UAEMEX

Proyecto - Segurdad de la Información

01

Equipo 2

Descargar e instalar GnuPG

04

GnuPG binary releases

In general we do not distribute binary releases but leave that to the common Linux distributions. However, for some operating systems we list pointers to readily installable releases. We cannot guarantee that the versions offered there are current. Note also that some of them apply security patches on top of the standard versions but keep the original version number.

OS	Where	Description
Linux	**download sig**	*GnuPG Desktop*® AppImage with the current *GnuPG*
Windows	**Gpg4win**	Full featured Windows version of *GnuPG*
	download sig	Simple installer for the current *GnuPG*
	download sig	Simple installer for *GnuPG 1.4*
OS X	**Mac GPG**	Installer from the gpgtools project
	GnuPG for OS X	Installer for *GnuPG*
Debian	**Debian site**	GnuPG is part of Debian
RPM	**rpmfind**	RPM packages for different OS
Android	**Guardian project**	Provides a GnuPG framework
VMS	**antinode.info**	A port of GnuPG 1.4 to OpenVMS
RISC OS	**home page**	A port of GnuPG to RISC OS

```
Microsoft Windows [Versión 10.0.22631.3447]
(c) Microsoft Corporation. Todos los derechos reservados.

D:\UNIVERSIDAD\SI\cifrado>gpg --full-generate-key
gpg (GnuPG) 2.4.5; Copyright (C) 2024 g10 Code GmbH
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

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: 9
Seleccione el tipo de curva elíptica deseado:
   (1) Curve 25519 *default*
   (4) NIST P-384
   (6) Brainpool P-256
Su elección: 1
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)? 4
La clave caduca 05/06/24 14:58:36 Hora est♦ndar central (M♦xico)
¿Es correcto? (s/n) s

GnuPG debe construir un ID de usuario para identificar su clave.
```

```
Nombre y apellidos: Fernanda Rico Elizarraras
Dirección de correo electrónico: maria.fernanda.rico.e@gmail.com
Comentario: Clave pública para cifrado de archivos personal. Prueba 1 - Proyecto SI
Está usando el juego de caracteres 'CP850'.
Ha seleccionado este ID de usuario:
    "Fernanda Rico Elizarraras (Clave pública para cifrado de archivos personal. Prueba 1 - Proyecto SI) <maria.fernanda.rico.e@gmail.com>"

¿Cambia (N)ombre, (C)omentario, (D)irección o (V)ale/(S)alir? V
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.
gpg: C:\\Users\\OMEN\\AppData\\Roaming\\gnupg\\trustdb.gpg: se ha creado base de datos de confianza
gpg: creado el directorio 'C:\\Users\\OMEN\\AppData\\Roaming\\gnupg\\openpgp-revocs.d'
gpg: certificado de revocación guardado como 'C:\\Users\\OMEN\\AppData\\Roaming\\gnupg\\openpgp-revocs.d\\E6B95592A50EEDE4C1D6EA50CE26526CCBB4BB80.rev'
claves pública y secreta creadas y firmadas.

pub   ed25519 2024-05-02 [SC] [caduca: 2024-05-06]
      E6B95592A50EEDE4C1D6EA50CE26526CCBB4BB80
uid                      Fernanda Rico Elizarraras (Clave pública para cifrado de archivos personal. Prueba 1 - Proyecto SI) <maria.fernanda.rico.e@gmail.com>
sub   cv25519 2024-05-02 [E] [caduca: 2024-05-06]
```

```
D:\UNIVERSIDAD\SI\cifrado>gpg --export -a Fernanda Rico Elizarraras > clave_publica.asc

D:\UNIVERSIDAD\SI\cifrado>gpg --encrypt enPaz.txt
No ha especificado un ID de usuario (puede usar "-r")

Destinatarios actuales:

Introduzca ID de usuario. Acabe con una línea vacía: E6B95592A50EEDE4C1D6EA50CE26526CCBB4BB80
gpg: comprobando base de datos de confianza
gpg: marginals needed: 3  completes needed: 1  trust model: 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: 2024-05-06

Destinatarios actuales:
cv25519/96905F1399163FC7 2024-05-02 "Fernanda Rico Elizarraras (Clave p├╠blica para cifrado de archivos personal. Prueba 1 - Proyecto SI) <maria.fernanda.rico.e@gmail.com>"

Introduzca ID de usuario. Acabe con una línea vacía: E6B95592A50EEDE4C1D6EA50CE26526CCBB4BB80
gpg: omitida: clave pública ya establecida

Destinatarios actuales:
cv25519/96905F1399163FC7 2024-05-02 "Fernanda Rico Elizarraras (Clave p├╠blica para cifrado de archivos personal. Prueba 1 - Proyecto SI) <maria.fernanda.rico.e@gmail.com>"

Introduzca ID de usuario. Acabe con una línea vacía: E6B95592A50EEDE4C1D6EA50CE26526CCBB4BB80
gpg: omitida: clave pública ya establecida

Destinatarios actuales:
cv25519/96905F1399163FC7 2024-05-02 "Fernanda Rico Elizarraras (Clave p├╠blica para cifrado de archivos personal. Prueba 1 - Proyecto SI) <maria.fernanda.rico.e@gmail.com>"

Introduzca ID de usuario. Acabe con una línea vacía:

D:\UNIVERSIDAD\SI\cifrado>gpg --encrypt enPaz.txt
No ha especificado un ID de usuario (puede usar "-r")

Destinatarios actuales:
```

```
Introduzca ID de usuario. Acabe con una línea vacía:
gpg: no hay direcciones válidas
gpg: enPaz.txt: encryption failed: No hay identificador de usuario

D:\UNIVERSIDAD\SI\cifrado>gpg --encrypt enPaz.txt -r
uso: gpg [opciones] --encrypt [filename]

D:\UNIVERSIDAD\SI\cifrado>gpg --encrypt enPaz.txt -r Fernanda Rico Elizarraras
uso: gpg [opciones] --encrypt [filename]

D:\UNIVERSIDAD\SI\cifrado>gpg --encrypt enPaz.txt
No ha especificado un ID de usuario (puede usar "-r")

Destinatarios actuales:

Introduzca ID de usuario. Acabe con una línea vacía: E6B95592A50EEDE4C1D6EA50CE26526CCBB4BB80

Destinatarios actuales:
cv25519/96905F1399163FC7 2024-05-02 "Fernanda Rico Elizarraras (Clave p╠blica para cifrado de archivos personal. Prueba 1 - Proyecto SI) <maria.fernanda.rico.e@gmail.com>"

Introduzca ID de usuario. Acabe con una línea vacía:
El fichero 'enPaz.txt.gpg' ya existe. ¿Sobreescribir? (s/N) s

D:\UNIVERSIDAD\SI\cifrado>gpg --encrypt -r ubecerrilv001@alumno.uaemex.mx enPaz.txt
gpg: error recuperando 'ubecerrilv001@alumno.uaemex.mx' vía WKD: No such file or directory
gpg: ubecerrilv001@alumno.uaemex.mx: omitido: No such file or directory
gpg: enPaz.txt: encryption failed: No such file or directory
```

```
D:\UNIVERSIDAD\SI\cifrado>gpg --list-keys
[keyboxd]
---------
pub   ed25519 2024-05-02 [SC] [caduca: 2024-05-06]
      E6B95592A50EEDE4C1D6EA50CE26526CCBB4BB80
uid           [  absoluta ] Fernanda Rico Elizarraras (Clave p├╠blica para cifrado de archivos personal. Prueba 1 - Proyecto SI) <maria.fernanda.rico.e@gmail.com>
sub   cv25519 2024-05-02 [E] [caduca: 2024-05-06]


D:\UNIVERSIDAD\SI\cifrado>gpg --full-generate-key
gpg (GnuPG) 2.4.5; Copyright (C) 2024 g10 Code GmbH
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

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: 9
Seleccione el tipo de curva elíptica deseado:
   (1) Curve 25519 *default*
   (4) NIST P-384
   (6) Brainpool P-256
Su elección: 1
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)? 2w
```

C:\Windows\System32\cmd.e

```
¿Es correcto? (s/n) s

GnuPG debe construir un ID de usuario para identificar su clave.

Nombre y apellidos: Ulises Becerril Valdes
Dirección de correo electrónico: ubecerrilv001@alumno.uaemex.mx
Comentario: Clave publica para cifrado de archivos personal. Prueba 1 - Proyecto SI
Ha seleccionado este ID de usuario:
    "Ulises Becerril Valdes (Clave publica para cifrado de archivos personal. Prueba 1 - Proyecto SI) <ubecerrilv001@alumno.uaemex.mx>"

¿Cambia (N)ombre, (C)omentario, (D)irección o (V)ale/(S)alir? v
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.
gpg: certificado de revocación guardado como 'C:\\Users\\OMEN\\AppData\\Roaming\\gnupg\\openpgp-revocs.d\\C09D57B08BAE6CDB0376DE7C9C6121B1B1D4E53E.rev'
claves pública y secreta creadas y firmadas.

pub   ed25519 2024-05-02 [SC] [caduca: 2024-05-16]
      C09D57B08BAE6CDB0376DE7C9C6121B1B1D4E53E
uid                      Ulises Becerril Valdes (Clave publica para cifrado de archivos personal. Prueba 1 - Proyecto SI) <ubecerrilv001@alumno.uaemex.mx>
sub   cv25519 2024-05-02 [E] [caduca: 2024-05-16]


D:\UNIVERSIDAD\SI\cifrado>gpg --encrypt -r C09D57B08BAE6CDB0376DE7C9C6121B1B1D4E53E enPaz.txt
gpg: comprobando base de datos de confianza
gpg: marginals needed: 3  completes needed: 1  trust model: pgp
gpg: nivel: 0  validez:   2  firmada:   0  confianza: 0-, 0q, 0n, 0m, 0f, 2u
gpg: siguiente comprobación de base de datos de confianza el: 2024-05-06
```

```
gpg: siguiente comprobación de base de datos de confianza el: 2024-05-06
El fichero 'enPaz.txt.gpg' ya existe. ¿Sobreescribir? (s/N) s

D:\UNIVERSIDAD\SI\cifrado>gpg --encrypt -r ubecerrilv001@alumno.uaemex.mx enPaz.txt
El fichero 'enPaz.txt.gpg' ya existe. ¿Sobreescribir? (s/N) s

D:\UNIVERSIDAD\SI\cifrado>gpg --encrypt -r ubecerrilv001@alumno.uaemex.mx noTeDetengas.txt

D:\UNIVERSIDAD\SI\cifrado>gpg --decrypt enPaz.gpg > enPaz_gpgEncrypt.txt
gpg: encrypted with cv25519 key, ID 758A9BBB92D5B20E, created 2024-05-02
      "Ulises Becerril Valdes (Clave publica para cifrado de archivos personal. Prueba 1 - Proyecto SI) <ubecerrilv001@alumno.uaemex.mx>"
```