

## Trabajo Práctico #9

# “Cifrado y firma digital con GnuPG”

Fecha de Entrega: 17/11/2016  
Medina, Ma. Victoria [117024]  
medina.vicc@gmail.com

a) Cifrar un archivo: `$ gpg -c <archivo>` solicita la clave simétrica para cifrar y genera archivo.gpg. Por defecto se realizará el cifrado utilizando CAST5. Para utilizar otro método de cifrado:

```
$ gpg -c --cipher-algo nombre_algoritmo <archivo>
```

Para conocer los algoritmos soportados invocar `gpg -version`.

El siguiente ejemplo utiliza AES como método de cifrado:

```
$ gpg -c --cipher-algo AES <archivo>
```

Creamos el archivo que se va a cifrar:

```
root@debian2:/home/victoriamedina# nano puntoa.txt
```

Procedemos a cifrar el archivo con contraseña : *lunes*

```
root@debian2:/home/victoriamedina# gpg -c puntoa.txt
```

b) Descifrar un archivo cifrado: `$ gpg <archivo.gpg>`

Solicitará la clave y descifra el archivo, guardando el resultado en un nuevo archivo con el mismo nombre sin extensión

Ahora vamos a descifrar el archivo

```
root@debian2:/home/victoriamedina# gpg puntoa.txt.gpg
gpg: datos cifrados CAST5
gpg: cifrado con 1 contraseña
El fichero `puntoa.txt' ya existe. ¿Sobreescribir? (s/N) s
gpg: ATENCIÓN: la integridad del mensaje no está protegida
```

## Parte 2. Criptografía de clave pública

a) Administración de claves:

Primero debe generarse el par de clave publica y privada con:

```
$ gpg --gen-key
```

Complete los datos con su nombre y dirección de correo electrónico. Por ejemplo:

*Tipo de clave: (1) RSA y RSA (por defecto)*

*Tamaño de clave: 2048 bits*

*Validez de la clave: 0 (sin expiración)*

*Nombre y apellidos: Ester Pisco*

*Dirección de correo electrónico: episco@organizacion*

*Comentario: EstercitaFrase contraseña: 12 de marzo de 1976*

*(esta contraseña protegerá la clave privada y se requerirá para firmar o cifrar un documento)*

Ejemplo de datos a completar para otro par de claves pública y privada:

*Nombre y apellidos: Manuel Dario*

*Dirección de correo electrónico: mdario@organizacion*

*Comentario: Manolito*

*Frase contraseña: 19 de mayo de 1979*

## Trabajo Práctico #9 "Cifrado y firma digital con GnuPG"

Fecha de Entrega: 17/11/2016  
Medina, Ma. Victoria [117024]  
medina.vicc@gmail.com

En el archivo ~/.gnupg/secring.gpg se guardan las claves secretas.

En el archivo ~/.gnupg/pubring.gpg se guardan claves públicas.

Una clave pública se extrae en formato ASCII, para ser distribuida, con:

```
$ gpg --export -a dirección_correo_electrónico
```

Para importar una clave pública se utiliza:

```
$ gpg --import <archivo>
```

```
root@debian2:/home/victoriamedina# gpg --gen-key
gpg (GnuPG) 1.4.18; Copyright (C) 2014 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.
```

Seleccione el tipo de clave deseado:

- (1) DSA y ElGamal (por defecto)
- (2) DSA y ElGamal (por defecto)
- (3) DSA (sólo firmar)
- (4) RSA (sólo firmar)

¿Su elección? 1

las claves RSA pueden tener entre 1024 y 4096 bits de longitud.

¿De qué tamaño quiere la clave? (2048)

El tamaño requerido es de 2048 bits

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)?

La clave nunca caduca

¿Es correcto? (s/n) s

Necesita un identificador de usuario para identificar su clave. El programa construye el identificador de usuario a partir del Nombre Real, Comentario y Dirección

de Correo Electrónico de esta forma:

```
"Heinrich Heine (Der Dichter) <heinrichh@duesseldorf.de>"
```

Nombre y apellidos: Ester Piscoe

Dirección de correo electrónico: episcoe@organizacion

Comentario: Estercita

Ha seleccionado este identificador de usuario:

```
"Ester Piscoe (Estercita) <episcoe@organizacion>"
```

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

Necesita una contraseña para proteger su clave secreta.

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: /root/.gnupg/trustdb.gpg: se ha creado base de datos de confianza
gpg: clave BD7C147C marcada como de confianza absoluta
claves pública y secreta creadas y firmadas.
```

## Trabajo Práctico #9

# “Cifrado y firma digital con GnuPG”

Fecha de Entrega: 17/11/2016  
Medina, Ma. Victoria [117024]  
medina.vicc@gmail.com

```
gpg: comprobando base de datos de confianza
gpg: 3 dudosa(s) necesaria(s), 1 completa(s) necesaria(s),
modelo de confianza PGP
gpg: nivel: 0 validez: 1 firmada: 0 confianza: 0-, 0q, 0n, 0m, 0f, 1u
pub 2048R/BD7C147C 2016-11-12
    Huella de clave = B24B 1008 523A 4D3E BA1D AB5D 0254 F98E BD7C 147C
uid          Ester Pisco (Estercita) <episco@organizacion>
sub 2048R/9A4F14B5 2016-11-12
```

Visualizamos la clave pública:

```
root@debian2:/home/victoriamedina# gpg --export -a episco@organizacion
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1
```

```
mQENBFgnSBsBCAC4LhxiMSG4Prg7dIZwP/RzjnlkKQ5cJZ1WJ1sI8EcbQg58Gt7L
DwQHKHrFP+LOiUV5Con9xwD6mxbEJOLKLi8blSRIOkUJyDhIx/VC8GYc7DrNqH/
fEp2I8nt03iHb9ZhNPnyR9ky7hMCBZ4aY9p/EvBteUjRMgZYwkWfU95Bukg38u90
CgmbJSD0f5UxuAcgJgccuXroQ9QsZKNRp9vbYnt6ON3NKnBNL5y4Wqj0otFYAcDL
x3rtPbT0JONcvY0JaM/dmJIYKoKL8TxlojnJA0wOWfB3It3txUkh73NhglsbihUx
Tnn8Km8xoe80BOW2lJQ71kMsY1/MHTiDgb//ABEBAAG0MUVzdGVyIFBpc2NvcuUg
KEVzdGVyY2l0YSkgPGVwaXNjb3JlQG9yZ2FuaXphY2l0b3JlJATgEEwECACIFAlgn
SBsCGwMGcwKIBwMCBhUIAgkKCwQWAgMBAh4BAheAAAJEAJU+Y69fBR8AnUH+wTf
6BS43gW2r3gcMfOfB6ye5D/dbFWyGpY5OMRMilbcZL9TxpTNOSE5IrXGyoJ/e58
Qb5UZcvzBEpe0JwJHJphbkB7l22pqKxnefM5Ej15HFmJjiLY1frL3GbYAiPwPsDb
ppT4cXegGf7hOKMCNnxv+OE6pKuKXdrWJXYfUjaVbBeVMEDg4BFihRMk8o7P9omn
GIVgEPQCjxeB46N6k3q9R9wDF3nJuLdkq132996SyjbMPj5Vlbo0U1UEKEM+eCbR
hB4AkY7YbJkk6qATizjIWqCjntUVF9UQ6MoexJxx+wKZO9oINydes4wTxca0vMv
DH0UHjA4qdS+1Xde3Cu5AQ0EWCdIGwEIALubKY+9eXyZmN1EQR6OdgvF2+2D48NH
m90QTWOn7JVubjOahu478rTW8DDJP6L3f7F0i3QunpVn7oStaWJkchBKN7oJPOhe
+ZQPy4GYEI+utOEQz4FPlIu4z4Hbcf+rey/7a95860i348NHaxONVqV4dbmS9NC
FIT9MLAOHMD87ZRBN48PXNEg7Hkr2Kj+awlclJpEPgKgiKkPes0D7he6CNSZfq68
Qci7fX8RyaCEAEFuZjma4eHjmnYKaUzXxOs79curyUAUADg3Us000I66VXrQJfu1
ha6IV1Dzrxmfez9ENzSliuHB+WePkaORGAE1+disIKwBtpRBMM+ZW/cAEQEAAAYkB
HwQYAQIACQUCWCdIGwIbDAAKCRACVPmOvXwUfI0oCAC3d+oQiIEt1ZDwpJuuzYux
y1WbftT8aYre7T3nBTtee+dEhEe68zxiAtxsuH/LvGBtN5W9xpx8NJdDIAxzPRsw
/uhtsEEZWBZdEb03hF82mjEmH6Wf0u2Ac2GfdPAKswdArwXI3ZZCvMe1meFcM4/r
UHG8eY4bL1u0ggEifcYXNq4A4adG7h9URZgkkoIL1ZPUmn0DUeIgKL6jWOGGYPEi
ifpI92jDwqn3E9866QcY2v/daWjdPUvSSy+1R06p5myw8sfu1ISlcbLaym0TYRUQ
dZhgvOowFmDopeVvqCkKTYwDGGNS280bSBjNW049iPUoGqSm9mkdGakw5Gs7ZSsx
=bpUQ
-----END PGP PUBLIC KEY BLOCK-----
```

b) Cifrar un archivo:

Ahora para enviar un archivo cifrado a Ester Pisco:

```
$ gpg -r episco@organizacion -e archivo_a_encriptar
```

genera el archivo cifrado con extension gpg. Con -ea genera un archivo cifrado en ASCII  
(Para que pueda ser transmitido por email)

Creamos el archivo "archivoEncriptar" :

## Trabajo Práctico #9 “Cifrado y firma digital con GnuPG”

Fecha de Entrega: 17/11/2016  
Medina, Ma. Victoria [117024]  
medina.vicc@gmail.com

Ester Pisco que se caso con Garcia el Griego :)

```
root@debian2:/home/victoriamedina# nano archivoEncriptar
```

Lo enviamos a Ester Pisco:

```
root@debian2:/home/victoriamedina# gpg -r episcore@organizacion -e  
archivoEncriptar
```

c) Descifrar un archivo: Para descifrar un archivo cifrado utilizando clave pública:

```
$ gpg archivo_a_desencriptar
```

Solicitará la frase contraseña para acceder a la clave privada del recipiente.

```
root@debian2:/home/victoriamedina# gpg archivoEncriptar.gpg
```

```
Necesita una contraseña para desbloquear la clave secreta  
del usuario: "Ester Pisco (Estercita) <episcore@organizacion>"  
clave RSA de 2048 bits, ID 9A4F14B5, creada el 2016-11-12 (identificador de clave  
primaria BD7C147C)
```

```
gpg: cifrado con clave RSA de 2048 bits, ID 9A4F14B5, creada el 2016-11-12  
"Ester Pisco (Estercita) <episcore@organizacion>"  
El fichero `archivoEncriptar' ya existe. ¿Sobreescribir? (s/N) N  
Introduzca nuevo nombre de fichero: prueba
```

### Parte 3. Firma digital

Un archivo se FIRMA con: `$ gpg -u usuario_que_firma --clearsign <archivo>`  
para generar signatura que se anexa al mensaje en claro, o

```
$ gpg -u usuario_que_firma -s <archivo>
```

(-sa para utilizar ASCII de 7 bit) para generar una firma y comprimir el mensaje (con -u se indica quien lo firma).

Una vez que se firmó, se puede verificar si el archivo fue alterado posteriormente mediante el comando `$ gpg <archivo>`

Verifica la firma con la clave pública de quien firmó y genera un archivo en texto claro.

Se crea el archivo que será firmado:

```
root@viccm-C500:/home/viccm# nano arhiivoFirma
```

```
GNU nano 2.5.3 Archivo: arhiivoFirma  
  
este archivo será firmado por Victoria Medina :)  
  
Enjoy it..![]
```

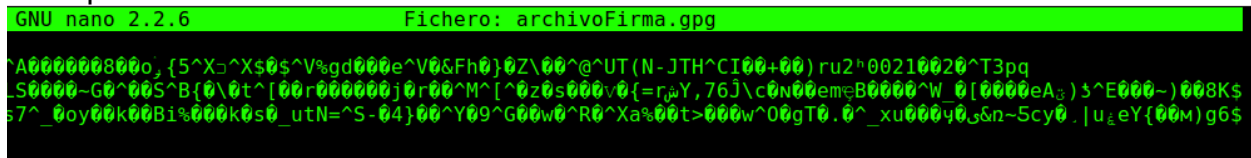
## Trabajo Práctico #9 "Cifrado y firma digital con GnuPG"

Fecha de Entrega: 17/11/2016  
Medina, Ma. Victoria [117024]  
medina.vicc@gmail.com

Se procede a firmar:

```
root@debian2:/home/victoriamedina# -u medina.vicc@gmail.com -s archivoFirma
Necesita una contraseña para desbloquear la clave secreta
del usuario: "Victoria Medina (Esta sera mi clave publica para el TP 8 de AyGR)
<medina.vicc@gmail.com>"
clave RSA de 2048 bits, ID ECDBBD28, creada el 2016-11-12
```

Una vez que se firmó el mensaje, se intenta visualizarlo sin la clave correspondiente:



```
GNU nano 2.2.6 Fichero: archivoFirma.gpg
^A000000800o,{5^X^X$0$^V%gd000e^V0&Fh0}0Z\00^@^UT(N-JTH^CI00+00)ru2^00210020^T3pq
LS0000~G0^00S^B{0\0t^[00r00000j0r00^M^[^0z0s000v0{=r,Y,76J\c0N00emeB0000^W_0[0000eA3}5^E000~)008K$
s7^_0oy00k00Bi%000k0s0_utN=^S-04}00^Y09^G00w0^R0^Xa%00t>000w^00gT0.0^_xu000y00&n-5cy0_|u_eY{00M)g6s
```

Verificamos de quien es la firma:

```
root@debian2:/home/victoriamedina# gpg archivoFirma.gpg
El fichero `archivoFirma' ya existe. ¿Sobreescribir? (s/N) s
gpg: Firmado el dom 13 nov 2016 17:32:41 ART usando clave RSA ID ECDBBD28
gpg: Firma correcta de "Victoria Medina (Esta sera mi clave publica para el TP 8
de AyGR) <medina.vicc@gmail.com>"
```

### Parte 4. Cifrado y firmado

Suponiendo que Manuel Darío desea enviar un mensaje a Ester (almacenado en el archivo a-ester.txt) que sólo ella pueda descifrar, y a su vez asegurar que el mensaje no sea modificado y sólo pueda haber sido generado por el mismo:

```
$ gpg -u mdario@organizacion -r episcore@organizacion -sea a-ester.txt
```

solicitará la contraseña para acceder a la clave privada de Manuel Darío.

Para descifrar y validar la firma \$ gpg a-ester.asc

solicitará la contraseña para acceder a la clave privada de Ester Piscore y así descifrar el mensaje y verificar la firma con la clave pública de Manuel Darío.

Creamos el archivo para Ester:

```
root@debian2:/home/victoriamedina# nano a-ester
```

```
root@debian2:/home/victoriamedina# gpg -u mdario@organizacion -r
episcore@organizacion -sea a-ester
```

```
Necesita una contraseña para desbloquear la clave secreta
del usuario: "Manuel Dario (Manolito) <mdario@organizacion>"
clave RSA de 2048 bits, ID E68C3E58, creada el 2016-11-12
```

Ciframos el archivo:

```
root@debian2:/home/victoriamedina# gpg a-ester.asc
```

```
Necesita una contraseña para desbloquear la clave secreta
del usuario: "Ester Piscore (Estercita) <episcore@organizacion>"
```

## Trabajo Práctico #9 "Cifrado y firma digital con GnuPG"

Fecha de Entrega: 17/11/2016  
Medina, Ma. Victoria [117024]  
medina.vicc@gmail.com

*clave RSA de 2048 bits, ID 9A4F14B5, creada el 2016-11-12 (identificador de clave primaria BD7C147C)*

*gpg: cifrado con clave RSA de 2048 bits, ID 9A4F14B5, creada el 2016-11-12  
"Ester Piscore (Estercita) <episcore@organizacion>"  
El fichero `a-ester' ya existe. ¿Sobreescribir? (s/N) N*

### Actividad a desarrollar

- Resuelva las consignas planteadas y realice los pasos necesarios para cifrar y firmar la resolución del presente trabajo de manera tal que sólo el docente sea capaz de descifrarlo, y a su vez asegurar que el mensaje mantenga la integridad y sólo pueda haber sido generado por Ud.
- Envíe el archivo cifrado y firmado, junto con su clave pública, por correo electrónico a la cuenta de correo [maurom@unlu.edu.ar](mailto:maurom@unlu.edu.ar)

```
root@debian2:/home/victoriamedina# gpg --import maurom_clave_publica.txt
gpg: clave 7AC5DE17: clave pública "Mauro A. Meloni (AyGR2016)
<maurom@unlu.edu.ar>" importada
gpg: Cantidad total procesada: 1
gpg:          importadas: 1 (RSA: 1)
root@debian2:/home/victoriamedina# nano medinatp8
root@debian2:/home/victoriamedina# gpg -u medina.vicc@gmail.com -r
maurom@unlu.edu.ar -sea medinatp8
```

*Necesita una contraseña para desbloquear la clave secreta  
del usuario: "Victoria Medina (Esta sera mi clave publica para el TP 8 de AyGR)  
<medina.vicc@gmail.com>"  
clave RSA de 2048 bits, ID ECDBBD28, creada el 2016-11-12*

*gpg: B0B57870: No hay seguridad de que esta clave pertenezca realmente  
al usuario que se nombra*

```
pub 2048R/B0B57870 2016-11-03 Mauro A. Meloni (AyGR2016) <maurom@unlu.edu.ar>
  Huella de clave primaria: A7CD 800B 29CA A3C6 C6D8 1F34 F592 5246 7AC5 DE17
  Huella de subclave: 721F DA4B 5069 225F 7D3B 6B0E 0DDC 3461 B0B5 7870
```

*No es seguro que la clave pertenezca a la persona que se nombra en el  
identificador de usuario. Si \*realmente\* sabe lo que está haciendo,  
puede contestar sí a la siguiente pregunta.*

*¿Usar esta clave de todas formas? (s/N) s*