

|  |  |
| --- | --- |
| **SEGURIDAD INFORMÁTICA** – 2º SMR | |
| UT5: Sistemas de identificación. Criptografía. | Práctica 2: Cifrado asimétrico. |
| Nombre: | |
| Nota: | Observaciones: |

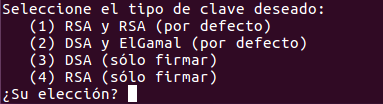
**Creación de una pareja de claves pública-privada.**

Recuerda que los algoritmos de cifrado asimétrico manejan dos claves, una para cifrar y otra para descifrar el mensaje. Cada interlocutor deberá disponer de una pareja de claves, siempre que queramos asegurar confidencialidad.

* 1. Investiga la opción de gpg (en Ubuntu) para generar parejas de claves.



* 1. Ejecuta el comando gpg con esa opción:
     1. ¿Qué algoritmos ofrece para elegir? ¿Qué clase de algoritmos son? Enumera un par de algoritmos del tipo contrario.



* + 1. Elige la opción que utilice RSA y que NO sea:





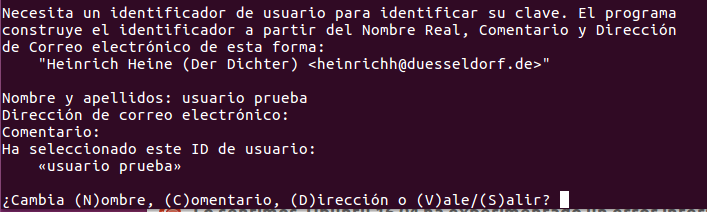
* + 1. Vamos a manejar claves de 2048 bits.



* + 1. Elegimos que la clave caduque en un mes.

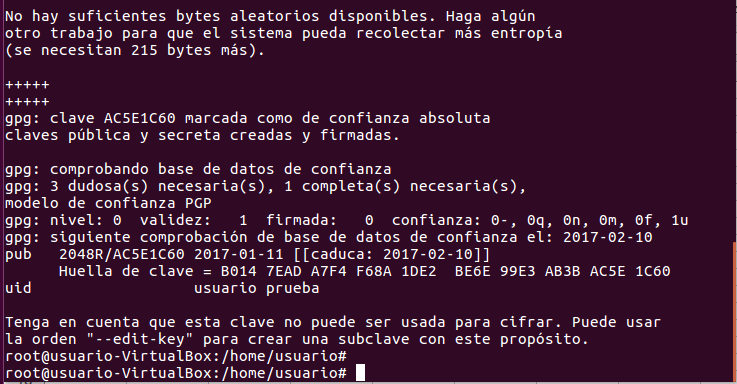


* + 1. Rellena los campos requeridos para generar un identificador de la clave.



No hay límite en la longitud de la “passphrase” y debe ser cuidadosamente elegida. Desde el punto de vista de la seguridad, la “passphrase” que desbloqua la clave privada es uno de los puntos más débiles de GPG ya que es la única protección que tienes si otra persona obtiene tu clave privada. Idealmente la “passphrase” no debe incluir palabras del diccionario y debe mezclar caracteres alfabéticos y no alfabéticos. Una buena “passphrase” es crucial para la seguridad del GPG.

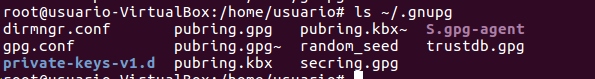
<http://www.gnupg.org/gph/es/manual.html>

* + 1. Piensa una frase para rellenar el siguiente campo. ***Anota esta frase aquí ( esto es por seguridad, para poder realizar más prácticas otros días y tengas un lugar dónde esté apuntado), pues será la que necesites para desbloquear tu clave privada.***
    2. Sigue las indicaciones de la herramienta tras completar el paso anterior.
    3. Anota el identificador de clave que te muestre la línea: 

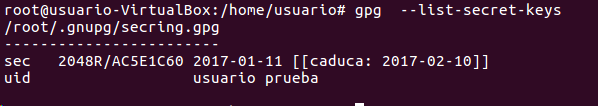
**gpg: key 0614C168 marked as ultimately trusted**

**En este ejemplo el id de la clave sería: 0614C168.**

* 1. Observa el contenido del directorio ~/.gnupg. Ahí aparecen los archivos secring.pgp y pubring.gpg. El primero almacena las claves privadas y el segundo las públicas. Muestra que se han creado.



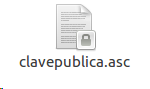
* 1. ¿Cómo puedes ver las claves privadas? ¿Cómo se podrían borrar?



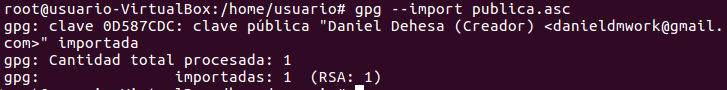
* 1. Ahora investiga la opción que has de añadir al comando gpg para exportar la clave pública. Esto te va a permitir visualizar la clave pública generada que deberás pasar a las personas que quieran establecer una conexión confidencial contigo.



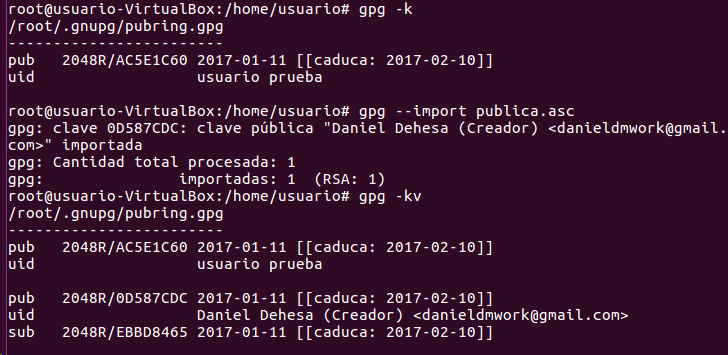
* 1. Almacena en un archivo con extensión .asc la clave obtenida (aparece en código ASCII la clave que has generado). Incluye dicho archivo en el correo que me envías con la práctica.



* 1. Envía ese archivo a varios compañeros. Al mismo tiempo tu deberás de recibir varios ficheros con claves públicas.
  2. Ahora importa las claves públicas recibidas, es decir, ejecuta el comando gpg con al opción adecuada para añadir la clave pública de tu compañero a tu keyring (anillo de claves) que es como GPG llama al lugar dónde se añaden todas las claves públicas que poseerás.



* 1. Ejecuta el comando gpg –kv. ¿Qué te permite visualizar este comando?



* 1. Por último, ejecuta el comando

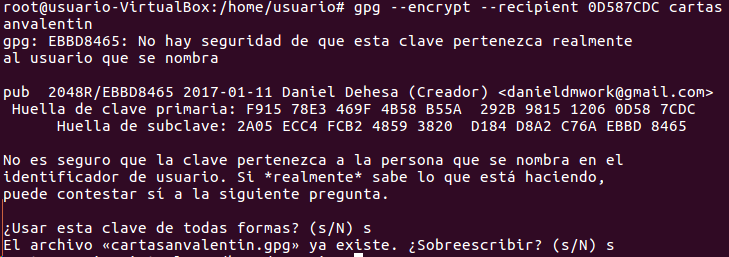
gpg –a –r identificador\_del\_destino –r identificador\_del\_destino --encrypt documento

*-r* especifica el identificador del destinatario, es el nombre que aparece antes del id entre < >. Se puede repetir tantas veces como destinatarios para los cuales quieras encriptar el documento

*--encrypt* indica que queremos encriptar

*documento* será el nombre del documento a encriptar,

**es decir, queremos encriptar documento con la clave pública especificada.** Lo que acabas de hacer es encriptar documento con la clave pública del usuario destinatario.

****

* 1. Envía documentos a usuarios válidos e inválidos, con el fin de que sólo el usuario cuya clave pública has usado y no otro sea capaz de descifrarlo.
  2. Averigua cual es el comando para descifrar los archivos que recibes.
  3. Confirma con tu compañero que ha sido capaz de descifrarlo. Mientras tú has de confirmar que eres capaz de descifrar el mensaje que alguien ha cifrado para ti, y en cambio no eres capaz de descifrar otro que no esté cifrado con tu clave pública.
  4. Hasta este punto, explica por qué tenemos o no tenemos:
* Confidencialidad
* Integridad
* Autenticación
* No repudio
  1. Justifica qué sería necesario para garantizar aquellas características que ahora no tenemos.
  2. ¿Cómo podrías obtener lo que falta?
  3. Para distribuir las claves, es mucho más habitual utilizar un servidor que distribuirlas por correo u otros medios. De esa manera los clientes podrán conectarse al servidor y descargar las claves públicas que necesiten y así añadirlas a su anillo de confianza.
     1. Genera la clave que revoca tu clave pública en caso de que haya problemas.
     2. Exporta tu clave pública al servidor pgp.rediris.es. NOTA: si no funciona rediris, lo puedes hacer en la web del MIT, http://pgp.mit.edu/
     3. Borra las claves públicas que hayas importando anteriormente y ahora impórtala de rediris.

Links:

<http://lamiradadelreplicante.com/2012/10/25/como-exportar-e-importar-las-claves-en-gnupg/>

https://www.genbetadev.com/seguridad-informatica/manual-de-gpg-cifra-y-envia-datos-de-forma-segura