PGP®
for Personal Privacy

Para
Macintosh

Guía del Usuario

(Traducción al español para la versión freeware 5.5.3i)

Pretty Good Privacy, Inc.

9-97. Impresión original en inglés en los Estados Unidos de América.
PGP for Personal Privacy, Versión 5.5.1 para Macintosh.
Traducido al español por Carlos Lamas, Arturo Quirantes y Víctor M. Álvarez.

Escriba el número de serie de su Acuerdo de Licencia en el espacio proporcionado abajo:

PRETTY GOOD PRIVACY, INC.
2121 South El Camino Real, Suite 902
San Mateo, CA 94403
(650) 631-1747 voz
(650) 572-1932 fax
info@pgp.com
http://www.pgp.com

GARANTÍA LIMITADA

Garantía Limitada. Pretty Good Privacy, Inc. ("PGP") garantiza que el Producto Software funcionará substancialmente de acuerdo con los materiales escritos acompañantes durante un período de sesenta (60) días desde la fecha de adquisición original. Con la extensión permitida por la ley aplicable, las garantías implícitas en el Producto Software, de haberlas, están limitadas a ese período de sesenta (60) días. Algunas jurisdicciones no permiten limitaciones de duración en garantías implícitas, así que la limitación de arriba puede no ser aplicable en su caso.

Recursos del Cliente. La completa responsabilidad de PGP y de sus distribuidores y su recurso exclusivo será, a elección de PGP o bien (a) devolución del precio de adquisición pagado por la licencia, o bien, (b) reparación o reemplazo del Producto Software que no satisfaga la garantía limitada de PGP y que se devuelve a PGP a cargo del cliente con una copia de su factura. Esta garantía limitada es nula si el fallo del Producto Software es el resultado de un accidente, de abuso, o de aplicación incorrecta. Cualquier Producto Software reparado o reemplazado se garantizará por el período restante de validez de la garantía original o por treinta (30) días, lo que sea más largo. Fuera de los Estados Unidos, ninguno de estos recursos ni servicios de soporte a productos ofrecidos por PGP están disponibles sin una prueba de compra de una fuente internacional autorizada y puede no estar disponible al alcance de PGP por su acatamiento de las restricciones por las leyes y regulaciones de control de exportaciones de los EE.UU.

NINGUNA OTRA GARANTÍA. EN LA MÁXIMA EXTENSIÓN PERMITIDA POR LA LEY APLICABLE, Y EXCEPTO PARA LAS GARANTÍAS LIMITADAS ESTABLECIDAS AQUÍ, EL SOFTWARE Y LA DOCUMENTACIÓN SE PROPORCIONAN "TAL CUAL" Y PGP Y SUS DISTRIBUIDORES RECHAZAN CUALQUIER OTRA GARANTÍA O CONDICIÓN, EXPLÍCITA O IMPLÍCITA, INCLUYENDO, PERO NO LIMITADAS A, GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN, IDONEIDAD PARA UN PROPÓSITO PARTICULAR, CONFORMIDAD CON LA DESCRIPCIÓN, TÍTULO Y NO INFRACCIÓN DE DERECHOS DE TERCERAS PARTES, Y LA PROVISIÓN DE O FALTA DE PROVISIÓN DE SERVICIOS DE ASISTENCIA. ESTA GARANTÍA LIMITADA LE DA A USTED DERECHOS LEGALES ESPECÍFICOS, PUEDE TENER OTROS, QUE VARÍEN DE JURISDICCIÓN EN JURISDICCIÓN.

LIMITACIÓN DE RESPONSABILIDAD. EN LA MÁXIMA EXTENSIÓN PERMITIDA POR LA LEY APLICABLE, EN NINGÚN CASO PGP O SUS DISTRIBUIDORES SERÁN RESPONSABLES DE CUALQUIER DAÑO INDIRECTO, INCIDENTAL, CONSECUENTE, ESPECIAL O EJEMPLAR; O PÉRDIDA DE BENEFICIOS DE NINGÚN TIPO (INCLUYENDO, SIN LIMITACIÓN, DAÑOS POR PÉRDIDA DE BENEFICIOS DE NEGOCIOS, INTERRUPCIÓN DE NEGOCIOS, PÉRDIDA DE INFORMACIÓN DE NEGOCIOS, O CUALQUIER PÉRDIDA PECUNIARIA) SURGIDA DEL USO O IMPOSIBILIDAD DE USO DEL PRODUCTO SOFTWARE O LA NO PROVISIÓN DE SERVICIOS DE ASISTENCIA, INCLUSO SI PGP HA SIDO ADVERTIDO DE LA POSIBILIDAD DE TALES DAÑOS. EN CUALQUIER CASO, LA RESPONSABILIDAD COMPLETA Y CUMULATIVA DE PGP CON USTED O CON CUALQUIER OTRA PARTE POR CUALQUIER PÉRDIDA O DAÑO RESULTANTE DE ALGUNA RECLAMACIÓN, DEMANDA O ACCIÓN SURGIDA DE O REFERENTE A ESTE ACUERDO NO EXCEDERÁ EL PRECIO DE ADQUISICIÓN PAGADO POR ESTA LICENCIA. COMO ALGUNAS JURISDICCIONES NO PERMITEN LA EXCLUSIÓN O LA LIMITACIÓN DE LA RESPONSABILIDAD, LAS LIMITACIONES DE ARRIBA PUEDEN NO SER APLICABLES EN SU CASO.

Prólogo

Este libro describe cómo utilizar PGP for Personal Privacy, Versión 5.5 para Macintosh. La Versión 5.5 de PGP tiene algunas características nuevas que se describen en el Capítulo 1.

Convenios utilizados en este documento

Tipos de notas

NOTA: Las Notas proporcionan información adicional sobre la utilización de PGP—por ejemplo, si usted no está utilizando PGP/MIME, debe cifrar desde el Finder todos los archivos que quiera enviar como adjuntos antes de enviar su mensaje.

SUGERENCIA: Las Sugerencias proporcionan guías para utilizar PGP con eficacia—por ejemplo, cómo crear una contraseña útil.

AVISO: Los Avisos proporcionan información para prevenir la pérdida de datos—por ejemplo, si usted está enviando su clave a colegas que utilizan PCs, introduzca un nombre con un máximo de ocho caracteres seguidos de un punto, y tres caracteres adicionales para la extensión del tipo de archivo (por ejemplo, correo.txt).

Para más información

Hay varios modos de encontrar más información acerca de PGP y sus productos.

Las páginas Web de PGP

En PGP proporcionamos información acerca de nuestros productos, la organización PGP, actualizaciones de productos, y aspectos relacionados, tales como Temas de Seguridad, en las páginas Web de PGP. Visítenos en www.pgp.com.

Información de Registro

A los usuarios se les pide que se registren en-línea. Esta información es únicamente para nuestro uso interno y nos permitirá servirle mejor en el futuro. Estos datos permanecerán confidenciales—nosotros respetamos su intimidad (es a los que nos dedicamos). Vea nuestra página de registro en el siguiente URL:

http://www.pgp.com/products/online-register.cgi

Asistencia

Para conseguir Asistencia Técnica para su producto PGP, vea nuestras páginas web de Asistencia Técnica en http://www.pgp.com/service/ o mándenos correo electrónico a PGPSupport@pgp.com.

Hay un servicio disponible para productos PGP enviando correo electrónico a PGPservice@pgp.com o contactando a través de las páginas Web de PGP en http://www.pgp.com/service/

El servicio está disponible para los siguientes temas:

- Devoluciones de Productos
- Problemas de Descarga
- Cuestiones de Controles de Exportación
- Preguntas sobre Mercado
- Petición de Información sobre Productos
- Gestión e Información de Pedidos

Bibliografía Introductoria Recomendada

Bacard, Andre *Computer Privacy Handbook,* Peachpit Press, 1995.

Garfinkel, Simson *Pretty Good Privacy,* O'Reilly & Associates, 1995.

Schneier, Bruce *Applied Cryptography: Protocols, Algorithms, and Source Code in C, Second Edition,* John Wiley & Sons, 1996.

Schneier, Bruce *E-mail Security,* John Wiley & Sons, 1995.

Stallings, William *Protect Your Privacy,* Prentice-Hall, 1994.

Más Bibliografía

Lai, Xuejia, "On the Design and Security of Block Ciphers," Institute for Signal and Information Processing, ETH-Zentrum, Zurich, Switzerland, 1992.

Lai, Xuejia, Massey, James L., y Murphy, Sean "Markov Ciphers and Differential Cryptanalysis," Advances in Cryptology—EUROCRYPT'91.

Rivest, Ronald "The MD5 Message Digest Algorithm" *MIT Laboratory for Computer Science*, 1991.

Wallich, Paul "Electronic Envelopes" *Scientific American*, Feb. 1993, página 30.

Zimmermann, Philip "A Proposed Standard Format for RSA Cryptosystems" *Advances in Computer Security*, Vol. III, editado por Rein Turn Artech House, 1988.

Sus comentarios son bienvenidos

Nosotros mejoramos PGP continuamente y damos la bienvenida a las sugerencias y comentarios de los clientes según diseñamos nuevas versiones. Apreciamos su interés en PGP y su confianza en el contenido del producto y funcionalidad, especialmente cuando ideamos características para mejorar los productos en opciones corporativas. Comentarios como los suyos nos ayudan a desarrollar software y servicios más ricos y fáciles de utilizar.

Aunque no podemos incorporar todas las sugerencias, tomaremos las suyas seriamente en consideración cuando desarrollemos futuros productos.

Si desea ponerse en contacto, por favor envíe correo electrónico mac-doc@pgp.com.

Contenidos

Capítulo 1

Presentando PGP for Personal Privacy

¡Bienvenido a PGP! Con PGP® for Personal Privacy, usted puede proteger de un modo seguro y con facilidad la intimidad de sus mensajes de correo electrónico y archivos adjuntos cifrándolos de manera que sólo los destinatarios deseados puedan leerlos. Usted puede también firmar digitalmente los mensajes y archivo, lo cual asegura su autenticidad. Un mensaje firmado verifica que la información en él no se ha alterado de ningún modo.

Qué novedades hay en la Versión 5.5 de PGP

La Versión 5.5 de PGP aporta las siguientes características nuevas:

- Usted puede crear grupos de destinatarios, en los cuales selecciona un grupo de claves de personas y cifra correo para todos ellos simultáneamente.
- Nuevas posibilidades de integración con servidores de claves que puede utilizar para almacenar, buscar y sincronizar claves automáticamente.
- Una nueva Ventana de Búsqueda de Claves que puede utilizar para localizar claves en servidores remotos con la misma interfaz de usuario que utiliza cuando busca en su archivo de claves.
- La Versión 1.0 de PGP Policy Management Agent for SMTP, que impone la norma de cifrado de correo electrónico de su organización. PGP Policy Management Agent for SMTP trabaja conjuntamente con un servidor de correo estándar SMTP para asegurar que el correo electrónico entrante y saliente se ajusta a las normas impuestas por un sitio dado.

- Una función Destrucción PGP que sobreescribe archivos para que no se puedan recuperar con herramientas software.
- Un menú Ver configurable que proporciona información acerca de las claves de su archivo de claves.
- Nuevas opciones de firma de claves que le permiten decidir si el propietario de la clave que usted está firmando es un presentador fiable o un presentador intermediario. Usted también puede decidir si su firma es exportable, lo que significa que se exporta junto a su clave, o no exportable.

Qué novedades hay en la documentación de la Versión 5.5 de PGP

Esta guía contiene información acerca de la Versión 5.5 de PGP. La documentación de PGP presenta las siguientes características nuevas:

- Los manuales para productos de usuario contienen información conceptual y procedimientos para usar PGP. La ayuda en línea para los productos de usuario de PGP está escrita específicamente para cada módulo, y contiene información más detallada sobre cómo utilizar PGP con cada módulo.
- La Versión 5.5 de PGP para Macintosh incluye ayuda en línea, y una copia electrónica de la documentación en formato .pdf (de Acrobat Reader) está disponible en el CD-ROM de la Versión 5.5 de PGP.

Utilizar PGP

Una de las formas más convenientes de utilizar PGP es a través de una de las populares aplicaciones de correo electrónico soportadas por los módulos de PGP. Esto le permite a usted cifrar, firmar, descifrar y verificar sus mensajes mientras compone y lee su correo con un simple clic sobre un botón. Si está utilizando una aplicación de correo electrónico no soportada por los módulos puede fácilmente cifrar el texto del mensaje utilizando PGPmenu. Además, si tiene que cifrar o descifrar archivos adjuntos, puede hacerlo directamente desde el Finder escogiendo la opción apropiada del menú.

Usted también puede utilizar PGP para cifrar y firmar archivos en el disco duro de su ordenador para almacenamiento seguro, y para destruir de forma segura archivos de su disco duro de forma de no se pueda recuperar información delicada utilizando software de recuperación de discos.

A primera vista

PGP se basa en una tecnología de cifrado de amplia aceptación conocida como *criptografía de clave pública* en la que se utilizan dos claves complementarias, denominadas par de claves para mantener las comunicaciones seguras. Una de las claves se conoce como *clave privada*, a la cual sólo usted tiene acceso, y la otra es una *clave pública* que usted puede intercambiar libremente con otros usuarios de PGP. Tanto sus claves públicas como sus claves privadas se almacenan en archivos de claves a los que se accede desde la ventana de PGPkeys. Es en esta ventana donde usted realiza todas las operaciones de manipulación de claves.

Para enviar un mensaje de correo electrónico privado, usted utiliza una copia de la clave pública de esa persona para cifrar la información, que solamente ese otro podrá descifrar utilizando su clave privada. A la inversa, cuando alguien quiere enviarle correo electrónico a usted, esa persona utiliza una copia de la clave pública de usted para cifrar los datos, que sólo usted podrá descifrar usando su clave privada.

Usted también utiliza su clave privada para firmar el correo electrónico que le envía a otros. Los destinatarios pueden utilizar la copia de la clave pública de usted para determinar si realmente usted envió el correo electrónico y si se ha sufrido alteraciones en el envío. Cuando una persona le envía correo electrónico firmado digitalmente, usted utiliza una copia de la clave pública de esa persona para comprobar la firma digital y asegurarse de que nadie ha alterado los contenidos.

Con el programa PGP usted puede crear y manipular fácilmente sus claves y acceder a todas la funciones para cifrar, firmar, descifrar y verificar sus mensajes de correo electrónico y archivos adjuntos.

La sección siguiente proporciona un rápido recorrido a través de los procedimientos que usted normalmente sigue con el fin de utilizar PGP. Para detalles concernientes a cualquiera de estos procedimientos consulte los capítulos correspondientes en este libro.

Crear un par de claves privada y pública

Antes de que pueda empezar a utilizar PGP, tiene que generar un par de claves. Un par de claves de PGP está formado por una clave privada a la que sólo usted tiene acceso y una clave pública que usted puede copiar y distribuir libremente a cualquiera con quien intercambie información.

Usted tiene la opción de crear un nuevo par de claves inmediatamente después de que haya completado el proceso de instalación de PGP, o puede hacerlo en cualquier momento abriendo la aplicación PGPkeys.

Intercambiar claves públicas con otros

Después de crear un par de claves, usted puede empezar a corresponderse con otros usuarios de PGP. Necesitará una copia de la clave pública de ellos y ellos necesitarán una copia de la clave pública de usted. Su clave pública es sólo un bloque de texto así que es realmente bastante fácil intercambiar claves con alguien. Usted puede incluir su clave pública en un mensaje de correo electrónico, copiarla en un archivo o puede mandarla a un servidor de claves público o corporativo, donde cualquiera pueda conseguir una copia cuando la necesite.

Validar sus claves

En cuanto tenga una copia de la clave pública de alguien, puede añadirla a su archivo de claves públicas. Usted debería en ese momento asegurarse de que la clave no se ha alterado y que realmente pertenece al supuesto propietario. Esto se hace comparando la *huella digital* única de su copia de la clave pública de alguien con la huella digital de la clave original de esa misma persona. Cuando usted está seguro de que tiene una clave pública válida, la firma para indicar que siente que la clave es segura para su uso. Además, puede asignar al propietario de la clave un nivel de fiabilidad indicando cuánta confianza tiene en esa persona para garantizarle la autenticidad de la clave pública de algún otro.

Cifrar y firmar su correo electrónico y archivos

Después de que haya generado su par de claves y haya intercambiado claves públicas, puede empezar a cifrar y firmar mensajes de correo electrónico y archivos.

- Si está usando una aplicación de correo soportada por los módulos, usted puede cifrar y firmar sus mensajes seleccionando las opciones apropiadas en la barra de herramientas de su aplicación.
- Si su aplicación de correo electrónico no está soportada por los módulos, usted puede copiar el mensaje en el portapapeles y realizar las funciones apropiadas desde allí. Usted también puede cifrar y firmar

archivos desde el Finder antes de adjuntarlos a su correo electrónico; cifrar archivos para almacenarlos de forma segura en su ordenador; y firmar archivos para verificar que no se han alterado.

Descifrar y verificar su correo electrónico y archivos

Cuando alguien le envía correo electrónico cifrado, usted puede recomponer su contenido y verificar cualquier firma añadida para asegurarse de que los datos se originaron en el remitente supuesto y de que su contenido no se ha alterado.

- Si está utilizando una aplicación de correo electrónico que está soportada por los módulos, usted puede descifrar y verificar sus mensajes seleccionando las opciones apropiadas en la barra de herramientas de su aplicación.
- Si su aplicación de correo electrónico no está soportada por los módulos, usted puede copiar el mensaje en el portapapeles y realizar las funciones apropiadas desde allí. Si quiere descifrar y verificar archivos adjuntos puede hacerlo desde el Finder. También puede descifrar archivos cifrados almacenados en su ordenador, y verificar archivos firmados para asegurarse de que no se han alterado.

Destruir archivos

Cuando usted necesite borrar de forma permanente un archivo, puede utilizar la función de Destrucción Segura para asegurarse de que el archivo es irrecuperable. El archivo se sobreescribe inmediatamente de manera que no puede recuperarse utilizando software de recuperación de discos.

Capítulo 2

Puesta en Marcha

Este capítulo explica cómo ejecutar PGP y da una ojeada rápida a los procedimientos que usted normalmente seguirá durante la utilización del producto. Contiene también una tabla con los iconos utilizados en PGPkeys.

Requisitos del sistema

Estos son los requisitos del sistema para instalar la Versión 5.5 de PGP:

- Macintosh IIci o modelo posterior con 68030 o superior
- Software del Sistema 7.5.3 o posterior
- 8 MB de RAM
- 10 MB de espacio libre en el disco duro

Los Macintosh con 68K deben tener activo el CFM 68K 4.0 de Apple o superior. El instalador de PGP lo instala si es necesario.

Compatibilidad con otras versiones

PGP ha experimentado múltiples revisiones desde que Phil Zimmermann lo empezó a distribuir como producto freeware en 1991, y se estima que hay actualmente cerca de 4 millones de copias en circulación. Aunque esta versión de PGP representa una reconstrucción significativa del programa original e incorpora una interfaz de usuario totalmente nueva, se ha diseñado para ser compatible con versiones anteriores de PGP. Esto significa que usted puede intercambiar correo electrónico seguro con personas que todavía utilizan esas versiones antiguas del producto:

- PGP 2.6 (Distribuido por el MIT)
- PGP 2.7.1 para el Macintosh (Distribuido por ViaCrypt)

- PGP 4.0 (Distribuido por ViaCrypt)
- PGP 4.5 (Distribuido por PGP, Inc.)
- PGP for Personal Privacy, Versión 5.0
- PGP for Business Security, Versión 5.5

Acerca de PGP for Personal Privacy

La Versión 5.5 de PGP for Personal Privacy soporta el uso de dos tipos de claves: RSA y Diffie-Hellman. Utilizando PGP for Personal Privacy Versión 5.5, usted sólo puede crear las nuevas claves Diffie-Hellman. Usted puede utilizar las claves RSA existentes pero no puede generar nuevas claves RSA.

Antes de la Versión 5.0 de PGP, las claves RSA eran la única opción. PGP ahora ofrece claves basadas en las tecnologías de cifrado Diffie-Hellman y firma digital DSS. La porción DSS de la clave se utiliza para firmar y la parte Diffie-Hellman se utiliza para cifrar.

Sin embargo, si usted necesita intercambiar correo electrónico o archivos con otros que están utilizando claves creadas con algoritmos de cifrado RSA, usted utilizará un conjunto de claves RSA existentes. Si está intercambiando correo electrónico o archivos con alguien que está utilizando una versión más vieja de PGP, esa persona deberá actualizarse a una de las nuevas versiones de PGP para aprovechar las ventajas de la interfaz de usuario mejorada y otras características.

Si está cifrando correo electrónico o archivos para múltiples destinatarios, algunos de los cuales tienen claves RSA y otros que tienen claves DSS/Diffie-Hellman, el correo electrónico se cifra empleando la clave apropiada para cada individuo. Sin embargo, para que los usuarios de versiones viejas de PGP puedan descifrar o verificar este correo electrónico, ellos tendrán que actualizarse a una de las versiones parcheadas que eliminan esta limitación. Estas versiones previas están disponibles como actualizaciones gratuitas en PGP.

La Versión 5.5 de PGP for Business Security contiene algunas características de las cuales usted debe estar informado si se corresponde con personas que la están utilizando.

PGP for Business Security ofrece una Clave Corporativa de Firmar y Claves Adicionales de Descifrado Entrantes y Salientes.

Una Clave Corporativa de Firmar es una clave pública que se ha designado como una clave del ámbito de la organización para que todos los usuarios puedan fiarse al firmar otras claves.

Las Claves Adicionales de Descifrado son claves que permiten a los oficiales de seguridad de las organizaciones, bajo determinadas circunstancias, descifrar mensajes enviados a o por personas de dentro de la organización. La Clave Adicional de Descifrado Entrante hace que el correo enviado a personas de la organización también se cifre con la Clave Adicional de Descifrado Entrante. La Clave Adicional de Descifrado Saliente hace que todo el correo cifrado enviado por personas de dentro de una organización también se cifre con la Clave Adicional de Descifrado Saliente. Usted puede consultar las Propiedades de la Clave para determinar si una clave tiene una Clave Adicional de Descifrado asociada con ella y a usted se le advertirá cuando esté cifrando con una clave con Clave Adicional de Descifrado.

Utilizar PGP/MIME

PGP/MIME es un estándar para algunos de los módulos que integran funciones de PGP directamente en aplicaciones de correo electrónico populares. Si está utilizando una aplicación de correo electrónico que está soportada por alguno de los módulos que ofrecen PGP/MIME, usted podrá cifrar y firmar así como descifrar y verificar sus mensajes de correo electrónico y archivos adjuntos automáticamente cuando envíe o reciba correo electrónico.

No obstante, compruebe antes de enviar correo electrónico PGP/MIME para asegurarse de que sus destinatarios utilizan una aplicación de correo electrónico que soporta este estándar, o pueden tener dificultades para descifrar y verificar sus mensajes.

También puede cifrar mensajes y archivos sin utilizar PGP/MIME.

Actualizar desde una versión anterior

Si se está actualizando desde una versión anterior de PGP (procedente de PGP, Inc. o de ViaCrypt) usted puede querer eliminar los archivos del programa viejo antes de instalar PGP para liberar algún espacio en el disco. Sin embargo, debería tomar la precaución de no borrar los archivos de claves privadas y públicas utilizados para almacenar todas las claves que haya creado o recogido mientras utilizaba la versión anterior.

Cuando instala PGP se le da la opción de conservar sus archivos de claves públicas y privadas existentes para que no tenga el problema de importar todas sus claves viejas. Para actualizarse desde una versión anterior, siga los pasos apropiados listados a continuación.

Para actualizarse desde la Versión 2.7.1 o 2.6.2 de PGP

1. Asegúrese de que sale de todos los programas que se ejecutan actualmente en su ordenador.
2. Haga copias de seguridad de sus archivos de claves PGP en otro volumen. Sus claves públicas están almacenadas en “pubring.pgp” y sus claves privadas están almacenadas en “secring.pgp”.

NOTA: Usted puede querer hacer dos copias de seguridad separadas de sus archivos de claves en dos disquetes diferentes para estar seguro. Tenga especial cuidado de no perder su archivo de claves privadas; de otra manera usted nunca podrá descifrar mensajes de correo electrónico o archivos adjuntos cifrados con las claves perdidas. Almacene los archivos de claves en un lugar seguro donde sólo usted tenga acceso a ellos.

3. Cuando haya hecho las copias de seguridad de sus viejos archivos de claves, elimine o archive el (viejo) software PGP. Usted tiene dos opciones aquí:
   - Borre manualmente la vieja carpeta PGP entera y todos sus contenidos; o bien
   - Borre manualmente el viejo programa PGP y conserve los archivos restantes, especialmente los de configuración y los archivos de claves.

NOTA: Si usted obtiene una copia de la versión 264 de PGP parcheada del MIT, su viejo software podrá leer las claves RSA de los nuevos archivos de claves 5.5 y no fallará si encuentra claves en el nuevo formato Diffie-Hellman/DSS.

4. Instale PGP 5.5 utilizando el Instalador suministrado.
5. Cuando el Instalador pregunte si tiene archivos de claves existentes, haga clic en Sí, localice sus viejos archivos de claves, y siga las

instrucciones para copiar esas claves a sus nuevos archivos de claves PGP 5.5.

6. Reinicie su ordenador.

Instalar la Versión 5.5 de PGP

Estos son los modos de instalar PGP 5.5:

- Desde un CD-ROM
- Desde la página web de PGP
- Desde el servidor de archivos de su compañía

Para Instalar PGP desde un CD-ROM

1. Arranque su Macintosh.
2. Inserte el CD-ROM.
3. Ejecute el Instalador.
4. Siga las instrucciones en pantalla.

Para instalar PGP desde la página web de PGP

1. Transfiera el programa PGP al disco duro de su ordenador.
2. Haga doble clic en el icono del programa de instalación de PGP.
3. Siga las instrucciones en pantalla.

Ejecutar PGP

PGP trabaja sobre los datos generados por otras aplicaciones. De ese modo, las funciones PGP se diseñaron para estar disponibles inmediatamente para usted basándose en la tareas que esté realizando en un momento dado. Hay cuatro formas principales de utilizar PGP:

- Desde el PGPmenu
- Desde dentro de las aplicaciones de correo electrónico soportadas
- Desde la ventana de PGPtools
- Desde PGPcontextmenu (para usuarios del Mac OS 8)

Utilizar PGP desde el PGPmenu

Usted puede realizar la mayoría de las operaciones de PGP desde el Finder o desde dentro de la mayoría de las aplicaciones escogiendo las opciones apropiadas en el icono PGPmenu, el cual aparece como un icono en la barra de menús del Finder y de otras aplicaciones que usted haya seleccionado. Esta característica proporciona acceso inmediato a las funciones de PGP con independencia de qué aplicación esté usando y es especialmente útil si está utilizando una aplicación de correo electrónico no soportada por los módulos de PGP.

Cuando esté utilizando aplicaciones de correo electrónico u otras basadas en texto, puede cifrar, firmar, descifrar y verificar texto seleccionando las opciones apropiadas en el PGPmenu. Cuando esté utilizando el Finder puede cifrar, firmar, descifrar, verificar y destruir archivos.

(Si no puede encontrar PGPmenu en alguna de sus aplicaciones, tiene que añadir la aplicación en el panel PGPmenu del diálogo de Preferencias de la aplicación PGPkeys.)

Abrir la aplicación PGPkeys

Al escoger PGPkeys en el PGPmenu o desde la carpeta de PGP 5.5, usted abre la aplicación PGPkeys, mostrando los pares de claves privada y pública que usted ha creado para sí mismo, y todas las claves públicas que usted ha añadido a su archivo de claves públicas. (Si no ha creado aún un nuevo par de claves el Asistente de Generación de Claves de PGP le guiará a través de los pasos necesarios para crear un nuevo par de claves. Sin embargo, antes de recorrer todo el proceso de creación de un nuevo par de claves, usted debería leer el Capítulo 3 para detalles completos referentes a las distintas opciones.)

Desde la ventana de PGPkeys usted puede crear nuevos pares de claves y manipular sus otras claves. Por ejemplo, aquí es donde usted examina los atributos asociados con una clave particular, especifica en qué medida confía en que la clave realmente pertenece a su supuesto propietario, e indica cuánto confía usted en esa persona para asegurar la autenticidad de las claves de otros usuarios. Para una explicación completa de las funciones de manipulación de claves que usted lleva a cabo desde la ventana PGPkeys, vea el Capítulo 6.

Establecer preferencias de PGP

Al escoger la opción de Preferencias en el menú Edición de PGPkeys, aparece la caja de diálogo de Preferencias, donde usted especifica opciones que afectan a cómo funciona el programa PGP basándose en su entorno operativo.

Al hacer clic en la lengüeta apropiada, usted puede avanzar a las opciones de preferencias que quiera modificar. Para una explicación completa de estas opciones, vea el Capítulo 6.

Obtener ayuda

PGPkeys soporta la ayuda de la Guía Apple, a la que se puede acceder desde el menú de Ayuda en el Mac OS 8 y en el menú con el icono de Interrogación en el Mac OS 7.

Utilizar PGP desde las aplicaciones de correo electrónico soportadas

Si usted tiene una de las populares aplicaciones de correo electrónico soportadas por los módulos de PGP, puede acceder a las funciones de PGP necesarias haciendo clic en los botones apropiados de la barra de herramientas de su aplicación. Por ejemplo, usted hace clic en el icono del candado para indicar que quiere cifrar su mensaje y en el icono de la pluma para indicar que quiere firmar. Algunas aplicaciones tienen un icono de candado y pluma juntos, lo que le permite hacer ambas cosas en un solo paso.

Cuando recibe correo electrónico de otro usuario de PGP, usted descifra el mensaje y verifica la firma digital de esa persona haciendo clic en el icono del sobre abierto, o seleccionando “Descifrar/Verificar” del menú.

Algunos módulos incorporan un botón con una llave y un sobre, que añade todas las claves incluidas en el mensaje a su archivo de claves. También puede acceder a la ventana de PGPkeys en cualquier momento mientras compone o recupera su correo haciendo clic en el botón con dos llaves en algunos módulos.

Si está utilizando una aplicación de correo electrónico con uno de los módulos que soportan el estándar PGP/MIME, y usted está comunicándose con otros usuarios cuyas aplicaciones de correo electrónico también soportan este estándar, pueden todos cifrar y descifrar sus mensajes de

correo electrónico y archivos adjuntos cuando envían o reciben su correo electrónico. Todo lo que tendrán que hacer para esto es activar las funciones de cifrado y firma PGP/MIME de la caja de diálogo de Preferencias de PGP.

Cuando usted reciba correo electrónico de alguien que utilice la función PGP/MIME, el correo llega con un icono añadido en la ventana de mensajes indicando que tiene codificación PGP/MIME.

Para descifrar el texto y los archivos adjuntos en correo electrónico con encapsulación PGP/MIME y para verificar cualquier firma digital, usted simplemente hace doble clic en el icono de sobre abierto. Los adjuntos permanecerán cifrados si no se usa PGP/MIME, pero el proceso de descifrado es normalmente más manual para el destinatario.

Utilizar PGP desde la aplicación PGPtools

Si está utilizando una aplicación de correo electrónico que no está soportada por los módulos, o si quiere realizar operaciones de PGP desde dentro de otras aplicaciones, usted puede cifrar y firmar, descifrar y verificar, o destruir de forma segura mensajes y archivos directamente desde la ventana PGPtools. Puede abrir la ventana PGPtools de una de las formas siguientes:

- Abra la carpeta de PGP y haga doble clic en el icono PGPtools.
- Coloque un alias de PGPtools en el menú Apple, y escoja PGPtools desde ese menú. También puede colocar un alias en el Escritorio.

Cuando aparece la ventana PGPtools, usted puede empezar su trabajo de cifrado.

Si está trabajando con texto, usted realiza sus operaciones de cifrado/descifrado, firma/verificación, y destrucción seleccionando el texto y arrastrándolo sobre el botón apropiado de la ventana PGPtools.

Si está trabajando con archivos, usted puede arrastrarlos simplemente sobre el botón apropiado.

Seleccionar destinatarios

Cuando usted envía correo electrónico a alguien que tiene una aplicación de correo electrónico soportada por los módulos de PGP, la dirección de correo electrónico del destinatario determina qué claves utilizar para cifrar los contenidos. Sin embargo, si usted introduce un nombre de usuario o

dirección de correo electrónico que no se corresponde a ninguna de las claves de su archivo de claves públicas, o si usted está cifrando desde el PGPmenu o desde PGPtools, usted debe seleccionar manualmente la clave pública del destinatario en la caja de diálogo de Selección de Claves de PGP.

Para seleccionar la clave pública del destinatario, arrastre el icono que representa la clave a la lista de Destinatarios y después haga clic en OK.

Para instrucciones completas sobre cómo cifrar y firmar y descifrar y verificar correo electrónico, vea el Capítulo 4. Si quiere cifrar archivos para almacenarlos en su disco duro o para enviarlos como adjuntos, vea el Capítulo 5.

Utilizar atajos

Aunque usted encontrará que PGP es bastante fácil de utilizar, hay disponibles un número de atajos para ayudarle a realizar las tareas de cifrado aún más rápido. Por ejemplo, usted puede efectuar la mayoría de las funciones PGP en archivos o volúmenes de su disco utilizando PGPcontextmenu o PGPmenu (para usuarios de Mac OS 7), o arrastrando el archivo o volumen y soltándolo sobre uno de los iconos de PGPtools.

Para acceder a las funciones de PGP utilizando PGPcontextmenu

1. Coloque el puntero sobre el archivo o volumen, en una ventana o en el escritorio.
2. Haga clic manteniendo pulsada la tecla Control.

   Aparece el menú contextual. Aparece PGP entre las opciones del menú.
3. Escoja una opción desde el menú PGP.

   Para cerrar el menú sin escoger ningún comando, haga clic fuera del menú.

Esta función está disponible en máquinas ejecutando MacOS 8 o posterior y es equivalente a lanzar y realizar las operaciones desde dentro de PGPtools.

PGPmenu trabaja de manera parecida para los usuarios de MacOS 7.

Definiciones de los iconos de PGPkeys

La tabla siguiente muestra todos los mini iconos utilizados en la ventana de PGPkeys, junto con la descripción de lo que representan.

ICONO	SIGNIFICADO
	Una pareja de llaves modernas doradas representa su par de claves Diffie-Hellman/DSS, que consta de su clave privada y su clave pública.
	Una llave moderna dorada representa una clave pública Diffie-Hellman/DSS.
	Una pareja de llaves de esqueleto azules representa su par de claves RSA, que consta de su clave privada y su clave pública.
	Una llave de esqueleto azul representa una clave pública RSA.
	Cuando una llave está atenuada, la clave correspondiente no está disponible temporalmente para cifrar. Usted puede desactivar una clave en la ventana de PGPkeys, lo que previene que claves raramente usadas colapsen la caja de diálogo de Selección de Claves.
	Una llave cruzada por una línea roja indica que la clave se ha revocado. Los usuarios revocan sus claves cuando dejan de ser válidas o se han visto comprometidas de alguna manera. Una clave con una X roja sobre ella representa una clave corrupta o dañada.
	Una llave con un reloj indica que la clave ha caducado. La fecha de caducidad de la clave se establece cuando se crea la clave.

ICONO	SIGNIFICADO
	Un sobre representa el propietario de la clave y lista los nombres de usuario y direcciones de correo electrónico asociadas con la clave.
	Un círculo vacío indica que la clave no es válida.
	Un círculo relleno indica que la clave es válida (verde) o que tiene una ADK (rojo).
	Un diamante indica que la clave es válida (verde) o que tiene una ADK (rojo).
	Un lápiz o una pluma indican la firma de los usuarios de PGP que han certificado la autenticidad de la clave. Una firma cruzada con una línea roja indica una firma revocada. Una firma con una X roja sobre ella indica una firma incorrecta o no válida. Una firma con una flecha azul próxima a ella indica que es exportable.
	Una barra vacía indica una clave no válida o un usuario no fiable.
	Una barra medio llena indica una clave marginalmente válida o un usuario marginalmente fiable.
	Una barra completa indica una clave completamente válida o un usuario completamente fiable.

Capítulo 3

Crear e Intercambiar Claves

Este capítulo describe cómo generar los pares de claves pública y privada que usted necesitará para corresponderse con otros usuarios de PGP. También explica cómo distribuir su clave pública y cómo conseguir las claves públicas de otros para poder empezar a intercambiar correo electrónico privado y autentificado.

Conceptos sobre claves

PGP se basa en un sistema de *cifrado por clave pública* de amplia aceptación y alta fiabilidad por el cual usted y otros usuarios de PGP generan un par de claves consistente en una clave privada y una clave pública. Como su nombre indica, sólo usted tiene acceso a su clave privada, pero para corresponderse con otros usuarios de PGP usted necesita una copia de la clave pública de esos usuarios y ellos necesitan una copia de la de usted. Usted utiliza su clave privada para firmar los mensajes de correo electrónico y los archivos adjuntos que usted envía a otros y para descifrar los mensajes y archivos que ellos le envían a usted. A la inversa, usted utiliza las claves públicas de otros para enviarles correo electrónico cifrado y para verificar las firmas digitales de ellos.

NOTA: Sin profundizar en detalles técnicos, a usted puede interesarle saber que realmente no es el contenido del correo electrónico lo que se cifra utilizando el esquema de cifrado por clave pública. En vez de eso, se cifran los datos utilizando un algoritmo mucho más rápido, de clave única, y es esta clave única la que en realidad se cifra utilizando la clave pública del destinatario. El destinatario después utiliza la clave privada de él para descifrar esta clave, lo que permite descifrar los datos cifrados.

Crear un par de claves

A menos que usted ya lo haya hecho utilizando otra versión de PGP, la primera cosa que necesita hacer antes de enviar o recibir correo electrónico cifrado y certificado es crear un nuevo par de claves. Un par de claves consta de dos claves: una clave privada que solamente usted posee y una clave pública que usted distribuye libremente a aquellos con quienes se corresponde. Usted genera un nuevo par de claves desde la ventana PGPkeys utilizando el Asistente de Generación de Claves de PGP, el cual le guía a través del proceso.

AVISO: Si usted se está actualizando desde una versión anterior de PGP, probablemente ya habrá generado una clave privada y habrá distribuido la clave pública recíproca a aquellos con quienes se corresponde. En este caso no tiene que crear un nuevo par de claves (como se describe en la sección siguiente). En vez de esto, usted especifica la posición de sus claves cuando ejecuta la aplicación PGPkeys. Puede ir al panel Archivos de la caja de diálogo de Preferencias e introducir el camino correcto a sus claves existentes en cualquier momento.

Para crear un nuevo par de claves

1. Escoja PGPkeys en PGPmenu.

   Se abre la aplicación PGPkeys.

2. Escoja Nueva en el menú Claves.

   El Asistente de Generación de Claves le proporciona alguna información introductoria en la primera pantalla.

3. Cuando acabe de leer esta información, haga clic en Siguiente para pasar a la siguiente caja de diálogo.

   El Asistente de Generación de Claves le pide que introduzca su nombre y su dirección de correo electrónico.

4. Introduzca su nombre en la primera línea y su dirección de correo electrónico en la segunda línea.

   No es estrictamente necesario que introduzca su nombre o su dirección de correo electrónico verdaderos. Sin embargo, utilizar su nombre verdadero facilita a otros el identificarle como el propietario de su clave

pública. Además, utilizando su dirección de correo electrónico correcta, usted y otros pueden aprovechar las ventajas de la funcionalidad de los módulos que automáticamente buscan la clave apropiada en su archivo de claves cuando usted envía correo a un destinatario concreto.

5. Haga clic en Siguiente para pasar a la siguiente caja de diálogo.

El Asistente de Generación de Claves de PGP le pide que especifique un tamaño para sus nuevas claves.

6. Seleccione uno de los tamaños de claves de 768 a 3072 bits, o introduzca un tamaño de clave personalizado entre 512 y 4096 bits.

NOTA: Un tamaño de clave personalizado puede invertir mucho tiempo para generarse, dependiendo de la velocidad del ordenador que esté usando. Los Macintosh antiguos con 68020 pueden tardar hasta un día en generar una clave de 4096 bits. El tiempo requerido para generar una clave es no determinístico, pero no debería llevar más que unos pocos minutos utilizando tamaños de clave estándares.

El tamaño de la clave corresponde al número de bits utilizados para construir su clave digital. Cuanto más grande sea la clave, menos posibilidades habrá de que alguien la reviente, pero llevarán más tiempo los procesos de cifrado y de descifrado. Usted debe buscar la solución de compromiso entre realizar con rapidez las operaciones de PGP con una clave pequeña y el nivel de seguridad mejorado que proporciona una clave más grande. A menos que usted esté intercambiando información extremadamente delicada que sea de suficiente interés para alguien como para que se decida a montar un costoso ataque criptográfico para leer esa información, usted estará seguro utilizando claves compuestas por 1024 bits.

NOTA: Cuando crea una clave Diffie-Hellman/DSS, el tamaño de la parte DSS de la clave se incrementa en cantidades constantes, es menor o igual que el tamaño de la parte Diffie-Hellman de la clave, y está limitado a un tamaño máximo de 1024 bits. La fortaleza de una clave de firmar DSS de 1024 bits es aproximadamente equivalente a la de una clave RSA de 2048 bits.

7. Haga clic en Siguiente para pasar a la caja de diálogo siguiente.

El Asistente de Generación de Claves de PGP le pide que indique cuándo debería caducar su par de claves.

8. Indique cuándo quiere que sus claves caduquen. Puede utilizar la opción por omisión, que es Nunca, o puede introducir una fecha específica después de la cual sus claves caducarán.

   Una vez haya creado un par de claves y haya distribuido su clave pública al mundo, usted probablemente continuará utilizando las mismas claves desde ese momento en adelante. Sin embargo, bajo determinadas condiciones usted puede querer crear un par de claves especial que planee usar solamente durante un período de tiempo limitado. En este caso, cuando la clave pública caduque, nadie más podrá utilizarla para cifrar correo para usted pero todavía podrá utilizarse para verificar su firma digital. De manera similar, cuando su clave privada caduca, todavía puede utilizarse para descifrar correo que le hayan enviado antes de que caducase su clave pública pero no puede volver a utilizarla para firmar correo para otros.

9. Haga clic en Siguiente para pasar a la caja de diálogo siguiente.

   El Asistente de Generación de Claves de PGP le pide que introduzca una *contraseña*.

10. En la caja de diálogo de Contraseña, introduzca la cadena de caracteres o palabras que quiera utilizar para mantener el acceso exclusivo a su clave privada. Para confirmar su entrada, pulse la tecla Tab para pasar a la línea siguiente y después escriba la misma contraseña otra vez.

11. Normalmente, como un nivel de seguridad añadido, los caracteres que usted introduce para la contraseña no aparecen en la pantalla. Sin embargo, si usted está seguro de que nadie está observando, y quiere ver los caracteres de la contraseña mientras escribe, borre la marca del cuadro Ocultar Tecleado.

SUGERENCIA:

Su contraseña debería tener múltiples palabras y puede incluir espacios, números y signos de puntuación. Escoja algo que usted recuerde fácilmente pero que otros no puedan adivinar. En la contraseña se distinguen mayúsculas de minúsculas. Las contraseñas fuertes incluyen letras mayúsculas y minúsculas, números, signos de puntuación y espacios. Cuanto más larga es la contraseña y mayor la variedad de caracteres que contiene, más segura es. Intente incluir la misma cantidad de caracteres alfabéticos en mayúsculas y en minúsculas, números, signos de puntuación y demás. La barra de calidad intenta sopesar la fortaleza de su contraseña comparada con la fortaleza de la clave que se está generando. Una barra completa indica que son más o menos equivalentes.

12. Haga clic en Siguiente para comenzar con el proceso de generación de claves.

El Asistente de Generación de Claves de PGP indica que está ocupado generando su clave.

Si ha introducido una contraseña inapropiada, aparecerá un mensaje de advertencia antes de generar las claves y usted tiene la opción de aceptar la contraseña mala o introducir una contraseña más segura antes de continuar.

Si no hay suficiente información aleatoria sobre la cual construir la clave, aparece la caja de diálogo de Datos Aleatorios de PGP. Como se le indica en la caja de diálogo, mueva su ratón por la pantalla e introduzca series de pulsaciones de teclas al azar hasta que la barra de progreso se rellene completamente. Los movimientos de su ratón y las teclas pulsadas generan información aleatoria que se necesita para crear un par de claves único.

Después de que comienza el proceso de generación de claves, puede llevar un rato generar las claves. De hecho, si usted especifica un tamaño diferente a los valores por defecto para una clave Diffie-Hellman/DSS, la opción de generación rápida de claves no se utiliza y puede llevar horas generar su clave con los tamaños más grandes. En algún momento el Asistente de Generación de Claves de PGP le indica que el proceso de generación de claves se completó.

NOTA: Las Versiones 5.0 y posteriores de PGP están constantemente recogiendo datos aleatorios de múltiples fuentes del sistema, incluyendo posiciones del ratón, tiempos, y pulsaciones de teclas. Si no aparece la caja de diálogo de Datos Aleatorios, indica que PGP ya ha recogido todos los datos aleatorios que necesita para crear el par de claves.

13. Haga clic en Siguiente para pasar a la caja de diálogo siguiente.

El Asistente de Generación de Claves de PGP indica que usted ha generado satisfactoriamente un nuevo par de claves y le pregunta si quiere enviar su clave pública a un servidor de claves.

14. Especifique si quiere que su nueva clave pública se envíe al servidor apropiado por el dominio del correo electrónico que usted introdujo y después haga clic en Siguiente.

Cuando usted envía su clave pública al servidor de claves, cualquiera que tenga acceso a ese servidor de claves puede conseguir una copia de su clave cuando la necesite. Para detalles completos, vea “Distribuir su clave pública,” más adelante en este capítulo.

Cuando el proceso de generación de claves se completa, aparece la caja de diálogo final.

15. Haga clic en Terminar.

Aparecerá un par de claves representando sus nuevas claves creadas en la ventana de PGPkeys. Notará que las viejas claves RSA son azules y las nuevas claves Diffie-Hellman/DSS son amarillas. En este lugar usted puede examinar las propiedades y atributos asociados a las claves; puede también añadir otras direcciones de correo electrónico que le pertenezcan. Vea el Capítulo 6 para detalles sobre cómo añadir un nuevo nombre de usuario.

Proteger sus claves

Una vez ha generado un par de claves, es interesante crear un par de repuesto y ponerlo en un lugar seguro por si acaso le ocurriese algo a los originales. PGP le invita a guardar una copia de seguridad cuando cierra la aplicación PGPkeys después de crear un nuevo par de claves.

Sus claves privadas y sus claves públicas se almacenan en archivos de claves separados, que usted puede copiar en otro lugar en su disco duro o en un

disquete como cualquier otro archivo. Por defecto, el archivo de claves privadas (Claves Privadas de PGP) y el archivo de claves públicas (Claves Públicas de PGP) se almacenan con los otros programas en la carpeta “Claves de PGP” dentro de la carpeta PGP 5.5, pero usted puede guardar sus copias de seguridad en cualquier lugar que desee.

Cuando usted especifica que quiere guardar una copia de seguridad de sus claves, aparece una caja de diálogo Guardar Como pidiéndole que especifique el lugar donde se crearán las copias de seguridad de los archivos de claves privadas y públicas.

Además de hacer copias de seguridad de sus claves, debería ser especialmente cuidadoso sobre dónde almacena su clave privada. Incluso aunque su clave privada está protegida por una contraseña que sólo usted debería conocer, es posible que alguien pueda descubrir su contraseña y después utilice su clave privada para descifrar su correo electrónico o falsificar su firma digital. Por ejemplo, alguien podría mirar sobre su hombro y observar las teclas que pulsa o interceptarlas en la red local o incluso en las ondas por el aire.

Para prevenir que cualquiera pueda hacerse con su contraseña y sea capaz de utilizar su clave privada, debería almacenar ésta última solamente en su propio ordenador. Si el ordenador está conectado a una red, debería además asegurarse de que sus archivos no se incluyen en una copia de seguridad del sistema donde otros puedan conseguir el acceso a su clave privada.

Si se da el caso en que los ordenadores están accesibles a través de redes y si está trabajando con información extremadamente delicada, puede querer guardar su clave privada en un disquete, el cual podrá introducir como una llave cuando quiera leer o firmar su correo privado.

Como otra precaución de seguridad, considere asignar un nombre diferente a su archivo de claves privadas y almacénelo en un lugar diferente a la carpeta de PGP donde no sea tan fácil de localizar. Puede utilizar el panel Archivos de la caja de diálogo de Preferencias de PGPkeys para especificar un nombre y posición para sus archivos de claves privadas y públicas.

Distribuir su clave pública

Después de crear sus claves, usted tiene que hacerlas accesibles a otros para que le puedan enviar correo electrónico cifrado y verificar su firma digital. Tiene tres alternativas para distribuir su clave pública:

- Hacer su clave pública disponible a través de un servidor de claves públicas.
- Incluir su clave pública en un mensaje de correo electrónico.
- Exportar su clave pública o copiarla en un archivo de texto.

Su clave pública se compone básicamente de un bloque de texto, así que es bastante fácil hacerla disponible a través de un servidor de claves públicas, incluirla en un mensaje de correo electrónico, o exportarla o copiarla en un archivo. El destinatario puede después utilizar aquel método que le resulte más conveniente para añadir su clave pública al archivo de claves públicas de él.

Hacer disponible su clave pública a través de un servidor de claves

El mejor método para hacer disponible su clave pública es colocarla en un servidor de claves públicas donde cualquiera pueda acceder a ella. De este modo, la gente puede enviarle correo electrónico sin tener que pedirle explícitamente una copia de su clave. También le libera a usted y a otros de tener que conservar un gran número de claves públicas que raramente utilizan. Hay cierto número de servidores de claves en el mundo, incluyendo aquellos ofrecidos por PGP, Inc. en los que usted puede dejar disponible su clave para que acceda cualquiera.

Si está utilizando PGP for Business Security, su Oficial de Seguridad generalmente preconfigurará sus opciones de servidores de claves para que todo trabaje correctamente en su empresa.

Para enviar su clave pública a un servidor de claves

1. Conéctese a Internet.
2. Abra la ventana PGPkeys.
3. Seleccione el icono que representa la clave pública que usted quiere mandar al servidor de claves.
4. Escoja Por Dominio en el submenú Enviar a Servidor del menú Claves.

Después de que usted coloca una copia de su clave pública en un servidor de claves, puede decir a las personas que quieran enviarle correo cifrado o verificar su firma digital que consigan una copia de su clave en el servidor.

Incluso si usted no les señala explícitamente su clave pública, ellos pueden conseguir una copia buscando su nombre o dirección de correo electrónico en el servidor de claves. Mucha gente incluye la dirección Web de su clave pública al final de sus mensajes de correo electrónico; en la mayoría de los casos el destinatario sólo hace doble clic en la dirección para acceder a una copia de su clave en el servidor.

Si algún día tiene que cambiar su dirección de correo electrónico, o si consigue firmas nuevas, todo lo que tiene que hacer para reemplazar su vieja clave es enviar una nueva copia al servidor; la información se actualiza inmediatamente. No obstante, debería tener en cuenta que los servidores de claves son capaces solamente de actualizar nueva información y no permitirán eliminar nombres de usuario o firmas de su clave. Si su clave se ve comprometida en algún momento, puede revocarla, lo que dice al mundo que ha dejado de confiar en esa versión de su clave. Vea el Capítulo 6 para más detalles sobre cómo revocar una clave.

Incluir su clave pública en un mensaje de correo electrónico

Otro método conveniente de entregar su clave pública a alguien es incluirla en un mensaje de correo electrónico.

Para incluir su clave pública en un mensaje de correo electrónico

1. Abra la ventana PGPkeys.
2. Seleccione su par de claves y después escoja Copiar en el menú Edición.
3. Abra el editor que usted utiliza para componer sus mensajes de correo electrónico, coloque el cursor en el área deseada, y después escoja Pegar en el menú Edición. En las aplicaciones modernas de correo electrónico, puede simplemente arrastrar su clave desde la ventana PGPkeys dentro del texto de su mensaje de correo electrónico para transferir la información de la clave.

Cuando envíe a alguien su clave pública, asegúrese de firmar el correo electrónico. De ese modo, el destinatario puede verificar su firma y estar seguro de que nadie ha alterado la información por el camino. Por supuesto, si su clave no está firmada por presentadores fiables, los

destinatarios de su firma sólo tendrán la certeza de que es de usted verificando la huella digital de su clave.

Exportar su clave pública a un archivo

Otro método de distribuir su clave pública es copiarla en un archivo y hacer accesible este archivo a la persona con quien usted quiere comunicar. Hay tres modos de copiar su clave pública en un archivo:

- Seleccione el icono que representa su par de claves en la ventana PGPkeys, después escoja Exportar en el menú Claves e introduzca el nombre y posición del archivo donde quiere que se guarde la clave.
- Arrastre el icono que representa su par de claves desde la ventana PGPkeys y suéltelo donde quiera que se guarde la clave.
- Seleccione el icono que representa su par de claves en la ventana PGPkeys, escoja Copiar en el menú Edición, y después escoja Pegar para insertar la información de la clave en un documento de texto.

AVISO: Si usted está enviando su clave a colegas que utilizan PCs, introduzca un nombre de como máximo ocho caracteres iniciales, seguidos de un punto, y tres caracteres adicionales para la extensión de tipo de archivo (por ejemplo, correo.txt).

Obtener las claves públicas de otros

Al igual que usted tiene que distribuir su clave pública a aquellos que quieren enviarle correo cifrado o verificar su firma digital, usted tiene que obtener las claves públicas de otros para poder enviarles correo cifrado o verificar las firmas digitales de ellos. Tiene tres alternativas para obtener la clave pública de alguien.

1. Conseguir la clave en un servidor de claves públicas.
2. Añadir la clave pública directamente desde un mensaje de correo electrónico.
3. Importar la clave pública desde un archivo.

Las claves públicas sólo son en realidad bloques de texto, así que son bastante fáciles de añadir a su archivo de claves importándolas desde un archivo o copiándolas desde un servidor de claves o mensaje de correo electrónico y después pegándolas en su archivo de claves públicas.

Conseguir claves públicas en un servidor de claves

Si la persona a quien quiere enviar correo cifrado es un usuario experimentado de PGP, lo más probable es que haya colocado una copia de la clave pública en un servidor de claves. Esto le resulta a usted muy conveniente para conseguir una copia de la clave de él lo más actualizada posible cuando quiera enviarle correo y también le libera de tener que almacenar un montón de claves en su archivo de claves públicas.

Con la Versión 5.5 de PGP, usted puede buscar claves en un servidor de claves utilizando estos criterios:

- ID de Usuario
- ID de Clave
- Tipo de Clave (Diffie-Hellman o RSA)
- Fecha de Creación
- Fecha de Caducidad
- Claves Revocadas
- Claves Desactivadas
- Tamaño de Clave
- Claves firmadas por una clave concreta

La inversa de la mayoría de estas operaciones también esta disponible. Por ejemplo, puede buscar utilizando como criterio “ID de Usuario no es Juan”.

Hay un cierto número de servidores de claves públicas, como el mantenido por PGP, Inc., donde usted puede localizar las claves de la mayoría de los usuarios de PGP. Si el remitente no le ha señalado la dirección Web donde se almacena su clave pública, usted puede acceder a cualquier servidor de claves y realizar una búsqueda del nombre de usuario o dirección de correo electrónico, porque todos los servidores de claves se actualizan con regularidad para incluir las claves almacenadas en todos los demás servidores. Con la Versión 5.5 de PGP, puede localizar rápidamente una clave de un usuario específico mientras envía correo electrónico o manipula sus claves desde la ventana PGPkeys.

Para conseguir la clave pública de alguien desde un servidor de claves

1. Abra la aplicación PGPkeys desde PGPmenu o haciendo doble clic en el icono de PGPkeys.
2. Escoja Buscar en Servidor en el menú Claves.

   Aparecerá la caja de diálogo de Buscar
3. Seleccione la localización del servidor en el que quiere buscar en el menú Buscar Claves.
4. Introduzca criterios de búsqueda para localizar la clave pública del usuario. Para limitar su búsqueda, haga clic en Más Opciones para especificar criterios adicionales.

   Si se encuentra la clave pública del usuario especificado, se le pregunta si quiere añadirla a su archivo de claves públicas. Cuando usted añade una clave pública a su archivo de claves, la clave se muestra en la ventana PGPkeys, donde puede examinarla para asegurarse de que es válida.

Añadir claves públicas desde mensajes de correo electrónico

Un modo conveniente de conseguir una copia de la clave pública de alguien es hacer que esa persona la incluya en un mensaje de correo electrónico. Si usted tiene una aplicación de correo electrónico soportada por los módulos de PGP, entonces puede añadir la clave pública del remitente a su archivo de claves públicas simplemente haciendo clic en un botón. Por ejemplo, cuando llega un mensaje de correo electrónico con un bloque de texto que contiene la clave pública de alguien, haga clic en el botón con la llave y el sobre para hacer que la clave se guarde en su archivo de claves públicas.

Si está utilizando una aplicación de correo electrónico que no está soportada por los módulos, puede añadir la clave pública al archivo de claves copiando el bloque de texto que representa la clave pública y pegándolo en la ventana PGPkeys.

Importar una clave pública desde un archivo

Otro método de obtener la clave pública de alguien es hacer que esa persona la guarde en un archivo desde el cual usted la pueda importar o copiar y pegar en su archivo de claves públicas. Hay tres métodos de extraer la clave pública de alguien y añadirla a su archivo de claves públicas.

- Escoja Importar en el menú Claves y después introduzca el nombre del archivo donde se encuentra la clave pública.
- Arrastre el archivo que contiene la clave pública sobre la ventana PGPkeys.
- Abra el documento de texto donde se almacena la clave pública, seleccione el bloque de texto que representa la clave y después escoja Copiar en el menú Edición. Vaya a la ventana PGPkeys y escoja Pegar en el menú Edición para copiar la clave. La clave se muestra como un icono en la ventana PGPkeys.

Verificar la autenticidad de una clave

Cuando usted intercambia claves con alguien, a veces es complicado decir si la clave pertenece realmente a esa persona. PGP proporciona un número de salvaguardas que le permiten comprobar la autenticidad de una clave y certificar que la clave pertenece a un propietario concreto. El programa PGP también le advierte si intenta utilizar una clave que no es válida y también le advierte por defecto cuando va a utilizar una clave de validez marginal.

Una de las mayores vulnerabilidades de los sistemas de cifrado por clave pública es la posibilidad de algún escucha oculto de montar un ataque de “hombre-en-el-medio” reemplazando la clave pública de alguien con otra propia. De este modo podrá interceptar cualquier mensaje de correo electrónico enviado a esa persona, descifrarlo utilizando la clave propia, después cifrarlo de nuevo con la clave real de la persona y enviarlo como si nada hubiera ocurrido. De hecho, esto podría hacerse todo automáticamente a través de un programa de ordenador sofisticado que se interpusiera y descifrara toda su correspondencia.

Basándose en esta escena, usted y aquellos con quienes intercambia correo electrónico necesitan un modo de determinar si realmente poseen copias legítimas de las claves de los demás. El mejor modo de estar completamente

seguro de que una clave pública pertenece realmente a una persona particular es que el propietario le entregue en mano una copia en un disquete. No obstante, usted pocas veces está suficientemente cerca de una persona para entregarle en mano un disco a alguien; usted generalmente intercambia claves públicas por correo electrónico o a través de un servidor de claves públicas.

A pesar de que estos son métodos algo menos seguros de intercambiar claves a prueba de alteraciones, usted puede aún determinar si una clave realmente pertenece a una persona concreta comprobando la firma digital de la clave, una serie única de números generados cuando se crea la clave. Comparando la huella digital en su copia de la clave pública de alguien con la huella digital de la clave original, usted puede estar absolutamente seguro de que sí tiene una copia válida de la clave de ese alguien.

La manera más definitiva de comprobar la huella digital de una clave es llamar a la persona y pedirle que le lea su huella digital por teléfono.

Una vez está absolutamente convencido de que tiene una copia legítima de la clave pública de alguien, puede firmar esa clave. Al firmar la clave pública de alguien con su clave privada, usted está certificando que está seguro de que la clave pertenece al usuario supuesto. Por ejemplo, cuando crea una nueva clave, ésta se certifica automáticamente con la propia firma digital, puesto que parece una suposición razonable que la persona que crea la clave es de hecho su verdadero propietario. La razón para firmar su propia clave es prevenir que cualquiera la modifique, lo que invalidaría inmediatamente su firma. Por defecto, las firmas que usted realiza en otras claves no son exportables, lo que significa que sólo se aplican a la clave mientras está en su archivo de claves local.

Conseguir claves a través de presentadores fiables

Los usuarios de PGP a menudo hacen que otros usuarios de confianza firmen sus claves públicas para atestiguar más adelante su autenticidad. Por ejemplo, usted puede enviar a un colega fiable una copia de su clave pública con una petición de que la certifique y se la devuelva para que pueda incluir la firma de él cuando usted envíe su clave a un servidor de claves públicas. Utilizando PGP, cuando alguien consigue una copia de su clave pública, no tiene que comprobar por él mismo la autenticidad de la clave, sino que puede basarse en cuánto se fían la persona o personas que firmaron la clave de usted.

PGP proporciona los medios para establecer este nivel de validez para cada una de las claves públicas que usted añade a su archivo de claves públicas y muestra el nivel de fiabilidad y el de validez asociados a cada clave en la ventana PGPkeys.

Esto significa que cuando usted consigue una clave de alguien y ésta está firmada por un presentador fiable, usted puede estar bastante seguro de que la clave pertenece al usuario supuesto. Para detalles sobre cómo firmar claves y validar usuarios, vea “Firmar la clave pública de alguien” en el Capítulo 6.

Su Oficial de Seguridad puede actuar como presentador fiable, y usted puede así fiarse de cualquier clave firmada con la clave corporativa como una clave válida. Si usted trabaja en una gran compañía con varias sucursales, puede tener presentadores regionales, y su Oficial de Seguridad puede ser un presentador intermediario, o un presentador fiable de presentadores fiables.

Capítulo 4

Enviar y Recibir Correo Electrónico Seguro

Este capítulo explica cómo cifrar y firmar el correo electrónico que usted envía a otros usuarios y descifrar y verificar los mensajes que otros le envían a usted.

Cifrar y firmar correo electrónico

La forma más rápida y fácil de cifrar y firmar correo electrónico es usar una aplicación soportada por los módulos de PGP. A pesar de que el proceso es ligeramente diferente para aplicaciones de correo electrónico distintas, puede realizar el cifrado y firma haciendo clic sobre los botones apropiados de la barra de herramientas de la aplicación.

Si está utilizando un programa de correo electrónico no soportado por los módulos de PGP, puede cifrar y firmar sus mensajes mediante PGPmenu, que es compatible con las aplicaciones basadas en texto más populares. Cuando accede a este menú desde el Finder, usted puede cifrar y firmar o descifrar y verificar archivos e incluso carpetas completas.

Como alternativa a otras interfaces, es posible utilizar también la ventana de PGPtools para cifrar y firmar texto y archivos. Cuando use esta interfaz para cifrar y firmar texto, debe copiar éste en el portapapeles, realizar la operación deseada utilizando el botón apropiado y seguidamente pegar el contenido de nuevo en la aplicación que usted estaba usando. Usted puede también cifrar y/o firmar una porción del texto o incluso archivos arrastrándolos sobre el botón apropiado.

NOTA: Si usted no envía inmediatamente su mensaje y en lugar de ello lo almacena en la bandeja de salida de su aplicación, debe ser consciente de que la información del mensaje no estará cifrada hasta que lo haya enviado realmente. Antes de poner en la cola mensajes cifrados, usted debe comprobar si su aplicación ha cifrado de hecho los mensajes de la bandeja de salida. Si no es así, es posible que usted quiera cifrar sus mensajes mediante PGPmenu antes de ponerlos a la cola en la bandeja de salida.

Si usted no posee una de la aplicaciones de correo electrónico que PGP soporta, vea el Capítulo 5 para informarse acerca de cómo cifrar y firmar archivos.

Cifrar y firmar mediante aplicaciones de correo electrónico soportadas por PGP

Cuando usted cifra y firma empleando una aplicación de correo electrónico que los módulos de PGP soportan, tiene dos posibilidades, dependiendo del tipo de programa de correo electrónico que el destinatario utilice. Si se está comunicando con otros usuarios de PGP que utilizan clientes de correo electrónico soportados por el estándar PGP/MIME, usted puede sacar partido de la función de PGP/MIME que le permite cifrar y firmar automáticamente sus propios mensajes de correo electrónico e incluso cualquier archivo vinculado a ellos en el momento en que los envía. Si por el contrario se está comunicando con alguien que no usa una aplicación de correo electrónico bajo el estándar PGP/MIME, usted deberá cifrar su correo electrónico con la función PGP/MIME desactivada para eliminar cualquier problema de compatibilidad.

Para cifrar y firmar utilizando aplicaciones de correo electrónico soportadas por PGP

1. Utilice su propio programa de correo electrónico para escribir el mensaje de la misma forma en que lo hace habitualmente.
2. Cuando haya finalizado de escribir el texto de su mensaje de correo electrónico, señale si quiere o no cifrar y firmar el texto de su mensaje haciendo clic sobre los botones que representan un candado y una pluma.

NOTA: Si usted sabe que usará PGP/MIME con regularidad, puede dejarlo activado seleccionando las opciones apropiadas desde la caja de diálogo de Preferencias.

3. Envíe su mensaje como habitualmente hace.

En caso de que haya elegido firmar los datos cifrados, aparecerá la caja de diálogo de Contraseña solicitando que escriba su contraseña antes de enviar el correo (En algunas aplicaciones este cuadro aparece antes.)

4. Escriba su contraseña y seguidamente haga clic en OK.

Si usted tiene una copia de las claves públicas para cada uno de los destinatarios, se usarán las clave apropiadas. Sin embargo, si usted especifica un destinatario para el que no se dispone de clave pública, aparecerá la caja de diálogo de Selección de Claves de PGP para que usted pueda especificar la clave apropiada.

5. Arrastre sobre el cuadro de listado de Destinatarios las claves públicas de aquellos usuarios que vayan a recibir una copia del mensaje de correo electrónico. Usted también puede hacer doble clic sobre cualquiera de las claves para moverlas de un área de la pantalla a otra.

El icono de Validez indica el nivel mínimo de confianza en que son válidas las claves públicas del listado de Destinatarios. Esta validez está basada en las firmas asociadas a la clave y la fiabilidad indica cuánto confía usted en el propietario de la clave para asegurar la autenticidad de las claves de otros usuarios. Vea el Capítulo 6 para más detalles.

6. Haga clic en OK para enviar su correo.

Cifrar correo electrónico para grupos de destinatarios

Usted puede usar PGP para crear listas de destinatarios. Por ejemplo, si usted desea enviar correo cifrado a 10 personas en ingenieria@xyz.com, usted podría crear un grupo con este nombre. El menú Ver contiene la opción Grupos que hace aparecer o desaparecer la sección Grupos de la ventana de PGPkeys.

Al usar la función de grupos, usted puede crear una lista de personas a las que desea enviar correo electrónico cifrado.

Para crear un grupo

1. Escoja Nuevo Grupo del menú Grupo.
2. Escriba un nombre para el Grupo. De forma opcional puede también escribir una descripción del grupo.
3. Por ejemplo, usted puede nombrar un grupo como "cualquiera@empresa.com" con la descripción "Todos los empleados."
4. Haga clic en OK para crear el grupo.

Para añadir miembros a un grupo

1. Seleccione en la ventana de PGPkeys los usuarios o grupos que usted desea añadir a su grupo.
2. Arrastre los usuarios desde la ventana de PGPkeys al panel de Grupos.

NOTA: Los grupos pueden también ser miembros de otros grupos.

Para borrar miembros de un grupo

1. Seleccione el miembro del grupo que debe ser borrado.
2. Pulse la tecla Borrar.

   PGP le pedirá que confirme su elección.

Para borrar un grupo

1. Seleccione el grupo desde el panel de Grupos de las ventanas de PGPkeys.
2. Pulse la tecla Borrar o escoja Borrar Grupos desde el menú desplegable.

Para añadir un grupo a otro grupo

1. Seleccione el grupo que usted desea colocar dentro de otro grupo.
2. Arrastre el grupo seleccionado encima del grupo en el que usted lo desea incluir.
3. Seleccione la opción Pegar sobre Grupo del menú desplegable.

Para enviar correo electrónico cifrado a grupos

1. Ponga como dirección de destino de su mensaje la de su grupo.

   El nombre de su grupo de cifrado debe corresponder con el nombre del grupo de correo electrónico.

2. Cifre el mensaje.

3. Envíe el mensaje.

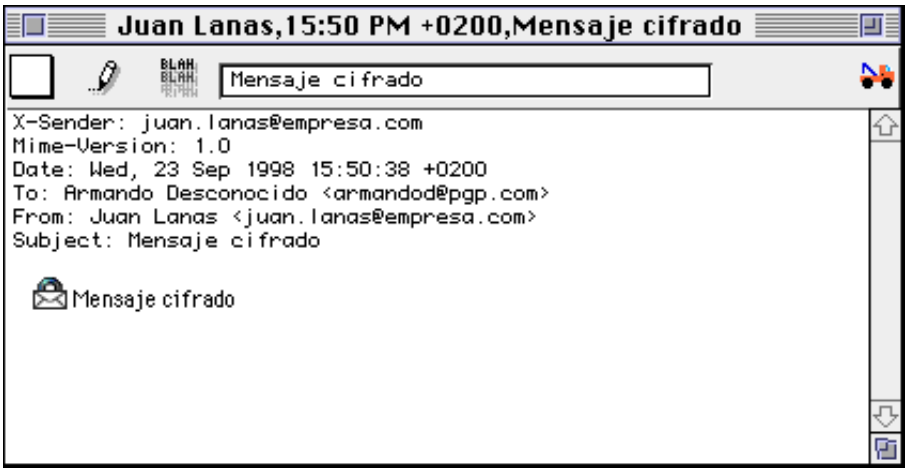
Descifrar y verificar correo electrónico

La manera más rápida y fácil de descifrar y verificar el correo electrónico que le envían es utilizando una aplicación soportada por los módulos de PGP. A pesar de que el procedimiento es ligeramente diferente para distintas aplicaciones de correo electrónico, cuando usted está usando una aplicación soportada por los módulos, usted puede realizar el proceso de descifrado y verificación haciendo clic sobre el icono que representa un sobre en el mensaje o en la barra de herramientas de su aplicación. Puede que usted necesite en algunos casos seleccionar Descifrar/Verificar desde el menú de su aplicación de correo electrónico. Además, si usted está utilizando una aplicación que soporta el estándar PGP/MIME, usted podrá descifrar y verificar tanto su propio correo electrónico como cualquier archivo adjunto simplemente con hacer clic sobre un icono asociado a su mensaje.

Si usted está utilizando una aplicación de correo electrónico que no está soportada por los módulos de PGP, deberá descifrar y verificar sus mensajes de correo electrónico mediante PGPmenu. Además, si su mensaje de correo electrónico incluye archivos cifrados, deberá descifrarlos de forma separada mediante PGPtools, PGPmenu en el Finder, o bien mediante el menú contextual de PGP de que disponen los usuarios de MacOS 8.

Descifrar y verificar desde aplicaciones de correo electrónico soportadas por PGP

Si usted se está comunicando con otros usuarios de PGP que han cifrado y firmado su correo usando el estándar PGP/MIME, aparecerá el icono de un sobre con candado en el mensaje que usted reciba.



En ese caso, usted puede descifrar y verificar el mensaje y cualquier archivo vinculado a él simplemente haciendo doble clic sobre dicho icono.

Si recibe correo electrónico de alguien que utiliza una aplicación que no sigue el estándar PGP/MIME, usted descifrará los mensajes de correo electrónico haciendo clic sobre el icono que representa un sobre abierto en la barra de herramientas de su aplicación o bien seleccionando Descifrar/Verificar desde el menú Módulos. Además, si también hay algún archivo adjunto cifrado, usted podrá descifrarlo desde PGPtools o desde PGPmenu en el Finder o bien, si es usuario de MacOS 8, desde el menú contextual de PGP.

Para descifrar y verificar desde aplicaciones de correo electrónico soportadas por PGP

1. Abra su mensaje de correo electrónico tal como hace habitualmente.

   Verá un bloque de texto cifrado totalmente incomprensible en el cuerpo de su mensaje de correo electrónico.

2. Para descifrar y verificar el contenido de este mensaje de correo electrónico, haga clic sobre el botón que representa un sobre abierto en la barra de herramientas de su aplicación.

NOTA: Si usted usa Eudora, deberá descifrar el texto escogiendo la opción Descifrar PGP del menú Módulos de Mensajes. Un atajo de teclado conveniente es mantener pulsada la tecla comando y a la vez pulsar el número 5.

Aparecerá el cuadro de diálogo Introducir Contraseña de PGP que le pedirá que escriba su contraseña.

3. Escriba su contraseña y seguidamente pulse OK.

El mensaje se descifra. Si además estaba firmado, aparecerá un mensaje indicando si la firma es válida.

4. En este punto usted puede guardar el mensaje descifrado, o bien puede guardar la versión original cifrada de forma que siga siendo segura.

Capítulo 5

Usar PGP para el Almacenamiento Seguro de Archivos

En este capítulo se describe cómo usar las funciones de PGP sin utilizar los módulos de correo electrónico. Se describe cómo usar PGP para cifrar y descifrar, así como también firmar y verificar la autenticidad de archivos desde el Finder usando PGPtools o PGPmenu de forma que usted pueda cifrar y firmar archivos tanto para correo electrónico como para almacenarlos de forma segura en su ordenador. También se describe la función Destruir de PGP que le permite eliminar archivos borrando completamente sus contenidos.

Usar PGP para cifrar y descifrar archivos

Puede usar PGP para cifrar y firmar archivos sin emplear ningún módulo de correo electrónico, de forma que usted los pueda enviar como archivos adjuntos a sus mensajes. También puede utilizar las técnicas que se describen en este capítulo para cifrar y firmar archivos almacenados en su ordenador.

Cifrar y firmar utilizando PGPmenu

Si tiene intención de enviar un archivo cifrado como documento adjunto a su mensaje o si quiere cifrar un archivo para protegerlo en su ordenador, puede usar PGPmenu.

Para cifrar y firmar utilizando PGPmenu

1. Seleccione desde el Finder el archivo o archivos que quiera cifrar, firmar, o cifrar y firmar.
2. Escoja la opción deseada desde el PGPmenu o desde el menú contextual de PGP, los usuarios de MacOS 8 pueden acceder pulsando la tecla Control a la vez que seleccionan el archivo.

   Aparecerá la caja de diálogo de Selección de Claves de PGP en la que puede seleccionar las claves públicas de los destinatarios del archivo que está cifrando o firmando.

   Dispone de las siguientes opciones de cifrado:

   - **Salida a Texto** Cuando envíe archivos adjuntos con alguna aplicación de correo electrónico, es posible que necesite seleccionar la opción Salida a Texto a fin de guardar el archivo como texto ASCII. Esto es necesario a veces cuando se envían archivos binarios utilizando aplicaciones de correo electrónico antiguas. Al seleccionar esta opción se aumenta el tamaño del archivo alrededor de un 30%.
   - **Cifrado Convencional** Seleccione esta opción para utilizar una contraseña común en lugar de criptografía por clave pública. El archivo se cifrará utilizando una clave que cifra mediante una contraseña escogida por usted.
   - **Destruir Original** Seleccione esta opción para sobreescribir el documento que está cifrando o firmando, de forma que la información delicada no pueda ser leída por nadie que tenga acceso a su disco duro.

   Si ha firmado los archivos, se le pedirá que proporcione su contraseña.
3. Seleccione las claves públicas arrastrándolas a la lista de Destinatarios y pulse OK.

   Si mira en la carpeta donde se encontraba el archivo original, encontrará un archivo con el mismo nombre seguido de un sufijo que indica el tipo de cifrado representado con uno de estos tres iconos:

.pgp

cifrado salida binaria

.asc

cifrado salida texto

.sig

firma separada binaria

Para cifrar y firmar utilizando PGPtools

1. Seleccione desde el Finder el archivo o archivos que quiere cifrar.

   Puede seleccionar varios archivos a la vez, pero deberá cifrar y firmar cada uno de ellos individualmente.

2. Arrastre el archivo o archivos sobre alguno de los botones: Cifrar, Firmar o Cifrar y Firmar, que se encuentran en la ventana de PGPtools.

3. Aparecerá la caja de diálogo de Selección de Claves de PGP, donde podrá escoger las claves públicas de los destinatarios del archivo que está cifrando o firmando. Las opciones disponibles se describen en "Descifrar y verificar utilizando PGPmenu".

4. Seleccione las claves públicas arrastrándolas a la lista de Destinatarios y haga clic en OK.

   El archivo se cifrará y/o firmará y el archivo resultante aparecerá en la misma carpeta que el original.

Descifrar y verificar utilizando PGPmenu

Si el correo electrónico que ha recibido tiene algún archivo vinculado y no está utilizando una aplicación de correo electrónico soportada por los módulos de PGP, deberá descifrarlo desde el Finder.

En primer lugar asegúrese de que dispone de PGPmenu.

Para descifrar y verificar utilizando PGPmenu

1. Seleccione desde el Finder el archivo o archivos que desea descifrar y verificar.

   Puede seleccionar varios archivos a la vez, pero deberá descifrarlos y verificarlos individualmente.

2. Escoja desde PGPmenu la opción Descifrar/Verificar o bien mantenga pulsada la tecla Control y seleccione el archivo para abrir el menú contextual de PGP, a continuación escoja Descifrar/Verificar desde el menú.

   Aparecerá la caja de diálogo de contraseña.

3. Escriba su contraseña y haga clic en OK.

Si el archivo está firmado, aparecerá un mensaje indicando si la firma es válida.

4. Haga clic en OK.

   El archivo descifrado se guardará en la misma carpeta que el original.

Para descifrar y verificar utilizando PGPtools

1. Seleccione desde el Finder el archivo o archivos que desea descifrar y verificar.

   Puede seleccionar varios archivos a la vez, pero deberá descifrarlos y verificarlos individualmente.

2. Arrastre el archivo sobre el botón Descifrar/Verificar de la ventana de PGPtools.

   Aparecerá la caja de diálogo de Introducción de Contraseña de PGP pidiéndole que introduzca su contraseña.

3. Introduzca su contraseña y a continuación haga clic en OK.

   Si el archivo está firmado, aparecerá un mensaje indicando si la firma es válida.

4. Haga clic en OK.

   El archivo descifrado se guardará en la misma carpeta que el original.

Utilizar Destruir de Forma Segura de PGP para borrar archivos

La opción Destruir de PGP borra los archivos y su contenido. La opción Destruir es una forma segura de eliminar permanentemente del disco duro un archivo y sus contenidos. Cuando borra un archivo de la forma habitual, tirándolo a la papelera, su nombre se borra del directorio de archivos pero los datos del archivo borrado aún están en el disco duro. Destruir elimina todo rastro de los datos del archivo, de forma que nadie podrá recuperar el archivo con herramientas software.

Para borrar permanentemente un archivo

1. Seleccione el archivo que desea borrar.
2. Seleccione Destruir desde PGPmenu.

Aparecerá una caja de diálogo de confirmación.

3. Haga clic en OK para borrar permanentemente el archivo

AVISO: Incluso en sistemas con memoria virtual, PGP escribe correctamente sobre todos los contenidos del archivo. Es preciso señalar la posibilidad de que las aplicaciones que hayan guardado el archivo antes de cifrarlo, hayan dejado fragmentos del mismo en lugares del disco duro que ya no se consideran parte del archivo. Véase "Archivos de intercambio o memoria virtual" en el Capítulo 8. Sea consciente también de que muchos programas hacen copias de seguridad mientras están utilizando los archivos de forma que pueden existir copias del mismo que desea borrar.
Es posible que quiera usar una utilidad de terceras partes para destruir todo el espacio libre de su disco duro para solucionar este problema. PGP no dispone por el momento de esta característica.

Capítulo 6

Manipular Claves y Establecer Preferencias

Este capítulo explica cómo examinar y gestionar las claves almacenadas en sus archivos digitales de claves. También describe cómo establecer las preferencias que se ajusten a su entorno de computación particular.

Manipular sus claves

Las claves que usted crea y aquellas que usted recoge de otros, se almacenan en archivos de claves, que son en esencia archivos almacenados en su disco duro o en un disquete. Normalmente sus claves privadas se almacenan en un archivo de nombre Claves Privadas PGP y sus claves públicas se almacenan en otro archivo de nombre Claves Públicas PGP. Estos archivos se encuentran normalmente en la carpeta Claves PGP.

NOTA: Si no se siente cómodo almacenando sus claves en el lugar usual puede escoger un nombre de archivo o un lugar diferentes. Para detalles, vea “Establecer sus preferencias,” más adelante en este capítulo.

Ocasionalmente, usted puede querer examinar o cambiar los atributos asociados con sus claves. Por ejemplo, cuando obtiene la clave pública de alguien, puede querer identificar su tipo (RSA o Diffie-Hellman/DSS), comprobar su huella digital, o determinar su validez basándose en las firmas digitales incluidas en la clave. Usted puede también querer firmar la clave pública de alguien para indicar que considera que es válida, asignar un nivel de fiabilidad al propietario de la clave, o cambiar una contraseña para su clave privada. Puede querer buscar la clave de alguien en un servidor de claves. Puede realizar todas estas funciones de manipulación desde la ventana PGPkeys.

La ventana PGPkeys

Para abrir la aplicación PGPkeys, escoja PGPkeys desde PGPmenu o haga doble clic en el icono de la aplicación en la carpeta del programa.

La ventana PGPkeys muestra las claves que usted mismo ha creado, y todas las claves públicas que ha añadido a su archivo de claves públicas.

Las llaves dobles representan los pares de claves privada y pública creados por usted, y las llaves simples representan las claves públicas que usted ha recogido de otros. Si tiene más de un tipo de clave, notará que las claves de tipo RSA son llaves de esqueleto azules y las claves Diffie-Hellman/DSS son llaves modernas amarillas.

Haciendo clic en el Triángulo de Revelación en el lado izquierdo del icono de llave, usted puede extender las entradas para revelar el ID de usuario y la dirección de correo electrónico del propietario de la clave tal como se representa en los iconos de la figura. Haciendo clic en el icono de sobre, puede ver las firmas de todos los usuarios que han certificado la clave, tal como representa uno de los cuatro iconos. Si no quiere extender cada clave individualmente, seleccione simplemente las claves de interés y escoja Extender Todo en el menú Edición.

Definiciones de los atributos de PGPkeys

A lo largo de la parte superior de la ventana hay etiquetas que corresponden a los atributos asociados con cada clave.

Nombre Muestra una representación en iconos de la clave junto con el nombre de usuario y dirección de correo electrónico del propietario, y los nombres de los firmantes de la clave.

Validez Indica el nivel de confianza en que la clave realmente pertenece al propietario supuesto. La validez se basa en quien ha firmado la clave y lo mucho que usted confía en el/los firmante(s) para afirmar la autenticidad de una clave. Las claves públicas que firma usted mismo tienen el nivel de validez más alto, basándose en el supuesto de que usted solamente firma la clave pública de alguien si está totalmente convencido de que es válida. La validez de cualquier otra clave, que no ha firmado personalmente, depende del nivel de fiabilidad que haya otorgado a los otros usuarios que la han firmado. Si no hay firmas

asociadas a la clave, entonces se considera no válida y aparece un mensaje indicando este hecho cuando se utiliza la clave.

La validez se indica con diamantes o barras con listas, indicando fiabilidad Implícita, y círculos o barras medio rellenas para fiabilidad Marginal. Cuando usted hace clic en un diamante o círculo, aparece la caja de diálogo de Firma de Claves, en la cual usted puede firmar las claves de otros usuarios. Vea “Firmar la clave pública de alguien,” más adelante en este capítulo.

La validez está representada por formas de puntos y de diamantes; o bien por formas de barras. Los diamantes representan validez implícita. Los círculos rellenos representan validez completa (o marginal si el cuadro Tratar Claves Marginalmente Válidas como Inválidas no está marcado en la lengüeta Avanzadas de la caja de diálogo de Preferencias). Los círculos vacíos representan no validez o validez marginal si el cuadro Tratar Claves Marginalmente Válidas como Inválidas está marcado.

Fiabilidad Indica el nivel de fiabilidad que usted ha otorgado al propietario de la clave para servir como un presentador de las claves públicas de otros. Esta fiabilidad entra en juego cuando usted no puede verificar personalmente la validez de la clave pública de alguien y en vez de eso se apoya en el juicio de otros usuarios que han firmado la clave. Cuando usted crea un par de claves, éste se considera de fiabilidad implícita, como muestran las listas en las barras de fiabilidad y validez, o por un diamante indicador de validez.

Cuando usted recibe una clave pública de alguien que se ha firmado con otra de las claves de usuario del archivo de claves públicas de usted, el nivel de autenticidad se basa en la fiabilidad que usted ha otorgado al firmante de esa clave. Usted asigna un nivel de fiabilidad, Completa, Marginal, o No Fiable, en la caja de diálogo de Propiedades de la Clave.

La fiabilidad no se muestra inicialmente en la ventana PGPkeys. Usted puede mostrar la columna Fiabilidad escogiendo Fiabilidad en el menú Ver. Haga clic en el

botón Validez en la ventana principal para abrir la caja de diálogo Firmar Clave. El botón Validez cambia a un diamante cuando una la clave es axiomáticamente fiable.

Si la Fiabilidad Implícita está activa, la fiabilidad se muestra con un diamante. Usted puede cambiar la fiabilidad mediante el menú de Propiedades de Claves. Las opciones de Fiabilidad son Ninguna, Marginal, y Completa.

Creación Muestra la fecha en que la clave fue creada originalmente. Usted puede a veces suponer la validez de una clave basándose en cuánto tiempo lleva en circulación. Si la clave ya lleva un tiempo en circulación, es menos probable que alguien intente reemplazarla porque hay muchas copias en circulación. Nunca se fíe de las fechas de creación como único indicador de validez.

Caducidad Muestra la fecha en que la clave caducará. En la mayoría de las claves es Nunca; sin embargo, hay circunstancias en las que usted puede querer utilizar una clave durante un período fijo de tiempo.

ADK (Clave Adicional de Descifrado)

Muestra cuándo la clave tiene una Clave Adicional de Descifrado. (Vea el Capítulo 2 para una definición.)

Tamaño Muestra el número de bits utilizados para construir la clave. Generalmente, cuanto mayor es la clave, menos posibilidades hay de que se vea comprometida. Sin embargo, las claves grandes requieren un tiempo ligeramente superior para cifrar y descifrar datos que las claves pequeñas. Cuando usted crea una clave Diffie-Hellman/DSS, hay un número para la porción Diffie-Hellman y otro número para la porción DSS. La porción DSS se utiliza para firmar, y la porción Diffie-Hellman para cifrar.

Examinar las propiedades de una clave

Además de los atributos generales mostrados en la ventana PGPkeys, usted también puede examinar y cambiar otras propiedades de las claves. Para acceder a las propiedades de una clave en particular, seleccione la clave deseada y después escoja Información en el menú Claves.

ID de la Clave Un número de identificación único asociado con esa clave. Este número de identificación es útil para distinguir entre dos claves que comparten el mismo nombre de usuario y dirección de correo electrónico.

Creada La fecha en la que la clave se creó.

Tipo de Clave El tipo de clave, RSA o Diffie-Hellman/DSS.

Caduca La fecha en que caduca la clave. Los propietarios especifican esta fecha cuando crean sus claves, y el valor se establece por lo general como Nunca. Sin embargo, algunas claves se dispone que caduquen en una fecha particular si el propietario quiere que se usen durante un período de tiempo limitado.

Tamaño El tamaño de la Clave.

Cifrado CAST, Triple DES, o IDEA. Este es el cifrado "preferido" con el cual el propietario de la clave pide que usted cifre para la clave de él o de ella. Si este algoritmo está permitido en sus preferencias Avanzadas, se utilizará cuando se cifre con esta clave.

Modelo de Fiabilidad

Indica la validez de la clave basándose en sus certificados y el nivel de fiabilidad que usted tiene en el propietario para afirmar la autenticidad de la clave pública de algún otro. Usted establece el nivel de fiabilidad arrastrando el dial de la barra al nivel apropiado (Completo, Marginal, o No Fiable). Esta barra está desactivada en claves revocadas, caducadas, e implícitamente fiables.

Activa Indica si la clave está ahora mismo activa. Cuando una clave está desactivada, aparece atenuada en la ventana PGPkeys y no está disponible para realizar funciones de PGP excepto Descifrar y Verificar. No obstante, la clave permanece en su archivo de claves y usted puede activarla de nuevo en cualquier momento. Para activar o desactivar una clave, marque o retire la marca del cuadro Activa. (El cuadro no está visible en claves implícitamente fiables.) Esta función es útil para prevenir que claves raramente utilizadas colapsen la caja de diálogo de Selección de Claves cuando usted está enviando correo electrónico cifrado.

Huella Digital Un número de identificación único que se genera cuando se crea la clave. Éste es el medio principal para comprobar la autenticidad de una clave. Una buena forma de comprobar una huella digital es hacer que el propietario le lea su huella digital por teléfono para que usted pueda compararla con la huella digital mostrada en la copia que usted tiene de la clave pública de él o de ella. También puede comprobar la autenticidad de la clave de alguien comparando la huella digital de la copia que usted posee con la que obtenga de un servidor de claves, puesto que se supone que el propietario la comprueba periódicamente para asegurarse de que es válida.

Cambiar Contraseña

Cambia la contraseña de una clave privada. Si usted piensa algún día que su contraseña no permanece en secreto (quizás usted sorprendió a alguien mirando sobre su hombro), haga clic en este botón para introducir una nueva contraseña.

Es buena idea cambiar la contraseña cada 6 meses o así. Para instrucciones sobre cambiar su contraseña, vea "Cambiar su Contraseña" más adelante en este capítulo.

Especificar un par de claves por defecto

Cuando usted firma un mensaje o la clave pública de alguien, se utiliza su par de claves por defecto. Si tiene más de un par de claves, puede querer designar específicamente un par como su par por defecto. El par de claves por defecto en este momento se muestra en negrilla para diferenciar esas claves suyas de otras.

Para especificar su par de claves por defecto.

1. Seleccione el par de claves que quiere designar como su par por defecto.
2. Escoja Establecer por Defecto en el menú Claves.

   El par de claves seleccionado se muestra en negrilla, indicando que ahora está designado como su par de claves por defecto.

Añadir un nuevo nombre de usuario o dirección

Usted puede tener más de un nombre de usuario o dirección de correo electrónico para los cuales quiera utilizar el mismo conjunto de claves. Después de crear un nuevo conjunto de claves, usted puede añadir nombres y direcciones alternativos a la clave. Sólo puede añadir un nuevo nombre de usuario o dirección de correo electrónico si tiene ambas claves, la pública y la privada.

Para añadir un nuevo nombre de usuario o dirección a una clave existente

1. Seleccione el par de claves al que quiere añadir otro nombre de usuario o dirección.
2. Escoja Añadir Nombre en el menú Claves.

   La caja de diálogo Nuevo Nombre de Usuario de PGP aparece.
3. Introduzca el nombre y la dirección de correo electrónico nuevos en los campos apropiados, y después haga clic en OK.

   La caja de diálogo Introducir Contraseña de PGP aparece.
4. Introduzca su contraseña y después haga clic en OK.

   El nuevo nombre se añade al final de la lista de nombres de usuario asociados con la clave. Si usted desea establecer el nuevo nombre de usuario y dirección como los identificadores principales de su clave, seleccione el nombre y la dirección y después escoja Establecer Nombre Principal en el menú Claves.

Comprobar la huella digital de una clave

A menudo es difícil tener la certeza de que una clave pertenece a un individuo en particular a menos que esa persona le entregue físicamente en mano la clave a usted en un disquete. Normalmente no es práctico intercambiar claves de esta manera, especialmente para usuarios que se encuentran separados muchas millas, pero usted puede basarse en la huella digital única asociada con cada clave para verificar que una clave realmente pertenece al propietario supuesto. Hay varios modos de comprobar una huella digital, pero el más seguro es llamar a la persona y pedirle que le lea su huella digital por teléfono. Es altamente improbable que alguien consiga

interceptar esta llamada aleatoria e imitar a la persona que usted espera oír al otro extremo del hilo. También puede comparar la huella digital en su copia de la clave pública de alguien con la que aparece para la clave original en un servidor público.

Para comprobar la huella digital de una clave

1. Seleccione la clave de la huella digital que quiere comprobar.
2. Escoja Información del menú Claves.
3. Anote la huella digital y compárela con la original.

Firmar la clave pública de alguien

Cuando usted crea un conjunto de claves, éste se firma automáticamente con su clave pública. De manera similar, cuando está seguro de que una clave pertenece al individuo apropiado, usted puede firmar la clave pública de esa persona, indicando que está seguro de que es una clave válida.

Para firmar la clave pública de alguien

1. Seleccione la clave que quiere firmar.
2. Escoja Firmar del menú Claves.

   La caja de alerta de PGPkeys aparece.
3. Haga clic en OK para indicar su certeza de que la clave afirmativamente pertenece al supuesto propietario.

   Aparece la caja de diálogo Introducir Contraseña.
4. Introduzca su contraseña y después haga clic en OK.

   Se incluye ahora un icono asociado a su nombre de usuario en la clave pública que acaba de firmar.

   Si le gustaría enviar la clave con su firma a un servidor de claves, marque el cuadro Enviar Firma a un Servidor de Claves. La clave pública en el servidor se actualiza para reflejar la inclusión de su firma. La mayoría de los usuarios prefieren utilizar su criterio para permitir a otros que firmen sus claves, así que es siempre buena idea comprobar con el propietario antes de añadir la firma de usted a la clave de él en un servidor.

Después se le pide que introduzca la contraseña para su par de claves por defecto.

5. Introduzca su contraseña y después haga clic en OK. Si quiere firmar con otro par de claves haga clic en la flecha de bajar y seleccione la clave deseada.

   Se muestra un cuadro que dice “Permitir que la firma se exporte. Otros podrán confiar en su firma.”

6. Marque este cuadro si quiere que su firma se exporte. Una firma exportable es una que puede enviarse a los servidores y viaja con la clave cuando se exporta, y también cuando se arrastra sobre un mensaje de correo electrónico.

   Cuando usted firma la clave pública de alguien, se muestra para esa clave un icono asociado a su nombre de usuario.

Otorgar fiabilidad para validaciones de claves

Además de certificar que una clave pertenece a alguien, usted puede asignar un nivel de fiabilidad al usuario de las claves indicando cuánto confía en esa persona para actuar como presentador de otros cuyas claves pueda conseguir en el futuro. Esto significa que si usted algún día consigue de alguien una clave que se haya firmado por un individuo al cual usted haya designado como de confianza, la clave se considera válida incluso aunque usted no la haya comprobado por sí mismo.

Para otorgar fiabilidad para una clave

1. Seleccione la clave a la cual quiere cambiar el nivel de fiabilidad.
2. Escoja Información en el menú Claves.

   Aparece la caja de diálogo de Información.

3. Utilice el dial de Nivel de Fiabilidad para escoger el nivel apropiado de fiabilidad para la clave: Nunca, Marginal, o Completo.
4. Cierre la caja de diálogo para aceptar los cambios.

Desactivar y activar claves

Algunas veces usted puede querer desactivar temporalmente una clave. La posibilidad de desactivar claves es útil cuando desea retener una clave pública para uso futuro, pero no quiere que le estorbe en la lista de destinatarios cada vez que envía correo.

Para desactivar una clave

1. Seleccione la clave que quiere desactivar.
2. Escoja Información en el menú Claves.

   Aparece la caja de diálogo de Información.
3. Retire la marca del cuadro Activa (El cuadro Activa no aparece en claves de fiabilidad implícita.)
4. Cierre el diálogo para aceptar los cambios.

La clave queda atenuada y temporalmente no disponible para uso.

Para activar una clave

1. Seleccione la clave que quiere activar.
2. Escoja Información del menú Claves.

   Aparece la caja de diálogo de Información.
3. Marque el cuadro Activa.
4. Cierre la caja de diálogo para aceptar los cambios.

La clave se vuelve visible y puede utilizarse como antes.

Borrar una clave o una firma

En algún momento usted puede querer eliminar una clave, una firma, o un ID de usuario asociados a una clave particular.

Para borrar una clave, firma, o ID de usuario

1. Seleccione la clave, firma, o ID de usuario que quiere borrar.
2. Escoja borrar del menú Edición o pulse la tecla Borrar.

Cambiar su Contraseña

Es buena idea cambiar su contraseña periódicamente.

Para cambiar su contraseña

1. Seleccione el par de claves al cual quiere cambiar la contraseña.
2. Escoja Información del menú Claves.

   Aparece la caja de diálogo de Información.
3. Haga clic en Cambiar Contraseña.

   Aparece la caja de diálogo de Cambiar Contraseña.
4. Introduzca su vieja contraseña en el campo superior y después pulse la tecla Tab para pasar al siguiente campo.
5. Introduzca su nueva contraseña en la caja de diálogo central y después pulse la tecla Tab para pasar al campo inferior.
6. Confirme su entrada introduciendo otra vez su nueva contraseña.
7. Haga clic en OK.

Importar y Exportar Claves

Aunque usted por lo general distribuya sus claves públicas y obtenga las claves públicas de otros cortando y pegando el texto desde un servidor de claves público o corporativo, usted también puede intercambiar claves importándolas y exportándolas como archivos de texto separados. Por ejemplo, alguien puede entregarle en mano un disco que contenga la clave pública de esa persona, o usted puede querer hacer su clave pública disponible en un servidor FTP.

Para importar una clave desde un archivo

1. Escoja Importar en el menú Claves.

   Aparece la caja de diálogo de Importar.
2. Seleccione el archivo que contiene la clave que quiere importar y después haga clic en Abrir.
3. Seleccione la clave o claves que quiere importar y haga clic en el botón Importar.

La clave importada aparece en la ventana PGPkeys. Después usted ya puede utilizarla para cifrar datos o para verificar la firma digital de alguien.

Para añadir una clave desde un mensaje de correo electrónico

Si un colega le envía un mensaje de correo electrónico con la clave de él incluida (como un bloque de texto) usted puede añadirla a su archivo de claves.

1. Con la ventana del mensaje de correo electrónico abierta, abra la ventana PGPkeys.
2. Acomode las dos ventanas de manera que pueda ver parte de la ventana PGPkeys detrás de la ventana del mensaje.
3. Seleccione el texto de la clave, incluyendo los textos START BLOCK y END BLOCK. Arrastre el texto sobre la ventana PGPkeys.
4. La nueva clave o claves aparecen en la ventana PGPkeys.

Para exportar la clave a un archivo

1. Seleccione la clave que quiere exportar a un archivo.
2. Escoja Exportar en el menú Claves.

   Aparece la caja de diálogo de Exportar.
3. Introduzca el nombre del archivo al cual quiere que se exporte la clave y después haga clic en Guardar.

   La clave exportada se guarda en el archivo y en la carpeta especificados.

Revocar una clave

Si en algún momento se da la situación en que usted ya no se fía de su par de claves personal, puede emitir una revocación al mundo diciendo a todos que dejen de utilizar su clave pública. El mejor modo de hacer circular una clave revocada es colocarla en un servidor de claves públicas.

Para revocar una clave

1. Seleccione el par de claves a revocar.
2. Escoja Revocar del menú Claves.

   Aparece la caja de diálogo de Confirmación de Revocación.
3. Haga clic en OK para confirmar su intención de revocar la clave seleccionada.

   Aparece la caja de diálogo de Introducir Contraseña de PGP.
4. Introduzca su contraseña y después haga clic en OK.

   Cuando usted revoca una clave, el icono de la llave se cruza con una línea roja para indicar que ya no es válida.
5. Envíe la clave revocada al servidor y así todos sabrán que no deben usar su vieja clave.

Es posible que usted pueda olvidar algún día su contraseña. En ese caso nunca podría utilizar su clave de nuevo y no tendría modo de revocar su vieja clave cuando creara una nueva. Para protegerse contra esta posibilidad, usted puede crear una clave revocada haciendo una copia de su clave privada, revocando la copia, y guardando la copia revocada en lugar seguro. Después puede enviar la copia revocada a un servidor de claves públicas incluso si olvida la contraseña. No obstante, debería tener mucho cuidado con el lugar donde almacena la versión revocada de su clave. Si alguien consiguiera acceder a la clave revocada, podrían revocar su clave sin su aprobación.

Establecer sus preferencias

PGP está configurado para acomodarse a las necesidades de la mayoría de los usuarios, pero usted tiene la opción de ajustar algunos de los parámetros para ajustarlos a su entorno de computación particular. Usted especifica estos parámetros a través de la caja de diálogo de Preferencias, a la cual puede acceder escogiendo Preferencias en el menú Edición de PGPkeys.

Preferencias Generales

Usted especifica opciones generales de cifrado en el panel General.

Cifrar Siempre a la Clave por Defecto

Cuando esta opción está seleccionada, todos los mensajes de correo electrónico y archivos adjuntos que usted cifre con la clave de un destinatario también se cifran para usted utilizando su clave pública por defecto. Es útil dejar esta opción activa para tener la opción de descifrar los contenidos de cualquier correo electrónico o archivo que haya cifrado previamente.

Retener Contraseña de Descifrado

Esta opción especifica la cantidad de tiempo (en horas: minutos: segundos) que su contraseña de cifrar se almacena en la memoria de su ordenador. Si usted regularmente compone o lee varios mensajes de correo electrónico sucesivos, puede querer aumentar el tiempo que su contraseña se retiene para no tener que introducirla una y otra vez para andar con todo su correo. No obstante, recuerde que cuanto más tiempo se almacene su contraseña en la memoria de su ordenador, más tiempo tendrá un sofisticado pirata de acceder a esta información altamente comprometedora. La opción por defecto es 2 minutos, que es probablemente suficiente para realizar la mayoría de sus operaciones PGP sin tener que introducir su contraseña demasiadas veces, pero no suficientemente grande para que usted se marche y una atacante la encuentre en la memoria de su ordenador.

Retener Contraseña de Firmar

Esta opción especifica la cantidad de tiempo (en horas: minutos: segundos) que su contraseña de firmar se almacena en la memoria de su ordenador. Si usted regularmente compone o lee varios mensajes de correo electrónico sucesivos, puede querer aumentar el tiempo que su contraseña se retiene para no tener que introducirla una y otra vez para andar con todo su correo.

NOTA: Usar su contraseña de firmar se considera una grave amenaza en algunos casos porque un atacante puede suplantarle. Esta es la razón por la que las dos opciones de retención se manejan por separado. Los tiempos de retención comienzan y se reinicializan cada vez que usted firma un mensaje y se borra la contraseña de la memoria inmediatamente cuando el temporizador avisa. Esta retención está inactiva por defecto debido a las implicaciones de seguridad potencialmente complejas.

Generación Rápida de Claves

Cuando esta opción está seleccionada, se necesita menos tiempo para generar un nuevo par de claves Diffie-Hellman/DSS. Este proceso se acelera utilizando un conjunto de números primos calculados previamente en vez de realizar el lento proceso de crearlos desde cero cada vez que se genera una nueva clave. No obstante, recuerde que la generación rápida de claves sólo se implementa para los tamaños de clave fijos por encima de 1024 y por debajo de 4096 proporcionados como opciones cuando usted crea una clave, y no se utiliza cuando usted introduce algún otro valor. Aunque sería casi imposible para cualquiera romper su clave basándose en el conocimiento de estos números primos enlatados, alguien puede querer pasar el tiempo extra en crear un par de claves con el máximo nivel de seguridad.

La creencia general en la comunidad criptográfica es que utilizar números primos enlatados no va en detrimento de la seguridad para los algoritmos Diffie-Hellman/DSS. Si esta característica le hace sentir incómodo, puede desactivarla. Para más información, lea la FAQ colocada en las páginas web de PGP.

Avisar Antes de Destruir Archivos

Cuando esta opción está seleccionada, aparece una caja de diálogo antes de destruir un archivo para darle una última oportunidad de cambiar de idea antes de que PGP sobreescriba de forma segura los contenidos del archivo y los borre de su ordenador.

Preferencias de Archivos

Haga clic en la lengüeta Archivos para pasar al panel en el que usted especifica la posición de los archivos de claves utilizados para almacenar sus claves públicas y privadas.

Establecer Posición del Archivo de Claves Públicas

Muestra la posición actual y el nombre del archivo en que el programa PGP espera encontrar su archivo de claves públicas. Si planea almacenar sus claves públicas en un archivo con un nombre diferente o en algún otro lugar, usted especifica esta información aquí. La posición que usted especifica también se utilizará para guardar todas las copias de seguridad automáticas del archivo de claves públicas.

Establecer Posición del Archivo de Claves Privadas

Muestra la posición actual y el nombre del archivo en que el programa PGP espera encontrar su archivo de claves privadas. Si planea almacenar sus claves privadas en un archivo con un nombre diferente o en algún otro lugar, usted especifica esta información aquí. Algunos usuarios prefieren mantener sus archivos de claves privadas en un disquete, que insertan como una llave cuando necesitan firmar o descifrar datos. La posición que usted especifica también se utilizará para guardar todas las copias de seguridad automáticas del archivo de claves privadas.

Establecer Posición del Archivo de Semilla Aleatoria

Muestra la posición del archivo de Semilla Aleatoria. Algunos usuarios pueden desear mantener su archivo de Semilla Aleatoria en un lugar seguro para prevenir alteraciones. Este ataque es muy complicado y PGP tiene varias protecciones diferentes contra él.

Preferencias de Correo Electrónico

Haga clic en la lengüeta Correo para pasar al panel en el que usted especifica preferencias que afectan al modo en que las funciones PGP se implementan en su aplicación de correo electrónico particular. Recuerde que no todas las opciones pueden ser aplicables a su aplicación de correo electrónico particular.

Utilizar Cifrado PGP/MIME

Si usted está utilizando Eudora y activa esta opción, todos sus mensajes de correo electrónico y archivos adjuntos se cifrarán automáticamente al destinatario deseado. Esta opción no tiene efecto en otros cifrados que usted realice desde PGPmenu y no debería utilizarse si usted planea enviar correo electrónico a destinatarios que utilicen aplicaciones de correo electrónico que no soporten el estándar PGP/MIME. Utilizando Eudora, los archivos adjuntos siempre se cifrarán con independencia de esta opción, pero si el destinatario no tiene PGP/MIME, el proceso de descifrado será más manual.

Utilizar Firma PGP/MIME

Si usted está utilizando Eudora y activa esta opción, todos sus mensajes de correo electrónico y archivos adjuntos automáticamente incluyen su firma digital. Esta opción no tiene efecto en otras firmas que usted añada desde PGPmenu y no debería utilizarse si planea enviar correo electrónico a destinatarios que estén utilizando aplicaciones que no soporten el estándar PGP/MIME.

Interrumpir líneas en mensajes firmados en columna [ ]

Esta opción especifica el número de columna en el que se insertará un retorno de carro para recolocar el texto de su firma digital en la línea siguiente. Esta función es necesaria porque no todas las aplicaciones manejan la interrupción de líneas del mismo modo, lo que podría ocasionar que las líneas de sus mensajes firmados digitalmente se truncaran de un modo que no serían fácilmente legibles. La opción por defecto es 70, lo que previene problemas con la mayoría de las aplicaciones.

AVISO: Si usted cambia la opción de interrupción de texto en PGP, asegúrese de que es un número más bajo que el utilizado por su aplicación de correo electrónico. Si lo establece en la misma o superior longitud, se añadirán retornos de carro que invalidarán su firma PGP.

Preferencias de PGPmenu

Haga clic en la lengüeta PGPmenu para pasar al panel donde usted añade y elimina el PGPmenu de variadas aplicaciones.

Añadir Use esta opción para añadir el icono de PGP en la barra de menú de las aplicaciones que seleccione. Por ejemplo, haga clic en el botón Añadir y añada SimpleText a la lista de aplicaciones. El icono PGP se añade a la barra de menú, para que usted pueda firmar, cifrar, descifrar, y verificar el texto seleccionado en el documento.

El icono de PGP está disponible automáticamente en la barra de menús del Finder, para que usted pueda cifrar carpetas enteras desde el Finder. Simplemente seleccione la carpeta que quiere cifrar y después escoja Cifrar en PGPmenu.

Haciendo doble clic en un nombre de aplicación en las preferencias de PGPmenu aparece una caja de diálogo de Preferencias de PGPmenu Avanzadas para esa aplicación particular, que contiene opciones que pueden ayudarle si experimenta problemas de compatibilidad utilizando PGPmenu con alguna aplicación particular.

Eliminar Utilice esta opción para eliminar el icono de PGP de la barra de menús de aplicaciones que usted haya seleccionado previamente.

Preferencias de Servidores

Haga clic en la lengüeta Servidor para pasar al panel donde usted especifica las opciones para los servidores de claves que está utilizando.

Dominio Especifica el dominio de Internet (tal como “empresa.com”) para el servidor de claves públicas que usa PGP para enviar y recuperar claves públicas. Cuando envíe claves públicas a un servidor, este dominio se utiliza para buscar el servidor apropiado basándose en el dominio de la clave.

Puerto La dirección del puerto para el servidor de claves públicas. Usted debe introducir la dirección en un formato de URL completo, tal como

"http://pgpkeys.mit.edu:11371". El protocolo LDAP también se admite.

Establecer por Defecto

Especifica qué servidor utilizar si no se encuentra servidor para el dominio de la clave.

Preferencias Avanzadas

Haga clic en la lengüeta Avanzadas para pasar al panel en el que usted escoge las siguientes opciones.

Algoritmo de cifrado

Puede seleccionar el algoritmo de cifrado para sus claves PGP: CAST (por defecto), IDEA, Triple-DES. Si quiere utilizar IDEA o Triple-DES, debe seleccionarlo antes de generar sus claves.

CAST es un nuevo algoritmo en el que PGP y otros criptógrafos tienen mucha confianza, y Triple-DES es un algoritmo del Gobierno de EE.UU. que ha soportado la prueba del tiempo. IDEA es el algoritmo tradicionalmente utilizado en PGP. Para más información acerca de estos algoritmos, vea "Los algoritmos simétricos de PGP" en el Capítulo 8.

Hay dos razones por las que PGP le da la opción de cambiar los algoritmos de cifrado:

- Cuando se usa cifrado convencional, el cifrado seleccionado aquí se utiliza para cifrar.
- Cuando se crea una clave, el cifrado preferido se graba como parte de la clave para que otras personas usen ese algoritmo cuando cifren para usted.

AVISO: Utilice los cuadros CAST, IDEA, y Triple-DES sólo si ha decidido repentinamente que un algoritmo particular no es seguro. Por ejemplo, si usted se entera de que han reventado Triple-DES, puede deseleccionar ese cuadro y todas las nuevas claves que usted genere tendrán registrado que Triple-DES no puede utilizarse cuando se cifre para usted.

Mostrar Nivel de Validez Marginal

Utilice este cuadro para especificar si mostrar claves marginalmente válidas o simplemente mostrar la validez como sí o no. Círculos verdes indican que una clave es válida; grises indican que la clave no se ha validado, que no la ha firmado ningún presentador de confianza ni usted mismo.

Tratar claves marginalmente válidas como inválidas

Utilice este cuadro para especificar si tratar todas las claves marginalmente válidas como no válidas. Seleccionar esta opción provoca que aparezca la caja de diálogo de Selección de Claves cuando cifra con claves válidas marginalmente.

Buscar una clave

Usted puede buscar claves en archivos de claves locales y en servidores de claves remotos.

Para buscar la clave de un usuario

1. Abra la ventana PGPkeys.
2. Escoja Buscar en el menú Claves.

   Aparece la ventana de Búsqueda de PGPkeys.
3. Escoja el lugar dónde desea buscar en el menú de Buscar Claves En.
4. Especifique sus criterios de búsqueda:

   Por defecto es ID de Usuario, pero puede hacer clic en el menú para seleccionar ID de la Clave, Tipo de Clave, Fecha de Creación, Fecha de Caducidad, Estado de la Clave, o Tamaño de la Clave. Por ejemplo, podría buscar todas las claves con ID de Usuario Juan.
5. Especifique la condición que está buscando.

   Puede especificar una de las condiciones siguientes:

   - Es
   - No Es
   - Contiene

- No Contiene
- Está Firmada Por
- No está Firmada Por
- En (para Fechas de Creación o Caducidad)
- En o Antes de (para Fechas de Creación o Caducidad)
- En o Después de (para Fechas de Creación o Caducidad)

6. Introduzca el valor que quiera buscar.

7. Haga clic en Más Opciones para añadir criterios adicionales a su búsqueda; por ejemplo, IDs de Clave con el nombre Juan creadas en o antes del 6 de octubre de 1997.

8. Para comenzar la búsqueda, haga clic en Buscar.

Una barra de progreso de búsqueda aparece en la ventana.

NOTA: Para cancelar una búsqueda en progreso, haga clic en Detener Búsqueda.

Los resultados de la búsqueda aparecen en la ventana.

9. Haga clic en Borrar Encontrados para vaciar la ventana de búsqueda y eliminar sus criterios de búsqueda.

Capítulo 7

Solucionar Problemas de PGP

Este capítulo presenta información acerca de problemas potenciales y sugiere soluciones.

Error	Causa	Solución
No se encuentran claves privadas en su archivo de claves.	No hay claves privadas en su archivo de claves.	Genere su propio par de claves en PGPkeys.
El período de evaluación para cifrado y firma PGP ha pasado. Operación abortada.	El período de evaluación del producto ha expirado.	Descargue la versión freeware o compre la versión comercial del producto.
La librería de PGP se ha quedado sin memoria	El sistema operativo se ha quedado sin memoria	Cierre otros programas que estén en funcionamiento. Si no es suficiente, puede necesitar más memoria en su máquina.

Error	Causa	Solución
Se produjo un error abriendo o escribiendo datos en su archivo de claves o en el archivo de salida.	Un archivo que se necesitaba no se pudo abrir.	Asegúrese de que las opciones en sus Preferencias de PGP son correctas. Si ha borrado recientemente archivos en la carpeta donde instaló PGP es posible que tenga que reinstalar el producto.
Imposible realizar la operación debido a que este archivo es sólo de lectura o está protegido. Si usted almacena sus archivos de claves en medios removibles el cartucho puede no estar insertado.	Un archivo que se necesitaba está activo en sólo lectura o está en uso por otro programa.	Cierre otros programas que puedan estar accediendo a los mismos archivos que el programa que usted está ejecutando. Si conserva sus archivos de claves en disquete, compruebe que el disquete está en la disquetera.
Se produjo un error al escribir el archivo de claves o el archivo exportado.	El programa falló al escribir datos en algún archivo.	Su disco duro puede estar lleno, o si el archivo está en un disquete, puede que no esté el disquete en la disquetera.
La acción no se puedo completar debido a una operación de archivo inválida.	El programa falló al leer o escribir datos en algún archivo.	Probablemente está corrupto el archivo. Intente cambiar sus Preferencias de PGP para utilizar un archivo diferente, si es posible.

Error	Causa	Solución
La contraseña que usted introdujo no coincide con la contraseña de la clave.	La contraseña que usted introdujo es incorrecta.	Usted puede tener activo BLOQUEO DE MAYÚSCULAS, o puede haber tecleado mal la contraseña. Inténtelo otra vez.
El archivo de claves contiene un paquete PGP malo (corrupto).	El mensaje PGP con el que usted está trabajando se ha corrompido, o su archivo de claves se ha corrompido.	Pida al remitente que le vuelva a enviar el mensaje si es un mensaje con lo que trabaja. Si es su archivo de claves, intente recuperarlo desde su copia de seguridad de los archivos de claves.
No se añadió el usuario especificado porque ya existía en la clave seleccionada.	Usted no puede añadir un ID de Usuario a una clave si ya existe uno idéntico en la clave.	Intente añadir un ID de usuario diferente, o borre el que coincide inicialmente.
Esta clave ya está firmada por la clave de firmar especificada.	No puede firmar una clave que ya ha firmado.	Usted puede haber escogido una clave equivocada. Si es así, escoja una clave diferente para firmar.
La clave especificada no aparece en su archivo de claves.	La clave necesaria para descifrar el mensaje actual no está en su archivo de claves.	Pida al remitente que le vuelva a enviar el mensaje y asegúrese de que le cifra el mensaje con la clave pública de usted.
El mensaje o archivo de datos contiene una firma suelta.	La firma del mensaje/archivo está en un archivo separado.	Haga doble clic en el archivo de firma separado antes.

Error	Causa	Solución
No se pudo cifrar con la clave especificada porque es una clave sólo para firmar.	La clave especificada sólo puede utilizarse para firmar.	Escoja una clave diferente, o genere una nueva clave que pueda cifrar datos.
No se puedo firmar con la clave especificada porque es una clave sólo para cifrar.	La clave seleccionada sólo puede utilizarse para cifrar.	Escoja una clave diferente, o genere una clave nueva que pueda firmar datos.
No hay suficientes datos aleatorios disponibles actualmente.	El generador de números aleatorios necesita más datos de entrada para generar números aleatorios correctos.	Cuando se le pida, mueva el ratón, o pulse teclas al azar, para generar datos de entrada.
El archivo de entrada especificado no existe.	El nombre de archivo tecleado no existe.	Utilice el Explorador para encontrar el nombre y ruta exactos para el archivo que desea.
No se puede realizar la operación requerida porque el buffer de salida es demasiado pequeño.	La salida es mayor de lo que los buffers internos pueden gestionar.	Si usted está cifrando o firmando, puede tener que partir el mensaje y cifrar/firmar trozos más pequeños cada vez. Si usted está descifrando o verificando, pida al remitente que cifre/firme trozos más pequeños y se los vuelva a enviar.

Error	Causa	Solución
El archivo de claves está corrupto.	El programa falló al leer o escribir datos en algún archivo.	Hay un archivo que probablemente está corrupto o no aparece. Puede ser o no un archivo de claves. Intente utilizar un nombre o ruta de archivo diferentes, si es posible.

Capítulo 8

Aspectos de Seguridad y Vulnerabilidades

Este capítulo contiene información introductoria y de fondo, escrita por Phil Zimmermann, acerca de criptografía.

"Lo que usted haga será insignificante, pero es muy importante que lo haga." —Mahatma Gandhi.

Por qué escribí PGP

Es personal. Es privado. Y no es asunto de nadie más que de uste. Puede estar planeando una campaña política, discutiendo acerca de sus impuestos o teniendo un romance secreto. O puede estar comunicándose con un disidente político de un país represivo. Lo que quiera que sea, usted no desea que su correo electrónico privado o documentos confidenciales los lea nadie más. No hay nada malo en afirmar sus derechos a la intimidad. La intimidad es tan legítima como la Constitución.

El derecho a la intimidad está implícitamente recogido a lo largo de toda la Carta de Derechos. Pero cuando se estableció la Constitución de los Estados Unidos, los Padres Fundadores no vieron la necesidad de expresar explícitamente el derecho a tener una conversación privada. Esto hubiese sido una bobada. Hace doscientos años, todas las conversaciones eran privadas. Si alguien más estuviera a distancia de oído, usted simplemente podría irse tras el granero y tener allí su conversación. Nadie podía escuchar sin su conocimiento. El derecho a una conversación privada era un derecho natural, no sólo en el sentido filosófico, sino en un sentido de ley física, dada la tecnología de la época.

Pero con la llegada de la era de la información, comenzando con la invención del teléfono, todo eso cambió. Ahora la mayoría de nuestras conversaciones tienen lugar electrónicamente. Esto permite que nuestras

conversaciones más íntimas sean expuestas a la luz sin nuestro conocimiento. Las llamadas de los teléfonos móviles puede monitorizarlas cualquiera que tenga una radio. El correo electrónico, enviado por Internet, no es más seguro que las llamadas por teléfono móvil. El correo electrónico está reemplazando rápidamente al correo postal y se convierte en la norma para todo el mundo, no la novedad que era en el pasado. Y el correo electrónico puede ser escudriñado habitual y automáticamente en busca de palabras interesantes, a gran escala, sin ser detectado. Es como pescar con red de deriva.

Tal vez piense que su correo electrónico es lo bastante legítimo para que no sea necesario cifrarlo. Si realmente es un ciudadano cumplidor de la ley, sin nada que esconder, entonces ¿por qué no envía siempre su correo de papel en postales? ¿Por qué no someterse a controles antidroga a petición de cualquiera? ¿Por qué exigir una orden judicial para que la policía pueda registrar su casa? ¿Está intentando esconder algo? Si esconde su correo en sobres, ¿significa acaso que debe de ser un subversivo, un traficante de drogas, o tal vez un chiflado paranoico? ¿Tienen los ciudadanos cumplidores de la ley necesidad de cifrar su correo electrónico?

¿Y si todo el mundo creyese que los ciudadanos amantes de la ley deberían usar postales para su correo? Si un inconformista intentase afirmar su intimidad usando un sobre para su correo, atraería sospechas. Tal vez las autoridades abrirían su correo para ver qué ocultaba. Afortunadamente, no vivimos en esa clase de mundo, porque todos protegen la mayoría de su correo con sobres. Así que nadie levanta sospecha al reafirmar su intimidad con un sobre. Hay seguridad en los números. Análogamente, sería bonito si todo el mundo usase de forma habitual el cifrado para todos sus mensajes de correo electrónico, inocentes o no, de modo que nadie parecería sospechoso al afirmar su intimidad con correo electrónico cifrado. Piense en ello como una forma de solidaridad.

Hasta ahora, si el gobierno quería violar la intimidad de los ciudadanos de a pie, tenía que hacer un cierto gasto en dinero y trabajo para interceptar y abrir al vapor el correo de papel. O tenía que escuchar, y posiblemente transcribir, conversaciones telefónicas habladas, al menos antes de que el reconocimiento automático de voz estuviera disponible. Esta clase de onerosas escuchas no eran prácticas a gran escala. Solamente se hacía en casos importantes en los que parecía que valía la pena.

La Ley del Senado 266, una ley anticrimen de múltiples fines de 1991, tenía una inquietante medida escondida en su interior. Si esta resolución no vinculante se hubiese convertido en ley, habría forzado a los fabricantes de equipos para comunicaciones seguras a insertar “puertas trampa”

especiales en sus productos, para que el gobierno pudiese leer los mensajes cifrados de cualquiera. Decía “Es el sentimiento del Congreso que los proveedores de servicios de comunicaciones electrónicas y los fabricantes de los equipos para servicios de comunicaciones electrónicas se aseguren de que los sistemas de comunicaciones permitan al gobierno obtener los contenidos en texto no cifrado de voz, datos, y otras comunicaciones, cuando sea debidamente autorizado por la ley.” Era ésta la ley que me llevó a publicar PGP electrónicamente y gratis aquel año, poco antes de que esa medida fuese derrotada tras una vigorosa protesta de los grupos de libertades civiles y de la industria.

La Ley de Telefonía Digital de 1994 ordenaba que las compañías telefónicas instalasen puertos remotos de intercepción en sus conmutadores digitales de las centrales, creando con ello una nueva infraestructura tecnológica para las escuchas de “apuntar y pulsar el botón”, con lo cual los agentes federales ya no tendrían que salir a aplicar pinzas de cocodrilo a las líneas telefónicas. Ahora pueden sentarse en su oficina central de Washington y escuchar nuestras llamadas telefónicas. Por supuesto, la ley sigue exigiendo una orden judicial para una escucha. Pero, si bien la infraestructura tecnológica puede persistir durante generaciones, la ley y la política pueden cambiar de la noche a la mañana. Una vez que una infraestructura de comunicaciones, optimizada para la vigilancia, se ha establecido, un cambio en las condiciones políticas puede llevar a un abuso de este nuevo poder. Las condiciones políticas pueden variar con la elección de un nuevo gobierno, o quizá más abruptamente por un atentado contra un edificio federal.

Un año después de que se aprobase la ley sobre Telefonía Digital de 1994, el FBI reveló unos planes que requerían que las compañías telefónicas incorporasen en su infraestructura la capacidad de interceptar simultáneamente un uno por ciento de todas las llamadas telefónicas en todas las grandes ciudades de EE.UU. Esto representaría un aumento de más de mil veces respecto a los niveles anteriores en la cantidad de teléfonos que podrían ser interceptados. En años anteriores hubo solamente cerca de un millar de escuchas mediante orden judicial en los Estados Unidos cada año, a niveles federal, estatal y local combinados. Es difícil ver cómo el gobierno podría siquiera emplear suficientes jueces para firmar las órdenes de escuchas para un uno por ciento de todas las llamadas telefónicas, y mucho menos de contratar suficientes agentes federales para sentarse y escuchar todo ese tráfico en tiempo real. La única manera plausible de procesar ese volumen de tráfico es una aplicación masiva, estilo Orwell, de tecnología automatizada de reconocimiento de voz, buscando palabras clave interesantes o buscando la voz de un interlocutor en

particular. Si el gobierno no encuentra su objetivo en el primer uno por ciento de muestra, las escuchas pueden dirigirse a otro uno por ciento diferente, hasta que el objetivo se encuentre, o hasta que todas las líneas telefónicas se hayan registrado en busca de tráfico subversivo. El FBI dice que necesita esta capacidad para planificar de cara al futuro. Este plan provocó tal indignación que fue derrotado en el Congreso, al menos esta vez, en 1995. Pero el mero hecho de que el FBI pidiese siquiera estos amplios poderes es revelador de sus intenciones. Y la derrota de este plan no es tan tranquilizadora si se considera que la ley sobre Telefonía Digital de 1994 también fue derrotada la primera vez que fue presentada en 1993.

Los avances en la tecnología no permitirán el mantenimiento del status quo en lo que se refiere a la intimidad. El status quo es inestable. Si no hacemos nada, las nuevas tecnologías darán al gobierno nuevas capacidades de intercepción automática que Stalin no habría soñado jamás. La única manera de mantener la intimidad en la era de la información es la criptografía fuerte.

No tiene que desconfiar del gobierno para querer usar criptografía. Su empresa puede estar siendo escuchada por rivales comerciales, por el crimen organizado, o por gobiernos extranjeros. El gobierno francés, por ejemplo, es conocido por usar su aparato de inteligencia contra compañías norteamericanas para ayudar a las empresas francesas a seguir siendo competitivas. Irónicamente, las restricciones del gobierno de EE.UU. a la criptografía han debilitado las defensas de las empresas norteamericanas contra el espionaje extranjero y la criminalidad organizada.

El gobierno sabe cuán importante será el papel que la criptografía va a tener en la relación de poder con su pueblo. En Abril de 1993, la administración Clinton desveló una audaz política nueva de cifrado, la cual había sido desarrollada en la Agencia de Seguridad Nacional, [NSA, National Security Agency], desde el comienzo de la administración Bush. La piedra angular de esta iniciativa es un dispositivo de cifrado construido por el gobierno, llamado chip Clipper, que contenía un nuevo y secreto algoritmo de cifrado de la NSA. El gobierno ha estado intentando animar a la industria privada para que lo incorpore en todos sus productos de comunicaciones seguras tales como teléfonos seguros, faxes seguros, etc. La AT&T ha incorporado el Clipper en sus productos seguros de voz. El truco: en el momento de fabricarlos, cada chip Clipper se cargaría con una clave propia, y el gobierno se guardaría una copia en depósito. No hay que preocuparse, claro… el gobierno promete que solamente usará esas claves para leer sus mensajes “cuando esté debidamente autorizado por la ley.”

Por supuesto, para hacer a Clipper completamente efectivo, el siguiente paso lógico sería proscribir otras formas de criptografía.

El gobierno afirmó inicialmente que usar Clipper sería voluntario, que nadie estaría obligado a usarlo en vez de otras formas de criptografía. Pero la reacción popular contra el chip Clipper ha sido fuerte, más de lo que el gobierno podía anticipar. La industria de ordenadores ha proclamado al unísono su oposición a usar Clipper. El director del FBI Louis Freeh respondió a una pregunta en una conferencia de prensa en 1994 diciendo que si Clipper no conseguía ganarse el apoyo del público, y las escuchas del FBI se neutralizaban por procedimientos criptográficos no controlados por el gobierno, su agencia no tendría otra opción que la de buscar ayuda legislativa. Más tarde, durante las secuelas de la Tragedia de Oklahoma City, el Sr. Freeh testificó ante el Comité Judicial del Senado que la disponibilidad pública de la criptografía fuerte debe estar limitada por el gobierno (aunque nadie había sugerido que los terroristas hubiesen usado criptografía).

El Centro de Información sobre Intimidad Electrónica [EPIC, Electronic Privacy Information Center] obtuvo documentos reveladores gracias a la Ley sobre Libertad de Información. En un documento titulado “Cifrado: Amenaza, Aplicaciones y Soluciones Potenciales” y enviado al Consejo de Seguridad Nacional en Febrero de 1993, el FBI, la NSA y el Departamento de Justicia concluían que “Las soluciones técnicas, tal como están, sólo funcionarán si se incorporan en todos los productos criptográficos. Para asegurarse de que esto suceda, se necesitan leyes que exijan el uso de productos de cifrado aprobados por el gobierno, o la adhesión a los criterios de cifrado del gobierno.”

El gobierno tiene un historial que no inspira confianza acerca de que nunca van a abusar de nuestras libertades civiles. El programa COINTELPRO del FBI actuaba sobre grupos que se oponían a las políticas del gobierno. Espiaron al movimiento antibélico y al movimiento de derechos civiles. Interceptaron el teléfono de Martin Luther King Hijo. Nixon tenía su lista de enemigos. Después llegó el escándalo del Watergate. El Congreso parece ahora empeñado en pasar leyes para limitar nuestras libertades civiles en Internet. En ningún momento del siglo pasado ha estado la desconfianza del público contra el gobierno tan extendida a lo largo de todo el espectro político como lo está hoy.

Si queremos resistirnos a esta inquietante tendencia que tiene el gobierno de prohibir los sistemas criptográficos, una medida que podemos aplicar es usar sistemas criptográficos tanto como podamos mientras siga siendo legal. Cuando el uso de la criptografía fuerte se haga popular, será más

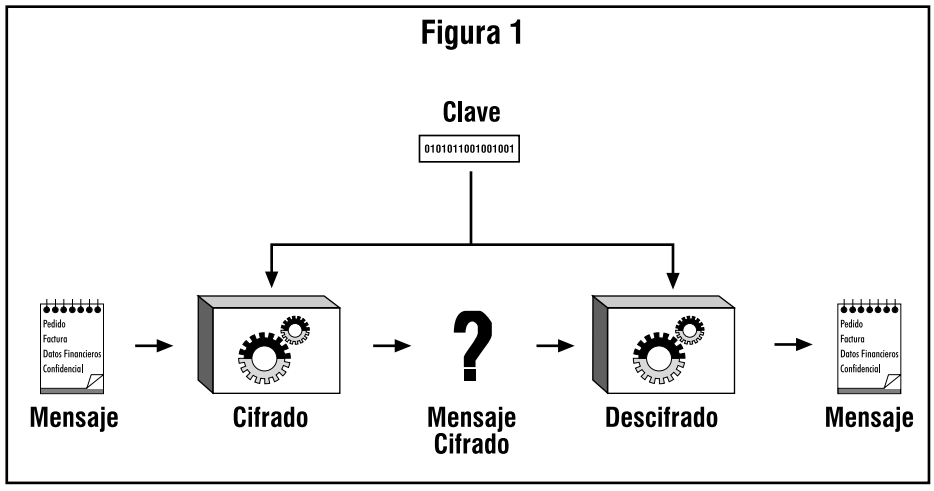
difícil para el gobierno ilegalizarlo. Por tanto, usar PGP es bueno para preservar la democracia.

Si la criptografía se ilegaliza, solamente los ilegales tendrán intimidad. Las agencias de inteligencia tienen acceso a buena tecnología criptográfica. También la tienen los grandes traficantes de armas y drogas. Pero la gente de a pie y las organizaciones políticas de base casi no han tenido acceso a tecnología criptográfica de clave pública de “calidad militar” y que se puedan permitir. Hasta ahora.

PGP da a la gente poder para tomar la intimidad con sus manos. Hay una creciente demanda social. Por eso lo creé.

Principios básicos del cifrado

Primero, algo de terminología básica. Supongamos que usted quiere enviar un mensaje a una colega, a quien llamaremos Alicia, y no quiere que nadie más que Alicia sea capaz de leerlo. Como muestra la Figura 1, puede cifrar el mensaje, lo que significa embrollarlo de manera harto complicada, y haciéndolo con ello ilegible para todos excepto usted y Alicia. Usted usa una clave criptográfica para cifrar y Alicia debe usar la misma clave para descifrar el mensaje. Al menos así es como funciona el cifrado convencional de “clave secreta”.



Se usa una única clave para el cifrado y para el descifrado. Esto significa que la clave debe transmitirse inicialmente por medio de canales de comunicación seguros para que ambas partes puedan conocerla antes de

que se envíen los mensajes cifrados por canales inseguros. Esto puede ser un inconveniente. Si usted tiene un canal seguro para intercambiar claves, ¿para qué necesita criptografía, para empezar?

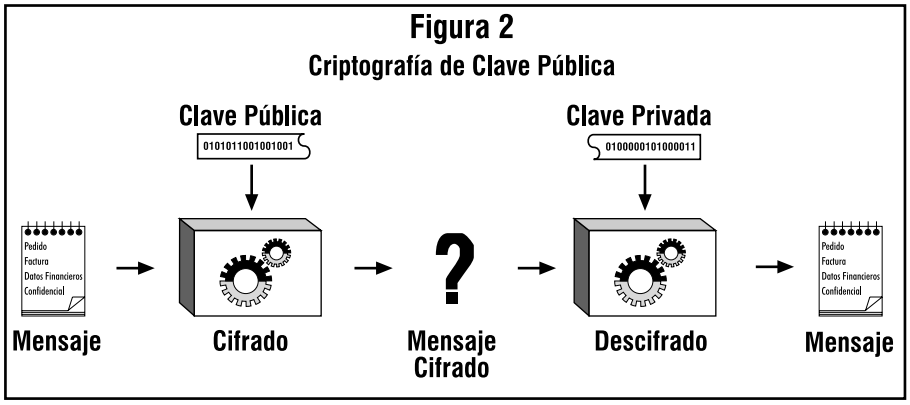
Cómo funciona la criptografía de clave pública

En la criptografía de clave pública, como se muestra en la Figura 2, todo el mundo tiene dos claves complementarias, una clave pública y una clave privada. Cada clave deshace el código que hace la otra clave. Conocer la clave pública no ayuda a deducir la clave privada correspondiente. La clave pública puede publicarse y diseminarse ampliamente a través de una red de comunicaciones.

Este protocolo proporciona intimidad sin necesitar canales seguros como los que requiere la criptografía convencional de clave secreta.

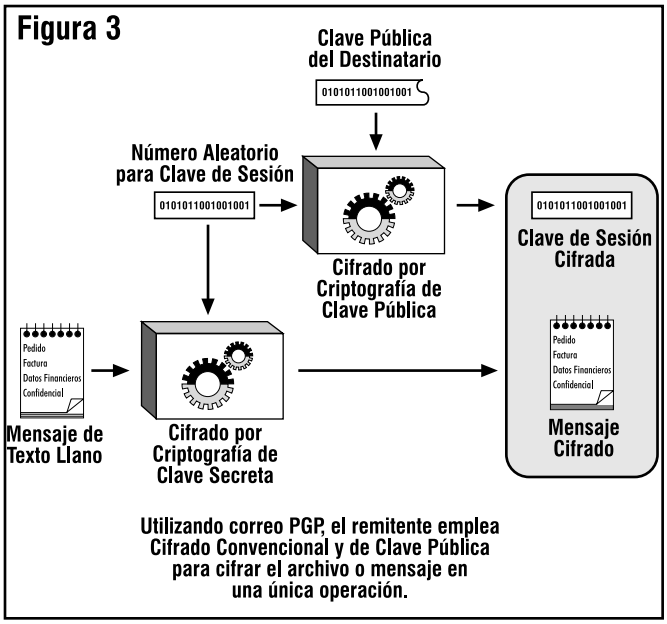
Cualquiera puede usar la clave pública del destinatario para cifrarle un mensaje a esa persona, y el destinatario usa la clave privada propia para descifrar ese mensaje. Nadie más que el destinatario puede descifrarlo, porque nadie más tiene acceso a esa clave privada. Ni siquiera la persona que cifró el mensaje con la clave pública del destinatario puede descifrarlo.

Figura 2
Criptografía de Clave Pública



Cómo se cifran sus archivos y mensajes

Debido al hecho de que el algoritmo de cifrado con clave pública es mucho más lento que el cifrado convencional de clave única, se logra un mejor cifrado por medio del proceso mostrado en la Figura 3.



Se usa un algoritmo de cifrado convencional mediante clave secreta, rápido y de alta calidad, para cifrar el mensaje. El mensaje original sin cifrar se llama “texto llano”. En un proceso invisible para el usuario, una clave aleatoria temporal, creada solamente para esta “sesión”, se usa para cifrar convencionalmente el archivo de texto llano. A continuación, la clave pública del destinatario se usa para cifrar esta clave convencional temporal. Esta “clave de sesión” convencional, cifrada mediante clave pública, se envía junto con el texto cifrado al destinatario.

Los algoritmos simétricos de PGP

PGP ofrece una selección de algoritmos en clave secreta para cifrar el mensaje real. Con algoritmo de clave secreta queremos decir un sistema de cifrado en bloque convencional, o simétrico, que usa la misma clave tanto para cifrar como para descifrar. Los tres cifrados simétricos en bloque ofrecidos por PGP son CAST, Triple-DES e IDEA. No son algoritmos “de mi cosecha”. Todos fueron desarrollados por equipos de criptógrafos reputados.

Para los curiosos en criptografía, los tres métodos de cifrado operan en bloques de 64 bits de textos llano y cifrado. CAST e IDEA tienen claves de 128 bits de tamaño, mientras que Triple-DES usa una clave de 168 bits. Al igual que el Estándar de Cifrado de Datos [DES: Data Encryption

Standard], cualquiera de estos tres métodos puede usarse en los modos de Retroalimentación de Cifrado [CFB, Cipher Feedback] y de Encadenado de Bloques de Cifrado [CBC, Cipher Block Chaining]. PGP los usa en modo CFB de 64 bits.

He incluido el algoritmo de cifrado CAST en PGP porque parece un prometedor sistema de cifrado en bloque con clave de 128 bits, es muy rápido y es gratuito. Su nombre se deriva de las iniciales de sus diseñadores, Carlisle Adams y Stafford Tavares, de la empresa Northern Telecom (Nortel). Nortel ha solicitado una patente para CAST, pero se ha comprometido por escrito a poner CAST a disposición de todo el mundo, libre de derechos de autor. CAST parece estar excepcionalmente bien diseñado por gente con buena reputación en su campo. El diseño está basado en una aproximación muy formal, con un cierto número de afirmaciones formalmente demostrables que ofrece buenas razones para creer que probablemente se precise agotar todas las claves posibles para reventar su clave de 128 bits. CAST no tiene claves débiles o semidébiles. Hay fuertes argumentos sobre que CAST es completamente inmune a los criptoanálisis lineal y diferencial, las dos formas de criptoanálisis más potentes conocidas en la literatura del tema y que han sido muy eficaces para romper el DES. CAST es demasiado nuevo para haber desarrollado un buen historial, pero su diseño formal y la buena reputación de sus diseñadores atraerán sin duda la atención y los ataques criptográficos del resto de la comunidad académica criptográfica. Tengo casi el mismo buen pálpito de confianza con CAST que el que tuve años atrás con IDEA, el método de cifrado que seleccioné para usarlo en versiones anteriores de PGP. En aquel momento, también IDEA era demasiado nuevo para tener un historial, pero ha aguantado bien.

El cifrado en bloque IDEA, de International Data Encryption Algorithm [Algoritmo Internacional para el Cifrado de Datos] está basado en el concepto de diseño de “mezclar operaciones de grupos algebraicos diferentes”. Fue desarrollado en la ETH de Zurich por James L. Massey y Xuejia Lau, y publicado en 1990. Algunos artículos publicados anteriormente sobre el algoritmo lo llamaban IPES, Propuesta de Estándar Mejorado de Cifrado [Improved Proposed Encryption Standard], pero posteriormente le cambiaron el nombre a IDEA. Hasta ahora, IDEA ha resistido ataques mucho mejor que otros métodos de cifrado como FEAL, REDOC-II, LOKI, Snefru y Khafre. IDEA es mucho más resistente que DES frente al altamente exitoso ataque mediante criptoanálisis diferencial de Biham y Shamir, así como ante ataques de criptoanálisis lineal. Conforme este sistema de cifrado continúa atrayendo esfuerzos de ataque por parte de los más formidables elementos del mundo criptográfico, la

confianza en IDEA está creciendo con el paso del tiempo. Lamentablemente, el mayor obstáculo para la aceptación de IDEA como estándar ha sido el hecho de que Ascom Systec tiene una patente sobre su diseño y, al contrario que DES y CAST, IDEA no se ha puesto a disposición del dominio público libre de derechos de autor.

Como añadido, PGP incluye Triple-DES, con tres claves, en su repertorio de cifrados en bloque disponibles. DES fue desarrollado por IBM a mediados de los setenta. Aunque tiene un buen diseño, su tamaño de clave de 56 bits es demasiado pequeño para los patrones de hoy. Triple-DES es muy fuerte y se ha estudiado bien durante muchos años, así que podría ser una apuesta más segura que los nuevos sistemas como CAST e IDEA. Triple-DES es DES aplicado tres veces al mismo bloque de datos, usando tres claves diferentes, excepto que la segunda operación DES se hace marcha atrás, en modo de descifrado. Si bien Triple-DES es mucho más lento que CAST o IDEA, la velocidad no suele ser un aspecto crítico para aplicaciones de correo electrónico. Aunque Triple-DES usa un tamaño de clave de 168 bits, parece tener una fortaleza efectiva de clave de al menos 112 bits frente a un atacante con una capacidad de almacenamiento de datos imposiblemente inmensa. Según un artículo presentado por Michael Weiner en Crypto96, cualquier cantidad remotamente plausible de almacenamiento de datos disponibles por el atacante podría permitir un ataque que exigiría tanto trabajo como romper una clave de 129 bits. Triple-DES no está cubierto por ninguna patente.

Las claves públicas PGP que fueron generadas por PGP versión 5.0 o posterior incorporan dentro de sí la información que cuenta a un remitente qué métodos de cifrado en bloque entiende el software del destinatario, de modo que el software del remitente sabe qué cifrado puede usarse para cifrar. Las claves públicas DSS/Diffie-Hellman aceptan CAST, IDEA o Triple-DES como métodos de cifrado en bloque, con CAST como opción por omisión. De momento, por razones de compatibilidad, las claves RSA no permiten esta selección. PGP solamente usa cifrado IDEA para enviar mensajes con claves RSA, ya que las versiones más antiguas de PGP aceptan solamente RSA e IDEA.

Compresión de datos

PGP suele comprimir el texto llano antes de cifrarlo, ya que es demasiado tarde comprimir el texto llano después de haberlo cifrado: los datos cifrados no son comprimibles. La compresión de datos ahorra tiempo de transmisión por módem, espacio de disco y, lo que es más importante, fortalece la seguridad criptográfica. La mayoría de las técnicas

criptoanalíticas explotan redundancias, que se encuentran en el texto llano, para romper el cifrado. La compresión de datos reduce esta redundancia en el texto llano, aumentando grandemente con ello la resistencia al criptoanálisis. Se necesita un tiempo extra para comprimir el texto llano, pero desde el punto de vista de la seguridad vale la pena.

Los archivos demasiado cortos para comprimir, o que simplemente no se comprimen bien, PGP no los comprime. Además de ello, el programa reconoce los archivos producidos por la mayoría de los programas populares de compresión, tales como PKZIP, y no intenta comprimir un archivo que ya está comprimido.

Para los curiosos en los aspectos técnicos, el programa usa las rutinas gratuitas ZIP escritas por Jean-Loup Gailly, Mark Adler y Richard B. Wales. Este software ZIP usa algoritmos de compresión funcionalmente equivalentes a los usados por PKZIP 2.x, de PKWare. Este software de compresión ZIP fue seleccionado para PGP fundamentalmente porque tiene una tasa de compresión muy buena y porque es rápido.

Sobre los números aleatorios usados como claves de sesión

PGP utiliza un generador criptográficamente fuerte de números pseudoaleatorios para crear claves temporales de sesión. Si este archivo “germen” [seed] no existe, se crea automáticamente y se carga con números auténticamente aleatorios derivados de eventos aleatorios, los cuales son recolectados por el programa PGP a partir de los cronometrajes de sus pulsaciones de teclado y movimientos del ratón.

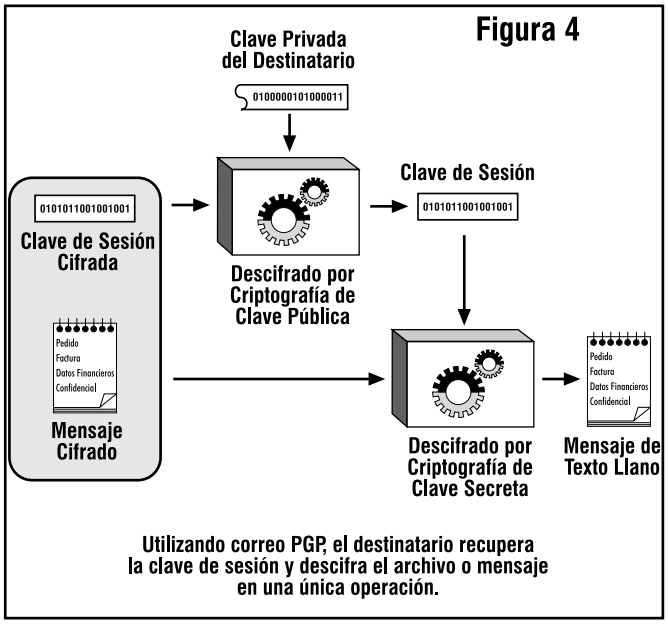
Este generador recarga el archivo germen cada vez que se usa, a base de mezclar nuevo material parcialmente derivado de la hora del día y otras fuentes verdaderamente aleatorias. Usa el algoritmo de cifrado convencional como medio de generar números aleatorios. El archivo germen contiene tanto material “germen” aleatorio como material aleatorio de clave usado como clave convencional de cifrado para el generador aleatorio.

Este archivo germen debe estar protegido contra revelación para reducir el riesgo de que un atacante pueda deducir la siguiente o la anterior clave de sesión. El atacante tendría un trabajo muy duro para obtener algo útil a partir de este archivo germen aleatorio, ya que el archivo se “lava” criptográficamente antes y después de cada uso. Ello no obstante, parece prudente intentar evitar que caiga en las manos equivocadas. Si es posible,

haga que el archivo solamente sea legible por usted. Si esto no es posible, no deje que otra gente copie indiscriminadamente discos desde el ordenador de usted.

Cómo funciona el descifrado

Como se muestra en la Figura 4, el proceso de descifrado es justamente el opuesto que el de cifrado. La clave privada del destinatario se usa para recuperar la clave temporal de sesión, y después esa clave de sesión se usa para activar el rápido algoritmo convencional de clave secreta que descifra el gran mensaje de texto cifrado.

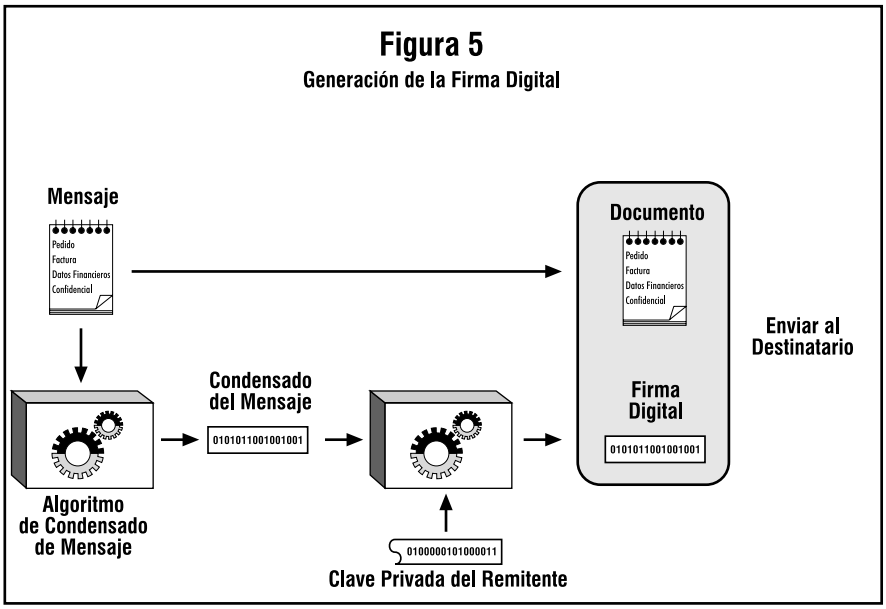


Cómo funciona el firmado digital

PGP usa firmas digitales para dotar al mensaje de autentificación. La propia clave privada del remitente puede usarse para cifrar un condensado del mensaje, “firmando” así el mensaje. Un *condensado de mensaje* [message digest] es una función “revoltillo” [hash] unidireccional, criptográficamente fuerte, de 160 o 128 bits. Es análogo a una “suma de comprobación” [checksum] o a un código de comprobación de errores CRC, en el sentido de que representa de modo compacto un mensaje y se usa para detectar cambios en el mismo. Al contrario que un CRC, sin

embargo, se cree que es computacionalmente inviable que un atacante consiga hacer un mensaje sustituto que produzca el mismo condensado de mensaje. El condensado de mensaje se cifra con la clave privada del remitente, creando así una firma digital del mensaje.

La Figura 5 muestra cómo se genera una firma digital.



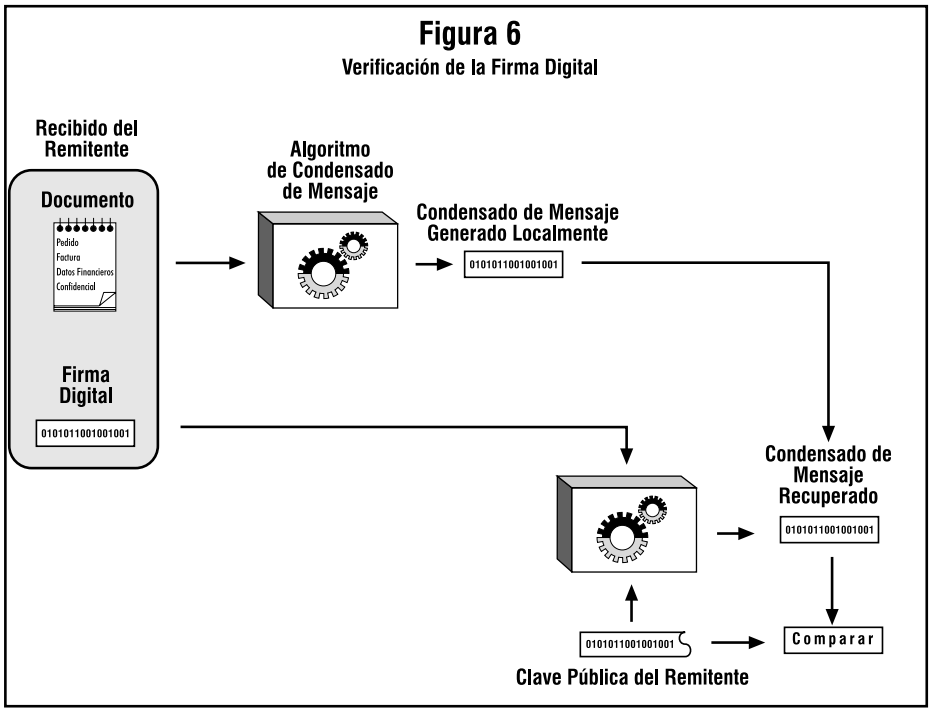
El destinatario (o cualquier otro) puede verificar la firma digital usando la clave pública del remitente para descifrarla, tal y como se muestran en la Figura 6. Esto demuestra que el remitente fue el auténtico originador del mensaje, y que el mensaje no lo ha alterado nadie posteriormente, ya que solamente el remitente posee la clave privada que hizo esa firma. No es posible una falsificación del mensaje, y el remitente no puede luego renegar de su firma.

Sobre el condensado de mensaje

El condensado de mensaje es un “destilado” compacto (160 bits o 128 bits) del mensaje o una suma de comprobación del archivo. Puedes pensar en ello como en una “huella dactilar” del mensaje o archivo. El condensado del mensaje “representa” su mensaje de tal manera que si el mensaje se alterase de cualquier modo, se computaría un condensado de mensaje diferente. Esto hace posible detectar cualquier cambio hecho al

mensaje por un falsificador. Un condensado de mensaje se computa usando una función revoltillo criptográficamente segura y unidireccional. Debería ser computacionalmente inviable para un atacante el construir un mensaje sustituto que produjese un condensado de mensaje idéntico. A este respecto un condensado de mensaje es mucho mejor que una suma de comprobación, porque es fácil hacer un mensaje diferente con la misma suma de comprobación. Pero, al igual que una suma de comprobación, no se puede deducir el mensaje original partiendo del condensado de mensaje.

Figura 6
Verificación de la Firma Digital



El algoritmo para el condensado de mensaje usado ahora en PGP (versión 5.0 y posteriores) se llama SHA, que significa Algoritmo Seguro de Revoltillo [Secure Hash Algorithm], diseñado por la NSA para el Instituto Nacional de Patrones y Tecnología, NIST [National Institute of Standards and Technology]. SHA es un algoritmo “revoltillo” [hash] de 160 bits. Algunas personas pueden considerar con suspicacia cualquier cosa que venga de la NSA porque la NSA está al mando de interceptar comunicaciones y romper códigos. Pero tengamos en mente que la NSA no tiene interés en falsificar firmas, y que el gobierno se beneficiaría de un buen estándar de firma digital no falsificable que evitaría que alguien repudiase sus firmas. Esto tiene distintos beneficios para los cuerpos de

seguridad y para recopilar información mediante espionaje. Asimismo, el SHA se ha publicado en la literatura abierta y lo han revisado extensamente la mayoría de los mejores criptógrafos del mundo que se especializan en funciones de revoltillo, y la opinión unánime es que SHA está extremadamente bien diseñado. Tiene algunas innovaciones de diseño que evita todas las debilidades observadas en algoritmos de condensado de mensaje previamente publicados por los criptógrafos académicos. Todas las nuevas versiones de PGP usan SHA como algoritmo de condensado de mensaje para crear firmas con las nuevas claves DSS que cumplen el Estándar de Firma Digital [Digital Signature Standard] del NIST. Por motivos de compatibilidad, las nuevas versiones de PGP todavía usan MD5 para firmas RSA, ya que las versiones antiguas de PGP usaban MD5 para firmas con RSA.

El algoritmo de condensado de mensaje usado por las versiones antiguas de PGP es el MD5, Algoritmo de Condensado de Mensaje [Message Digest Algorithm], puesto a disposición del público por RSA Data Security, Inc. MD5 es un algoritmo de revoltillo de 128 bits. En 1996, MD5 casi fue reventado por un criptógrafo alemán, Hans Dobbertin. Aunque MD5 no se rompió totalmente en ese momento, se descubrió que tenía tan serias debilidades que nadie debería seguir usándolo para generar firmas. Trabajos ulteriores en este campo puede que consigan romperlo totalmente, permitiendo que se falsifiquen firmas. Si usted no quiere encontrar algún día su firma digital PGP en una confesión falsa, sería un buen consejo que se cambiase a las nuevas claves DSS de PGP como su método preferido para hacer firmas digitales, porque DSS usa SHA como algoritmo de revoltillo seguro.

Cómo proteger las claves públicas contra alteraciones

En un criptosistema de clave pública usted no tiene que proteger sus claves públicas contra exposición. De hecho, es mejor que estén ampliamente diseminadas. Pero es importante proteger las claves públicas contra alteraciones para asegurarse que una clave pública realmente pertenece a la persona a la que parece pertenecer. Esta puede que sea la vulnerabilidad más importante de un criptosistema de clave pública. Vea “Proteger sus claves” en el Capítulo 3 para los procedimientos adecuados. Veamos primero un desastre potencial, para después describir cómo evitarlo con PGP.

Supongamos que usted quiere enviar un mensaje privado a Alicia. Descarga el certificado de clave pública de Alicia desde un sistema de tableros electrónicos BBS [Bulletin Board Service]. Cifra su carta a Alicia con esta clave pública y se la envía a través del sistema de correo electrónico del BBS.

Desafortunadamente, y desconocido por usted y por Alicia, otro usuario llamado Carlos se ha infiltrado en el BBS y ha generado una clave pública propia con el ID de Alicia adosado a ella. Coloca furtivamente su clave falsa en lugar de la clave pública real de Alicia. Sin darse cuenta, usted usa esta clave falsa, que pertenece a Carlos, en lugar de la clave pública de Alicia. Todo parece normal porque esta clave falsa tiene el ID de Alicia. Ahora Carlos puede descifrar el mensaje preparado originariamente para Alicia porque él tiene la clave privada correspondiente. Puede incluso volver a cifrar con la clave pública auténtica de Alicia el mensaje descifrado, y enviárselo a ella para que nadie sospeche de ninguna irregularidad. Más aún, puede incluso hacer firmas aparentemente correctas de Alicia con esta clave privada porque todo el mundo usará la clave pública falsa para comprobar la firma de Alicia.

La única manera de evitar este desastre es evitar que nadie altere las claves públicas. Si usted consiguió la clave pública de Alicia directamente de Alicia, esto no es problema. Pero esto puede resultar difícil si Alicia está a miles de kilómetros de distancia o no se encuentra disponible.

Tal vez usted podría obtener la clave pública de Alicia a partir de un amigo en el que ambos confíen, David, quien sabe que tiene una buena copia de la clave pública de Alicia. David podría firmar la clave pública de Alicia, respondiendo de la integridad de la clave pública de Alicia. David crearía esta firma con su propia clave privada.

Esto crearía un certificado de clave pública firmado, y mostraría que la clave de Alicia no se ha alterado. Esto requiere que usted tenga una copia buena de la clave pública de David para comprobar la firma de él. Quizá David podría también dar a Alicia una copia firmada de la clave pública de usted. David sirve así como un “Presentador” entre Alicia y usted.

Este certificado firmado de clave pública para Alicia podrían ponerlo David o Alicia en el BBS, y usted podría descargarlo más tarde. Después usted podría comprobar la firma por medio de la clave pública de David y así asegurarse de que esa es realmente la clave pública de Alicia. Ningún impostor puede engañarle haciéndole aceptar la clave falsa de él como si fuese de Alicia, porque nadie puede falsificar firmas hechas por David.

Una persona de confianza para muchas personas podría incluso especializarse en ofrecer este servicio de “presentación” mutua de usuarios por medio de firmas para sus certificados de clave pública. Esta persona de confianza podría considerarse una “Autoridad de Certificación”. Se podría confiar en que cualquier certificado de clave pública que llevase la firma de esta Autoridad de Certificación pertenezca realmente a la persona a la que parece pertenecer. Todos los usuarios que quisiesen participar necesitarían una copia de validez reconocida solamente de la clave pública de la Autoridad de Certificación, para que las firmas de la Autoridad de Certificación pudiesen verificarse. En algunos casos, la Autoridad de Certificación también puede actuar como servidor de claves, permitiendo que los usuarios de una red obtengan claves públicas pidiéndolas al servidor de claves, pero no hay razón por la que un servidor de claves deba también certificar claves.

Una Autoridad de Certificación centralizada de confianza es especialmente apropiada para instituciones gubernamentales o corporativas grandes, impersonales y con un control central. Algunos ambientes institucionales usan jerarquías de Autoridades de Certificación.

Para ambientes más descentralizados, permitir que todos los usuarios actúen como presentadores fiables de cara a sus amigos podría funcionar mejor que una autoridad centralizada de certificación de claves.

Una de las características atractivas de PGP es que puede operar de modo igualmente bueno en un ambiente centralizado con una Autoridad de Certificación o en un ambiente más descentralizado donde los individuos intercambian claves personales.

Todo este asunto de proteger claves públicas contra alteraciones es el problema más difícil en las aplicaciones prácticas de clave pública. Es el “talón de Aquiles” de la criptografía de clave pública, y un montón de complejidad de software está dedicado a resolver este problema.

Usted debe usar una clave pública sólo si está seguro de que es una buena clave pública que no ha sido alterada, y de que realmente pertenece a la persona con la que se supone que está asociada. Puede estar seguro de esto si obtuvo el certificado de clave pública directamente del propietario, o si lleva la firma de algún otro en quien usted confíe, cuya clave pública buena usted ya posea. Asimismo, el ID de usuario debería llevar nombre y apellidos del propietario de la clave y no solamente el nombre.

No importa lo tentado que esté, *nunca* debe ceder a la tentación y confiar en una clave pública descargada de un tablero electrónico, a no ser que esté firmada por alguien en quien confíe. Esta clave pública no certificada

podría haberla manipulado cualquiera, puede que incluso el administrador del sistema del tablero electrónico.

Si se le pide que firme el certificado de clave pública de alguien, asegúrese de que realmente pertenece a la persona indicada por el ID de usuario de ese certificado de clave pública. Esto se debe a que su firma en el certificado de clave pública de esa persona es una promesa suya de que esa clave pública realmente pertenece a dicha persona. Otras personas que confíen en usted aceptarán la clave pública porque lleva su firma. Puede ser un error confiar en información de segunda mano… no firme una clave pública a no ser que tenga conocimiento independiente y de primera mano de que realmente pertenece a su dueño. Preferiblemente, debería firmar la clave solamente si la obtuvo directamente de su dueño.

Para firmar una clave pública, debe estar mucho más seguro de la propiedad de la clave que si simplemente quiere usarla para cifrar un mensaje. Para convencerse de la validez de una clave a efectos de usarla, las firmas de certificación de presentadores de confianza deberían bastar. Pero para firmar una clave usted mismo, deber exigir información independiente y de primera mano sobre quién posee dicha clave. Tal vez podría llamar al propietario de la clave por teléfono y leer la huella digital de ésta para confirmar que la clave que tiene usted es realmente de él… y asegúrese de que está hablando con la persona adecuada.

Tenga en cuenta que su firma en un certificado de clave pública no responde por la integridad de esa persona, sino solamente por la integridad (la propiedad) de la clave pública de esa persona. Usted no está arriesgando su credibilidad al firmar la clave pública de un psicópata si confía totalmente en que la clave realmente le pertenece. Otras personas aceptarán que esa clave le pertenece porque usted la firmó (suponiendo que confíen en usted), pero no deberían confiar en el propietario de la clave. Fiarse de una clave no es lo mismo que fiarse del propietario de ésta.

Sería una buena idea mantener su propia clave pública con una colección de firmas adosadas de certificación de un conjunto de “presentadores”, con la esperanza de que la mayoría de la gente confiará en al menos uno de los presentadores que respondan de la validez de su clave pública. Puede poner su clave, con su colección adosada de firmas de certificación, en diversos tableros electrónicos. Si firma la clave pública de alguien, devuélvasela con su firma para que él/ella pueda añadirla a la colección de credenciales para la clave pública que esa persona posee.

Asegúrese de que nadie pueda manipular el archivo de claves públicas de usted. Comprobar un nuevo certificado de clave pública firmado

dependerá, en último término, de las claves públicas de confianza que ya están en su propio archivo de claves. Mantenga un control físico de su archivo de claves públicas, preferentemente en su propio ordenador personal mejor que en un sistema remoto de acceso compartido, igual que haría con su clave privada. Esto es para protegerlo contra alteración, no contra revelación. Mantenga una copia de seguridad fiable para su archivo de claves públicas y su clave privada en medios protegidos contra escritura.

Puesto que su propia clave pública fiable se usa como autoridad final para certificar, directa o indirectamente, todas las otras claves de su archivo de claves, es la clave más importante a proteger contra manipulación. Debería conservar una copia de seguridad en un disquete protegido contra escritura.

PGP supone por lo general que usted mantendrá control físico sobre su sistema y sobre sus archivos de claves, así como sobre su propia copia de PGP. Si un intruso puede manipularle el disco, en teoría podría manipular el propio programa, burlando así las salvaguardas que el programa pueda tener para detectar la manipulación de claves.

Una forma algo complicada de proteger todo su archivo de claves frente a manipulaciones es firmarlo con su clave privada. Puede hacer esto mediante un certificado de firma separada del archivo de claves públicas.

Cómo controla PGP qué claves son válidas

Antes de leer esta sección, debería leer la sección anterior, “Cómo proteger las claves públicas contra alteraciones.”

PGP sigue la pista de qué claves de su archivo de claves públicas están convenientemente certificadas mediante las firmas de presentadores en quienes usted confía. Todo lo que tiene que hacer es decir a PGP en qué personas confía como presentadores, y certificar las claves de esas personas con su propia clave de confianza definitiva. PGP puede seguir a partir de ahí, validando automáticamente cualquier otra clave que hayan firmado sus presentadores designados. Y, por supuesto, puede firmar claves usted mismo.

Hay dos criterios totalmente separados que PGP usa para juzgar la validez de una clave pública… no los confunda:

1. ¿Pertenece realmente la clave a la persona a quien parece pertenecer? En otras palabras, ¿se ha certificado con una firma fiable?
2. ¿Pertenece a alguien en quien pueda confiar para certificar otras claves?

PGP puede calcular la respuesta a la primera pregunta. Para responder a la segunda pregunta usted debe decírselo explícitamente a PGP. Cuando dé la respuesta a la pregunta 2, PGP podrá calcular la respuesta a la pregunta 1 para otras claves firmadas por el presentador al que ha designado como fiable.

Las claves que han certificado presentadores fiables se consideran válidas por PGP. Las claves pertenecientes a presentadores fiables deben estar certificadas, bien por usted, bien por otros presentadores fiables.

PGP también permite la posibilidad de que usted tenga varios grados de fiabilidad para las personas que actúan como presentadores. Su confianza en que el propietario de una clave actúe como presentador no solamente refleja su estimación de la integridad personal de esa persona… también debería reflejar cuán competente cree que es esa persona para comprender la administración de claves y para usar un buen juicio al firmar claves. Puede designar a una persona como no fiable, como marginalmente fiable o como totalmente fiable para certificar las claves públicas de otros. Esta información de fiabilidad se almacena en su archivo de claves junto con sus claves, pero cuando le ordena a PGP que copie una clave fuera de su archivo de claves, PGP no copia junto a la clave la información de fiabilidad, porque sus opiniones sobre fiabilidad se consideran confidenciales.

Cuando PGP calcula la validez de una clave pública, examina el nivel de fiabilidad de todas las firmas certificadoras adosadas. Computa un valor sopesado de validez… por ejemplo, dos firmas de fiabilidad marginal se consideran tan creíbles como una firma de fiabilidad total. El escepticismo del programa es ajustable… por ejemplo, puede sintonizar PGP para que exija dos firmas de fiabilidad total o tres de fiabilidad marginal para juzgar una clave como válida.

Su propia clave es “axiomáticamente” válida para PGP, y no necesita firmas de presentadores para demostrar su validez. PGP sabe qué claves públicas son suyas buscando las claves privadas correspondientes en el archivo de claves privadas. PGP también supone que usted se fía completamente de sí mismo para certificar otras claves.

Con el paso del tiempo usted acumulará claves de otras personas a quienes querrá designar como presentadores fiables. Todos los demás elegirán sus propios presentadores fiables. Y todo el mundo acumulará y distribuirá gradualmente con sus claves una colección de firmas de certificación de otras personas, con la esperanza de que cualquiera que la reciba confiará al menos en una o dos de las firmas. Esto lleva a la construcción de una red

de fiabilidad descentralizada y tolerante a fallos para todas las claves públicas.

Esta idea de nivel de base contrasta fuertemente con esquemas estándar para administración de claves públicas desarrollados por el gobierno y otras instituciones monolíticas, tales como el Correo de Intimidad Acrecentada PEM [Private Enhanced Mail] de Internet, que está basado en control centralizado y fiabilidad centralizada obligatoria. Los esquemas estándar confían en una jerarquía de Autoridades de Certificación que dictan en quién debe confiar. El método probabilístico descentralizado del programa para determinar la legitimidad de una clave pública es la piedra angular de su arquitectura de administración de claves. PGP le permite a usted, y solamente a usted, elegir en quiénes confía, poniéndole en la cima de su propia pirámide privada de certificación. PGP es para personas que prefieren empaquetar sus propios paracaídas.

Nótese que, aunque aquí se enfatiza la idea descentralizada de nivel base, no significa que PGP no se comporte igualmente bien en los esquemas más jerárquicos de administración de claves públicas centralizados. Los usuarios de grandes empresas, por ejemplo, querrán seguramente una figura o persona central que firme las claves de todos los empleados. PGP maneja el modelo centralizado como un caso especial degenerado del modelo de confianza más generalizado de PGP.

Cómo proteger sus claves privadas contra revelación

Proteja su propia clave privada y su contraseña con mucho cuidado. Si su clave privada resulta comprometida en algún momento, será mejor que corra rápidamente la voz a todas las partes interesadas antes de que alguien la use para hacer firmas en nombre suyo. Por ejemplo, alguien podría usarla para firmar certificados falsos de clave pública, lo que crearía problemas para mucha gente, especialmente si su firma goza de amplia confianza. Y por supuesto, una clave privada comprometida podría abrir todos los mensajes enviados a usted.

Para proteger su clave privada, puede comenzar por mantener siempre un control físico sobre ella. Dejarla en su ordenador personal en casa vale, o guardarla en un ordenador portátil que lleve siempre consigo. Si debe usar un ordenador de la oficina cuyo control físico no siempre tenga, mantenga sus archivos de claves públicas y privadas en un disquete extraíble y protegido contra escritura, y no lo deje en la oficina cuando salga de ésta. No sería buena idea permitir que su clave privada residiese en un ordenador

remoto de acceso compartido, como un sistema UNIX de acceso remoto. Alguien podría pinchar su línea de módem, capturar su contraseña y obtener su clave privada desde el sistema remoto. Sólo debe usar su clave privada en una máquina que esté bajo su control físico directo. Vea el Capítulo 6 para información adicional.

No guarde su contraseña en el ordenador en el que tiene su archivo de claves privadas. Almacenar la clave privada y la contraseña en el mismo ordenador es tan peligroso como guardar el número personal de identificación en la misma cartera que la tarjeta del cajero automático. No le gustaría que alguien pusiese sus manos en el disco que tiene tanto la contraseña como el archivo de claves privadas. Sería más seguro si se limitase a memorizar la contraseña y no la guardase en ningún otro lugar excepto su cerebro. Si cree que debe escribir la contraseña, manténgala bien protegida, quizá incluso mejor protegida que el archivo de claves privadas.

Y guarde copias de seguridad de su archivo de claves privadas… recuerde, usted tiene la única copia de su clave privada, y perderla convertirá en inútiles todas las copias de su clave pública que haya dispersado por todo el mundo.

El esquema descentralizado y no institucional que PGP soporta para la administración de claves públicas tiene sus beneficios, pero desafortunadamente también significa que usted no puede conocer qué claves han sido comprometidas desde una lista centralizada única. Esto hace un poco más difícil contener los daños derivados de una clave privada comprometida. Ha de hacer correr la voz y tener la esperanza de que todo el mundo se entere.

Si ocurre lo peor (su clave privada y su contraseña han sido ambas comprometidas, y esperemos que de algún modo se haya dado cuenta de ello), tendrá que emitir un certificado de “clave comprometida”. Este tipo de certificado se usa para avisar a otras personas de que dejen de usar la clave pública de usted. Puede usar PGP para crear ese certificado, usando el comando Revocar del menú de PGPkeys. Después debe enviar de algún modo este certificado de compromiso al mundo entero, o al menos a todos sus amigos y a los amigos de éstos, etc. El software PGP de ellos instala este certificado de clave comprometida en sus archivos de clave pública y automáticamente evita que usen jamás la clave pública de usted accidentalmente. Después puede generar una nueva pareja de claves privada/pública y publicar la nueva clave pública. Podría enviar un paquete que contenga su nueva clave pública y el certificado de clave comprometida para su vieja clave.

¿Y si pierde su clave privada?

Normalmente, si quiere revocar su propia clave privada puede usar el comando Revocar del menú de PGPkeys para emitir un certificado de revocación, firmado con su propia clave privada.

Pero ¿qué puede hacer si pierde su clave privada, o si su clave privada se ha destruido? No puede revocarla, porque debe usar su propia clave privada para revocarla, y ya no la tiene. Puede pedirle a cada persona que firmó su clave que retire su certificación. Así, cualquiera que intente usar su clave basándose en la fiabilidad de uno de los presentadores sabrá que no debe confiar en la clave pública de usted.

Ojo con el aceite de serpiente

Cuando se examina un paquete de software criptográfico, siempre queda la misma pregunta: ¿por qué debería fiarme de este producto? Incluso si examina usted mismo el código fuente, no todo el mundo tiene la experiencia criptográfica para juzgar su seguridad. Aunque sea un criptógrafo experimentado, puede haber debilidades sutiles en los algoritmos que se le pasen por alto.

Cuando yo estaba en la Universidad a comienzos de los setenta, diseñé lo que creía ser un brillante método de cifrado. Un conjunto simple de números pseudoaleatorios se añadía al texto llano para crear texto cifrado. Esto parecía frustrar cualquier ataque de frecuencias contra el texto cifrado, y sería imposible de reventar incluso por las agencias gubernamentales con más recursos. Me sentí muy pagado de mí mismo por mi hazaña.

Años después descubrí el mismo método en varios tratados introductorios y textos tutoriales sobre criptografía. Mira qué bien. Otros criptógrafos habían pensado en el mismo método. Por desgracia, el método se presentaba como un simple trabajo sobre cómo usar técnicas criptoanalíticas elementales para reventarlo. Ahí quedó mi brillante esquema.

De esta humillante experiencia aprendí lo fácil que es caer en una falsa idea de seguridad cuando se idea un algoritmo de cifrado. La mayoría de la gente no se da cuenta de lo infernalmente difícil que resulta diseñar un algoritmo de cifrado que pueda soportar un ataque prolongado y resuelto por parte de un oponente con recursos. Muchos ingenieros de software han diseñado esquemas de cifrado igualmente bobos (a menudo incluso el mismo método de cifrado), y algunos de ellos se han incorporado en

paquetes comerciales de software de cifrado y vendido a buen precio a miles de ingenuos usuarios.

Esto es como vender cinturones de seguridad para automóviles, que parecen buenos pero se abren en la prueba de choque más floja. Depender de ellos puede ser incluso peor que no llevar cinturones en absoluto. Nadie sospecha que son malos hasta que llega un choque de verdad. Depender de software criptográfico débil puede hacer que, sin sospecharlo, usted arriesgue información delicada cuando no habría hecho tal cosa de no haber tenido software criptográfico en absoluto. Incluso puede que nunca descubra que sus datos han sido comprometidos.

A veces los paquetes comerciales usan el Estándar de Cifrado de Datos Federal (DES), un algoritmo convencional bastante bueno recomendado por el gobierno para uso comercial (pero no para información secreta, curiosamente… hummmm). Hay varios “modos de operación” que DES puede usar, algunos mejores que otros. El gobierno recomienda específicamente no usar el modo individual más débil para mensajes, el modo de Libro de Código Electrónico, ECB [Electronic Codebook]. Pero sí recomiendan los modos, más seguros y complejos, de Retroalimentación de Cifrado [CFB, Cipher Feedback] y de Encadenado de Bloques de Cifrado [CBC, Cipher Block Chaining].

Desafortunadamente, la mayoría de paquetes de cifrado comercial que he visto usan el modo ECB. Cuando hablé con los autores de varias de estas implementaciones, dijeron que nunca habían oído hablar de modos CBC o CFB, y que no sabían nada sobre las debilidades del modo ECB. El mismo hecho de que ni siquiera hayan aprendido lo bastante sobre criptografía para conocer estos conceptos elementales resulta poco alentador. Y a veces administran sus claves DES de manera inapropiada o insegura. Además, estos mismos paquetes de software a menudo incluyen un segundo algoritmo de cifrado más rápido que puede usarse en lugar del más lento DES. El autor del programa piensa a menudo que su algoritmo rápido patentado es tan seguro como DES, pero después de preguntarle suelo descubrir que es simplemente una variación de mi propio y brillante método de mis días de universidad. O tal vez ni siquiera revelará como funciona su algoritmo de cifrado patentado pero me asegura que es un método brillante y que debería confiar en él. Estoy seguro de que él cree que su algoritmo es brillante, pero ¿cómo puedo saberlo yo sin verlo?

Para ser honrado debo hacer notar que en muchos casos estos productos terriblemente débiles no proceden de empresas especializadas en tecnología criptográfica.

Hasta los programas realmente buenos, que usan DES en los modos correctos de operación, tienen problemas. El DES estándar usa una clave de 56 bits, que es demasiado pequeña para los niveles de hoy día, y puede reventarse fácilmente mediante búsquedas exhaustivas de claves en máquinas especiales de alta velocidad. DES ha llegado al fin de su vida útil, y con él cualquier paquete de software que se base en él.

Hay una empresa llamada AccessData (87 East 600 South, Orem, Utah 84058, teléfono 1-800-658-5199) que vende un paquete de software por 185 dólares que revienta los sistemas de cifrado incorporado que usan WordPerfect, Lotus 1-2-3, MS Excel, Symphony, Quattro Pro, Paradox, MS Word y PKZIP. No se limita a adivinar palabras clave… efectúa auténtico criptoanálisis. Algunas personas lo compran cuando olvidan la palabra clave para sus propios archivos. Las fuerzas de seguridad lo usan también, para poder leer los archivos que capturan. Hablé con Eric Thompson, el autor, y me dijo que su programa sólo necesita una fracción de segundo para reventarlos, pero que añadió algunos bucles de retardo para ralentizarlo y que no le pareciese tan fácil al cliente.

En el campo de la telefonía segura, las opciones son desoladoras. El competidor líder es el STU-III (Secure Telephone Unit, Unidad Telefónica Segura), hecho por Motorola y AT&T por entre 2.000 y 3.000 dólares, y usado por el gobierno para aplicaciones clasificadas secretas. Tiene sistemas de criptografía fuerte, pero hace falta una especie de licencia especial del gobierno para comprar esa versión fuerte. Hay una versión comercial del STU-III que está debilitada porque le conviene a la NSA, y hay una versión para la exportación que está aún más debilitada. Luego está el AT&T Surity 3600, por 1.200 dólares, que usa el famoso chip Clipper del gobierno para el cifrado, con claves que están bajo depósito [escrow] gubernamental para facilitar las escuchas. Y, por supuesto, están los mezcladores de voz analógicos (no digitales) que puedes comprar en los catálogos de aspirantes a espía, y que realmente son juguetes inútiles en lo que respecta a criptografía, pero que se venden como productos de comunicación “seguros” a clientes que simplemente no conocen nada mejor.

En algunos aspectos, los productos criptográficos son como los farmacéuticos. Su integridad puede ser absolutamente vital. La mala penicilina tiene el mismo aspecto que la buena. Usted puede darse cuenta de que su programa de hoja de cálculo va mal, pero ¿cómo distinguir si su programa criptográfico es débil? El texto cifrado que produce un algoritmo de cifrado débil tiene el mismo buen aspecto que el producido por un algoritmo de cifrado fuerte. Hay un montón de aceite de serpiente

ahí fuera. Muchas curas de charlatán. Al contrario que los buhoneros vendedores de medicina patentada de antaño, estos implementadores de software ni siquiera saben que lo que venden es aceite de serpiente. Puede que sean buenos ingenieros de software, pero generalmente ni siquiera han leído nada de la bibliografía académica sobre criptografía. Pero piensan que pueden escribir buen software de criptografía. ¿Y por qué no? A fin de cuentas, parece intuitivamente fácil hacerlo. Y su software parece funcionar bien.

Cualquiera que crea haber diseñado un esquema de cifrado imposible de reventar, o es un genio increíble, o es un ingenuo sin experiencia. Desgraciadamente, a veces tengo que tratar con aprendices de criptógrafo que quieren hacer "mejoras" a PGP añadiendo algoritmos de cifrado de su propio diseño.

Recuerdo una conversación con Brian Snow, un criptógrafo de alto nivel en la NSA. Dijo que nunca confiaría en un algoritmo de cifrado diseñado por alguien que antes no se hubiese "ganado sus galones" pasando un montón de tiempo reventando códigos. Esto tenía mucho sentido. Le hice notar que prácticamente nadie en el mundo de la criptografía comercial está cualificado según ese criterio. "Sí", dijo, con una sonrisa de confianza, "y eso hace nuestro trabajo en la NSA mucho más fácil". Un pensamiento estremecedor. Yo tampoco estaba cualificado.

También el gobierno ha vendido aceite de serpiente. Tras la Segunda Guerra Mundial, los Estados Unidos vendieron máquinas alemanas de cifrado Enigma a gobiernos del tercer mundo. Pero no les dijeron que los Aliados reventaron el código Enigma durante la guerra, un hecho que permaneció secreto durante muchos años. Incluso hoy muchos sistemas UNIX de todo el mundo usan el cifrado Enigma para cifrar archivos, en parte porque el gobierno ha creado obstáculos legales contra el uso de algoritmos mejores. Hasta intentaron evitar la publicación inicial del algoritmo RSA en 1977. Y durante muchos años han echado por tierra todos los esfuerzos comerciales para desarrollar teléfonos seguros efectivos para el público en general.

La tarea principal de la Agencia de Seguridad Nacional [NSA] del gobierno de EE.UU. es reunir información, principalmente mediante escuchas encubiertas de las comunicaciones privadas de la gente (véase el libro de James Bamford *The Puzzle Palace*). La NSA ha amasado considerables habilidades y recursos para reventar códigos. Cuando la gente no puede obtener buenos productos criptográficos para protegerse, el trabajo de la NSA se hace mucho más fácil. La NSA tiene también la responsabilidad de aprobar y recomendar algoritmos de cifrado. Algunos

críticos afirman que esto es un conflicto de intereses, algo así como poner al zorro a cuidar las gallinas. En los años 80, la NSA estuvo promoviendo un algoritmo de cifrado convencional que habían diseñado (el Programa de Adhesión COMSEC), y no le contaban a nadie cómo funcionaba porque eso es secreto. Querían que otros confiaran en él y lo usaran. Pero cualquier criptógrafo le dirá que un algoritmo de cifrado bien diseñado no tiene que ser secreto para permanecer seguro. Solamente las claves deberían necesitar protección. ¿Cómo sabe nadie si realmente el algoritmo secreto de la NSA es seguro? No sería tan difícil para la NSA diseñar un algoritmo de cifrado que solamente ellos pudiesen reventar, si nadie más puede revisar el algoritmo. Y ahora con el chip Clipper la NSA está promoviendo SKIPJACK, otro método secreto de cifrado que han diseñado. ¿Están vendiendo aceite de serpiente deliberadamente?

Hay tres factores fundamentales que han minado la calidad del software criptográfico comercial en los Estados Unidos.

- El primero es la virtual ausencia universal de implementadores competentes de software para cifrado comercial (aunque esto está comenzando a cambiar desde la publicación de PGP). Todo ingeniero de software se considera criptógrafo, lo que ha llevado a la proliferación de software criptográfico realmente malo.
- El segundo es la supresión deliberada y sistemática, por parte de la NSA, de toda tecnología de cifrado buena, por medio de intimidación legal y presión económica. Parte de esta presión se plasma en la forma de estrictos controles a la exportación de software de cifrado que, por la economía del marketing de software, tiene el efecto neto de suprimir el software de cifrado doméstico.
- El tercer método de supresión viene de la concesión de todas las patentes de software para todos los algoritmos de cifrado con clave pública a una sola compañía, creando con ello un cuello de botella para suprimir la diseminación de esta tecnología (aunque este cártel de criptopatentes se rompió a comienzos de 1995).

El efecto neto de todo esto es que, antes de que PGP fuese publicado, casi no había disponible software de cifrado altamente seguro para uso general en los Estados Unidos.

No estoy tan seguro sobre la seguridad de PGP como una vez lo estuve sobre mi brillante software universitario de cifrado. Si lo estuviese, sería una mala señal. Pero no creo que PGP contenga debilidades claras (aunque estoy seguro de que contiene fallos de programación). He seleccionado los mejores algoritmos de entre la bibliografía académica de criptología civil.

En su mayor parte, estos algoritmos han estado individualmente sometidos a extensas revisiones. Conozco a muchos de los principales criptógrafos del mundo, y he discutido con algunos muchos de los algoritmos y protocolos usados en PGP. Está bien documentado, y se ha ido haciendo durante años. Y no trabajo para la NSA. Pero usted no tiene que creer en mi palabra sobre la integridad criptográfica de PGP, porque el código fuente está disponible para facilitar una revisión crítica.

Un detalle más sobre mi compromiso a la calidad criptográfica de PGP: desde que desarrollé y distribuí PGP gratuitamente por primera vez en 1991, me he pasado tres años bajo una investigación criminal por Aduanas de EE.UU. por la diseminación de PGP fronteras afuera, con riesgo de proceso criminal y años de encarcelamiento. Por cierto, usted no habrá visto que el gobierno se enfade por otros programas de cifrado,… es PGP el que los puso de los nervios. ¿Qué le dice eso sobre la fortaleza de PGP? Me he ganado mi reputación sobre la integridad criptográfica de mis productos. No traicionaré mi compromiso a nuestro derecho a la intimidad, por el cual he arriesgado mi libertad. No voy a permitir que un producto con mi nombre tenga ninguna puerta trasera.

Vulnerabilidades

Ningún sistema de seguridad para datos es impenetrable. PGP puede burlarse de diversas maneras. En cualquier sistema de seguridad para datos, usted tiene que preguntarse si la información que intenta proteger es más valiosa para su atacante que el coste del ataque. Esto debería llevarle a protegerse de los ataques más baratos, sin preocuparse por los ataques más complejos.

Parte de la discusión que sigue puede parecer realmente paranoica, pero esa actitud es apropiada para una discusión razonable de los temas de vulnerabilidad.

"Si todos los ordenadores personales del mundo -260 millones- se pusiesen a trabajar en un solo mensaje cifrado con PGP, aún serían necesarios 12 millones de veces la edad del Universo, como promedio, para reventar un solo mensaje." William Cromwell, Vicedirector, Agencia de Seguridad Nacional, 20 de Marzo de 1997.

Contraseña y clave privada comprometidas

Probablemente el ataque más simple proviene de que usted se deje la contraseña de su clave privada escrita en algún sitio. Si alguien la consigue

y también obtiene su archivo de clave privada, podrán leer sus mensajes y hacer firmas en su nombre.

He aquí algunas recomendaciones para proteger su contraseña:

1. No use frases obvias que puedan ser fácilmente adivinadas, como los nombres de sus hijos o de su cónyuge.
2. Use espacios y una combinación de números y letras en su frase. Si hace que su frase sea una sola palabra, puede adivinarse fácilmente haciendo que un ordenador pruebe todas las palabras en un diccionario hasta que encuentre la suya. Es por eso que una contraseña de frase es mucho mejor que una contraseña de palabra. Un atacante más sofisticado podría hacer que su ordenador escanease un libro de citas famosas para encontrar su contraseña.
3. Sea creativo. Use una contraseña fácil de recordar pero difícil de adivinar; puede construir fácilmente una a base de algunos refranes sin sentido o citas literarias oscuras.

Alteración de claves públicas

Existe una vulnerabilidad aguda si las claves públicas son manipuladas. Este puede ser el punto individual más crucialmente vulnerable de un criptosistema de clave pública, en parte porque muchos novatos no lo reconocen de inmediato. La importancia de esta vulnerabilidad, y las contramedidas higiénicas apropiadas, se detallan en “Cómo proteger las claves públicas contra alteraciones”, al principio de este capítulo.

Para resumir: cuando usted use la clave pública de alguien, asegúrese de que no ha sido alterada. Una clave pública nueva de otra persona debería ser de fiar solamente si la obtuvo directamente de su propietario, o si la ha firmado alguien en quien usted confía. Asegúrese de que nadie más puede manipular su archivo de claves públicas. Mantenga un control físico tanto de su archivo de claves públicas como de su clave privada, preferentemente en su propio ordenador personal en vez de en un sistema remoto de acceso compartido. Guarde una copia de seguridad de ambos archivos de claves.

Archivos no del todo borrados

Otro problema potencial de seguridad está causado por cómo la mayoría de sistemas operativos borran los archivos. Cuando usted cifra un archivo y borra el archivo original de texto llano, el sistema operativo no borra físicamente los datos. Simplemente marca esos bloques de disco como

borrados, permitiendo que el espacio se reutilice con posterioridad. Es algo así como tirar documentos confidenciales de papel en la papelera de reciclaje en vez de en la trituradora de papel. Los bloques del disco aún contiene los datos delicados que usted quería borrar, y probablemente los sobreescribirán nuevos datos en algún momento del futuro. Si un atacante lee esos bloques de disco borrados poco después de que se hayan desasignado, podría recuperar su texto llano.

En realidad, esto podría incluso suceder accidentalmente, si algo fuese mal en el disco y algunos archivos se borrasen o dañasen accidentalmente. Un programa de recuperación de discos podría usarse para recuperar los archivos dañados, pero esto a menudo significa que algunos archivos, anteriormente borrados, resucitan junto con todo lo demás. Hasta los archivos confidenciales que usted pensaba que habían desaparecido para siempre podrían aparecer y ser reinspeccionados por quienquiera que estuviese intentando recuperar su disco dañado. Incluso mientras crea el mensaje original con un procesador o editor de textos, el editor puede estar creando múltiples copias temporales de su texto en el disco, simplemente debido a su modo interno de funcionamiento. Estas copias temporales de su texto las borra el procesador de textos cuando ha terminado, pero esos fragmentos delicados siguen en algún lugar de su disco.

La única manera de evitar que el texto llano reaparezca es conseguir de algún modo que los archivos de texto llano borrado se sobreescriban. A menos que sepa con seguridad que todos los bloques borrados del disco se reutilizarán enseguida, debe tomar medidas para sobreescribir el archivo de texto llano, así como cualquier fragmento que haya dejado en el disco su procesador de textos. Puede ocuparse de cualquier fragmento del texto llano dejado en el disco por medio de la opción Destrucción Segura de PGP.

Ataques de virus y caballos de Troya

Otro ataque puede involucrar a un virus o gusano de ordenador, hostil y especialmente diseñado para que infecte PGP o su sistema operativo. Este virus hipotético podría prepararse para capturar su contraseña o clave privada, o sus mensajes descifrados, y escribir furtivamente la información capturada en un archivo o enviarla a través de una red hasta el propietario del virus. O podría alterar el funcionamiento de PGP para que las firmas no se comprueben correctamente. Este ataque es más barato que un ataque criptoanalítico.

Defenderse contra esta clase de ataque cae en la categoría de defenderse contra infecciones virales. Hay productos antivirus moderadamente capaces que se pueden conseguir comercialmente, y hay procedimientos higiénicos que se pueden seguir para reducir grandemente las probabilidades de una infección de virus. Un tratamiento completo de contramedidas antivirus y antigusanos está más allá del alcance de este documento. PGP no tiene defensas contra virus, y supone que su propio ordenador personal es un entorno de ejecución fiable. Si apareciese tal virus o gusano, espero que se corra la voz rápidamente para alertar a todos.

Un ataque similar pasa por que alguien cree una buena imitación de PGP que se comporte como PGP en muchos casos, pero que no funcione como se supone que debe. Por ejemplo, podría estar debilitado deliberadamente para que no compruebe adecuadamente las firmas, permitiendo la aceptación de certificados de clave falsos. Debe hacer un esfuerzo para obtener su copia de PGP directamente de Pretty Good Privacy.

Hay otras maneras de comprobar la alteración de PGP, usando firmas digitales. Usted podría usar otra versión de confianza de PGP para comprobar la firma de una versión sospechosa de PGP. Pero esto no ayudará en absoluto si su sistema operativo está infectado, ni detectará si su copia original de pgp.exe se ha alterado maliciosamente de tal manera que comprometa la propia capacidad del programa para comprobar firmas. Este test también supone que usted tiene una copia fiable de la clave pública que puede usar para comprobar la firma de los archivos ejecutables de PGP.

Archivos de intercambio o memoria virtual

PGP se desarrolló originariamente para MS-DOS, un sistema operativo primitivo según los patrones de hoy. Pero al migrar hacia otros sistemas operativos más complejos, como Microsoft Windows y MacOS, emergió una nueva vulnerabilidad. Esta vulnerabilidad nace del hecho de que estos bonitos sistemas operativos usan una técnica llamada *memoria virtual.*

La memoria virtual le permite ejecutar en su ordenador grandes programas, más grandes que el espacio disponible en los chips semiconductores de memoria de su ordenador. Esto es útil porque el software ha engordado más y más desde que las interfaces gráficas de usuario se convirtieron en la norma y los usuarios comenzaron a ejecutar varias aplicaciones grandes al mismo tiempo. El sistema operativo usa el disco duro para almacenar porciones de software que no se estén usando en ese momento. Esto significa que el sistema operativo podría, sin su conocimiento, escribir en el

disco cosas que usted suponía que estaban solamente en la memoria principal… cosas como claves, contraseñas y texto llano descifrado. PGP no guarda esa clase de datos delicados en memoria más de lo necesario, pero siempre existe la posibilidad de que el sistema operativo lo escriba en el disco de todos modos.

Los datos se escriben en alguna zona no usada del disco, conocida como *archivo de intercambio* [swap file]. Los datos se vuelven a leer desde el archivo de intercambio conforme se necesitan, de modo que solamente parte de sus datos o programa están en memoria física en un momento dado. Toda esta actividad es invisible al usuario, quien simplemente percibe que el disco hace ruido. Microsoft Windows intercambia trozos de memoria, llamados *páginas*, usando un algoritmo de reemplazo del Menos Usado Recientemente, LRU [Least Recently Used]. Esto significa que las páginas más antiguas a las que no ha accedido son las primeras que se intercambian al disco. Esta idea sugiere que en muchos casos el riesgo de que los datos delicados se intercambien al disco es bastante bajo, ya que PGP no los deja en memoria mucho tiempo. Pero no damos garantías al respecto.

A este archivo de intercambio puede acceder cualquiera que pueda tener acceso físico a su ordenador. Si usted está preocupado por este problema, puede resolverlo obteniendo software especial que sobreescriba su archivo de intercambio. Otra posible cura es desactivar la opción de memoria virtual de su sistema operativo. Microsoft Windows lo permite, así como el MacOS. Desactivar la memoria virtual puede significar que necesite más chips físicos de memoria RAM instalados para que todo quepa en la RAM.

Brechas físicas de seguridad

Una brecha de seguridad física podría permitir a alguien obtener físicamente sus archivos de texto llano o mensajes impresos. Un oponente obstinado podría conseguirlo por medio de hurto, examen de basura, registro y captura, o por medio de soborno, extorsión o infiltración de sus empleados. Algunos de estos ataques pueden ser especialmente posibles contra organizaciones políticas de base, las cuales dependen de un personal en su mayoría voluntario.

No se deje caer en una falsa sensación de seguridad simplemente porque tiene una herramienta criptográfica. Las técnicas criptográficas protegen los datos solamente mientras estén cifrados… las violaciones físicas directas de seguridad pueden aún comprometer datos en texto llano o información escrita o hablada.

Esta clase de ataques es más barato que los ataques criptoanalíticos contra PGP.

Ataques tempest

Otro tipo de ataque usado por oponentes bien equipados involucra la detección remota de las señales electromagnéticas de su ordenador. Este ataque, caro y muy laborioso, es con todo más barato que un ataque criptoanalítico directo. Una furgoneta con instrumental apropiado puede aparcar cerca de su oficina y captar desde lejos todas las pulsaciones de teclas y mensajes mostrados en la pantalla de su ordenador. Esto comprometería todas sus contraseñas, mensajes, etc. Este ataque puede evitarse apantallando adecuadamente todo el equipo de ordenador y el cableado de red para que no emita esas señales. Esta tecnología de apantallamiento, conocida como “Tempest”, la usan algunas agencias del gobierno y contratistas de defensa. Hay vendedores de hardware que suministran apantallamientos Tempest comercialmente.

Protección contra sellos de fechado falso

Una vulnerabilidad algo oscura de PGP consiste en que un usuario deshonesto cree un sello de fechado [timestamp] falso en su propios certificados de clave pública y firmas. Usted puede saltarse esta sección si no es un usuario habitual y no está metido en profundidad en protocolos raros de clave pública.

No hay nada que evite que un usuario deshonesto altere la fecha y hora del reloj de su propio sistema, y genere sus propios certificados de clave pública y firma que parezcan haber sido creados en un momento diferente. Esa persona puede aparentar que firmó algo antes o después de cuando realmente lo hizo, o que su par de claves pública/privada se creó, bien antes, bien después. Puede haber en ello beneficios legales o financieros, por ejemplo crear algún tipo de vacío legal que le permita repudiar una firma.

Creo que este problema de los sellos de fechado falsificado en firmas digitales no es peor de lo que ya es en las firmas manuscritas. Cualquiera puede escribir cualquier fecha tras su firma manuscrita en un contrato, pero nadie parece alarmarse ante este estado de cosas. En algunos casos, una fecha “incorrecta” en una firma manuscrita no tiene por qué estar asociada a un fraude real. La fecha puede ser aquella en la que el firmante confirma que firmó un documento, o aquella en la que quiere que la firma tenga validez.

En situaciones en las que es vital que una firma tenga una fecha correcta, la gente se limita a usar notarios para dar fe y fechar una firma manuscrita. Lo análogo a esto en las firmas digitales es conseguir que una tercera parte, de confianza, firme un certificado de firma, usando un sello de fechado de confianza. No se necesita para ello ningún protocolo exótico o formal en demasía. Las firmas con testigos están desde hace tiempo reconocidas como modo legítimo de determinar cuándo se firmó un documento.

Una Autoridad de Certificación de confianza, o un notario, crearía firmas notariales con un sello de fechado de confianza. Esto no necesariamente requiere de una autoridad centralizada. Quizás cualquier presentador fiable, o parte no interesada, pueda servir al efecto, igual que los notarios públicos reales hoy día. Cuando un notario firma las firmas de otras personas, crea un certificado de firma acerca de un certificado de firma. Esto serviría como testigo de la firma igual que hacen ahora los notarios reales al hacer de testigos en firmas manuscritas. El notario puede introducir el certificado separado de firma (sin el documento real que ha sido firmado) en un archivo especial controlado por el notario. Cualquiera puede leer dicho archivo. La firma del notario tendría un sello de fechado de confianza, lo que le daría mayor flexibilidad o más validez legal que el sello de fechado de la firma original.

Hay un buen tratamiento del tema en el artículo de Denning de 1983 en IEEE Computer. Mejoras futuras de PGP podrían contener opciones para administrar con facilidad firmas notariales de firmas, con sellos de fechado fiables.

Exposición en sistemas multiusuario

PGP se diseñó originariamente para un PC de un solo usuario, bajo su control físico directo. Si usted ejecuta PGP en casa en su propio PC, sus archivos cifrados están por lo general seguros, a no ser que alguien entre en su casa, robe su PC y le persuada para que le dé su contraseña (o si su contraseña es lo bastante fácil para ser adivinada).

PGP no está diseñado para proteger sus datos en forma de texto llano en un sistema comprometido. Tampoco puede evitar que un intruso emplee medidas sofisticadas para leer su clave privada mientras se usa. Usted tendrá que reconocer estos riesgos en sistemas multiusuario, y ajustar sus expectativas y comportamiento en consecuencia. Tal vez su situación sea tal que deba considerar usar PGP solamente en un sistema aislado, de un solo usuario, bajo su control físico directo.

Análisis de tráfico

Aunque el atacante no pueda leer el contenido de sus mensajes cifrados, puede ser capaz de deducir al menos algo de información útil observando de dónde vienen los mensajes, adónde van, el tamaño de los mensajes y la hora del día en que se envían. Esto es análogo a si el atacante le mirase la factura telefónica de larga distancia para ver quién le llamó, cuándo y durante cuánto tiempo, aunque el contenido real de sus llamadas le sea desconocido al atacante. A esto se le llama análisis de tráfico. PGP no puede por su cuenta proteger contra el análisis de tráfico. Resolver este problema requerirá protocolos especializados de comunicación diseñados para reducir la exposición al análisis de tráfico en su entorno de comunicaciones, posiblemente con alguna ayuda criptográfica.

Criptoanálisis

Un ataque criptoanalítico caro y sofisticado posiblemente podría montarlo alguien con grandes recursos de superordenadores, como una agencia de inteligencia del gobierno. Podrían reventar su clave RSA usando algún nuevo avance secreto en factorización. Pero la comunidad académica civil ha estado atacándolas activamente desde 1978 sin éxito.

Tal vez el gobierno tenga algún método secreto para reventar el algoritmo de cifrado convencional IDEA usado en PGP. Esta es la peor pesadilla de todo criptógrafo. No puede haber garantías absolutas de seguridad en las implementaciones prácticas de criptografía.

Con todo, se justifica cierto optimismo. Los diseñadores del algoritmo IDEA se cuentan entre los mejores criptógrafos de Europa. Ha sufrido extensos análisis de seguridad y revisiones de los mejores criptoanalistas del mundo no secreto. Parece tener algunas ventajas de diseño sobre DES respecto al criptoanálisis diferencial.

Además, aunque este algoritmo tenga alguna debilidad sutil y desconocida, PGP comprime el texto llano antes del cifrado, lo que debería reducir grandemente estas debilidades. La carga computacional de trabajo necesaria para reventarlo será, con toda probabilidad, mucho más onerosa que el valor del mensaje.

Si su situación justifica el preocuparse sobre un ataque a escala formidable de este calibre, puede que deba ponerse en contacto con un consultor en seguridad de datos para obtener seguridad de datos adaptada a sus necesidades especiales.

Resumiendo, sin una buena protección criptográfica de sus comunicaciones de datos, puede que sea sencillo e incluso habitual para un oponente el interceptar sus mensajes, especialmente los enviados a través de un sistema de módem o correo electrónico. Si usted usa PGP y sigue unas razonables precauciones, el atacante tendrá que dedicar muchos más esfuerzos y gastos para violar su intimidad.

Si se protege contra los ataques más sencillos, y se siente confiado en que su intimidad no la va a violar un atacante obstinado y de grandes recursos, probablemente le irá bien usando PGP. PGP le da una Intimidad Bastante Buena [Pretty Good Privacy].

Apéndice A

Transferencia de Archivos entre el MacOS y Windows usando PGP

Transferir archivos a y desde el sistema operativo MacOS es un problema clásico al usar casi cualquier clase de software de intercambio de datos, tal como aplicaciones de correo electrónico, FTP, utilidades de compresión y PGP. Este apéndice está orientado a documentar cómo este problema se resuelve finalmente en la Versión 5.5 de PGP, y a discutir cómo comunicarse con versiones previas de PGP.

El MacOS almacena archivos de manera diferente a otros sistemas operativos. Incluso el formato de los archivos de texto del MacOS es diferente. Los archivos de MacOS son realmente dos archivos formados por un segmento de Datos y un segmento de Recursos. Para enviar un archivo de MacOS a Windows sin perder datos, ambos segmentos deben ser fusionados en uno. El método estándar por el que un archivo MacOS se convierte en un archivo único para que pueda transferirse a otro Macintosh o PC sin perder ninguna de las mitades se denomina MacBinary.

El problema es que, sin software especial, Windows y otras plataformas no pueden comprender el formato MacBinary de forma inherente. Si se da el caso de que el software receptor no consigue convertir un archivo de formato MacBinary en archivo Windows, el archivo resultante es inutilizable. Existen utilidades de terceros en Windows para convertirlo más tarde en un archivo utilizable, pero esto puede resultar inconveniente.

Las versiones anteriores de PGP y la mayoría de utilidades disponibles hoy en el mercado intentan, por lo general, ignorar este problema en lo posible y dejar que el usuario tome todas las decisiones acerca de si codificar un archivo con MacBinary al enviarlo desde el MacOS o no. Esto traslada la responsabilidad de decidir, bien enviarlo con MacBinary y no arriesgarse a perder datos, bien enviarlo sin MacBinary con la esperanza de que no se

pierdan datos importantes, al usuario, quien a menudo no tiene idea de cuál es la decisión correcta. La decisión debería de estar basada en si el archivo va a ser enviado a Windows o a MacOS. Pero, ¿y si usted está enviando a ambos al mismo tiempo? No hay una buena solución a este problema con versiones anteriores de PGP y muchas otras utilidades. Esto ha conllevado mucha confusión e inconvenientes a los usuarios.

Lo opuesto, enviar un archivo de Windows a MacOS, también ha sido un gran problema. Windows usa extensiones de nombres de archivos, como .doc, para identificar el tipo de archivo. Esto no tiene sentido en MacOS. Estos archivos se envían a un ordenador Macintosh sin información sobre el tipo y creador del archivo. El proceso de hacerlos legibles tras la recepción generalmente involucra varios movimientos extraños en el diálogo Abrir de la aplicación que creó el archivo, o en muchos casos exige que el usuario entienda la jerga MacOS de códigos de tipo y creador y los establezca manualmente en una utilidad de terceros.

Afortunadamente, la Versión 5.5 PGP finalmente nos saca de esta confusión. Si todos los usuarios de PGP usasen la Versión 5.5 de PGP, nadie tendría que pensar en cómo enviar archivos de MacOS a Windows y viceversa.

Enviar de MacOS a Windows

En MacOS hay tres opciones con PGP 5.5 para cifrar o firmar un mensaje:

- MacBinary: Sí
- MacBinary: No
- MacBinary: Inteligente

MacBinary: Sí

Esta es la opción recomendada para todos los cifrados cuando se envían a otro usuario de la Versión 5.5 de PGP o superior en cualquier plataforma. Esto significa que los usuarios de MacOS recibirán el archivo exacto que se quería, y la versión de Windows descodificará automáticamente el MacBinary, e incluso añadirá la extensión de nombre de archivo apropiada, como .doc para Microsoft Word o .ppt para Microsoft PowerPoint. PGP incluye información sobre la mayoría de las extensiones de nombre de archivos usuales y códigos creadores de Macintosh. En casos en los que el tipo de archivo sea desconocido o que se sepa que es un archivo sólo para MacOS, como una aplicación MacOS, el archivo permanece en formato

MacBinary para que posteriormente pueda ser enviado a un ordenador Macintosh completamente intacto.

MacBinary: No

Si usted está comunicándose con usuarios que tienen una versión más antigua de PGP, la decisión de enviar con MacBinary suele terminar en las manos del que envía, igual que en la mayoría de programas y en las versiones anteriores de PGP para MacOS. Al enviar a un PC con una versión anterior, si usted sabe que el archivo que está enviando puede leerse con aplicaciones Windows cuando no se use MacBinary, seleccione esta opción. Esto incluye la mayoría de archivos de aplicaciones multiplataforma tales como los de Microsoft Office, archivos de gráficos, archivos comprimidos y muchos otros. El destinatario o el remitente tendrán que cambiar manualmente el nombre al archivo para que tenga la extensión correcta en Windows. Esto es necesario porque el destinatario Windows no tiene la información del creador codificada normalmente con MacBinary.

MacBinary: Inteligente

Hay algunos casos concretos en los que esta opción puede ser útil al comunicarse con usuarios que no usen la versión 5.5. Esta opción toma la decisión sobre si codificar con MacBinary o no, basándose en un análisis de los datos del archivo. Si el archivo es uno de los siguientes tipos, no será codificado con MacBinary, haciéndolo con ello legible en un PC con cualquier versión de PGP:

- Archivos comprimidos con PKZIP
- Archivos comprimidos con Lempel-Ziv
- Archivos de formato musical MIDI
- Archivos comprimidos con PackIt
- Archivos de gráficos GIF
- Archivos comprimidos con StuffIt_
- Archivos comprimidos con Compactor
- Archivos comprimidos con Arc
- Archivos de gráficos JPEG

Como se ve, solamente de una selección limitada de archivos resultará un archivo legible por versiones antiguas de PGP en otras plataformas usando la opción Inteligente. Cualquier otro archivo recibido en un PC con una versión anterior de PGP será ilegible sin antes quitarle la codificación MacBinary con un programa a tal efecto. Asimismo, el archivo no tendrá la extensión de nombre de archivo correcta en el PC a menos que esa extensión la añada manualmente el usuario que envía. Usando el modo Inteligente, el archivo resultante puede que no sea el mismo que el original cuando se envía a otro Macintosh, ya que puede perder sus códigos de tipo y creador. Este modo permanece en el producto fundamentalmente debido al hecho que estaba en PGP versión 5.0 y algunos usuarios puede que solamente tengan necesidad de enviar los tipos de archivo mencionados anteriormente. Esta opción no se recomienda en la mayoría de los casos.

En resumen, si usted está enviando solamente a Versiones 5.5 o superiores, seleccione siempre MacBinary: Sí (la opción por defecto). Así, no hace falta darle vueltas si todos están usando la Versión 5.5 de PGP exclusivamente. Cuando usted envíe a usuarios con versiones más antiguas, debe seleccionar MacBinary: No para tipos de archivo multiplataforma y MacBinary: Sí para archivos que de todos modos no serían legibles para usuarios de PC (como una aplicación MacOS).

Nota a la Versión 5.0 de PGP: la Versión 5.0 de PGP no tenía una opción MacBinary: No. Para enviar tipos de archivo sin MacBinary, y que no estén incluidos en la lista de MacBinary: Inteligente, a un PC que use 5.0, el archivo debe cambiarse manualmente a uno de los códigos de creador y tipo que esté en la lista de Inteligente antes de enviar.

Recibir archivos de Windows en el MacOS

Al descifrar, PGP versión 5.5 intenta automáticamente traducir las extensiones de nombre de archivo para los archivos no MacBinary a información de creador y tipo de MacOS. Por ejemplo, si usted recibe un archivo de Windows con una extensión .doc, el archivo será guardado como documento de Microsoft Word. La misma lista de aplicaciones, usada al añadir extensiones de nombre de archivo cuando se recibe un archivo de MacBinary en Windows, se usará al volver a traducir extensiones de nombre de archivos al equivalente MacOS cuando se reciban en un ordenador Macintosh. En casi todos los casos, esto significa que los archivos son inmediatamente legibles y manipulables mediante doble clic en MacOS.

Las versiones anteriores de PGP para MacOS no tienen esta opción. El usuario tendrá que determinar manualmente que un archivo llamado “informe.doc” es un archivo de Microsoft Word. Tras determinar la aplicación creadora, en el caso de Microsoft Word, puede simplemente usarse el diálogo de Abrir para abrir el archivo, seleccionando ‘Todos los archivos˝ en el menú. Muchas otras aplicaciones tienen asimismo esta característica, pero algunos no la tienen. Si el documento no puede abrirse desde la aplicación, el usuario debe averiguar cuáles con los códigos de creador y tipo apropiados para ese archivo, y establecerlos manualmente con otro programa a tal fin. Existen varias utilidades gratuitas para hacer esto. Actualizarse a la Versión 5.5 es probablemente la opción más sencilla en este caso, ya que elimina este problema.

Aplicaciones aceptadas

Las aplicaciones de la lista siguiente generan documentos que PGP 5.5 traduce automáticamente cuando se envían de Windows a MacOS y viceversa. Actualmente no hay modo para el usuario de añadir o cambiar estas conversiones, sin embargo, añadiremos esa funcionalidad en el futuro.

- PhotoShop (GIF, documentos nativos PhotoShop, TGA, JPEG)
- PageMaker (versiones 3.x, 4.x, 5.x, 6.x)
- Microsoft Project (archivos de proyecto y plantillas)
- FileMaker Pro
- Adobe Acrobat
- Lotus 123
- Microsoft Word (texto, RTF, plantillas)
- PGP
- Microsoft PowerPoint
- StuffIt
- QuickTime
- Corel WordPerfect
- Microsoft Excel (varios tipos diferentes de archivos)
- Quark XPress

Asimismo, se convierten las siguientes extensiones generales de nombres de archivo:

.cvs	.arj	.ima	.eps	.mac	.cgm
.dl	.fli	.ico	.iff	.img	.lbm
.msp	.pac	.pbm	.pcs	.pcx	.pgm
.plt	.pm	.ppm	.rif	.rle	.shp
.spc	.sr	.sun	.sup	.wmf	.flc
.gz	.vga	.hal	.lzh	.Z	.exe
.mpg	.dvi	.tex	.aif	.zip	.au
.mod	.svx	.wav	.tar	.pct	.pic
.pit	.txt	.mdi	.pak	.tif	.eps

Glosario de Términos

archivo de claves: Un conjunto de claves. Cada usuario tiene dos tipos de archivos de claves: un archivo de claves públicas y un archivo de claves privadas.

archivo de claves privadas: Un conjunto de una o más claves privadas, todas ellas pertenecientes al propietario del archivo. —Ver clave privada.

archivo de claves públicas: Un conjunto de claves públicas. Su archivo de claves públicas contiene además su(s) propia(s) clave(s) pública(s). —Ver clave pública.

autentificación: La determinación del origen de una información cifrada mediante la verificación de la firma digital, o de la clave pública de alguien comprobando la huella digital única de la clave. —Ver huella digital, verificación.

autoridad certificadora: A uno o más individuos de confianza se les asigna la responsabilidad de certificar el origen de las claves y añadirlas a una base de datos común. —Ver certificar, presentador.

certificar: Firmar la clave pública de otra persona. —Ver clave pública, firmar.

cifrado: Un método de descomponer la información para hacerla ilegible a todos menos al destinatario deseado, que debe descifrarla para poder leerla. Ver cifrado convencional, criptografía por clave pública.

cifrado convencional: Cifrado que al contrario de la criptografía por clave pública se basa en una contraseña común. El archivo se cifra usando una clave de sesión, la cual a su vez se cifra con una contraseña que a usted se le pedirá que escoja. Se necesita un canal seguro de comunicación para transmitir la contraseña.

cifrado por clave pública: Ver criptografía por clave pública.

clave: Un código digital usado para cifrar, firmar, descifrar y verificar mensajes de correo electrónico y archivos. Las claves se encuentran como pares de claves y se almacenan en archivos de claves. —Ver archivo de claves, par de claves.

clave privada: La parte secreta de un par de claves, utilizada para firmar y descifrar información. La clave privada del usuario debería mantenerse secreta, solamente conocida por el usuario. —Ver contraseña.

clave pública: Una de las dos claves del par de claves, usada para cifrar información y verificar firmas. La clave pública de un usuario se puede distribuir extensamente a colegas y extraños. Conocer la clave pública de una persona no ayuda a nadie a descubrir la clave privada correspondiente.

contraseña: Una serie de caracteres tecleados que le dan acceso exclusivo a su clave privada que es la que usted usará para firmar y descifrar mensajes de correo electrónico y archivos adjuntos.

criptografía de clave pública: Criptografía en la que se utiliza un par de claves, pública y privada, y no se necesita seguridad en el canal de comunicación para enviar las claves.

depósito de claves: Una práctica consistente en que un usuario de un sistema de cifrado por clave pública entrega su clave privada a terceros permitiéndoles de este modo monitorizar comunicaciones cifradas.

descifrado: Un método de recomponer información cifrada para volverla legible de nuevo. Para descifrar se usa la clave privada del destinatario.

fiable: Se dice que una clave pública es fiable para usted si ha sido certificada por usted mismo o por alguien a quien usted haya designado como presentador.

firma (digital): Un código digital creado con una clave privada. Las firmas permiten la autentificación de la información mediante el proceso de la verificación de firmas. Cuando usted firma un mensaje o archivo, el programa PGP utiliza su clave privada para crear un código digital único tanto para los contenidos del mensaje como para su clave privada. Cualquiera puede utilizar su clave pública para verificar su firma. —Ver resumen de mensaje.

firmar: Aplicar una firma. —Ver firma.

huella digital (de la clave): Una cadena identificativa y única de números y caracteres utilizada para autentificar claves públicas. Por ejemplo, usted puede telefonear al propietario de una clave pública y pedirle que le lea la huella digital asociada a la clave de forma que usted pueda compararla con la de su copia de la clave pública de él o de ella para ver si coinciden. Si la huella digital no coincide usted sabrá que tiene una clave falsa.

ID de la clave: Un código legible que identifica a un par de claves. Dos pares de claves pueden tener el mismo ID de usuario, pero tendrán diferentes IDs de clave.

ID de usuario: Una frase con texto que identifica a un par de claves. Por ejemplo, un formato común para un ID de usuario es el nombre del propietario y su dirección de correo electrónico. El ID de usuario ayuda a los usuarios (al propietario y a los colegas) a identificar al propietario del par de claves.

par de claves: Una clave pública y su clave privada complementaria. En criptosistemas de clave pública, como el programa PGP, cada usuario tiene al menos un par de claves. —Ver clave privada, clave pública.

presentador (fiable): Una persona u organización a la que se le permite afirmar la autenticidad de la clave pública de alguien. Cuando un presentador fiable firma las claves de otra persona, usted se fía de que esas clave son válidas, y no necesita verificarlas antes de utilizarlas. Usted designa a un presentador firmando la clave pública del mismo.

red de confianza: Un modelo de fiabilidad distribuida utilizado por PGP para validar al propietario de una clave pública en el que el grado de fiabilidad es acumulativo y se basa en el conocimiento de los presentadores por parte del individuo. —Ver presentador.

resumen de mensaje: Un “destilado” compacto de su mensaje o suma de control de su archivo. Representa a su mensaje de tal modo que si el mensaje se alterase de cualquier modo, se obtendría un resumen de mensaje diferente.

texto: Texto ASCII de 7 bits estándar, imprimible. —Ver texto ASCII-blindado, texto llano.

texto ASCII-blindado: Información binaria que se ha codificado utilizando un conjunto de caracteres ASCII de 7 bits estándar e imprimible, por su conveniencia para el transporte de información por sistemas de comunicación. En el programa PGP, a los nombres de los archivos de texto ASCII-blindado se les asigna por defecto la extensión .asc, y se codifican y descodifican con el formato ASCII base-64.

texto llano: Texto normal, legible, no cifrado, no firmado.

verificación: El acto de cotejar una firma creada con una clave privada usando la clave pública. La verificación demuestra que la información la envió realmente el firmante, y que el mensaje no lo ha alterado nadie más a posteriori. —Ver firma.

Índice

D

E

F

G

H

I

M

N

P

R

S

T

U

V