Text Do
💻 Desktop	Usuario_0xA2BB081D_public.asc 8/30/2021 8:47 PM	M OpenPo
🖆 Documen	ts	
🖊 Download	ts	
🎝 Music	v <	>
	File name: archivo.txt	
	Open	Cancel

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

Kleopatra <u>File</u> <u>View</u> <u>Certificates</u> <u>To</u>	🔊 Sign/Encrypt Files - Kleopatra ? 🗙	(	
Sign/Encrypt Decrypt/Verify	Sign / Encrypt Files         Prove authenticity (sign)         Sign as:       Usuario <usuario@mail.com> (certified, created: 8/30/2021)</usuario@mail.com>	cates	~ <b>(</b>
Name Usuario	Encrypt  Encrypt for me: Usuario <usuario@mail.com> (certified, created: 8/30/2021)  Encrypt for others:  Fico <usuario@mail.com> (certified, OpenPGP, created: 8/30/2021)  Fico <usuario@mail.com> (certified, OpenPGP, created: 8/30/2021) Fico <usuario@mail.com> (certified, OpenPGP, created: 8/30/2021) Fico <usuario@mail.com> (certified, OpenPGP, created: 8/30/2021) Fico <usuario@mail.com> (certified, OpenPGP, created: 8/30/2021) Fico <usuario@mail.com> (certified, OpenPGP, created: 8/30/2021) Fico <usuario@mail.com> (certified, OpenPGP, created: 8/30/2021) Fico <usuario@mail.com> (certified, OpenPGP, created: 8/30/2021) Fico <usuario@mail.com> (certified, OpenPGP, created: 8/30/2021) Fico <usuario@mail.com> (certifie</usuario@mail.com></usuario@mail.com></usuario@mail.com></usuario@mail.com></usuario@mail.com></usuario@mail.com></usuario@mail.com></usuario@mail.com></usuario@mail.com></usuario@mail.com></usuario@mail.com></usuario@mail.com></usuario@mail.com></usuario@mail.com></usuario@mail.com></usuario@mail.com></usuario@mail.com></usuario@mail.com></usuario@mail.com></usuario@mail.com></usuario@mail.com></usuario@mail.com></usuario@mail.com></usuario@mail.com></usuario@mail.com></usuario@mail.com></usuario@mail.com></usuario@mail.com></usuario@mail.com></usuario@mail.com></usuario@mail.com>	Key-ID 28EC A2BB 081E	5
	Output       Encrypt / Sign each file separately.       D:/Alexei/Desktop/gpg/archivo.tdt.gpg       Encrypt       Encrypt	_	



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

🕡 Kleopatra	🕡 Sign/Encrypt Files - Kleopatra	?	×	] -	
Sign/Encrypt Decrypt/Verify	Results Status and progress of the crypto operations is shown here.			_	
Search <alt+q></alt+q>	OpenPGP: All operations completed.			icates	~
Name				Key-ID	-
Usuario	archivo.txt $\rightarrow$ archivo.txt.gpg: Encryption succeeded.	Show Audit Log		28EC A2BB 081	D
	Encryption succeeded.				
	Eir	nish <u>C</u> ance	el		





# 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.

📅 Kleopatra	🕝 Decrypt/Verify Files - Kleopatra ? X	×
Sign/Encrypt Decrypt/Verify	Output folder:       D:/Alexei/Desktop/gpg         Operation 1: Decrypting: archivo.bd.gpg	
Search <alt+q> Name Usuario</alt+q>	pinentry-qt       —       X         Please enter the passphrase to unlock the OpenPGP secret key:       "Usuario <usuario@mail.com>"         4096-bit RSA key, ID SA2128DS8E866222,       created 2021-08-31 (main key ID 122828ECA288081D).         Passphrase:       ••••••••         QK       Cancel</usuario@mail.com>	Key-ID 28EC A2BB 081D
	Save All Discard	



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

Kleopatra File View Certificates T	🗇 Decrypt/Verify Files - Kleopatra ? X	-	
Sign/Encrypt Decrypt/Verify.	Qutput folder:       D:/Alexel/Desktop/gpg         All operations completed.		
Search <alt+q> Name Usuario</alt+q>	archivo.txt.gpg → archivo.txt: Decryption succeeded.     Show Audit Log	ificates Key-ID 28EC A2BB 081	
	Note: You cannot be sure who encrypted this message as it is not signed.		
	Save All Discard		

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

📕 🗹 📕 🔻   gpg				— 🗆 X				
File Home Share View				^ ?				
Pin to Quick Copy Paste shortcut	Move Copy to to Delete Rename	New item •		Select all Select none Invert selection				
Clipboard	Organize	INEW	Open	Select				
$\leftarrow \rightarrow \checkmark \uparrow$ 📮 $\rightarrow$ This PC $\rightarrow$ Deskt	op > gpg		<b>∨ ひ</b> / ∽ Se	arch gpg				
▲ Name		Date modified	Туре	Size				
archivo	.txt	8/30/2021 8:58 PM	Text Document	1 KB				
OneDrive archive	.txt.gpg	8/30/2021 8:55 PM	OpenPGP Binary I	Fi 2 KB				
📗 archivo.txt - Notepad				- 🗆 ×				
File Edit Format View Help								
Lorem salutandi eu mea, eam i	n soleat iriure assent	ior. Tamquam lobo	ortis id qui. Ea	sanctus democritur ^				
Est ei erat mucius quaeque. Ei his quas phaedrum, efficiantur mediocritatem ne sed, hinc oratio bland:								
				· · · · · · · · · · · · · · · · · · ·				
		Ln 1, Col 1	100% Windows (CR	LF) UTF-8				



# 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 <u>https://gpgtools.org/</u>



#### Generación de llaves GPG

Una vez instalada, ingresar la palabra "GPG KeyChain" en el Spotlight 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 "+".

•••	+ Nueva	山 亡 Importar Exportar	Q i Q Filtrar Buscar clave Detalles	
Tipo Nombre	Correo electrónico:	Creado	Huella de validación (fingerprint)	Validez

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.

Create new key pair	
Nombre: Alberto Barajas Celis	<i>• 1 •</i>
Correo electrónico: alberto.barajas@ciencias.unam.mx 💙	Su clave fue creada con éxito
Contraseña	Para facilitar que sus amigos y colegas encuentren su clave
Confirme la contraseña:	pública y comiencen a comunicarse con usted de forma segura – cifrar mensajes para usted y verificar la autenticidad de los mensajes que usted envíe – se recomienda subir su clave pública e los conjúderos de olavos
Fortaleza:	publica a los selvidores de claves.
<ul> <li>Opciones avanzadas</li> </ul>	Advertencia: Los servidores de claves son públicos, así que el nombre y correo electrónico que uese en su clave serán visibles públicamente. Las claves no se pueden borrar de los servidores
Comentario:	de claves. Se pueden revocar, pero no eliminar.
Tipo de clave: RSA y RSA (por defecto) 📀	Si prefiere en cambio no usar servidores de claves, por favor, considere adjuntar su clave pública a sus correos firmados y/o
Longitud: 4096 🕑	cifrados.
Key will expire on: 25/ 9/2025 文	¿Quiere subir su clave pública?
Cancelar Create Key	Subir clave pública ¡No, gracias!

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

•••		+ Nueva	් ෆ් Importar Exportar	Q i Q Filtrar Buscar clave Detalles	
Тіро	Nombre	<ul> <li>Correo electrónico:</li> </ul>	Creado	Huella de validación (fingerprint)	Validez
sec/pub	Alberto Barajas Celis	alberto.barajas@ciencia	s.una 25 sep 2021	CA94 D4AD 3738 5584 BF04 F316 702A	



#### 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**",

•••		+ Nuev	a Importa	ப் ar Exportar	Q Buscar clave	i Detalles	Q Filtrar	
Tipo	Nombre	<ul> <li>Correo electrónico:</li> </ul>		Creado	Huella de validac	ión (fingerprir	nt)	Validez
sec/pul	Alberto Baraias Celis	Utreste beschool of a Exportar Enviar clave pública por cor Enviar clave pública al servi Actualizar desde el servidor Detalles Firmar Generar certificado de revo Revocar Copiar Borrar	dor de claves reo dor de claves r de claves	25 sep 2021	<u>CA94 D4AD 3</u> 7	738 5584 1	8604 F316 702A	833A D942 C852

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

Guardar como: alberto.barajas.pub.gpg						
Ubicación: [ 📄 Escritorio 📀 🗸						
Incluir clave secreta (privada) en el fichero exportado						
. Cancelar 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**".

•••			+ Nueva	⊡ Importa	r Exportar	Q Buscar clave	i Detalles	Q Fi	ltrar				
Tipo	Nombre	^	Correo electrónico:		Creado	Huella de validaci	ón (fingerpr	int)					Validez
sec/pub	Alberto Barajas Celis		alberto.barajas@ciencias.	una	25 sep 2021	CA94 D4AD 37	38 5584	BF04	F316	702A	833A D	942 C852	

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".

Favoritos		Escritorio	Q Buscar
🙏 Aplicacio			
Precientes	Nombre		<ul> <li>Fecha de mo</li> </ul>
Escritorio			
🕒 Documen	👔 alberto.barajas.pub.asc		hoy 10:32
Descargas			
😭 omar			
Creative			
iCloud			
iCloud Dri			
Etiquetas			
			Cancelar Abrir



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

< > archi	vos		88 ∷≣		<u> </u>
Nombre			∧ Fecł	na de modificación	Т
A archivo.pdf	Abrir Abrir con Transferir al basurero Obtener información Renombrar Comprimir "archivo.pdf" Duplicar	>	hoy	11:54	
	Crear alias Vista rápida Copiar Compartir	>			
	C C C C C C C C C C C C C C C C C C C	>			
	Servicios	>	OpenPGP: I OpenPGP: I OpenPGP: I	Decrypt File Encrypt File mport Key from Fil	le

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**"

• •				
Select Recipients				
✔ Name	^ Email	Validity	Fingerprint	
🗹 Alberto Barajas Celis	alberto.barajas@ciencias.unam		5A26 1EB1 FA61 2358 6563	E7D2 D1B2 066D 37DF 3802
🗌 busuario	bomartinez@ciencias.unam.mx		9FB5 EF4A 9237 F4E7 7D56	91F2 225F 8EDD F59C FA76
Select all	Q Search			0 of 4 keys selected
Your Key: busuario <bomartinez@ciencias.unam.mx> (225F8EDDF59CFA76)</bomartinez@ciencias.unam.mx>				Sign Add to Recipients
Encrypt with password				
Version: 2.2 Build: 1146				Cancel Encrypt



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

Encryption finished archivo.pdf.gpg	Show in Finder OK			
Nombre	^	Fecha de modificación	Tamaño	Clase
🋃 archivo.pdf		hoy 11:54	146 KB	Documento PDF
archivo.pdf.gpg		hoy 12:02	126 KB	GnuPGpted File

#### 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** 

archivo.pdf.gpg	Abrir		
	Abrir con	>	
	Transferir al basurero		
	Obtener información		
	Renombrar		
	Comprimir "archivo.pdf.gpg"		
	Duplicar		
	Crear alias		
	Vista rápida		
	Copiar		
	Compartir	>	
	$\bigcirc \bigcirc $		
	Etiquetas		
	Menú de acciones rápidas	>	
	Servicios	>	OpenPGP: Decrypt File
			OpenPGP: Encrypt File
			OpenPGP: Import Key from File



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

 Pinentry Mac				
Introduzca frase contraseña para desbloquear la clave secreta OpenPGP: "Alberto Barajas Celis <a href="mailto:alberto.barajas@ciencias.unam.mx">alberto.barajas@ciencias.unam.mx</a> " clave de 4096-bit RSA, ID AAD73C1E4DD587A0, creada el 2021-09-25 (ID de clave primaria D1B2066D37DF3802).				
Frase contraseña: Show typing 🗹 Save in Keychain				
Cancel OK				

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

		Decryption fin Decrypted 'arcl	nished chivo.pdf.gpg' Show in Finder	
•	• •		< > archivos	
Favo	oritos		Nombre	
	AirDrop		B prohive pdf	
Å	Aplicaciones	5	archivo.pdf	
a	Pacientes			
	Recientes			
	Escritorio			



# 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 (<u>https://brew.sh/</u>).

#### 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 Q 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.



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?  ${\bf V}$ 

Ahora, solicitará una contraseña para salvaguardar las llaves GPG.

```
Por favor introduzca frase contraseña para
proteger su nueva clave
Frase contraseña:
<OK> <Cancelar>
```

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>
```

# Envío de llave pública

sub rsa4096 2021-09-24 [E]

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.



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?  ${\bf V}$ 

Ahora, solicitará una contraseña para salvaguardar las llaves GPG.

Por favor introduzca frase contraseña para proteger su nueva clave	
rase contraseña:	_
<ok> <cancelar></cancelar></ok>	

Y volverá a solicitar la misma contraseña.

Por favor vuelva a introducir frase contrase	ña
Frase contraseña:	
<ok></ok>	<cancelar></cancelar>

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

