I.E.S. «SAN VICENTE»
Código centro: 03008423
www.iessanvicente.com
03008423@edu.gva.es

C/ Lillo Juan, 128
03690 Sant Vicent del Raspeig
Telf.: 965 93 65 05
Fax: 965 93 65 06

Práctica 4 – Criptografía Asimétrica en Linux

Mediante el comando gpg de linux vamos a realizar la comunicación mediante criptografía asimétrica.

Generación de la clave:

1. Mediante el parámetro *--gen-key* vamos a generar la pareja de claves pública/privada.

Terminal - david@debian: ~
root@debian:/# gpg --gen-key
gpg (GnuPG) 2.2.12; Copyright (C) 2018 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.
gpg: creado el directorio '/root/.gnupg'
gpg: caja de claves '/root/.gnupg/pubring.kbx' creada
Nota: Usa "gpg --full-generate-key" para el diálogo completo de gene
clave.
GnuPG debe construir un ID de usuario para identificar su clave.
Nombre y apellidos: david piñuel bosque
Dirección de correo electrónico: davidpi31bosque1999@gmail.com
Está usando el juego de caracteres 'utf-8'.
Ha seleccionado este ID de usuario:
"david piñuel bosque <davidpi31bosque1999@gmail.com>"
¿Cambia (N)ombre, (D)irección o (V)ale/(S)alir?
Práctica 4 – Criptografía Asimétrica en Linux
Mediante el comando gpg de linux vamos a realizar la comunicación mediante criptografía asimétrica.
Generación de la clave
1. Mediante el parámetro --gen-key vamos a generar la pareja de claves pública/privada.
2. Dejaremos todas las opciones por defecto y la validez para 1m (un mes).
3. También nos pedirá información sobre nosotros, que debemos rellenar.
4. Para la generación de las claves necesita muchos bytes aleatorios así que nos pedirá que realicemos acciones en el ordenador para que esos bytes sean variados. Lo mejor es navegar por internet escribiendo cosas y tener un poco de paciencia.

Terminal - david@debian: ~
Por favor introduzca frase contraseña para
proteger su nueva clave
Frase contraseña: ********
<OK>
<Cancelar>
Práctica 4 – Criptografía Asimétrica en Linux
Mediante el comando gpg de linux vamos a realizar la comunicación mediante criptografía asimétrica.
Generación de la clave
1. Mediante el parámetro --gen-key vamos a generar la pareja de claves pública/privada.
2. Dejaremos todas las opciones por defecto y la validez para 1m (un mes).
3. También nos pedirá información sobre nosotros, que debemos rellenar.
4. Para la generación de las claves necesita muchos bytes aleatorios así que nos pedirá que realicemos acciones en el ordenador para que esos bytes sean variados. Lo mejor es navegar por internet escribiendo cosas y tener un poco de paciencia.

Terminal - david@debian: ~
Archivo Editar Ver Terminal Pestañas Ayuda
Por favor vuelva a introducir frase contraseña
Frase contraseña: ********
<OK>
<Cancelar>
practica04 (1).docx - LibreOffice Writer
Práctica 4 – Criptografía Asimétrica en Linux
Mediante el comando gpg de linux vamos a realizar la comunicación mediante criptografía asimétrica.
Generación de la clave:
1. Mediante el parámetro --gen-key vamos a generar la pareja de claves pública/privada.
2. Dejaremos todas las opciones por defecto y la validez para 1m (un mes).
3. También nos pedirá información sobre nosotros, que debemos rellenar.
4. Para la generación de las claves necesita muchos bytes aleatorios así que nos pedirá que realicemos acciones en el ordenador para que esos bytes sean variados. Lo mejor es navegar por internet escribiendo cosas y tener un poco de paciencia.

Terminal - david@debian: ~
Archivo Editar Ver Terminal Pestañas Ayuda
¿Cambia (N)ombre, (D)irección o (V)ale/(S)alir? V
Es necesario generar muchos bytes aleatorios. Es una buena idea real
alguna otra tarea (trabajar en otra ventana/consola, mover el ratón,
la red y los discos) durante la generación de números primos. Esto d
generador de números aleatorios mayor oportunidad de recoger suficie
entropía.
Es necesario generar muchos bytes aleatorios. Es una buena idea real
alguna otra tarea (trabajar en otra ventana/consola, mover el ratón,
la red y los discos) durante la generación de números primos. Esto d
generador de números aleatorios mayor oportunidad de recoger suficie
entropía.
gpg: /root/.gnupg/trustdb.gpg: se ha creado base de datos de confian
gpg: clave 5D0754CDE335D646 marcada como de confianza absoluta
gpg: creado el directorio '/root/.gnupg/openpgp-revocs.d'
gpg: certificado de revocación guardado como '/root/.gnupg/openpgp-r
8DB4462AE45DFF211CEDC25D0754CDE335D646.rev'
claves pública y secreta creadas y firmadas.
pub rsa3072 2021-02-16 [SC] [caduca: 2023-02-16]
EA8DB4462AE45DFF211CEDC25D0754CDE335D646
uid david piñuel bosque <davidpi31bosque1999@gm
sub rsa3072 2021-02-16 [E] [caduca: 2023-02-16]
root@debian:/#
practica04 (1).docx - LibreOffice Writer
Práctica 4 – Criptografía Asimétrica en Linux
Mediante el comando gpg de linux vamos a realizar la comunicación mediante criptografía asimétrica.
Generación de la clave:
1. Mediante el parámetro --gen-key vamos a generar la pareja de claves pública/privada.
2. Dejaremos todas las opciones por defecto y la validez para 1m (un mes).
3. También nos pedirá información sobre nosotros, que debemos rellenar.
4. Para la generación de las claves necesita muchos bytes aleatorios así que nos pedirá que realicemos acciones en el ordenador para que esos bytes sean variados. Lo mejor es navegar por internet escribiendo cosas y tener un poco de paciencia.

I.E.S. «SAN VICENTE»
Código centro: 03008423
www.iessanvicente.com
03008423@edu.gva.es

C/ Lillo Juan, 128
03690 Sant Vicent del Raspeig
Telf.: 965 93 65 05
Fax: 965 93 65 06

2. Dejaremos todas las opciones por defecto y la validez para 1m (un mes).

3. También nos pedirá información sobre nosotros, que debemos rellenar.

I.E.S. «SAN VICENTE»
Código centro: 03008423
www.iessanvicente.com
03008423@edu.gva.es

C/ Lillo Juan, 128
03690 Sant Vicent del Raspeig
Telf.: 965 93 65 05
Fax: 965 93 65 06

4. Para la generación de las claves necesita muchos bytes aleatorios así que nos pedirá que realicemos acciones en el ordenador para que esos bytes sean variados. Lo mejor es navegar por internet escribiendo cosas y tener un poco de paciencia.

I.E.S. «SAN VICENTE»
Código centro: 03008423
www.iessanvicente.com
03008423@edu.gva.es

C/ Lillo Juan, 128
03690 Sant Vicent del Raspeig
Telf.: 965 93 65 05
Fax: 965 93 65 06

5. Mediante el parámetro *-k* listamos las claves que tenemos instaladas.

➔ **Saca una captura de pantalla del último punto que demuestre que lo has hecho.**

<u>Intercambio de claves</u>:

1. Primero debemos exportar nuestra clave pública para poder pasarla a las personas con las que nos queramos comunicar. Se realizará con el comando –export

   gpg --output claveAlvaro.gpg --export IDClave

   NOTA: la opción –armor sirve para exportar la clave en ASCII

2. Se envia ese fichero .gpg a la persona con la que te quieres comunicar por email y esa persona la tendrá que importar:

gpg --import claveAlvaro.gpg

3. Ahora listar las claves y tendrá que aparecer la nueva que se ha importado. **Captura de pantalla.**

I.E.S. «SAN VICENTE»
Código centro: 03008423
www.iessanvicente.com
03008423@edu.gva.es

C/ Lillo Juan, 128
03690 Sant Vicent del Raspeig
Telf.: 965 93 65 05
Fax: 965 93 65 06

Cifrar con la clave pública

1. Ahora encriptaremos un fichero usando la clave pública que nos ha mandado el compañero con el siguiente comando:

gpg --encrypt --recipient IDClave documento.txt

I.E.S. «SAN VICENTE»
Código centro: 03008423
www.iessanvicente.com
03008423@edu.gva.es

C/ Lillo Juan, 128
03690 Sant Vicent del Raspeig
Telf.: 965 93 65 05
Fax: 965 93 65 06

2. Ahora vamos a desencriptar el fichero que nos ha mandado el compañero. Para ello usamos:

gpg -d [Archivo encriptado] –o [Fichero de salida]

I.E.S. «SAN VICENTE»
Código centro: 03008423
www.iessanvicente.com
03008423@edu.gva.es

C/ Lillo Juan, 128
03690 Sant Vicent del Raspeig
Telf.: 965 93 65 05
Fax: 965 93 65 06

Firmar archivos

1. Ahora vamos a firmar un documento usando la clave privada:

   gpg -u IDClavePrivada --output firmar.txt.gpg --sign firmar.txt

   Este documento se lo mandaremos al compañero

2. Verifica el fichero que te ha mando el compañero para ver que él es el propietario del fichero. Para verificar un archivo firmado usamos:

   gpg --verify firmar.txt.gpg

I.E.S. «SAN VICENTE»
Código centro: 03008423
www.iessanvicente.com
03008423@edu.gva.es

C/ Lillo Juan, 128
03690 Sant Vicent del Raspeig
Telf.: 965 93 65 05
Fax: 965 93 65 06

3. Si queremos desencriptar usamos la opción –d vista anteriormente.

Eliminar certificados:

En caso de que nuestra clave se vea comprometida, enviaremos un certificado de revocación a las personas a las que les enviamos la clave pública de forma que a partir de ese momento la clave deja de tener validez

1. *gpg --output certificadoRevok.asc --gen-revoke IDClave*

Una vez el certificado de revocación esté en su poder deben de importarlo para que se borre su certificado o sea revocado.

➔ Crea un certificado de revocación y mándaselo al compañero.

I.E.S. «SAN VICENTE»
Código centro: 03008423
www.iessanvicente.com
03008423@edu.gva.es

C/ Lillo Juan, 128
03690 Sant Vicent del Raspeig
Telf.: 965 93 65 05
Fax: 965 93 65 06

➔ Importa el fichero de revocación que te ha mandado el compañero.