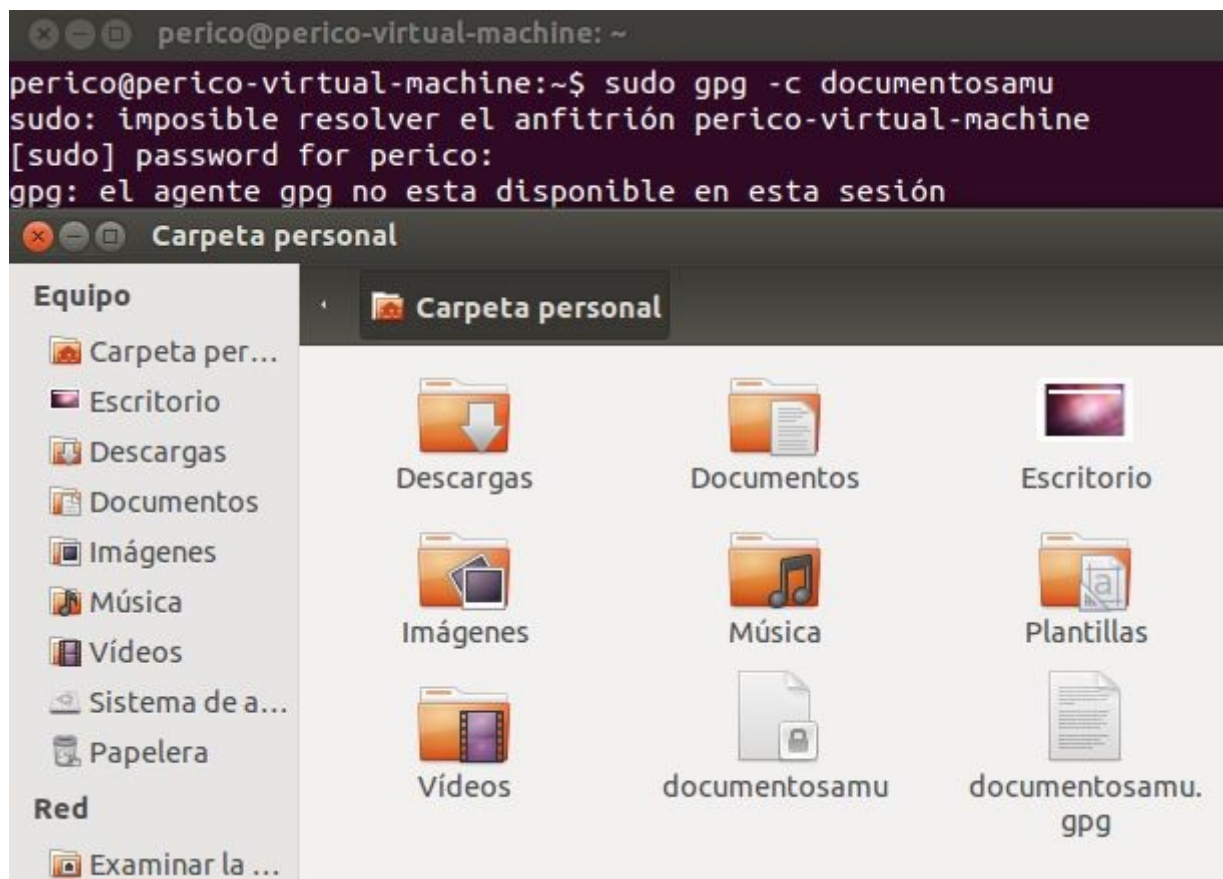
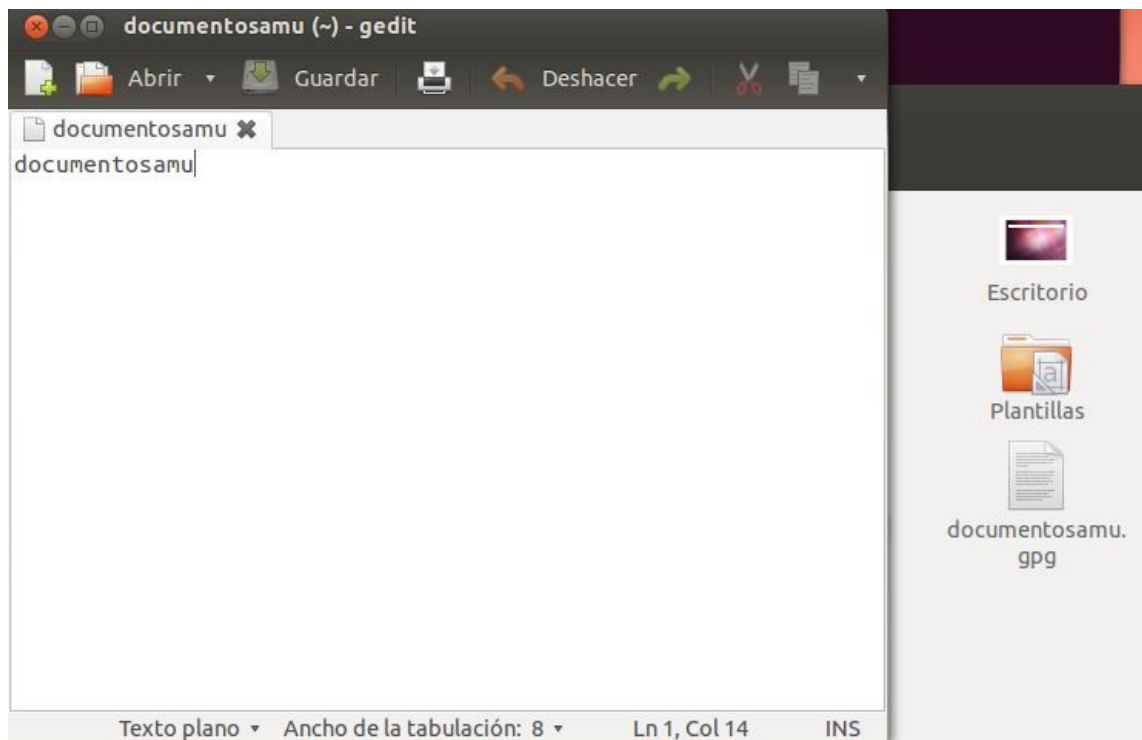


# TRABAJO DE ENCRYPTACIÓN

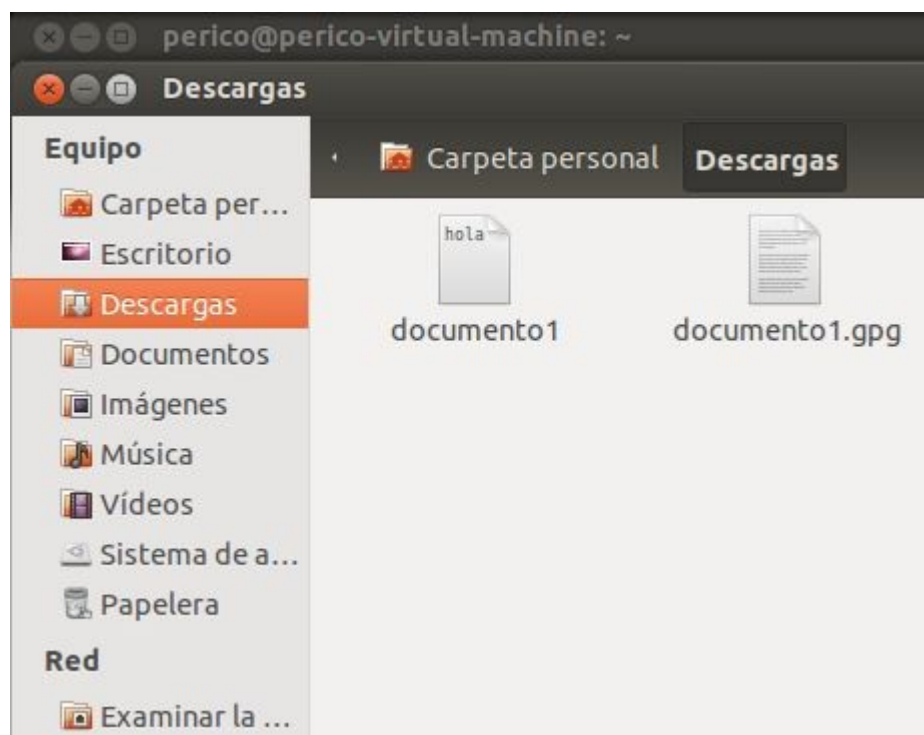
Autor: Samuel Matencio Prado  
Profesor: Javier Morcillo Marín

## CIFRADO SIMETRICO DE UN DOCUMENTO

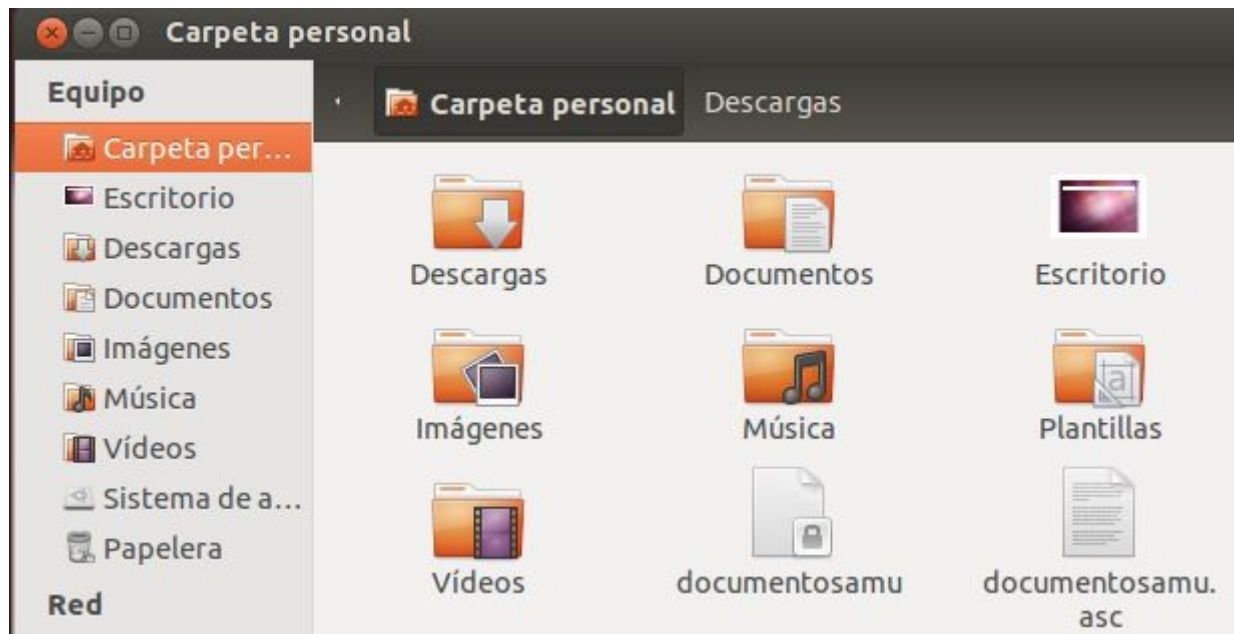




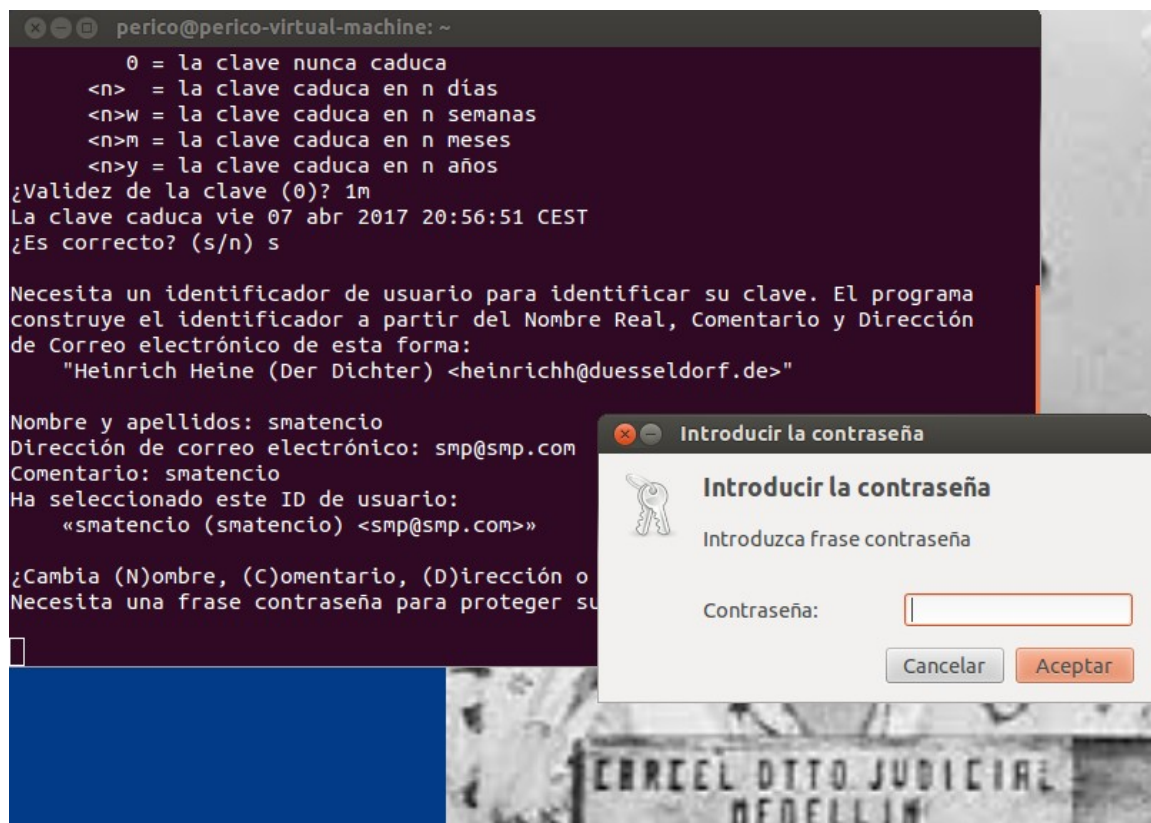
Documento cifrado y descifrado que me envió Jose por email.



Utilizando la opción -a .



## CREACIÓN CLAVE PUBLICA Y PRIVADA



```

No hay suficientes bytes aleatorios disponibles. Por favor, haga algún
otro trabajo para que el sistema pueda recolectar más entropía
(se necesitan 14 bytes más).
..+++++
gpg: clave 475B9E90 marcada como de confianza absoluta
claves pública y secreta creadas y firmadas.

gpg: comprobando base de datos de confianza
gpg: 3 dudosa(s) necesarias, 1 completa(s) necesarias,
modelo de confianza PGP
gpg: nivel: 0 validez: 3 firmada: 0 confianza: 0-, 0q, 0n, 0m, 0f, 3u
gpg: siguiente comprobación de base de datos de confianza el: 2017-04-07
pub 2048R/475B9E90 2017-03-08 [[caduca: 2017-04-07]]
    Huella de clave = E4F5 7794 B33D EBA7 55DE 2977 C05D E13A 475B 9E90
uid                               smatencio (smatencio) <smp@smp.com>
sub 2048R/E3DB33FC 2017-03-08 [[caduca: 2017-04-07]]

```

Exportar clave a ASCII

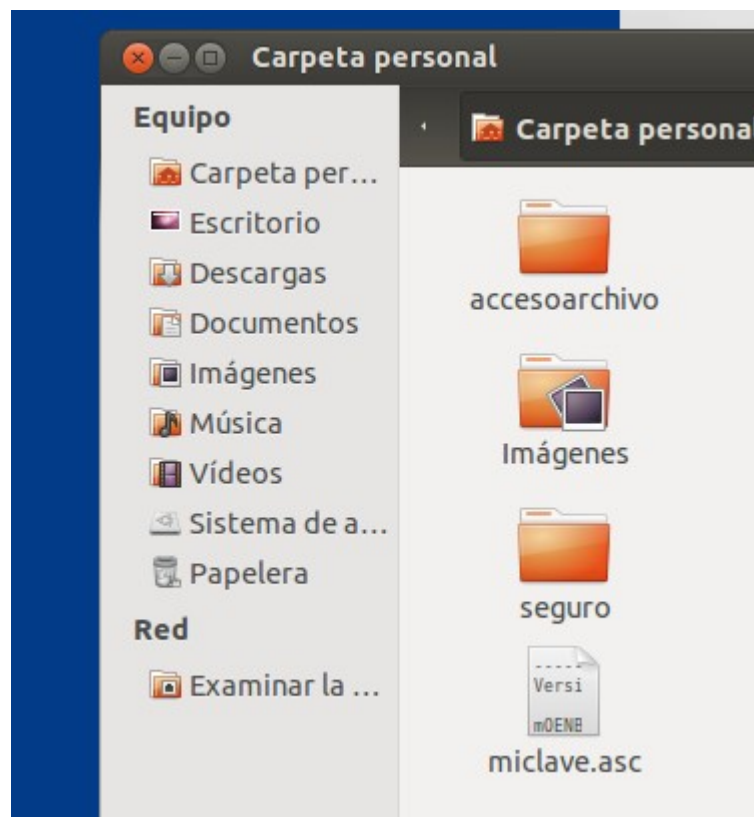
```

perico@perico-virtual-machine: ~
bnJexO+bcxQuDUZo0mnFJ8bFKVICd3DyL4Z6xAiwf0SjqqTodCEpNdIbrdHKu2ia
Lz32U09HcIeTe/W6K/wkXiGta6Z8R5z/oNuDABEBAAAG0I3NtYXRlbmNpbyAoc21h
dGVuY2lvKSA8c21wQHNTcC5jb20+iQE+BBMBAGAoBQJYwFTLAhsDBQkAJ40ABgsJ
CacDAgYVCAIJCgsEFgIDAQIeAQIXgAAKCRDAXeE6R1uekM5aB/wPfcNRG9+Qixyc
Z9Pq/srcjGfeUIbis0fTF0wSLmmBu3EDct/Ls1nzZ7MEX8ABLIWsdFLEGFdZeY9p
fWfLUYRMuZyA1Hsz5/dRJMvXBXT3kckxwzIr4WVY+ieIO8Fx0lg4naXy88EeuSyh
Vna4n94SKoqeXYG34TJZxzI/CqUZBw0gW1QnGrAOZAJUmAqw/JPtsom10ABhIJME
4nUIsT1ktv2LZuop4BqpzKacAu/+AojrYZ1BQBPIqXw9CxHEM6SJY5edPp+Ex7xx
ON2wGAEICAL20ZTgfdCT/4N/12uKAaDA/uNND9NEu/iK3XpPaAtF4XJVvEr8K302
Lu0a/xUpuQENBFjAVMsBCAC/gYX1VbSPb94E98x/mGi7itxmYUPJU0miV+v8+ei4
lqYnq9z32yXL9uPqPNDBYYKuLUV6qS2v353JtKpBSC/lBdagN2v8utZ/IKU1M2w9
OvmMRQIZe71JqVua84DdBae2zlwIsg08MEtFaqhAe1dhY2cM3hmpd440kNAzmnd7
tFatME0LMqiceL/EkyLriLmhPmMfbSgNyl+e+2J+CkVAE0KJYTLcMz2zRHRUMsb/
xzLSxN4yi0vOWvsdX24WCoIDJu54Y4kyKfsL8cxsTWKpfsXE0xJkg7JoozU0oexS
K9K7g6IovdBV6/LfJvP3GUT7qptDBW859jjyn+qpPcNxABEBAAAGJASUEGAECAAF
AljAVMsCGwwFCQAnjQAACgkQwF3h0kdbnpA1IQf+NyL1DofnLDto3fZ172sNu+y1
24ilC+50JeEcBXBB0GhL5lqm+CH9xXQV1IhZErmg2YFIFD5zij7b03+cQPlvBNUM
WlvG3ywhwvo9IxISB08TfgCIoM5jqcYKust2xigM4c4cwxd5DIF0DurXyKADeJA
OPNQ+mKrCsJpad3gR1wlvq27t09hGmQ8uMXCemzkPAw50/V8FHFADICrgdQsXEXI
6ddhi6JQ2nvZ5ZsPG/lFAiIiORIPr8Kmbf/AuUF2jA3r2RCpjkrX1JpTeglmddtt
G5+6udlIRduhxtetPTJwKMs0SRipLCUEnyKJAwjdCg/zxZEUoVv4q141MPTCVg==
-----END PGP PUBLIC KEY BLOCK-----

```



Guardar mi clave en ASCII



Importar clave

```
perico@perico-virtual-machine:~$ gpg --import miclave.asc
gpg: clave 475B9E90: «smatencio (smatencio) <smp@smp.com>» sin cambios
gpg: Cantidad total procesada: 1
gpg: sin cambios: 1
```

## Mi Keyring

```

pub 2048R/5A7995C9 2016-12-14
uid Samuel Matencio (toma torta) <caranchoa123@gmail.com>
sub 2048R/BD142F63 2016-12-14

pub 1024D/54AE28D6 2017-02-03
uid Samuel Matencio (eefgfdgfdgf) <sam9@pepe.com>
sub 1024g/AD2BFCEB 2017-02-03

pub 2048R/668B5152 2016-12-14
uid antonio soler (hola, buenos dias buen señor) <antonio@gmail
.COM>
sub 2048R/D3305603 2016-12-14

pub 1024D/DC0C20B5 2017-02-03
uid antonio soler (hola) <antonio@hotmail.com>
sub 1024g/E2CCDD3 2017-02-03

pub 2048R/475B9E90 2017-03-08 [[caduca: 2017-04-07]]
uid smatencio (smatencio) <smp@smp.com>
sub 2048R/E3DB33FC 2017-03-08 [[caduca: 2017-04-07]]

```

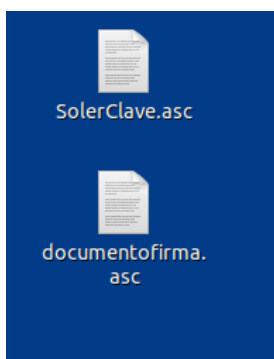
## CIFRADO SIMETRICO CON CLAVE PUBLICA.

```

perico@perico-virtual-machine: ~
perico@perico-virtual-machine:~$ gpg -aer smatencio miclave.asc
perico@perico-virtual-machine:~$ gpg miclave.asc
pub 2048R/475B9E90 2017-03-08 smatencio (smatencio) <smp@smp.com>
sub 2048R/E3DB33FC 2017-03-08 [[caduca: 2017-04-07]]
perico@perico-virtual-machine:~$

```

## Crear Firma



```

perico@perico-virtual-machine:~/Escritorio$ gpg -sb -a documentofirma
Necesita una frase contraseña para desbloquear la clave secreta
del usuario: "Samuel Matencio (toma torta) <caranchoa123@gmail.com>"
clave RSA de 2048 bits, ID 5A7995C9, creada el 2016-12-14

perico@perico-virtual-machine:~/Escritorio$

```

## Verificar Firma.

```

perico@perico-virtual-machine:~/Escritorio$ gpg documentofirma.asc
gpg: Firmado el mié 08 mar 2017 20:50:10 CET usando clave RSA ID 5A7995C9
gpg: Firma correcta de «Samuel Matencio (toma torta) <caranchoa123@gmail.com>»
perico@perico-virtual-machine:~/Escritorio$ gpg --verify documentofirma.asc
gpg: Firmado el mié 08 mar 2017 20:50:10 CET usando clave RSA ID 5A7995C9
gpg: Firma correcta de «Samuel Matencio (toma torta) <caranchoa123@gmail.com>»

```