Universidad Politécnica de Cartagena

Escuela Técnica Superior de Ingeniería de Telecomunicación

SEGURIDAD EN REDES DE COMUNICACIONES

Práctica: Instalación y manejo de PGP.

María Dolores Cano Baños
Natalio López Martínez

Referencias:

- William Stalling, "Fundamentos de seguridad en redes de aplicaciones y estándares," 2ª edición, Pearson Education, 2003. ISBN 84-205-4002-1. Capítulo 5.

- James F. Koruse, Keith W. Ros, "Redes de Computadores. Un enfoque descendente basado en Internet," 2ª edición, Pearson Education, 2003. ISBN 84-7829-061-3. Capítulo 7.

- http://www.pgpi.com

1. Introducción

PGP (*Pretty Good Privacy*) es un programa de cifrado híbrido, escrito por Phil Zimmerman en 1991. Desde su aparición se ha convertido en una de las herramientas más utilizadas a nivel mundial para conseguir privacidad y autenticación tanto en los mensajes de correo como en los archivos almacenados en el disco duro del ordenador. A ello ha contribuido indudablemente su distribución como herramienta gratuita, así como su puesta al día en sucesivas versiones aparecidas mejorando los algoritmos criptográficos utilizados. PGP se puede encontrar como *plug-in* para la mayoría de agentes de usuario de correo electrónico, incluyendo Exchange y Outlook de Microsoft, Eudora o Pine.

PGP nos permite dos cosas:

- Cifrar mensajes y archivos para que no resulten legibles sin nuestra autorización (Confidencialidad).
- Firmarlos digitalmente para asegurarnos que no son modificados sin nuestro consentimiento (Integridad y autenticación).

Su funcionamiento podría resumirse de la siguiente manera. Antes de cifrar un texto, PGP lo comprime. La compresión de los datos tiene dos ventajas fundamentales, por un lado, el ahorro en el tiempo de transmisión y espacio de almacenamiento y, por otro -en nuestro caso más importante-, fortalece la seguridad. La mayoría de las técnicas de criptoanálisis se aprovechan de patrones existentes en el texto claro para atacar una cifra. La compresión reduce estos patrones, reforzando la resistencia al criptoanálisis.

Una vez comprimido el texto, PGP crea una clave de sesión: una clave secreta de un solo uso. Esta clave es un número aleatorio generado a partir de los movimientos del ratón y de la pulsación de teclas por parte del usuario. Con la clave y algún algoritmo de cifrado convencional (3DES, IDEA o CAST-128), se obtiene el texto cifrado. A continuación se cifra la clave de sesión con la clave pública del receptor. El resultado, junto con el texto cifrado se envía al receptor.

En recepción se ejecuta el proceso inverso. El destinatario utiliza su clave privada para recuperar la clave de sesión y con esa clave de sesión PGP recupera los datos cifrados.

- La combinación de los dos métodos de cifrado compagina la idoneidad del cifrado de clave pública con la velocidad del cifrado convencional. En el cifrado simétrico los algoritmos ofrecidos por PGP son CAST, 3DES e IDEA. Todos trabajan con bloques de 64 bits de texto plano y cifrado. Las claves CAST e IDEA tienen un tamaño de 128 bits, mientras Triple-DES usa una clave de 168 bits (aunque su longitud efectiva sería de 112 bits). El algoritmo por defecto en la versión 6.5 es el CAST, mientras en las versiones más antiguas de PGP es el IDEA.

En cuanto al cifrado asimétrico el algoritmo por defecto es el DSA, aunque la versión que vamos a utilizar en esta práctica es también compatible con el cifrado RSA, empleado en las versiones más antiguas de PGP.

El algoritmo empleado para la función *hash* es el SHA, que proporciona un resumen de mensaje de 160 bits, frente a versiones más antiguas de PGP que utilizaban el MD5.

1.1 Notación

K_S = clave de sesión usada en el esquema de cifrado simétrico
KR_a = clave privada del usuario A
KU_a = clave pública del usuario A
EP = cifrado de clave pública
DP = descifrado de clave pública
EC = cifrado simétrico
DC = descifrado simétrico
H = función *hash*
|| = concatenación
Z = compresión utilizando el algoritmo ZIP
R64 = conversión al formato ASCII radix 64

1.2 Descripción

Autenticación

Como puede verse en la figura 1, el servicio de firma se proporciona de la siguiente manera:

1. El emisor crea un mensaje.
2. Se usa SHA-1 para generar un código *hash* del mensaje de 160 bits.
3. El código *hash* se cifra con RSA usando la clave privada del emisor y el resultado se añade antepuesto al mensaje.
4. La firma junto con el mensaje se comprime y se transmite.
5. El receptor, descomprime el mensaje y usa RSA con la clave pública del emisor para descifrar y recuperar el código *hash*.
6. El receptor genera un nuevo código *hash* para el mensaje y lo compara con el código *hash* descifrado. Si los dos coinciden, el mensaje se considera auténtico y se acepta.

Confidencialidad

El servicio de confidencialidad se utiliza tanto para cifrar mensajes que se van a transmitir o almacenarse localmente en ficheros. En ambos casos se puede utilizar el algoritmo de cifrado simétrico CAST-128 y, como alternativa, IDEA o 3DES, utilizando siempre el modo CFB de 64 bits.

La secuencia seguida en este caso es la siguiente:

1. El emisor genera un mensaje y PGP lo comprime.
2. El mensaje se cifra, usando CAST-128 (o IDEA o 3DES) con la clave de sesión.
3. La clave de sesión se cifra con RSA, usando la clave pública del receptor, y se añade antepuesta el mensaje.
4. El receptor usa RSA con su clave privada para descifrar y recuperar la clave de sesión.
5. La clave de sesión se usa para descifrar el mensaje comprimido.

6. El mensaje ya en texto claro se descomprime.

Autenticación y confidencialidad

Ambos servicios se pueden utilizar con un mismo mensaje. En este caso, primero se genera una firma para el mensaje en texto claro y se adjunta antepuesta a dicho mensaje. El resultado (mensaje +firma) se comprime y se cifra usando la clave de sesión. Por último, la clave de sesión se cifra usando RSA (o ElGamal), con la clave pública del receptor.

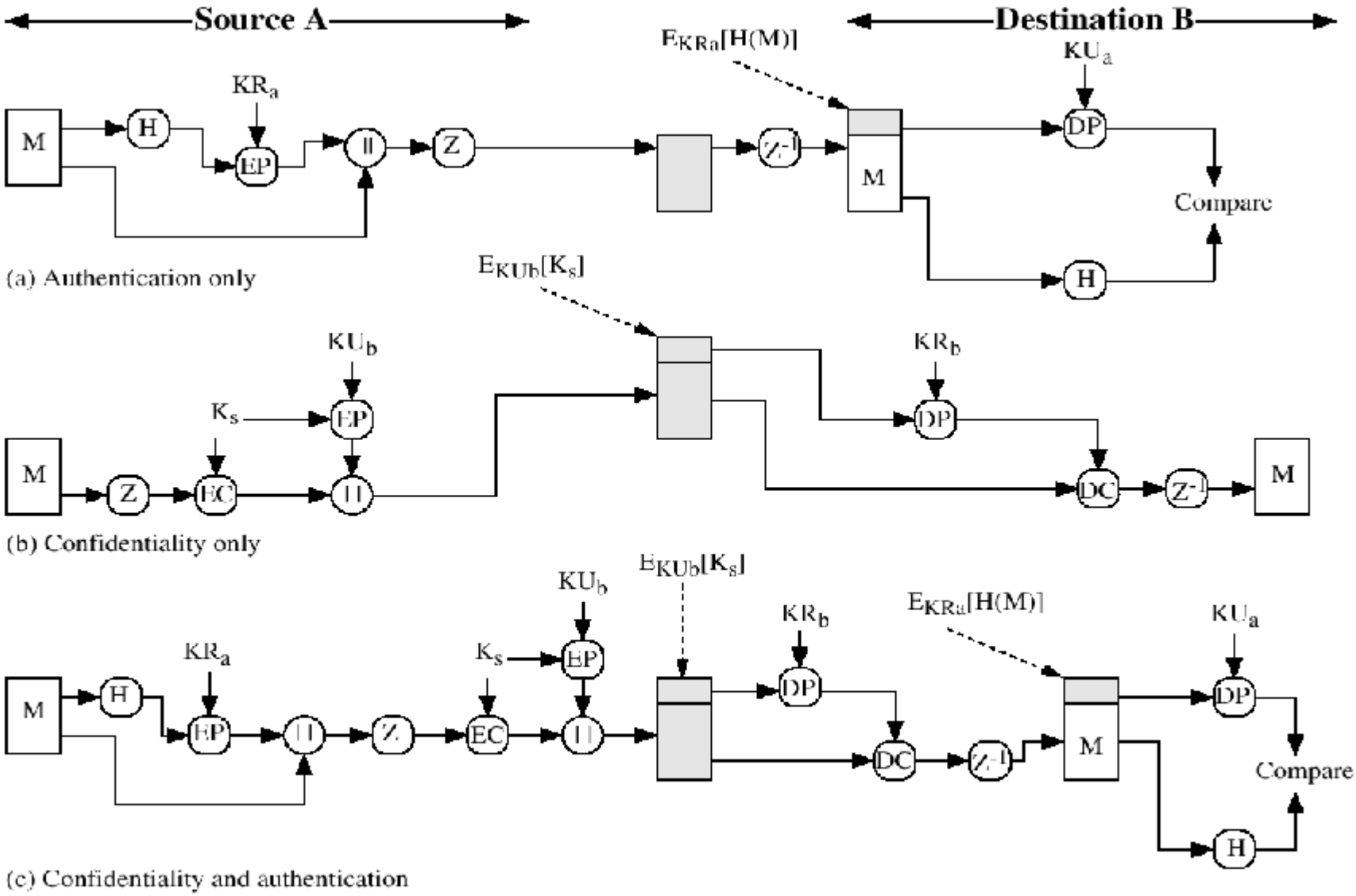

Figura 1 **PGP Cryptographic Functions**

Compresión

De forma predeterminada, PGP comprime el mensaje después de aplicar la firma, pero antes del cifrado.

La firma se genera antes de la compresión debido a dos razones fundamentales:

a) Es preferible firmar un mensaje descomprimido para poder almacenar solamente el mensaje descomprimido junto con la firma para su verificación posterior. Si se firma un documente comprimido, sería necesario almacenar una versión comprimida del mensaje para su posterior verificación o volver a comprimir el mensaje cuando se requiera verificación.

b) El algoritmo de compresión no es determinista; distintas implementaciones del algoritmo permiten diferentes compromisos entre la velocidad de ejecución y el ratio de compresión y, como resultado, producen distintas secuencias comprimidas. Sin embargo, los distintos algoritmos de compresión pueden operar entre sí, ya que cualquier versión del algoritmo puede descomprimir correctamente la salida de cualquier otra versión. Aplicar la función *hash* y la firma después de a compresión obligaría a utilizar siempre la misma versión del algoritmo de compresión.

El algoritmo de compresión que se utiliza es ZIP.

Compatibilidad con el correo electrónico

Después del cifrado el bloque de bits resultante forma una cadena de octetos arbitraria. Sin embargo, muchos sistemas de correo electrónico sólo permiten el uso de bloques de texto ASCII. Para ajustarse a esta restricción, PGP proporciona un servicio de conversión de una secuencia arbitraria a una secuencia de caracteres ASCII imprimibles. El esquema que se usa para ello es la conversión radix 64.

El grupo de caracteres radix está formado por 65 caracteres ASCII imprimibles, de los cuales uno es de relleno ("="). Con $64=2^6$ caracteres, cada carácter se puede usar para representar 6 bits de entrada.

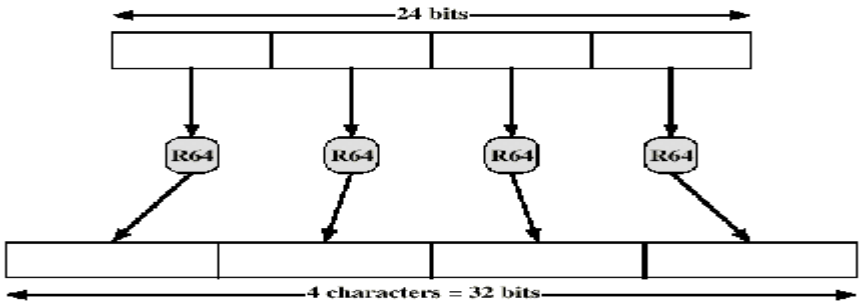

Figura 2. **Printable Encoding of Binary Data into Radix-64 Format**

En la figura 2 podemos ver que la entrada binaria se procesa en bloques de 3 octetos (24 bits) y cada grupo de 6 bits en el bloque de 24 se convierte en un carácter.

Por tanto el uso de radix expande un mensaje un 33%. Cabe esperar que el algoritmo de compresión utilizado compense esta expansión.

La conversión radix 64 se aplica justo antes de la transmisión, una vez se ha firmado, comprimido y cifrado el mensaje.

Identificadores de clave

Un usuario podría querer tener múltiples parejas de claves pública/privada para interactuar con diferentes grupos de interlocutores o simplemente para mejorar la seguridad limitando la cantidad de material cifrado con una de las claves. El resultado de todo esto es que no hay una relación uno a uno entre los usuarios y sus claves públicas. Por tanto, se necesita algún mecanismo para identificar claves particulares.

Una solución simple sería transmitir la clave pública junto con el mensaje cifrado. Entonces el receptor podría verificar que efectivamente se trata de una de sus claves públicas, y continuar. Este esquema funcionaría, pero constituye un gasto innecesario de espacio.

Otra solución sería asociar un identificador a cada clave pública que sea única al menos en un usuario. Es decir, la combinación del identificador de usuario (*user ID*) y el identificador de clave (*key ID*) sería suficiente para identificar una clave en especial. Sin embargo, esta solución trae consigo un problema de gestión y de costes adicionales: los identificadores de claves deben ser asignados y almacenados para que tanto emisor como receptor pueden establecer la relación entre identificador de clave y clave pública.

Para eliminar este último problema, la solución adoptada por PGP consiste en utilizar como identificador de clave los 64 bits menos significativos de cada clave pública. Con esta longitud se garantiza que la probabilidad de duplicidad de identificadores es muy pequeña.

También se necesita un identificador de clave para la firma digital PGP. Como un emisor puede usar una clave privada, de una serie de claves privadas, para cifrar el resultado del mensaje, el receptor debe saber qué clave pública debe de usar. Por lo tanto el componente de firma digital de un mensaje incluye el identificador de clave de 64 bits de la clave pública que se requiere. Cuando se recibe el mensaje, el receptor verifica que el identificador de clave es el de una clave pública para ese emisor y entonces procede a verificar la firma.

Ficheros de claves

PGP almacena las claves en unas estructuras denominadas anillos (o llaveros). Cada usuario tendrá dos anillos, uno para las claves públicas de otros usuarios (PUBRIG.PKR) y otro para sus claves pública/privada (SECRING.SRK).

Cada una de las claves, además de la secuencia binaria correspondiente, posee una serie de datos, como son el identificador del usuario que la emitió, la fecha de expiración, la versión de PGP con la que fue generada, y la huella digital (*fingerprint*). Este último campo es bastante útil, pues se trata de una secuencia hexadecimal lo suficientemente larga como para que sea única, y lo suficientemente corta como para que pueda ser escrita en un papel, o leída de viva voz. La huella digital se emplea para asegurar la autenticidad de la clave. Si alguien quisiera asegurarse de la autenticidad de una clave, bastaría con que llamara por teléfono al autor, y le pidiera que leyese su huella digital.

Aunque se intenta que el anillo de claves privadas se almacene sólo en la máquina del usuario que lo creó y que sólo ese usuario pueda acceder a él, tiene sentido hacer que el valor de la clave privada sea lo más seguro posible. Para ello, antes de almacenar la clave en el fichero, se cifra usando CAST-128 (IDEA o 3DES), usando el *hash SHA-1* de una frase clave elegida por el usuario. Por tanto, para recuperar la clave privada es necesario recordar la frase clave con la que se ha cifrado.

Gestión de clave pública

PGP también proporciona un mecanismo para la certificación de la clave pública. Pero este mecanismo resulta bastante diferente del más convencional de la autoridad de certificación. Las claves públicas de PGP son certificadas por una red de confianza. Un usuario A puede certificar cualquier par clave/nombre de usuario cuando crea que cada miembro del par realmente se corresponde con el otro. Además PGP permite que el usuario A diga que confía en otro usuario B para garantizar la autenticación de más claves.

Algunos usuarios de PGP firman las claves de otros, celebrando "fiestas de firmado de claves". Los usuarios recogen físicamente disquetes con claves públicas, los intercambian y certifican las claves públicas de los demás firmándolas con sus claves privadas. Una de las particularidades de PGP es precisamente que un certificado puede tener varias firmas.

Las claves públicas de PGP también se distribuyen a través de los servidores de claves públicas PGP en Internet (RedIRIS). Cuando un usuario envía una clave pública a estos servidores, el servidor almacena una copia de la clave, envía una copia a los demás servidores, y sirve la clave a cualquiera que la solicite. Aunque las fiestas de firmado de claves y los servidores de claves públicas PGP existen, el modo más común de distribución de claves públicas para los usuarios es colocarlas en sus páginas WEB y anunciarlas en sus correos electrónicos.

Revocación de claves públicas

Un usuario podría querer revocar su clave pública actual porque sospecha que existe un riesgo o simplemente para evitar el uso de la misma clave durante un periodo largo de tiempo.

El convenio para revocar una clave pública es que el propietario emita un certificado de revocación de clave, firmado por él. Este certificado tiene la misma forma que un certificado de firma normal pero incluye un indicador que señala que su propósito es revocar la clave pública que contiene.

Es aconsejable generar un certificado de revocación, cuando se genera un para de claves pública y privada. De esta forma, si se nos olvida la frase clave, o perdemos la clave privada, siempre podremos revocar la clave pública.

2. Objetivo de la práctica

Familiarizarse con la aplicación software de libre distribución *PGPTools* (PGP versión 6.5.1i) con la que se realizarán distintas actividades destinadas a la creación de *anillos de confianza,* el cifrado de archivos, la firma de mensajes, etc.

3. Desarrollo de la práctica

3.1 Instalación de PGP

Para poder instalar PGP v 6.5.1i se necesita:

- Windows 95, 98 o NT.
- 8 MB de RAM.
- 15 MB de espacio en el disco duro.

Existen también versiones para Linux, Unix, Mac, etc.

Aunque la versión 6.5 incorpora una interfaz totalmente nueva sigue siendo compatible con las versiones anteriores del producto. Podemos obtener PGP a través de Internet. Entre otros sitios se encuentra disponible en:

PGP Internacional

http://www.pgpi.com/download/

En esta página podemos encontrar desde *software* de libre distribución incluido el PGPTools hasta distintos enlaces a otras páginas de interés así como recursos para programadores y listas de preguntas/respuestas más comunes en relación con PGP (FAQs).

PGP en castellano

http://www.geocities.com/SiliconValley/Pines/2332/index.html

Página en castellano sobre el PGP. Entre otras cosas incluye enlaces a PGP Internacional y PGP Inc. (para USA). De igual forma, podemos encontrar otras facilidades acerca del PGP tales como documentación, manuales, interfaces para otras herramientas, etc.

Para el desarrollo de esta práctica podéis encontrar el *software* necesario en la carpeta compartida SRC2005 del equipo PC-08.

Una vez tenemos el programa en nuestro disco es necesario descomprimirlo, hacer doble clic sobre el icono de instalación y seguir las instrucciones de la pantalla. Existen también *plug-ins* que permiten incorporar las herramientas de PGP en diversos programas de correo electrónico. En este caso, debéis incluir sólo el *plug-in* para Microsoft OutLook. Antes de terminar la instalación, el ayudante nos preguntará si disponemos ya de un par de claves pública y privada o no. Podéis contestar que sí, con lo que termina la instalación o que no. En este caso seguir las instrucciones del punto 3.2.1.

Una vez finalizada la instalación, lanzar la aplicación PGPTools. Esta aplicación incorpora los siguientes módulos, a los que se puede acceder directamente desde su botonera (figura 3):

- *PGPKeys* (gestor de claves)
- Cifrado de archivos

- Firma digital de archivos
- Firma y cifrado simultánea de archivos
- Descifrado de archivos y verificación de firmas.
- Borrado de archivos.
- Borrado de espacio libre en disco.

Figura 3 Botonera principal de *PGPTools*.

3.2 Gestión de claves

Para poder trabajar con PGP necesitaremos disponer de un par de claves: una pública y una privada. Esto nos permitirá firmar mensajes digitalmente, así como recibir correo cifrado por otros usuarios. También será necesario acceder a sus claves cuando deseemos enviarles mensajes cifrados. Empezaremos viendo cómo generar nuestra pareja de claves.

Podemos generar una nueva pareja de claves al finalizar la instalación de PGP o en cualquier otro momento.

3.2.1 Creación de un nuevo par de claves

Empezaremos la práctica generando nuestro propio par de claves. Los pasos a seguir son los siguientes:

1. Abre la ventana PGP, que estará en la carpeta Archivos de programa y haz doble clic sobre PGPkeys. Esto abrirá la ventana PGPkeys.
2. Elige *New Key*... desde el menú *Keys*. El asistente de generación de claves proporciona alguna información introductoria en la primer pantalla.
3. Una vez leída esta información hacer clic en *Next*. El Asistente de Generación de Claves te pedirá que escribas tu nombre de usuario y dirección de correo electrónico.
4. Haz clic en *Next* para avanzar a la pantalla siguiente. El asistente solicitará un tamaño para las nuevas claves que va a generar. Puede elegirse un tamaño de clave entre 1024 y 4056 bits. (Las claves de tamaño personalizado resultan bastante más costosas de calcular). Cuanto más grande sea el tamaño de la clave elegido, menor es la posibilidad de que alguien pueda descubrirla, pero resulta más costoso llevar a cabo los procesos de cifrado y de descifrado. En general, una clave de 1024 bits resulta más que suficiente, a no ser que la información que va a intercambiarse sea extremadamente confidencial.
5. Haz clic en *Next* para avanzar a la pantalla siguiente. El Asistente solicitará la fecha de caducidad de las claves. La opción predeterminada es Nunca. Una vez que una clave pública ha caducado no puede utilizarse para cifrar, pero sí para verificar una firma digital.
6. Haz clic en *Next.* El Asistente de Generación de Claves solicitará una contraseña o frase de acceso. En el cuadro de diálogo Contraseña PGP,

escribe la secuencia de caracteres que desees usar para restringir el acceso a tu clave privada. La barra Calidad muestra la vulnerabilidad de la frase de contraseña comparada con la vulnerabilidad de la clave que está siendo generada. Una barra llena significa que son aproximadamente equivalentes.

La elección de la frase de acceso es fundamental en la generación y posterior utilización de un par de claves. Debe ser lo suficientemente larga como para no poder sufrir un ataque eficiente y lo suficientemente "pegadiza" como para no olvidarla. El olvido de la frase de acceso implica que no se pueda volver a utilizar el par de claves y que deberíamos revocarlo y eliminarlo, informado a todo aquel que hubiese recibido nuestra clave pública.

7. Hacer clic en *Next* para empezar el proceso de generación de claves. Podéis enviar vuestra nueva clave pública a un servidor de claves, aunque en nuestro caso no resultará necesario para el desarrollo de la práctica. Para facilitar el intercambio de claves con vuestros compañeros colocar vuestra clave pública en un directorio compartido con permisos sólo de lectura.
8. Cuando el proceso de generación está completo, aparece la pantalla final. Haz clic en Terminar.

En la ventana PGPkeys aparece un par de llaves que representa el par de claves que acabamos de crear. Las claves RSA se representan mediante llaves azules de tipo antiguo, y las claves Diffie-Hellman/DSS por llaves amarillas de tipo moderno.

Las claves creadas, así como las que recogemos de otros usuarios se almacenan en archivos de claves. Generalmente, las claves privadas se almacenan en archivos `secring.skr` y las públicas en archivos `pubring.pkr`.

3.2.2 Distribución de la clave pública

Una vez creada nuestra pareja de claves es necesario poner nuestra clave pública a disposición de los otros usuarios, para ello existen diversas posibilidades:

- Publicar la clave en un servidor de claves.
- Enviar la clave en un mensaje de correo electrónico.
- Exportarla o copiarla a un archivo de texto.

La mejor opción es publicarla en un servidor de claves, lo que puede hacerse fácilmente desde la ventana PGPkeys, eligiendo la opción *Send Key To Server* del menú keys. Sin embargo, os recomiendo que no utilicéis esta opción, ya que los servidores solamente son capaces de agregar información, y no permiten eliminar nombres ni firmas de usuarios. Enviar solamente al servidor la clave que vayáis a utilizar de forma definitiva (si pensáis hacerlo) y no la de la práctica.

Para la práctica elegiremos la tercera opción. Podemos copiar nuestra clave pública a un archivo de tres formas distintas: seleccionar el icono que representa vuestro par de claves desde la ventana PGPkeys, elegir la opción *Export*, desde el menú *Keys*, y escribir el nombre del archivo dónde deseáis guardar la clave. Recuerda que debéis ponerla a disposición de vuestros compañeros del laboratorio colocándola en una carpeta compartida bajo el nombre de **ClavePublica.**

Ejercicio 1. Exportad vuestras claves a vuestro directorio compartido ClavePublica.

Si las visualizáis en un editor de texto tendrá el siguiente aspecto:

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: PGPfreeware 6.5.1i for non-commercial use <http://www.pgpi.com>
mQGiBDU10ZwRBADteYhtTpsGflf9H+fyskbQASGzSbKAGkmve9pNt/+R/xJgG
WSkyx8vU7H2ODJwuvgOsyhl/ZdIa9Bneu0OTUak/laR4VQukFgJOHYuJgQcRK
VKFUN6UV6UpoevjuW8kO2FVq3oo48QO5YyLcsxH09cbyEvadEcYIaOhZDKN
aAvDwCg/3yYY1Q0J6qE+YHaAuib/XdOq7UD/
RuCKH61nycFHu0ki976hSNa87U00ith6fBAC4FsLWQVEJZoZaxwnOeJ/Kmxhha
3rQBnc4oIR9XLTlo7LZBD/0vPxRSZoFg6Bisb9zHexww02MC0Ddfgd11w6kQgL
8cpBfDaLr1PWAHEdqnTwzX43hsUB+zPQQUT/oSlLAkSujRVfWRH/T/bi9mIR
R9d2Ltv6XS0yp5ske0fK9O7QjRWx2aXJhIEJheWRhbCA8ZWx2aXJhQGRpc2Nh
LnVwdi5lcz6JAEsEEBECAAsFAjU10ZwECwMCAQAKCRBqXOIGP0/s9SynAK
CwKj7gIzGa8WYv+zvKA8vTOfGb0gCeIcy8/p86aZvLi0AJANpSDwva+GG5Ag0
ENTXRnBAIAPZCV7cIfwgXcqK61qlC8wXo+VMROU+28W65Szgg2gGnVqMU
6Y9AVfPQB8bLQ6mUrfdMZIZJ+AyDvWXpF9Sh01D49Vlf3HZSTz09jdvOmeF
XklnN/biudE/F/Ha8g8VHMGHOfMlm/xX5u/2RXscBqtNbno2gpXI61Brwv0YAW
Cvl9Ij9WE5J280gtJ3kkQc2azNsOA1FHQ98iLMcfFstjvbzySPAQ/ClWxiNjrtV
=Rh91
-----END PGP PUBLIC KEY BLOCK-----

3.2.3 Obtención de las claves públicas de otros

Para poder enviar mensajes cifrados a otro usuarios, así como verificar sus firmas será necesario obtener sus claves públicas, lo que podemos hacer con las mismas opciones que tenemos para publicar nuestra clave.

Para obtener una clave pública de un servidor de claves debemos acceder al menú *server* de la ventana PGPkeys y utilizar la opción *Search*. Nos aparecerá un menú con una serie de opciones para seleccionar el criterio de búsqueda: identificador de usuario, tipo de clave, fecha de creación, etc. Si se encuentra la clave para el usuario especificado, nos preguntará si deseamos agregarla a nuestro archivo de claves públicas. Podéis buscar alguna de las claves incluidas durante la instalación, por ejemplo la de Zimmermann.

Para importar la clave desde un archivo existen tres posibilidades:

- Desde el menú Claves, elegimos la opción *Import* y seleccionamos el archivo.
- Arrastrar el archivo que contiene la clave pública desde el Explorador de Windows a la ventana PGPkeys.
- Abrir el archivo que contiene la clave, *Copy* desde el menú *Edit*. Desde la ventana PGPkeys, elegir *Edit* y *Paste*. La clave nueva aparecerá en la ventana PGPkeys.

Ejercicio 2. Importad las claves de vuestros compañeros.

3.2.4 Autenticidad de una clave

Un punto importante en los sistemas basados en clave pública es como verificar la autenticidad de una clave de otra persona. La única forma realmente fiable es que el otro usuario nos entregue una copia de la misma mediante un disquete. Desgraciadamente, esto resulta imposible en la mayoría de los casos, en los que tendremos que conformarnos con obtener las claves a través de servidores o mediante mensajes de correo electrónico. Una protección adicional es verificar la huella de la

clave pidiéndosela al autor de la misma, por ejemplo por teléfono y comprobando que es la correcta. Para encontrar la huella de una clave, seleccionar la clave en la ventana PGPkeys, y luego desde el menú claves elegir Propiedades de la Clave. La huella aparece en el apartado "ID" de la pestaña General".

Ejercicio 3. ¿Cuál es la huella digital de uno de vuestros compañeros? Verificar su validez con ellos.

Una vez estamos convencidos que tenemos una copia legítima de la clave pública de una persona hay que firmarla. En otro caso se considera por defecto que no es de confianza y no se nos permite verificar firmas ni descifrar mensajes con ella. Para ello selecciona la clave y al pulsar el botón de la derecha aparecerá un menú donde puedes escoger la opción *Sign* y firmarla.

Ejercicio 4. Firmad las claves de vuestros compañeros. Durante el proceso de firma, seleccionar la opción "Permitir la explotación de la firma". ¿Qué símbolos han cambiado en la ventana PGPKeys?

3.2.5. Confianza y validez

Uno de los conceptos más confusos en el uso del PGP es el de validez. Dicho problema consiste en saber si la clave pública que hemos recibido pertenece realmente a un supuesto remitente. Para resolver dicho problema, entran en juego las propiedades de validez y confianza:

Una **clave** es **válida** si estoy seguro de que pertenece a su dueño.

Una **clave** es de **confianza** si su dueño es de fiar, es decir, es una persona responsable a la hora de firmar claves. Una firma de alguien de confianza permite establecer una "red de confianza" entre claves que han sido distribuidas por medios no directos (un servidor de claves, un archivo adjunto a un correo electrónico, etc.)

Ejercicio 5. Declarad las claves importadas de confianza y exportadlas a vuestro directorio ClavePública. ¿Cuántas firmas tienen las claves de vuestros compañeros? ¿Son claves válidas? ¿Se pueden verificar correos electrónicos de vuestros compañeros con ellas.

3.2.6 Revocación de una clave (SOLO INFORMATIVO: NO HAY QUE HACER NADA)

Si dejamos de confiar en nuestro par de claves personal podemos revocarlo, indicando a todos que dejen de utilizarla. La mejor manera de darle publicidad al tema es ubicarlo en un servidor de claves públicas.

Para revocar una clave tendremos que seguir los siguientes pasos:

1. Abrir la ventana PGPkeys y seleccionar el par de claves que deseamos revocar.

2. Elegir Revocar desde el menú Claves. Aparece un mensaje con una información breve sobre las consecuencias de revocar una clave, y nos pide confirmación sobre la revocación de la clave seleccionada.

3. Hacer clic sobre Sí para confirmar. Aparece el cuadro de diálogo Contraseña PGP, solicitando la contraseña.

4. Escribir nuestra contraseña y hacer clic en Aceptar. Al revocar una clave, ésta aparece cruzada con una línea roja para indicar que ya no es válida.

Nota: Si las claves se hubiesen enviado a un servidor de claves, enviar la clave revocada al servidor para que todos sepan que no deben seguir utilizando esta clave.

3.3 Envío y recepción de correo electrónico privado

3.3.1 Cifrar y firmar un mensaje

Comprobad que vuestro cliente de correo Microsoft Outlook tiene el *plug-in* de PGP, tal y como se indica en la figura 4. En caso contrario, reiniciar el PC.

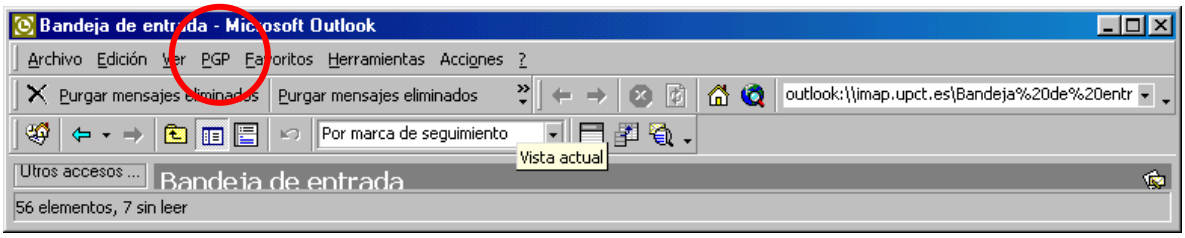

Figura 4: Plug-in de PGP en Microsoft Outlook

Ejercicio 6. Escribid un mensaje nuevo y firmarlo con la opción Firmar ahora. ¿Qué es lo que ha cambiado?

Ejercicio 7. Escribid un nuevo mensaje, firmarlo y cifrarlo en el envío. Enviad el correo a uno de vuestros compañeros. ¿Qué claves han intervenido? ¿Qué ocurre?

3.3.2 Descifrar y verificar un mensaje

Ejercicio 8. Leed alguno de los correos que hayáis recibido. Usad la opción Decrypt/Verify para comprobar y descifrar el mensaje. ¿Se pueden leer mensajes de correo cifrado por alguno de vuestros compañeros, si declaráis sus firmas como de "no confianza"?

3.4 Cifrado de archivos

El cifrado de información para su posterior envío por correo electrónico o simplemente almacenamiento en disco se puede realizar de forma sencilla mediante el botón de *PGPTools* "*Encrypt*". La acción se inicia mediante un cuadro de diálogo donde se nos solicita el fichero que deseamos cifrar. A continuación debemos seleccionar una clave de nuestro anillo de confianza del usuario destinatario de la información cifrada. Tras la selección, debemos arrastrar el ítem al cuadro inferior de "*Recipients*". Por

último, podemos marcar aquellas opciones que creamos convenientes de entre las que se muestran en el cuadro de diálogo.

Las opciones que podemos activar son las siguientes:

- **Text output**. El fichero cifrado será de tipo texto.
- **Wipe original**. Elimina el fichero original tras haber obtenido el fichero cifrado.
- **Conventional encryption**. Nos pide una frase de acceso única para ese fichero.
- **Self decrypting archive**. Obtiene un fichero ejecutable que se descifra mediante la frase de acceso.

Ejercicio 9. Cread un fichero de texto y cifrarlo con la clave pública de alguno de vuestros compañeros, eliminando el fichero original. ¿Cuál es el tamaño del fichero antes y después de cifrado? ¿Es posible leer el fichero original? ¿Qué se necesitaría para hacerlo?

3.4.1 Firma digital de archivos

La firma digital de archivos se utiliza cuando deseamos certificar el origen de algún documento sin importarnos que su contenido pueda ser accedido. Debemos considerar que el firmado de documentos no necesariamente protege al mismo.

Para acceder a la firma de un archivo debemos pulsar el botón de *PGPTools* "*Sign*". Las acciones que se inician son similares a las explicadas en el apartado de cifrado de archivos.

Aquí, en la ventana de diálogo se añade una nueva opción con respecto al cifrado de archivos que es "**Detached Signature**". Por defecto esta opción está activa y origina un fichero distinto al original y que contiene únicamente la firma digital del documento. Si por el contrario desactivamos esta opción, entonces se origina un fichero donde, a parte de encontrarse la firma del documento, también se encuentra el propio archivo cifrado (equivale a cifrar y firmar simultáneamente).

Ejercicio 10. Cread un fichero de texto y firmarlo. ¿Cuál es el tamaño del fichero antes y después de firmado?

3.4.2 Firma y cifrado simultáneo de archivos

Esta opción, que se activa con el botón de *PGPTools* "*Encrypt & Sign*", combina las dos opciones de cifrado y firma que hemos explicado anteriormente. Equivale a una firma con "**Detached Signature**" desactivado.

3.4.3 Descifrado y verificación de archivos

Esta opción, que se activa mediante el botón de *PGPTools* "*Decrypt/Verify*" sirve para descifrar y/o verificar la firma de documentos cifrado y/o firmados. Al activarlo, se abre una ventana de diálogo donde podemos seleccionar un archivo y a continuación se nos pide la frase de acceso para el descifrado y verificación del archivo.

Ejercicio 11. Descifrad y verificad la firma de los archivos creados en los apartados anteriores. ¿Qué clave se debe utilizar en cada caso?

3.4.4 Borrado seguro de archivos

El borrado seguro de archivos, activado mediante el botón de *PGPTools* "*Wipe*", es una utilidad añadida al sistema PGP que permite la eliminación definitiva de archivos. Por lo general, el borrado de un archivo no implica su total desaparición del sistema hasta no realizar un formateo activo del disco. Esta utilidad equivale a realizar un formateo local del espacio ocupado por el archivo. Su utilización se realiza mediante una ventana de diálogo donde podemos seleccionar aquellos archivos que deseemos eliminar de forma segura.

Ejercicio 12. Borrad de forma segura los ficheros creados con anterioridad.

3.5 Otras cuestiones

Ejercicio 13. ¿Puedo utilizar PGP sin haber generado mi par de claves? ¿Para qué?

Ejercicio 14. ¿Qué clave tengo que utilizar para firmar los mensajes que envío? ¿Y para cifrarlos? ¿Y si lo que deseo es almacenar mensajes cifrados en le disco duro?

Ejercicio 15. ¿Qué utilidad tienen las firmas que acompañan a algunas de las claves?