Práctica de Criptografía

Morgana Morales Sagasta, 2º SMR G
IES Severo Ochoa, 2016/17

Cifrado simétrico

Creo un archivo y lo cifro con una contraseña

```
perico@perico-virtual-machine:~/Escritorio$ nano archivo.txt
perico@perico-virtual-machine:~/Escritorio$ gpg -c archivo.txt
perico@perico-virtual-machine:~/Escritorio$ gpg ejemplo.gpg
gpg: datos cifrados CAST5
gpg: cifrado con 1 frase contraseña
gpg: AVISO: la integridad del mensaje no está protegida
perico@perico-virtual-machine:~/Escritorio$
```

Alejandro me pasa su archivo y yo lo descifro con la clave

```
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$
```

Hicimos -a y se creó el archivo y al hacer cat nos lo muestra

```
perico@perico-virtual-machine:~/Escritorio$ cat ejemplo.asc
-----BEGIN PGP MESSAGE-----
Version: GnuPG v1.4.11 (GNU/Linux)

jA0EAwMCpIhG9t/Gv3RgySiworS04+QKVQcsJLGJSz7PDEVeaB4ORx4I6MpLwemc
DHzP11gDooaa
=5xye
-----END PGP MESSAGE-----
perico@perico-virtual-machine:~/Escritorio$
```

Creación de la pareja de claves pública-privada

Creamos una clave con las siguientes opciones:

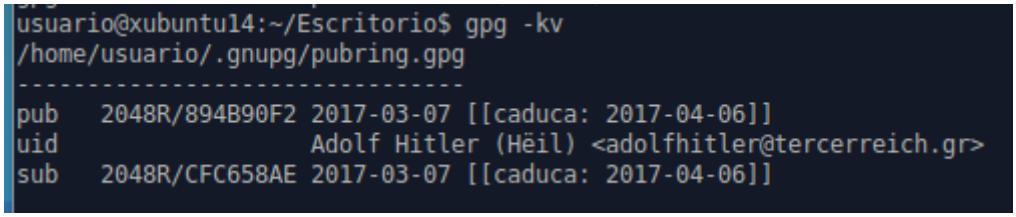
```
perico@perico-virtual-machine:~$ gpg --gen-key
gpg (GnuPG) 1.4.11; Copyright (C) 2010 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Por favor seleccione tipo de clave deseado:
   (1) RSA y RSA (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 sáb 25 mar 2017 02:10:37 CET
¿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: Morgana Morales
Dirección de correo electrónico: morgana@correo.es
Comentario: hola
Ha seleccionado este ID de usuario:
    «Morgana Morales (hola) <morgana@correo.es>»
```

Ejecutamos -kv para ver que se ha creado

```
gpg: comprobando base de datos de confianza
gpg: 3 dudosa(s) necesarias, 1 completa(s) necesarias,
modelo de confianza 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: 2017-03-25
pub   2048R/11858F63 2017-02-23 [[caduca: 2017-03-25]]
      Huella de clave = 5064 5AC4 4AF7 4E63 F9D7  88BB 3CA5 5D1E 1185 8F63
uid                  Morgana Morales (hola) <morgana@correo.es>
sub   2048R/93D4B9A1 2017-02-23 [[caduca: 2017-03-25]]
```

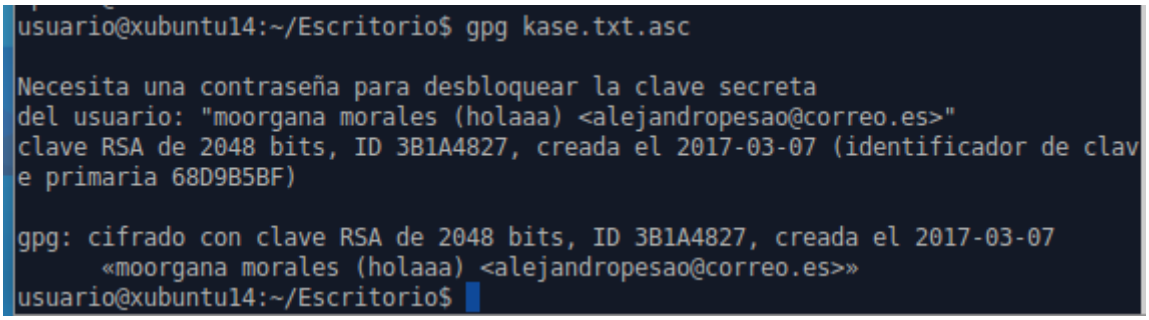
Importar y exportar claves públicas

Alejandro me pasa su clave y la importo a mi ordenador y al hacer -kv me aparece su clave.



Cifrado asimétrico con claves públicas

Cifro un archivo con la clave pública de Alejandro y se lo paso y el lo descifra con su clave.



Firma digital de un documento

Creo otro archivo y lo firmo con mi clave publica. Alejandro me pasa su archivo y al comprobar su firma es correcta. Por último modifico su archivo y al intentar abrirlo da error.