

# Práctica de Criptografía

*Alejandro Abad*



## Ejercicio: Cifrado simétrico de un documento

Creo un documento y lo cifro:

```
perico@perico-virtual-machine: ~/Escritorio
perico@perico-virtual-machine:~$ cd Escritorio
perico@perico-virtual-machine:~/Escritorio$ nano archivo.txt
perico@perico-virtual-machine:~/Escritorio$ gpg -c archivo.txt
perico@perico-virtual-machine:~/Escritorio$
```

Le mando el documento a mi compañera Morgana y lo descifra:

```
perico@perico-virtual-machine:~/Escritorio$ gpg archivo.txt.gpg
gpg: /home/perico/.gnupg: directorio creado
gpg: creado un nuevo archivo de configuración '/home/perico/.gnupg/gpg.conf'
gpg: AVISO: las opciones en '/home/perico/.gnupg/gpg.conf' no están aún activas
en esta ejecución
gpg: anillo «/home/perico/.gnupg/secring.gpg» creado
gpg: anillo «/home/perico/.gnupg/pubring.gpg» creado
gpg: datos cifrados CAST5
gpg: cifrado con 1 frase contraseña
gpg: AVISO: la integridad del mensaje no está protegida
perico@perico-virtual-machine:~/Escritorio$
```

Lo ciframos con -a y le hacemos un cat al contenido:

```
gpg: no se han encontrados datos OpenPGP válidos
gpg: processing message failed: eof
perico@perico-virtual-machine:~/Escritorio$ gpg -c -a archivo.txt
perico@perico-virtual-machine:~/Escritorio$ cat archivo.txt.asc
-----BEGIN PGP MESSAGE-----
Version: GnuPG v1.4.11 (GNU/Linux)

jA0EAWMC5IB1HLDpPrxgyS6DWhdoTiTRzaU3uL44/gN+6BGXpiaCCAU98Mr+Ufs
dtdDx1wT1gzg6KKeTH4y
=16uP
-----END PGP MESSAGE-----
perico@perico-virtual-machine:~/Escritorio$
```

## Ejercicio: Cifrado simétrico de un documento

Creo mi clave pública y privada:

```
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 (predeterminado)
  (2) DSA y Elgamal
  (3) DSA (sólo firmar)
  (4) RSA (sólo firmar)
¿Su selección?: 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
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)? 30
La clave caduca jue 06 abr 2017 20:20:50 CEST
¿Es correcto? (s/n) s

Necesita un identificador de usuario para identificar su clave. El programa
construye el identificador a partir del Nombre Real, Comentario y Dirección
de Correo electrónico de esta forma:
    "Heinrich Heine (Der Dichter) <heinrichh@duesseldorf.de>"

Nombre y apellidos: Alejandro Adolf
Dirección de correo electrónico: heilhatler@gmail.com
Comentario: Hëil Hatler
Está usando el juego de caracteres 'utf-8'.
Ha seleccionado este ID de usuario:
    «Alejandro Adolf (Hëil Hatler) <heilhatler@gmail.com>»

¿Cambia (N)ombre, (C)omentario, (D)irección o (V)ale/(S)alir? v
Necesita una frase contraseña para proteger su clave secreta.

gpg: el agente gpg no esta disponible en esta sesión
```



## Ejercicio: Exportar e importar

Mi compañera Morgana me pasa su llave y la importo a mi llavero de claves:

```
-----  
pub 2048R/894B90F2 2017-03-07 [[caduca: 2017-04-06]]  
uid Adolf Hitler (Hëil) <adolfhitler@tercerreich.gr>  
pub 2048R/CFC658AE 2017-03-07 [[caduca: 2017-04-06]]  
  
pub 2048R/11858F63 2017-02-23 [[caduca: 2017-03-25]]  
uid Morgana Morales (hola) <morgana@correo.es>  
pub 2048R/93D4B9A1 2017-02-23 [[caduca: 2017-03-25]]  
  
usuario@xubuntu14:~/Escritorio$
```

## Ejercicio: Cifrado y descifrado de un documento

Cifro un archivo con la clave pública de Morgana:

```
usuario@xubuntu14:~/Escritorio$ gpg -aer morgana@correo.es kase.txt  
gpg: 93D4B9A1: No hay seguridad de que esta clave pertenezca realmente  
al usuario que se nombra  
  
pub 2048R/93D4B9A1 2017-02-23 Morgana Morales (hola) <morgana@correo.es>  
Huella de clave primaria: 5064 5AC4 4AF7 4E63 F9D7 88BB 3CA5 5D1E 1185 8F63  
Huella de subclave: F18A 8A32 9F3E 5225 A6AD 7B71 8B73 EBA6 93D4 B9A1  
  
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  
usuario@xubuntu14:~/Escritorio$ gpg -aer morgana@correo.es kase.txt
```

Morgana me pasa un archivo codificado con mi clave pública y lo descifro:

```
El archivo «kase.txt.asc» ya existe. ¿Sobreescribir? (s/N) s  
usuario@xubuntu14:~/Escritorio$ gpg encriptar.asc  
  
Necesita una contraseña para desbloquear la clave secreta  
del usuario: "Adolf Hitler (Hëil) <adolfhitler@tercerreich.gr>"  
clave RSA de 2048 bits, ID CFC658AE, creada el 2017-03-07 (identificador de clave  
primaria 894B90F2)  
  
gpg: cifrado con clave RSA de 2048 bits, ID CFC658AE, creada el 2017-03-07  
«Adolf Hitler (Hëil) <adolfhitler@tercerreich.gr>»  
usuario@xubuntu14:~/Escritorio$
```



## Ejercicio: Firma digital de un documento

Creo un archivo y lo firmo:

```
usuario@xubuntu14:~/Escritorio$ gpg -sb -a firmameloscojones
Necesita una contraseña para desbloquear la clave secreta
del usuario: "Adolf Hitler (Hëil) <adolfhitler@tercerreich.gr>"
clave RSA de 2048 bits, ID 894B90F2, creada el 2017-03-07
usuario@xubuntu14:~/Escritorio$
```

Morgana me pasa un archivo firmado por ella, compruebo la firma, y es correcta:

```
usuario@xubuntu14:~/Escritorio$ gpg morganamoraes.asc
gpg: Firmado el mar 07 mar 2017 20:42:33 CET usando clave RSA ID B922B1D3
gpg: Firma correcta de «Morgana Morales (hola) <morgana@correo.es>»
gpg: AVISO: ¡Esta clave no está certificada por una firma de confianza!
gpg: No hay indicios de que la firma pertenezca al propietario.
Huellas digitales de la clave primaria: 1569 9D00 B554 AA2F 0963 6941 7EF3 E76F
B922 B1D3
usuario@xubuntu14:~/Escritorio$
```

Modifico el archivo que me ha pasado firmado Morgana, y al volver a comprobar la firma me salta un error porque la integridad del archivo ya no es la misma:

```
usuario@xubuntu14:~/Escritorio$ gpg morganamoraes.asc
gpg: Firmado el mar 07 mar 2017 20:42:33 CET usando clave RSA ID B922B1D3
gpg: Firma INCORRECTA de «Morgana Morales (hola) <morgana@correo.es>»
usuario@xubuntu14:~/Escritorio$
```

