

## 1. Generando Claves

```
uca@debian:~$ gpg --full-generate-key
gpg (GnuPG) 2.2.27; Copyright (C) 2021 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.

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)
(14) Existing key from card
Su elección: 1
Las claves RSA pueden tener entre 1024 y 4096 bits de longitud.
¿De qué tamaño quiere la clave? (3072)
El tamaño requerido es de 3072 bits
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)?

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 E5843D70BF1BF8F7 marcada como de confianza absoluta
gpg: creado el directorio '/home/uca/.gnupg/openpgp-revocs.d'
gpg: certificado de revocación guardado como '/home/uca/.gnupg/openpgp-revocs.d/
DEA9567BE5A1F40CA427E37DE5843D70BF1BF8F7.rev'
claves pública y secreta creadas y firmadas.

pub   rsa3072 2022-08-24 [SC]
       DEA9567BE5A1F40CA427E37DE5843D70BF1BF8F7
uid    katya herrera (katya017) <00188119@uca.edu.sv>
sub    rsa3072 2022-08-24 [E]

uca@debian:~$
```

## 2. Certificado de revocación

```
uca@debian: ~
Por favor elija una razón para la revocación:
0 = No se dio ninguna razón
1 = La clave ha sido comprometida
2 = La clave ha sido reemplazada
3 = La clave ya no está en uso
Q = Cancelar
(Probablemente quería seleccionar 1 aquí)
¿Su decisión? 0
Introduzca una descripción opcional; acábela con una línea vacía:
> no hay ninguna razón
>
Razón para la revocación: No se dio ninguna razón
no hay ninguna razón
¿Es correcto? (s/N) s
se fuerza salida con armadura ASCII.
Certificado de revocación creado.

Por favor consérvelo en un medio que pueda esconder; si alguien consigue
acceso a este certificado puede usarlo para inutilizar su clave.
Es inteligente imprimir este certificado y guardarlo en otro lugar, por
si acaso su medio resulta imposible de leer. Pero precaución: ¡el sistema
de impresión de su máquina podría almacenar los datos y hacerlos accesibles
a otras personas!
uca@debian:~$
```

### 3. Administración de claves

```
uca@debian:~$ gpg --list-keys
/home/uca/.gnupg/pubring.kbx
-----
pub   rsa3072 2022-08-24 [SC]
      DEA9567BE5A1F40CA427E37DE5843D70BF1BF8F7
uid    [ absoluta ] katya herrera (katya017) <00188119@uca.edu.sv>
sub    rsa3072 2022-08-24 [E]
```

```
uca@debian:~$
```

```
uca@debian:~$ gpg --list-secret-keys
/home/uca/.gnupg/pubring.kbx
-----
sec   rsa3072 2022-08-24 [SC]
      DEA9567BE5A1F40CA427E37DE5843D70BF1BF8F7
uid    [ absoluta ] katya herrera (katya017) <00188119@uca.edu.sv>
ssb    rsa3072 2022-08-24 [E]
```

```
uca@debian:~$
```

### 4. Clave de usuario katya

```
uca@debian: ~
a@debian:~$ gpg --output nextor.gpg --export 00188119@uca.edu.sv
a@debian:~$ gpg --armor --export 00188119@uca.edu.sv
---BEGIN PGP PUBLIC KEY BLOCK-----
```

```
5NBGMGSFMBADnBfr6Wz51j+mZkkGw4GlllLFrJZP5ko/Ljx0ngI6y2Q7mjZpz
c/hKnDx4mgNnpzkqGxWdFQ+hSxN39fYWMrweG2UMjndSAv60aVAISAVvcRidnq
r/GhoiJQas5JU5YXreTANW6+cIa5URvEaLfH00XZqR/ooCpf8vwrJ33orOutZk
yMXcGX/Ob7PuFoGnz4qGindpsRNWq8RSMYXuU1lhJshK4VuqvSDt9veHw7tfd
tLCKEhwZgGwIWPYP8DQInIvVvCUN6n9Gg2+TBZezb3mLSAYUI93YLEd6HuZtLM6
rPBQIysf7qQPWY56CYSdpq+20wC/wxnDtC+4AyeCBJ8BhUavmyBjTcT3q+cNS
6vPo91yR3sTef2s1Bhzm0HQ89qV50LZd6n0m3P5zkN3x2yix4tL45XKNtRuN0
cRh/viCJBW+/XuQUUwf4X7Dwp3zIdUhcDSm1wMVRTRUIB6mHFWRIMFYdHPQWck
<7oHufoWA1qecAEQEAAbQua2F0eWEgaGVycmVYSAoA2F0eWEwMTcpIDwwMDE4
Ex0UB1Y2EuZWRLlNn2PokBzGQTAQoA0BYhBN6pVnvlofQmPcfjfewEPXC/G/j3
JjBkhTAhsDBQsJCAcCBhUKCQGLAgQWAgMBAh4BAheAAAJE0WEPXC/G/j34SgM
cBnWT3JvF2L/4MTcYqvgfabPp6rHnuGT2vK3PfnhgouuIbngN4avSix4Sw4y1D
<UUCKKzm/rLa4C8gr04gKbcBC9ToPHGam07U948pEbfoiZYDaIdYHRG/AP8mnz
Wc+ahKF2oj+Acm0bhWkAsFK9u7L+I3k13+avCmfa0nzgiUP7XXpMcQ996lkgw5
/Ex4BLKFLc7c0ZC031MZAkI9N5c1/ZyWKFabHvrm4EnWAJIradBBcDcldc6f6G
jXfcwPER0VIRuNFcdRKdJZi0IwenefzI3hR1zvJCpXDt9eoA0zsIzcXnFmid5w
cKzR0pWvVmkmqQqHswYwpZ6oUhnAT6CaypQDa1D4aYVJdcb8CB1Q/t/jjhnbf
s0eq0EU8o0KbBMfQSmw4n7DlCWZQezAWKnNri4PF56F4/kXHUS2VNwFGG0YK
VmJ0XwVKI5hYls63MpGtxeZzJT0YqJwLtGH0Yp0eG9xYIDqRP56kX31h0cY6zg
<BjQRjBkhTAQwAywZ5v70a0KfBqLzi6Jn7mmoBjqaI1Fxnwzj2JH0B/uZcApnJ
3BC22wGgoNjTkPaNImzQxn8Hz05zULrQL6Ks5Zh2x44HcGEVYy3jQ0uzrrS/5Z
savlDyHf9lV4lT6sd8g9yKNVol16Jrx4xXTHHVOtIwfkYAH/NKGxBeLQ5xnF/
nyrwaq9SE/dqxsKd8VbAzaKe45bPpBsJ EjkpMI80J/+ieY+oUsBnTNUe18Cqq
c1AubR90VL4vWZp8BPuPoZvz+22NUUCRB1jBXjHtaNrH4wnVXS7wXp+kBLWWTn
eqaJJdfo+PzBsazGY8IH3J2R8X5IThQ1sFgVL/wsyof4hPh1++Sq4pdycTLbLm
+kpUQPThwpVxQfmPTIrtJvN/W+LC1v2GmEjR/hzuG+RXxRbT3y/G31dfkCck0Z
tfeAhn9f7mES45XPSXG2p3kkHvNtfZRn29HWWqwnbie518Bhm3Rc87obZD5KLe
4N3hUUJnX0myWBABEBAAGJAbYEGAeKACAWIQTeqVZ75aH0DKQn433lhD1wvxv4
JCYwZiUwIbDAACRDLhD1wvxv495Q+DAXCvWP6y+j1Lc1lrXkPT5P1toGNTiD
cXNRhZpErs3kDy4unVJMJSmyOtM4wKZ0cEe7zQYw8zQ40TGXFWUoIc5uCFzG
c6jsMZy26XQjYnFdb8r665NpCDwbxWkronk2TwPv9RnUhqDEsWnCTxXy0Ht9y
VhZpRKcMYsVmGEPby+1zQ7vNj7LYxxPrZo+oDws5I00Zx/i/mQg3KZsaYJ13B
5FElfZrKiz+gKGgwLQsNweF116YTFPqZy6iudUwmkMadC0IrmnI2ZMAiL9Mj
nUMGGoLMIRMGc8Db6jXRka3GCB3yv+d/iD6/R6VB617LGAA3W2BuptF3N9hEe
JcbLVUrLoZv+Ihi8GZNgGIFayB+5xdpvNuN++jC4dbFEi27quUjHp0Hr2qoZ
yQ1r8p8sP4k/2o5zNbnLy0FEyAefVeCboBBmMkBCkVNRtWeAcdeFl1Ruoo+Tk7
Zgi7ZPQjDAYMlmbQZpmn/BTgL/70lxP1Y=
vOU
---END PGP PUBLIC KEY BLOCK-----
```

```
a@debian:~$
```

## 5. Exportando clave privada y creando archivo de miguel

```
uca@debian:~$ gpg --export-secret-keys --armor 00188119@uca.edu.sv > ./my-priv-gpg-key.asc
uca@debian:~$ touch miguel.gpg
uca@debian:~$ ls
checksum  Escritorio  miguel.gpg          my-priv-gpg-key.asc~      Plantillas
Descargas Imágenes      Música              my_revocation_certificate.asc Público
Documentos katya          my-priv-gpg-key.asc nextor.gpg                Vídeos
uca@debian:~$ nano miguel.gpg
uca@debian:~$
```

## 6. Importando clave de miguel

```
uca@debian:~$ touch miguel.gpg
uca@debian:~$ ls
checksum  Escritorio  miguel.gpg          my-priv-gpg-key.asc~      Plantillas
Descargas Imágenes      Música              my_revocation_certificate.asc Público
Documentos katya          my-priv-gpg-key.asc nextor.gpg                Vídeos
uca@debian:~$ nano miguel.gpg
uca@debian:~$ gpg --import ~/Downloads/miguel.gpg
gpg: no se puede abrir '/home/uca/Downloads/miguel.gpg': No existe el fichero o el directorio
gpg: Cantidad total procesada: 0
uca@debian:~$ gpg --import ~/miguel.gpg
gpg: clave 22FD98109A7AB1C3: clave pública "miguel rivas (clave for uca sei) <00087518@uca.edu.sv>" importada
gpg: Cantidad total procesada: 1
gpg:          importadas: 1
uca@debian:~$
```

## 7. Creando archivo de nexxtor e importando la clave

```
uca@debian:~$ touch nexxtor.gpg
uca@debian:~$ ls
checksum  Imágenes      my-priv-gpg-key.asc  nexxtor.gpg
Descargas katya          my-priv-gpg-key.asc~ Plantillas
Documentos miguel.gpg     my_revocation_certificate.asc Público
Escritorio Música        nextor.gpg           Vídeos
uca@debian:~$ nano nexxtor.gpg
uca@debian:~$ gpg --import ~/Downloads/nexxtor.gpg
gpg: no se puede abrir '/home/uca/Downloads/nexxtor.gpg': No existe el fichero o el directorio
gpg: Cantidad total procesada: 0
uca@debian:~$ gpg --import ~/Downloads/nexxtor.gpg
gpg: no se puede abrir '/home/uca/Downloads/nexxtor.gpg': No existe el fichero o el directorio
gpg: Cantidad total procesada: 0
uca@debian:~$ gpg --import ~/nexxtor.gpg
gpg: clave CB584318958A9202: clave pública "Nestor Santiago Aldana Rodriguez (GnuPG Guide - For UCA in SED) <naldana@uca.edu.sv>" importada
gpg: Cantidad total procesada: 1
gpg:          importadas: 1
uca@debian:~$
```

## 8. Enlistando las claves publicas

```
uca@debian:~$ gpg --list-keys
/home/uca/.gnupg/pubring.kbx
-----
pub   rsa3072 2022-08-24 [SC]
      DEA9567BE5A1F40CA427E37DE5843D70BF1BF8F7
uid   [ absoluta ] katya herrera (katya017) <00188119@uca.edu.sv>
resub rsa3072 2022-08-24 [E]

pub   rsa3072 2022-08-17 [SC] [caduca: 2022-10-16]
      FE42FA6AEB275595B093D4F322FD98109A7AB1C3
uid   [ total ] miguel rivas (clave for uca sei) <00087518@uca.edu.sv>
sub   rsa3072 2022-08-17 [E] [caduca: 2022-10-16]

pub   rsa3072 2022-08-17 [SC]
      9EE66B446C0E7BC1B74E6DE9CB584318958A9202
uid   [desconocida] Nestor Santiago Aldana Rodriguez (GnuPG Guide - For UCA in SED)
      <naldana@uca.edu.sv>
sub   rsa3072 2022-08-17 [E]

uca@debian:~$
```

## 9. REALIZAR LOS EJERCICIOS DEL CIFRADO

Cifrado simetrico

```
uca@debian: ~
49  ls
50  nano nexxtor.gpg
51  gpg --import ~/Downloads/nexxtor.gpg
52  gpg --import ~/nexxtor.gpg
53  gpg --list-keys
54  gpg --edit-key naldana@uca.edu.sv
55  gpg --list-keys
56  gpg --output doc.gpg --symmetric doc
57  history > history.txt
uca@debian:~$ gpg --output history.txt.gpg --symmetric history.txt
uca@debian:~$ cat history.txt.gpg
T00%00e0000kVF00K00Gvh0040M000c0w-000.000000S(l0000Rf0cl      090(f0 0U"\0k0_0h+
000@&3XaH0r00{0%0n00|00I00a0C[,`&00]000#H0000Bb`Y600
2z00000W00avp8J000Xy0?0)uL;00(W0t0/00A
3IU290wWbVe
Y50$0*XF00000h000!00a0000^0000[0S0050{[00
0Yy770000J00%D+P?^aI40f0C0030<f0P000
06p9>i]00R00N0000d00#0Q00000 0>0r00B8000E0)000Y_0000N000i0c300o000|NPts_)=000;0G0n0p0.
1D0f0<\0f]0"00_00d00
!LN}00h00
0
u00,
00001RjJ8/00b000C000B0%0J00F00#d00B00/oR0p[000000000{>
0<)00%6Cx0000z}0_Y+!000b00
^0'uca@debian:~$
```

## 10. Cifrado asimétrico

```
uca@debian:~$ history > historyPublicKey.txt
uca@debian:~$ at historyPublicKey.txt
bash: at: orden no encontrada
uca@debian:~$ cat historyPublicKey.txt
 1 sudo su -
 2 su -
 3 sudo su
 4 exiyt
 5 exit
 6 sudo su
 7 sudo su
 8 cp -r ./ ~ /Escritorio/cd
 9 cp -r ./ ~ /Escritorio/cd
10 cd ~/Escritorio
11 cd cd
12 sudo chmod +x autorun.sh
13 ./autorun.sh
14 touch katya
15 ls
16 nano katya
17 md5sum katya
```

```
uca@debian: ~
59 gpg --output history.txt.gpg --symmetric history.txt
60 cat history.txt.gpg
61 history > historyPublicKey.txt
uca@debian:~$ gpg --output historyPublicKey.txt.gpg --encrypt --recipient naldana@uca.edu
.sv historyPublicKey.txt
uca@debian:~$ cat historyPublicKey.txt
 1 sudo su -
 2 su -
 3 sudo su
 4 exiyt
 5 exit
 6 sudo su
 7 sudo su
 8 cp -r ./ ~ /Escritorio/cd
 9 cp -r ./ ~ /Escritorio/cd
10 cd ~/Escritorio
11 cd cd
12 sudo chmod +x autorun.sh
13 ./autorun.sh
14 touch katya
15 ls
16 nano katya
17 md5sum katya
18 md5sum katya
19 md1sum katya
20 sha256sum katya >checksum
```