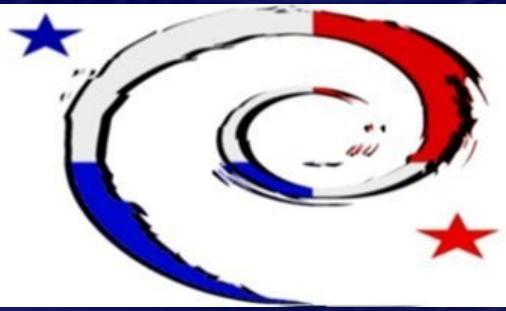

Panamá

MiniDebConf

2010

GnuPG

Fernando C. Estrada

fcestrada@fcestrada.com

Como buena parte de las tecnologías aplicadas, la criptografía muy probablemente nació con una aplicación militar: ¿Cómo transmitir un mensaje secreto del general A al general B habiendo elementos enemigos en el medio?

¿Cómo asegurarse de que, incluso siendo capturado el mensajero, el mensaje permanecería secreto?

GPG o GNU Privacy Guard es una herramienta para cifrado y firmas digitales, que viene a ser un reemplazo del PGP (Pretty Good Privacy) pero con la principal diferencia que es software libre licenciado bajo la GPL.

Aunque básicamente el programa tiene una interfaz textual, actualmente hay varias aplicaciones gráficas que utilizan recursos de GPG. Por ejemplo, GNU Privacy Assistant (GPA), Seahorse, así como también ha sido integrado dentro de clientes de correo como Kmail y Evolution, también hay un plugin llamado Enigmail que se integra con Mozilla Thunderbird (Icedove en Debian) que trabajan en Windows, GNU/Linux y otros sistemas operativos.

GPG cifra los mensajes usando pares de claves individuales asimétricas generadas por los usuarios. Las claves públicas pueden ser compartidas con otros usuarios de muchas maneras, un ejemplo de ello es depositándolas en los servidores de claves.

Basarse en un esquema de claves simétricas resulta muy limitado, por eso surgió la necesidad de las claves asimétricas.

Instalando a la manera Debian:

$ sudo aptitude update

$ sudo aptitude install gnupg

El paquete GnuPG en Debian cuenta con una prioridad de nivel importante, es decir, seguramente se instaló por defecto cuando instalaste Debian por primera vez.

```
fcestrada@hypatia:~$ gpg --gen-key
gpg (GnuPG) 1.4.10; Copyright (C) 2008 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 and RSA (default)
   (2) DSA and Elgamal
   (3) DSA (sólo firmar)
   (4) RSA (sólo firmar)
Su elección: 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)? 10y
La clave caduca lun 16 mar 2020 15:40:12 CST
¿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: Fernando C. Estrada
Dirección de correo electrónico: fcestrada@fcestrada.com
Comentario:
Ha seleccionado este ID de usuario:
    "Fernando C. Estrada <fcestrada@fcestrada.com>"

¿Cambia (N)ombre, (C)omentario, (D)irección o (V)ale/(S)alir? V
Necesita una frase contraseña para proteger su clave secreta.

Es necesario generar muchos bytes aleatorios. Es una buena idea realizar
alguna otra tarea (trabajar en otra ventana/consola, mover el ratón, usar
la red y los discos) durante la generación de números primos. Esto da al
generador de números aleatorios mayor oportunidad de recoger suficiente
entropía.
```

pubring.gpg --> Clave pública

secring.gpg --> Clave privada

```
fcestrada@hypatia:~$ ls -la .gnupg
total 316
drwx------  2 fcestrada fcestrada   4096 mar 19 15:11 .
drwxr-xr-x 63 fcestrada fcestrada   4096 mar 19 15:23 ..
-rw-------  1 fcestrada fcestrada   9427 dic 25 10:04 gpg.conf
-rw-------  1 fcestrada fcestrada 284460 feb 28 21:44 pubring.gpg
-rw-------  1 fcestrada fcestrada    600 mar  1 03:24 random_seed
-rw-------  1 fcestrada fcestrada   4891 dic 25 10:04 secring.gpg
-rw-------  1 fcestrada fcestrada   2080 feb 28 21:44 trustdb.gpg
fcestrada@hypatia:~$
```

Generando un certificado de revocación:

$ gpg --output <RevocarIdClave.asc> --gen-revoke <IdClave>

Recomendable imprimir o guardar en un CD o USB, en caso que nuestras claves se vean comprometidas.

Firmando un documento:

$ gpg --clearsign <Documento>

Cifrando un documento:

$ gpg --output <ArchivoSalida>.gpg --encrypt
--recipient <IdDestinatario> <ArchivoEntrada>

¿Diferencia entre firmar y cifrar?

Descifrando un archivo cifrado dirigido a mí:

$ gpg --output <ArchivoSalida> --decrypt <ArchivoCifrado>.gpg

Administrando claves:

$ gpg --edit-key IdClave

Más información:

$ man gpg

Intercambiando claves por medio de los servidores de claves.

Enviar una clave:

$ gpg --keyserver <servidor> --send-key IdClave

Recibir una clave:

$ gpg --keyserver <servidor> --recv-key IdClave

Firmar una clave:

$ gpg --edit-key IdClave

Command> sign

Intercambiar (aumentando el círculo de confianza) y validar una clave por medio de:

Identificación Oficial

Fingerprint

Conocer al usuario, en caso de duda es mejor abstenerse de firmar una clave

¿Que papel juega GnuPG en Debian?

Si se quiere ser desarrollador del proyecto Debian es necesario contar con la firma de al menos un DD actual, esto es para ingresar al círculo de confianza de Debian.

Gracias a esto se podrán firmar paquetes, emitir votos, y demás actividades que requieren de una autenticación segura.

Signing Party (Mañana):

Evento en el que l@s asistentes intercambian entre ell@s sus claves compatibles PGP.

Paquete signing-party:

$ sudo aptitude install signing-party

Generar e imprimir claves usando:

$ gpg-key2ps <IdClave>

¡¡¡GRACIAS!!!