Universidad Nacional de Luján
Departamento de Ciencias Básicas
Teleinformática y Redes

Trabajo práctico de laboratorio #6 - 2006
Práctica guiada
Encriptación y firma digital con GPG

1) Criptografía convencional (simétrica)

a) *Encriptar un archivo*:

gpg -c <archivo>

pide la clave para encriptar y genera archivo.gpg.

Por defecto se realizará el cifrado utilizando CAST5. Par utilizar otro método:

gpg -c –cipher-algo nombre_algoritmo <archivo>

(Para conocer los algoritmos soportados invocar gpg –version)

El siguiente ejemplo utiliza AES como método de cifrado:

gpg -c --cipher-algo AES <archivo>

b) *Desencriptar archivo*:

gpg <archivo.gpg>

Solicitará la clave y desencripta el archivo, guardando el resultado en un nuevo archivo con el mismo nombre sin extensión.

2) Criptografía de clave pública

a) *Administración de claves*:

Primero debe generarse el par de clave publica y privada con:

gpg –gen-key

Tipo de clave: (1) DSA y ElGamal (por defecto)
Tamaño de clave: 1024 bits
Validez de la clave: 0 (sin expiración)
Nombre y apellidos: Ester Piscore
Dirección de correo electrónico: episcore@organizacion
Comentario: Estercita
Frase contraseña: 12 de marzo de 1976
(esta contraseña es para proteger la clave secreta. Se requerirá para firmar o encriptar algo)

Generar otro par de claves con los siguientes datos:

Nombre y apellidos: Manuel Dario
Dirección de correo electrónico: mdario@organizacion
Comentario: Manolito
Frase contraseña: 19 de mayo de 1979

En el archivo ~/.gnupg/secring.gpg se guardan las claves secretas
En el archivo ~/.gnupg/pubring.gpg se guardan claves públicas

Una clave pública se extrae en formato ASCII, para ser distribuida, con:

gpg –export -a dirección_correo_electrónico

Para importar una clave pública se utiliza:

gpg --import <archivo>

Descargar la clave pública de tyr desde www.tyr.unlu.edu.ar/clavetyr.asc e importarla con:

gpg --import clavetyr.asc

b) *Encriptar un archivo:*

Ahora para enviar un archivo encriptado a Ester Piscore:

gpg -r episcore@organizacion -e archivo_a_encriptar

genera el archivo encriptado con extension gpg. Con -a genera un archivo encriptado en ASCII (Para que pueda ser transmitido por email)

b) *Desencriptar un archivo:*

Para desencriptar un archivo cifrado utilizando clave pública

gpg archivo_a_desencriptar

Solicitará la frase contraseña para acceder a la clave privada del recipiente.

3) Firma digital

Un archivo se FIRMA con:

gpg -u usuario_que_firma --clearsign <archivo>

para generar signatura que se anexa al mensaje en claro, o

gpg -u usuario_que_firma -s <archivo> (-sa para utilizar ASCII de 7 bit)

para generar una firma y comprimir el mensaje

con -u se indica quien lo firma
Una vez que se firmó no debe modificarse el archivo.

Para verificar FIRMA

gpg <archivo>

Verifica la firma con la clave pública de quien firmó y genera un archivo en texto claro.

Descargar el archivo www.tyr.unlu.edu.ar/mensaje_de_tyr.asc y verificar integridad del mensaje firmado por tyr.

gpg mensaje_de_tyr.asc

4) Encripción y firmado

Supongamos que Manuel Darío desea enviar un mensaje a Ester (almacenado en el archivo a-ester.txt) que sólo ella pueda descifrar, y a su vez asegurar que el mensaje no sea modificado y sólo pueda haber sido generado por el mismo:

gpg -u mdario@organizacion -r episcore@organizacion -sea a-ester.txt

solicitará la contraseña para acceder a la clave privada de Manuel Dario.

Para desencriptar y validar la firma

```
gpg a-ester.asc
```

solicitará la contraseña para acceder a la clave privada de Ester Piscore y así descifrar el mensaje y verificar la firma con la clave pública de Manuel Darío.

Genere un par de clave pública y privada para usted.
Cree un breve mensaje que contenga al menos su nombre y número de legajo. Encríptelo y fírmelo utilizando las claves que ha generado.
Exporte la clave pública en ASCII, y envíela por correo electrónico junto con el archivo del mensaje firmado y encriptado a florge@unlu.edu.ar.