Práctica Criptografía: GnuPG

Juan José Domínguez Jiménez, Antonio García Domínguez y Juan Boubeta Puig

Seguridad y Competencias Profesionales
Curso 2012-2013
12 diciembre 2012

1. Descripción general

GnuPG es una herramienta de software libre empleada para comunicaciones seguras y almacenamiento de datos. Se puede usar tanto para cifrar como para crear firmas digitales.

Para obtener autenticidad, crea un resumen (normalmente SHA-1) del mensaje, y lo cifra con la clave privada, usando un algoritmo de cifrado asimétrico (normalmente ElGamal, aunque también puede usar DSA o RSA). Posteriormente, el destinatario puede comprobar que el resumen calculado a partir del mensaje recibido coincide con el descifrado.

Para obtener confidencialidad, utiliza un esquema híbrido, en el que un algoritmo asimétrico (ElGamal por omisión) cifra una clave para un algoritmo simétrico (AES, entre otros), que es el que realmente cifra el fichero indicado.

2. Generación y distribución de claves

1. Genere su par de claves pública y privada:

```
gpg --gen-key
```

   Al ejecutar por primera vez este comando se creará el directorio `.gnupg` con el fichero de configuración y los ficheros `secring.gpg` y `pubring.gpg`. En el fichero `secring.gpg` se almacenarán las claves privadas y en `pubring.gpg` las claves públicas.

   NOTA: si está usando un ordenador del aula y desea conservar estas claves después de la práctica, haga una copia de seguridad del subdirectorio `.gnupg` de su directorio personal (`$HOME/.gnupg`) en sistemas basados en UNIX (como GNU/Linux o los *BSD), y de `C:\Documents and Settings\Usuario\Datos de programa\gnupg` en Windows (sustituyendo USUARIO por el nombre de su cuenta). Cópielo a la misma ruta en su máquina, y asegúrese que sólo su propio usuario tenga derechos de lectura y escritura sobre sus ficheros.

Para mantener los permisos bajo un sistema basado en UNIX, le vendrá bien comprimir en formato `tar.gz` y luego descomprimir en un sistema de ficheros que permita establecerlos automáticamente al descomprimir, como EXT2, EXT3, EXT4 o REISERFS, entre otros. Los propios de Windows (FAT32 y NTFS) son problemáticos en estos casos.

2. Exporte su clave pública a un fichero y mándela al foro de criptografía para que esté disponible para todos los alumnos.

```
gpg -a -o usuario.asc --export (identificador)
```

3. Obtenga del Campus Virtual la clave pública de su compañero e impórtela a su fichero de claves.

```
gpg --import usuario.asc
```

4. Visualice la lista de claves públicas que posee.

```
gpg --list-keys
```

5. Obtenga la huella dactilar de su clave pública.

```
gpg --fingerprint
```

6. Verifique que la huella coincide con la de su compañero y dé la confianza necesaria sobre la clave:

```
gpg --edit-key (identificador)

  Orden> fpr
  Orden> trust
```

3. Firma y cifrado

A diferencia de la sección anterior, en ésta sólo se dan las instrucciones generales para cada acción. El proceso a seguir en el resto de la práctica se indicará a través de la correspondiente tarea del Campus Virtual.

- Firmar un texto en claro con su clave privada, dejando los contenidos visibles y codificando la firma en Base-64 («ASCII armored»):

```
gpg -o (fichero firmado) --clearsign (fichero)
```

- Verificar la firma incrustada en un fichero:

```
gpg --verify (fichero firmado)
```

- Cifrar un fichero para una serie de destinatarios que se pedirán en la línea de órdenes, codificándolo en Base-64:

```
gpg −a −o (fichero cifrado) −−encrypt (fichero)
```

- Cifrar y firmar un fichero, codificando el resultado en Base-64:

```
gpg −o (fichero cifrado y firmado) −a −−sign −−encrypt (fichero)
```

- Descifrar el fichero, comprobando su firma, si la tiene:

```
gpg −−decrypt (fichero cifrado y opcionalmente firmado)
```

4. Otras acciones de interés

- Visualizar la lista de claves privadas disponibles:

```
gpg −−list−secret−keys
```

- Borrar claves de los anillos: Si se desea borrar alguna clave, en primer lugar hay que borrar la clave privada y a continuación la pública.

```
gpg −−delete−secret−key (identificador-clave)
gpg −−delete−key (identificador-clave)
```