Taller de Seguridad Informática –WALC 2016

PRÁCTICA DE LABORATORIO

Criptografía Asimétrica

Prof. Reinaldo Mayol. V. 16.9

## Entorno de la práctica:

1. Se utilizarán dos shells. En uno de ellos se utilizar al usuario root y en otro al usuario ubuntu
2. Durante la ejecución de la práctica se crearán las llaves correspondientes a cada uno de los usuarios mencionados.
3. En letra negrita encontrará el comando que debe introducir. En cursivas encontrará las salidas de cada comando.
4. Es MUY importante que ud. sepa en cada caso con que usuario esté trabajando.

# PRIMERA PARTE (USUARIO ROOT)

1. UTILIZANDO AL USUARIO root.

1.1 Cree las claves (privada y pública) .

**$ gpg --gen-key**

*gpg (GnuPG) 1.2.5; Copyright (C) 2004 Free Software Foundation, Inc.*

*This program comes with ABSOLUTELY NO WARRANTY.*

*This is free software, and you are welcome to redistribute it*

*under certain conditions. See the file COPYING for details.*

*Please select what kind of key you want:*

*(1) DSA and ElGamal (default)*

*(2) DSA (sign only)*

*(4) RSA (sign only)*

*Your selection? 1* ***<----------------------------------SU RESPUESTA***

*DSA keypair will have 1024 bits.*

*About to generate a new ELG-E keypair.*

*minimum keysize is 768 bits*

*default keysize is 1024 bits*

*highest suggested keysize is 2048 bits*

*What keysize do you want? (1024) 2048****<----------------------------------SU RESPUESTA***

*Requested keysize is 2048 bits*

*Please specify how long the key should be valid.*

*0 = key does not expire*

*<n> = key expires in n days*

*<n>w = key expires in n weeks*

*<n>m = key expires in n months*

*<n>y = key expires in n years*

*Key is valid for? (0) 0****<----------------------------------SU RESPUESTA***

*Key does not expire at all*

*Is this correct (y/n)? y****<----------------------------------SU RESPUESTA***

*You need a User-ID to identify your key; the software constructs the user id*

*from Real Name, Comment and Email Address in this form:*

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

*Real name: elroot****<----------------------------------SU RESPUESTA***

*Email address: root@eslared****<----------------------------------SU RESPUESTA***

*Comment:*

*You selected this USER-ID:*

*"elroot <root@eslared>"*

*Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit? o****<----------------------------------SU RESPUESTA***

*You need a Passphrase to protect your secret key.* ***<-----------------SU CONTRASENA***

*We need to generate a lot of random bytes. It is a good idea to perform*

*some other action (type on the keyboard, move the mouse, utilize the*

*disks) during the prime generation; this gives the random number*

*generator a better chance to gain enough entropy.*

*++++++++++++++++++++..++++++++++++++++++++++++++++++.+++++++++++++++++++++++++++++++++++++++++++++++++++++++..++++++++++++++++++++.+++++>++++++++++........+++++*

*We need to generate a lot of random bytes. It is a good idea to perform*

*some other action (type on the keyboard, move the mouse, utilize the*

*disks) during the prime generation; this gives the random number*

*generator a better chance to gain enough entropy.*

*.+++++++++++++++++++++++++..++++++++++++++++++++.+++++++++++++++..++++++++++.+++++.++++++++++++++++++++++++++++++....+++++...+++++++++++++++++++++++++++++++++++>+++++..+++++>+++++......+++++^^^*

***public and secret key created and signed.***

***key marked as ultimately trusted.***

***pub 1024D/8C236030 2005-07-16 elroot <root@eslared>***

***Key fingerprint = EF82 DCCA 107A DF51 D2F3 4133 71F0 B709 8C23 6030***

***sub 2048g/188BED03 2005-07-16***

* 1. Verifique ahora la localización de sus nuevas claves

**$ cd .gnupg/**

**$ ls**

*gpg.conf pubring.gpg pubring.gpg~ random\_seed secring.gpg trustdb.gpg*

* 1. Utilizando la intuición, o con ayuda del instructor identifique cada archivo.
  2. Regrese nuevamente al subdirectorio hogar del usuario

$ **cd**

2. Cree un archivo e introduzca una frase cualquiera en el mismo.

**$ touch elarchivo\_del\_root <------CAMBIE EL NOMBRE POR EL QUE DESEE**

$ **echo "una frase" > elarchivo\_del\_root**

$ **more elarchivo\_del\_root**

una frase

1. Firme el archivo que ha creado. Recuerde con que llave debe firmarse un archivo.

**$ gpg --clearsign elarchivo\_del\_root**

*You need a passphrase to unlock the secret key for*

*user: "elroot <root@eslared>"*

*1024-bit DSA key, ID 0A2C8D64, created 2005-07-16*

*Enter passphrase:* ***<-------------------------INTRODUZCA AQUI LA contraseña DE SU LLAVE***

* 1. Note que se ha creado un archivo de extensión .asc. Este es el archivo firmado.
  2. Muestre el contendido del archivo firmado e identifique cada parte del mismo.

**$ more elarchivo\_del\_root.asc**

*-----BEGIN PGP SIGNED MESSAGE-----*

*Hash: SHA1*

*una frase* ***<----------------EL TEXTO DEL ARCHIVO***

***EL HASH CIFRADO CON LA Kp DEL ROOT***

*-----BEGIN PGP SIGNATURE-----*

*Version: GnuPG v1.2.5 (GNU/Linux)*

*iD8DBQFC2UWb3RXnxAosjWQRAq2OAJ9/u0qSYrFN77ieoKTjSDDI9dqHxgCfYmjH*

*9N1r0E+Mi5egf4fH4YFsozc=*

*=vmGr*

*-----END PGP SIGNATURE-----*

* + 1. Modifique, utilizando un editor de texto, el archivo firmado.
    2. Verifique la firma del mensaje.

**$ gpg --verify elarchivo\_del\_root.asc**

* + 1. Explique y comente los resultados.
    2. Cifre el archivo original.

**$ gpg -e elarchivo\_del\_root**

*You need a passphrase to unlock the secret key for*

*user: "elroot <root@eslared>"*

*1024-bit DSA key, ID 0A2C8D64, created 2005-07-16*

*Enter passphrase:* ***<--------------INTRODUZCA AQUI LA contraseña DE SU LLAVE***

*You did not specify a user ID. (you may use "-r")*

*Enter the user ID. End with an empty line: <---****INTRODUZCA AQUI EL USERID DEL USUARIO DE DESTINO.***

1. Muestre el contendido del archivo cifrado e identifique cada parte del mismo.

**$ more elarchivo\_del\_root.gpg**

l?*gSo=^VV00sWk{J[ h!97{*

*+@j:GT)E)frZHzuxT4(LSFm$f.Ffsq^ysE7(zA[z>.O/ùln-0*

*Lc\_AC\*,>rDEzHJY?-\q/VN$a+0bt*

*CyP~e\_KC<?vn3<@0h?Cw }39: |I,LW/"LXQm{bW/{z{,$kiBO(e}10Z` f*

*Lv#|u'U$6!6Z*

*%L8t'VP7gldE\CFIySDl`!*

* + 1. Firme siguiendo el procedimiento descrito en el paso 3 de esta parte de la práctica el archivo cifrado obtenido en el paso anterior (paso 11)
    2. Muestre nuevamente el contenido del archivo firmado y cifrado ( extensiones .gpg.asc) e identifique cada parte del mismo.

**$more elarchivo\_del\_root.gpg.asc**

-*----BEGIN PGP SIGNED MESSAGE-----*

*Hash: SHA1*

*l?gSo=^VV00sWk{J[ h!97{*

*+@j:GT)E)frZHzuxT4(LSFm$f.Ffsq^ysE7(zA[z>.O/ùln-0*

*Lc\_AC\*,>rDEzHJY?-\q/VN$a+0bt*

*CyP~e\_KC<?vn3<@0h?Cw }39: |I,LW/"LXQm{bW/{z{,$kiBO(e}10Z` f*

*Lv#|u'U$6!6Z*

*%L8t'VP7gldE\CFIySDl`!7*

*-----BEGIN PGP SIGNATURE-----*

*Version: GnuPG v1.2.5 (GNU/Linux)*

*iD8DBQFC2Ylf3RXnxAosjWQRAgjOAJ9HuNpcm7dHS5s/VJ8hRDEMcIcsJwCfQVhB*

*N11JQV6f+ANDobyEGF7nNW4=*

*=OUWi*

*-----END PGP SIGNATURE-----*

1. Cree un archivo con nombre uno.txt. Introduzca cualquier texto en el archivo.



1. Ahora crearemos el hash de este archivo. **Copie el resultado**



1. Haga una copia del archivo uno.txt y llámelo dos.txt
2. Verifique, repitiendo el paso 13, que los hash son idénticos
3. Ahora modifique un **único bit** del archivo dos.txt. Para esto utilizaremos un editor hexadecimal. En esta práctica proponemos hexedit. ( si no se encuentra disponible puede instalarlo con #sudo apt-get install hexedit). NO REALICE NINGUN CAMBIO EN EL ARCHIVO UNO.TXT





1. Salve el archive (Crt-X o F2 si utiliza hexedit).
2. Verifique los hash de los archivos uno,txt y dos.txt ¿Son iguales? ¿Por qué?

# SEGUNDA PARTE (USUARIO ubuntu)

1. UTILIZANDO AL USUARIO Ubuntu repita el paso 1 de la primera parte. De esta forma habrá generado las llaves para el usuario Ubuntu.

IMPORTANTE: Utilice una nueva clave, un nuevo userID,etc... que diferencien esta clave de la creada anteriormente.

# TERCERA PARTE (USUARIOS ROOT y Ubuntu)

1. UTILIZANDO AL USUARIO root copie hacia el subdirectorio personal del usuario Ubuntu el archivo cifrado y firmado que creó en la primera parte.
2. UTILIZANDO AHORA AL USUARIO Ubuntu y verifique nuevamente la firma del archivo copiado. (Por favor antes de hacer este paso verifique los permisos del archivo copiado)

**# gpg --verify elarchivo\_del\_root.gpg.asc**

gpg: keyring `/root/.gnupg/pubring.gpg' created

gpg: Signature made sáb 16 jul 2005 18:25:35 VET using DSA key ID 0A2C8D64

gpg: Can't check signature: public key not found **<-------ERROR**

1. Comente la causa del error
2. UTILIZANDO AHORA AL USUARIO root exporte las llaves públicas de su llavero. Recuerde donde crea el archivo con las llaves exportadas y como lo llama.

$**gpg --export -o llavesexportadas**

1. Comente con el instructor por qué realizar esta operación.

# CUARTA PARTE (USUARIO UBUNTU)

1. UTILIZANDO AL USUARIO Ubuntu importe la llave publica del usuario root hacia el llavero del usuario Ubuntu. Tenga en cuenta la localización de las llaves de cada usuario y los permisos de las mismas.

**$gpg --fast-import /root/llavesexportadas**

*gpg: key 0A2C8D64: public key "elroot <root@eslared>" imported*

*gpg: Total number processed: 1*

*gpg: imported: 1*

1. Liste el contenido del llavero del usuario

**# gpg --list-public-keys**

*/root/.gnupg/pubring.gpg*

*------------------------*

*pub 1024D/0A2C8D64 2005-07-16 elroot <root@eslared>*

LLAVE PUBLICA DE ROOT

*sub 2048g/E21953A7 2005-07-16*

*pub 1024D/F3D6831E 2005-07-16 Ubuntu <Ubuntu@eslared>*

LLAVE PUBLICA DE UBUNTU

*sub 2048g/62A4AE69 2005-07-16*

1. Repita nuevamente el paso 2 de la tercera parte

$**gpg --verify elarchivo\_del\_root.gpg.asc**

*gpg: Signature made sáb 16 jul 2005 18:25:35 VET using DSA key ID 0A2C8D64*

*gpg: Good signature from "elroot <root@eslared>"*

*gpg: checking the trustdb*

*gpg: checking at depth 0 signed=0 ot(-/q/n/m/f/u)=0/0/0/0/0/1*

*gpg: WARNING: This key is not certified with a trusted signature!*

*gpg: There is no indication that the signature belongs to the owner.*

*Primary key fingerprint: E469 DA56 CB8B 4D56 3C41 4F05 DD15 E7C4 0A2C 8D64*

1. Comente ahora los resultados. Note el mensaje de alerta (WARNING) al final del paso anterior. Comente con el instructor su implicación.
2. Cambie el nivel de confianza de la clave del usuario root dentro del llavero del usuario Ubuntu

**$gpg --edit-key elroot <--CAMBIE elroot por el USERID DEL USUARIO ROOT QUE UD. ELIGIO**

*gpg (GnuPG) 1.2.5; Copyright (C) 2004 Free Software Foundation, Inc.*

*This program comes with ABSOLUTELY NO WARRANTY.*

*This is free software, and you are welcome to redistribute it*

*under certain conditions. See the file COPYING for details.*

*pub 1024D/0A2C8D64 created: 2005-07-16 expires: never trust: u/u*

*sub 2048g/E21953A7 created: 2005-07-16 expires: never*

*(1). elroot <root@eslared>*

*Command> trust* ***<----------------OPCION PARA CAMBIAR EL NIVEL DE CONFIANZA***

*pub 1024D/0A2C8D64 created: 2005-07-16 expires: never trust: u/u*

*sub 2048g/E21953A7 created: 2005-07-16 expires: never*

*(1). elroot <root@eslared>*

*Please decide how far you trust this user to correctly*

*verify other users' keys (by looking at passports,*

*checking fingerprints from different sources...)?*

*1 = Don't know*

*2 = I do NOT trust*

*3 = I trust marginally*

*4 = I trust fully*

*5 = I trust ultimately*

*m = back to the main menu*

*Your decision? 5* ***<---------------INTRUDUZCA EL NIVEL DE CONFIANZA***

*Do you really want to set this key to ultimate trust? y* ***<---- CONFIRME***

*pub 1024D/0A2C8D64 created: 2005-07-16 expires: never trust: u/u*

*sub 2048g/E21953A7 created: 2005-07-16 expires: never*

1. *elroot <*[root@eslared](mailto:root@eslared)*>*

*Command> q* ***<---SALIDA***

1. Repita nuevamente el paso 2 de la tercera parte

$**gpg --verify elarchivo\_del\_root.gpg.asc**

*gpg --verify /home/mayol/elarchivo\_del\_root.gpg.asc*

*gpg: Signature made sáb 16 jul 2005 18:25:35 VET using DSA key ID 0A2C8D64*

*gpg: Good signature from "elroot <*[root@eslared](mailto:root@eslared)*>"*

1. Comente ahora los resultados. Note que ha desaparecido el mensaje de advertencia.

# QUINTA PARTE (USUARIO ROOT)

1. UTILIZANDO AL USUARIO root liste las llaves que contiene el llavero. Note que solo contiene una llave publica.

**$ gpg --list-key**

*/home/test/.gnupg/pubring.gpg*

*-----------------------------*

*pub 1024D/0A2C8D64 2005-07-16 elroot <root@eslared>*

*sub 2048g/E21953A7 2005-07-16*

1. Cifre un archivo para enviarlo al usuario Ubuntu

**$ gpg -e elarchivo\_del\_root**

*You did not specify a user ID. (you may use "-r")*

*Enter the user ID. End with an empty line: Ubuntu*

*No such user ID.* ***<-----ERROR***

1. Comente con el instructor la causa del error.
2. Que acciones necesita realizar para poder cifrar un mensaje cuyo destino sea otro usuario?

# ULTIMA PARTE

1. Con la información y los conocimientos que ha adquirido trate de llenar la tabla siguiente. Marque aquellas casillas que puedan obtenerse con las funciones que se mencionan en cada caso. Tome como ejemplo la primera fila.

|  | Confidencialidad | Integridad | Autenticidad |
| --- | --- | --- | --- |
| Mensaje Cifrado | SI | NO | Solo si se puede garantizar que solo el receptor correcto conoce la clave correcta |
| Mensaje Plano |  |  |  |
| Mensaje Cifrado + HASH Plano |  |  |  |
| Mensaje Cifrado + Firma |  |  |  |
| Mensaje Plano + Firma |  |  |  |

2. ¿Su respuesta sería la misma si nos refiriésemos solo a criptografía de clave simétrica? ¿Por qué?