

**PGP for Personal Privacy**  
**Versión 5.5**

Para

Windows 95/NT

**Guía del Usuario**  
**Versión Gratuita [Freeware]**

Network Associates, Inc.

**Traducción al castellano para la versión 5.5.3i Internacional**

Copyright © 1990-1998 Network Associates, Inc. y sus compañías afiliadas. Todos los derechos reservados.

PGP\* for Personal Privacy para Windows/Diffie-Hellman Versión 5.5.5

PGP y Pretty Good Privacy son marcas comerciales registradas de Network Associates, Inc. y sus compañías afiliadas.

El Producto Software puede usar algoritmos de clave pública descritos en las patentes de EEUU números 4.200.770, 4.218.582, 4.405.829 y 4.424.414, licenciados exclusivamente por Public Key Partners; el algoritmo de cifrado criptográfico IDEA (tm) descrito en la patente de EEUU número 5.214.703, licenciado por Ascom Tech AG, Algoritmo de Cifrado CAST, licenciado por Northern Telecom, Ltd. IDEA es una marca comercial de Ascom Tech AG. El Producto de Software puede asimismo incluir cualquiera de lo que sigue: código de compresión provisto por Mark Adler y Jean-loup Gailly, usado con permiso de la implementación gratuita Info-ZIP; software LDAP provisto por cortesía de la Universidad de Michigan en Ann Arbor, Copyright © 1992-1996 Regentes de la Universidad de Michigan, todos los derechos reservados; software DB 2.0 que tiene Copyright © 1990, 1993, 1994, 1995, 1996, 1997 Sleepycat Software Inc., todos los derechos reservados; software desarrollado por el Grupo Apache para uso en el proyecto de servidor HTTP Apache (<http://www.apache.org/>), Copyright © 1995-1997 The Apache Group, todos los derechos reservados. Network Associates, Inc. y sus compañías afiliadas pueden tener patentes y/o aplicaciones de patentes pendientes que cubran materiales en este software o su documentación; arreglos en este software o documentación no le dan a usted ninguna licencia a estas patentes.

Vea los archivos de textos incluidos en el software, o el emplazamiento web de Network Associates, para más información. El software provisto con esta documentación está licenciado a usted para su uso individual bajo los términos del Acuerdo de Licencia para Usuario Final y la Garantía Limitada provistos con el software. La información de este documento es susceptible de cambios sin previo aviso. Network Associates, Inc. no garantiza que la información se ajuste a los requerimientos de usted, o que la información esté libre de errores. La información puede incluir inexactitudes técnicas o errores tipográficos. Puede que se hagan cambios a la información e incorporados en nuevas ediciones de este documento, si y cuando sean hechas disponibles por Network Associates, Inc.

Nota: Algunos países tienen leyes y reglamentaciones acerca del uso y la exportación de productos criptográficos; por favor, consulte a las autoridades locales de su gobierno para más detalles. Caso de tener cualquier pregunta acerca de estos términos y condiciones, o si desea contactar con Network Associates, Inc. por cualquier razón, por favor escriba a:

Network Associates, Inc. Customer Service  
2805 Bowers Avenue  
Santa Clara, CA 95051-0963

<http://www.nai.com>

\* se utiliza a veces en vez de (R) para marcas registradas para proteger marcas registradas fuera de los EEUU.

## GARANTÍA LIMITADA

Garantía Limitada. Network Associates 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 arriba indicada puede no ser aplicable en su caso.

Recursos del cliente. La completa responsabilidad de Network Associates y de sus distribuidores, y su recurso exclusivo, será, a elección de Network Associates, o bien (a) devolución del precio de adquisición pagado por la licencia, si lo hay, o (b) reparación o reemplazo del Producto Software que no satisfaga la garantía limitada de Network Associates y que se devuelva a Network Associates 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, ni estos recursos ni servicio de soporte técnico a productos ofrecidos por Network Associates están disponibles sin una prueba de compra de una fuente internacional autorizada y puede no estar disponible en Network Associates por el acatamiento de las restricciones según las leyes y regulaciones de exportaciones de 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 NETWORK ASSOCIATES Y SUS DISTRIBUIDORES RECHAZAN CUALQUIER OTRA GARANTÍA, O CONDICIÓN, EXPRESA 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 NETWORK ASSOCIATES 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 TÉCNICA, INCLUSO SI NETWORK ASSOCIATES HA SIDO ADVERTIDO DE LA POSIBILIDAD DE TALES DAÑOS. EN CUALQUIER CASO, LA RESPONSABILIDAD CUMULATIVA Y COMPLETA DE NETWORK ASSOCIATES CON USTED O CON CUALQUIER OTRA PARTE POR CUALQUIER PÉRDIDA O DAÑO RESULTANTE DE ALGUNA RECLAMACIÓN, DEMANDA O ACCIÓN SURGIDA 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 ARRIBA MENCIONADAS PUEDEN NO SER APLICABLES EN SU CASO.

Traducción al castellano:

Juan Manuel Velázquez ([velazquez@usa.net](mailto:velazquez@usa.net))

Arturo Quirantes Sierra ([aquiran@goliat.ugr.es](mailto:aquiran@goliat.ugr.es))

# Contenido

<b>Prefacio .....</b>	<b>ix</b>
Convenios usados en este documento .....	ix
Para más información .....	ix
Desde la Web .....	ix
Soporte técnico .....	x
Se agradece su colaboración .....	x
Lectura básica recomendada .....	x
Otra bibliografía .....	xi
Contenido de este manual .....	xi
<b>Capítulo 1: Introducción .....</b>	
<b>12</b>	
Lo nuevo en PGP versión 5.5 .....	12
Lo nuevo en la documentación de PGP versión 5.5 .....	12
Cómo usar PGP .....	13
Repaso rápido .....	13
Creación de un par de claves .....	14
Intercambio de claves públicas con otros usuarios .....	14
Validación de sus claves .....	14
Cifrado y firma de sus mensajes de correo electrónico y archivos .....	15
Descifrado y verificación de sus mensajes de correo electrónico y archivos	
15	
Tachado irreversible de archivos .....	15
<b>Capítulo 2: Puesta en Marcha .....</b>	
<b>16</b>	
Requerimientos de sistema .....	16
Compatibilidad con otras versiones .....	16
PGP for Personal Privacy .....	17
PGP for email and files .....	17
PGP/MIME, su uso .....	18
Actualización desde una versión anterior .....	18
PGP Versión 2.6.2 o 2.7.1; actualización .....	18
PGPmail 4.0; actualización .....	19
PGPmail 4.5; actualización .....	19
PGP versión 5.0; actualización .....	20
PGP versión 5.5; instalación .....	21

Desde un CD ROM .....	21
Desde el sitio Web de Network Associates .....	22
Uso de PGP .....	22
Barra de tareas de Windows; uso desde .....	22
Aplicaciones de correo electrónico, cómo usar PGP desde .....	24
Explorador de Windows, uso de PGP desde .....	25
Destinatarios, cómo seleccionarlos .....	25
Atajos .....	25
Iconos de PGPkeys, definiciones .....	26
<b>Capítulo 3: Creación e Intercambio de Claves .....</b>	<b>28</b>
Conceptos clave .....	28
Par de claves .....	28
Frase de contraseña, cómo recordarla .....	32
Protección de la clave .....	33
Distribución de su clave pública .....	34
Servidor de claves, hacer disponible su clave pública .....	34
Inclusión de su clave pública en un mensaje de correo electrónico .....	35
Exportación de su clave pública a un archivo .....	36
Obtención de las claves públicas de otros .....	36
Obtención de claves públicas mediante un servidor de claves .....	37
Adición de claves públicas desde sus mensajes de correo electrónico .....	38
Importación de una clave pública desde un archivo .....	39
Verificación de la autenticidad de una clave .....	39
Obtención de claves a través de presentadores de confianza .....	40
<b>Capítulo 4: Envío y Recepción de Correo Electrónico Privado .....</b>	<b>41</b>
Cifrado y firma de mensajes de correo electrónico .....	41
Cifrado y firma con aplicaciones soportadas de correo electrónico .....	41
Descifrado y verificación de mensajes de correo electrónico .....	43
Descifrado y verificación con aplicaciones soportadas de correo electrónico .....	43
PGPlog .....	44
Grupos de destinatarios .....	45
<b>Capítulo 5: Uso de PGP para Almacenamiento Seguro de Archivos .....</b>	<b>47</b>
Uso de PGP para cifrar y descifrar archivos .....	47
Cifrado y firma por medio del portapapeles .....	47
Descifrado y verificación por medio del portapapeles .....	49

Cifrado y firma desde el Explorador de Windows .....	49
Descifrado y verificación desde el Explorador de Windows .....	51
Funciones de PGP desde el Explorador de Windows .....	52
Tachado de archivos .....	53
<b>Capítulo 6: Administración de Claves y Configuración de Preferencias .</b>	<b>54</b>
Administración de sus claves .....	54
La ventana de PGPkeys .....	55
Atributos en PGPkeys, definiciones .....	56
Propiedades de una clave .....	58
Par de claves predeterminado .....	59
Nuevo nombre o dirección de usuario, añadir .....	59
Huella de una clave, comprobación .....	60
Firmar una clave pública .....	60
Nivel de confianza para validaciones de clave .....	62
Inhabilitación y habilitación de claves .....	62
Eliminación de una clave o firma .....	63
Cambio de contraseña .....	63
Importación y exportación de claves .....	64
Revocación de una clave .....	65
Configuración de sus preferencias .....	66
Preferencias generales .....	66
Preferencias de archivos .....	68
Preferencias de correo electrónico .....	69
Preferencias del servidor de claves .....	70
Preferencias avanzadas .....	71
Acerca de la búsqueda de claves .....	72
Búsqueda de la clave de un usuario, procedimiento .....	72
<b>Capítulo 7: Solución de Problemas .....</b>	<b>74</b>
<b>Capítulo 8: Aspectos de Seguridad y Vulnerabilidades .....</b>	<b>77</b>
Por qué escribí PGP .....	77
Fundamentos del cifrado .....	81
Cómo funciona la criptografía de clave pública .....	82
Cómo se cifran archivos y mensajes .....	83
Los algoritmos simétricos de PGP .....	84
Compresión de datos .....	86
Acerca de los números aleatorios usados como claves de sesión .....	86
Cómo funciona el descifrado .....	87
Cómo funciona la firma digital .....	87
Claves públicas, cómo protegerlas contra alteraciones .....	90

¿Cómo controla PGP qué claves son válidas? .....	93
Cómo evitar la exposición de sus claves privadas .....	95
Cuidado con el aceite de serpiente .....	97
Vulnerabilidades .....	101
Contraseña y clave privada comprometidas .....	101
Alteración de claves públicas .....	102
Archivos no del todo borrados .....	102
Fugas en la seguridad .....	105
Ataques Tempest .....	105
Protección contra fechados falsos .....	105
Exposición en sistemas multiusuario .....	106
Análisis de tráfico .....	107
Criptoanálisis .....	107
<b>Capítulo 9: Transferencia de Archivos entre MacOS y Windows usando PGP</b> .....	<b>108</b>
Envío desde MacOS a Windows .....	109
MacBinary: Sí .....	109
MacBinary: No .....	109
MacBinary: Inteligente .....	110
Recepción de archivos Windows en MacOS .....	111
Aplicaciones soportadas .....	111
<b>Glosario .....</b>	<b>113</b>
<b>Índice .....</b>	<b>117</b>



# Prefacio

Este libro describe cómo usar PGP® for Personal Privacy [PGP® para la Privacidad Personal] para Windows 95 y NT, Versión 5.5. PGP Versión 5.5 tiene nuevas opciones, descritas en el Capítulo 1.

Véase "Qué hay en este libro", al final del Prefacio, para más información sobre cada Capítulo.

## Convenios usados en este documento

### Tipos de notas:

**NOTA:**

Las notas proporcionan información adicional sobre cómo usar PGP... por ejemplo, si usted no está usando PGP/MIME, debe cifrar cualquier archivo que desee enviar como adjuntos desde el Explorador de Windows antes de enviar su mensaje.

**SUGERENCIA:**

Las sugerencias proporcionan guías para usar PGP eficientemente... por ejemplo, cómo usar una frase de contraseña útil.

**ALERTA:**

Si usted usa Tachar PGP para borrar un atajo de Windows a una aplicación, también está borrando la propia aplicación.

## Para más información

Hay diversos procedimientos para averiguar más sobre Network Associates y sus productos

### Desde la Web

El sitio Web de Network Associates, Inc. proporciona información sobre nuestra organización, nuestros productos, actualizaciones de productos y temas relacionados, tales como Asuntos de Privacidad. Visítenos en:

<http://www.nai.com>

También puede localizarnos desde AOL y Compuserve como:

Go NAI

## Soporte Técnico

PGP no facilita Soporte Técnico para sus productos gratuitos [freeware]. Visite nuestra página web en <http://www.nai.com> para información sobre cómo adquirir nuestros productos.

## Se agradece su colaboración

Mejoramos continuamente PGP y agradecemos las aportaciones de los clientes al diseñar nuevas versiones. Apreciamos su interés en PGP y sus ideas sobre contenidos y funciones de productos. Aportaciones como la suya nos ayudan a desarrollar programas y servicios más ricos y sencillos de usar. Si bien no podemos incorporar todas las sugerencias, daremos a sus aportaciones una seria consideración al desarrollar productos futuros.

Si desea hacernos llegar sus ideas, por favor envíenos un mensaje de correo electrónico a [win-doc@pgp.com](mailto:win-doc@pgp.com)

## Lectura básica 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 *Email Security*, John Wiley & Sons, 1995

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

## Otra bibliografía

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

Lai, Xueia, 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 20

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

## **Contenido de este manual**

El Capítulo 1 presenta el programa PGP y proporciona un repaso rápido.

El Capítulo 2 describe cómo instalar y ejecutar PGP.

El Capítulo 3 describe cómo hacer e intercambiar claves PGP.

El Capítulo 4 describe cómo usar PGP para enviar y recibir correo electrónico privado. Asimismo discute cómo usar PGP para enviar correo electrónico cifrado a grupos de personas.

El Capítulo 5 describe cómo usar PGP para almacenar datos de forma segura en su equipo informático o servidor de archivos, y explica cómo usar Tachar PGP [PGP Wipe].

El Capítulo 6 describe cómo establecer las preferencias de PGP.

El Capítulo 7 contiene mensajes de error para la corrección de problemas en PGP.

El Capítulo 8 fue escrito por Phil Zimmerman, fundador de PGP, y describe la seguridad y las vulnerabilidades de la protección de datos.

El apéndice A discute cómo PGP trata con la transferencia de archivos entre los sistemas operativos Macintosh y Windows.

El glosario contiene definiciones de términos usados en esta guía.

# Introducción

¡Bienvenido a PGP! Con PGP for Personal Privacy [PGP para la Privacidad Personal], usted puede proteger de un modo fácil y seguro la privacidad de sus mensajes de correo electrónico y archivos adjuntos, cifrándolos de modo que solamente los destinatarios puedan leerlos. También puede firmar digitalmente mensajes y archivos, asegurando su autenticidad. Un mensaje firmado verifica que la información en él no ha sido adulterada de ningún modo.

## Lo nuevo en PGP Versión 5.5

PGP Versión 5.5 incluye estas nuevas características:

- \* Usted puede crear grupos de destinatarios, en los que selecciona las claves de un grupo de personas y cifra el correo a todas ellas simultáneamente.
- \* Nueva capacidad de integración para servidor de claves que puede usar para guardar, buscar y sincronizar claves automáticamente.
- \* Una nueva ventana Buscar Clave que puede usar para localizar claves en servidores remotos con la misma interfaz de usuario que usa para buscar en su archivo de claves.
- \* Nuevo PGPkeys que puede usar para cifrar, firmar, descifrar, verificar o borrar de modo irreversible desde el Explorador de Windows.
- \* Una opción Tachar [Wipe] PGP que sobrescribe archivos de modo que no puedan ser recuperados con herramientas de software.
- \* Un menú Ver configurable que proporciona información sobre las claves de su archivo de claves.

## Lo nuevo en la documentación de PGP Versión 5.5

Esta guía contiene información sobre PGP Versión 5.5. La documentación de PGP tiene las siguientes características nuevas:

- \* Los manuales de usuario contienen información conceptual y procedimientos para el uso de PGP. La Ayuda en línea es escrita de manera específica para cada complemento de programa [plug-in], y contiene información más detallada sobre cómo usarlo.
- \* PGP Versión 5.5 para Windows incluye Ayuda en línea, y una copia electrónica de la documentación está disponible en formato Adobe Acrobat en el CD ROM PGP Versión 5.5.

## **Cómo usar PGP**

Uno de los modos más convenientes de usar PGP es a través de una de las aplicaciones de correo electrónico soportada por los complementos PGP. Con estas aplicaciones, usted puede cifrar y firmar, así como descifrar y verificar mensajes, mientras redacta y lee su correo con el clic de un botón.

Si usted está usando una aplicación de correo electrónico que no es soportada por los complementos PGP, puede usar PGPtools para realizar las funciones PGP en archivos. También puede usar PGP para cifrar y firmar archivos del disco duro de su equipo para guardarlos en forma segura de modo que datos sensibles no puedan ser recuperados por otros.

## **Repaso rápido**

PGP está basado en una tecnología de cifrado ampliamente aceptada conocida como criptografía de clave pública, en la cual dos claves complementarias llamadas par de claves, son usadas para mantener comunicaciones seguras. De ellas, una es una clave privada a la cual solamente usted tiene acceso, y la otra es una clave pública que usted intercambia libremente con otros usuarios PGP. Ambas claves, su clave privada y su clave pública, son guardadas en archivos de claves, siendo accesibles desde la ventana PGPkeys. Es desde esta ventana que usted realiza todas sus funciones de administración de claves.

Para enviar a alguien un mensaje de correo electrónico privado, usted usa una copia de la clave pública de esa persona para cifrar la información, la cual solamente podrá ser descifrada usando la clave privada de esa persona. Al contrario, cuando alguien desea enviarle correo cifrado usa una copia de la clave pública de usted para cifrar los datos, los cuales solamente usted podrá descifrar usando su clave privada. También puede usar PGP para cifrar o firmar archivos que son guardados en su equipo, para autenticar que no han sido alterados.

Usted también puede usar su clave privada para firmar el correo electrónico dirigido a otros o para firmar archivos para autenticarlos. Los destinatarios pueden entonces usar una copia de la clave pública suya para asegurarse que fue realmente usted quien envió el mensaje de correo electrónico, y que no fue alterado mientras estaba en tránsito. Cuando alguien le envía un mensaje

de correo electrónico con una firma digital, usted usa una copia de la clave pública de esa persona para comprobar la firma digital y asegurarse que nadie haya adulterado el contenido del mensaje.

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

El resto de esta sección echa una rápida mirada a los procedimientos que usted normalmente sigue al usar PGP. Para más detalles concernientes a cualquiera de estos procedimientos, refiérase a los Capítulos apropiados de este libro.

## **Creación de un par de claves**

Antes de empezar a usar PGP, usted necesita generar un par de claves. Un par de claves PGP está compuesto de una clave privada a la cual solamente usted tiene acceso, y una clave pública que usted puede copiar y hacer disponible libremente a cualquiera con quien intercambie información.

Usted tiene la opción de crear un nuevo par de claves inmediatamente después de haber finalizado el procedimiento de instalación de PGP, o puede hacerlo en cualquier momento abriendo la aplicación GPGkeys.

## **Intercambio de claves públicas con otros usuarios**

Después de haber creado un par de claves, puede empezar a intercambiar correspondencia con otros usuarios de PGP. Usted necesitará una copia de la clave pública de ellos, y ellos necesitarán una copia de la suya. Su clave pública es un simple bloque de texto, de modo que es fácil intercambiar claves con cualquiera. Usted puede incluir su clave pública en un mensaje de correo electrónico, copiarla a un archivo, o publicarla en un servidor de claves público o corporativo donde cualquiera pueda obtener una copia cuando la necesite.

## **Validación de sus claves**

Una vez obtenida una copia de la clave pública de alguien, puede agregarla a su archivo de claves públicas. Debería entonces asegurarse que la clave no ha sido alterada, y que realmente pertenece al usuario deseado. Para ello debe comparar la huella única de su copia de la clave pública de esa persona, con la huella de la clave original de esa persona. Cuando esté seguro que tiene una clave pública válida, fírmela para indicar que su uso es seguro. Además, usted puede conceder al usuario de la clave un nivel de confianza que indica cuánta confianza tiene usted en esa persona para garantizar la autenticidad de la clave pública de otra persona.

## **Cifrado y firma de sus mensajes de correo electrónico y archivos**

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

- \* Si está usando una aplicación de correo electrónico soportada por los complementos PGP, puede cifrar y firmar sus mensajes seleccionando las opciones apropiadas desde la barra de herramientas de su aplicación.
- \* Si su aplicación de correo electrónico no está soportada por los complementos PGP, puede copiar el mensaje al portapapeles y realizar desde allí las funciones apropiadas. También puede cifrar y firmar archivos desde el Explorador de Windows antes de adjuntarlos a su correo electrónico. El cifrado asegura que solamente usted y los destinatarios pueden descifrar el contenido de los archivos; la firma asegura que cualquier alteración será rápidamente advertida.

## **Descifrado y verificación de sus mensajes de correo electrónico y archivos**

Cuando alguien le envía correo electrónico cifrado, usted puede descifrar el contenido y verificar cualquier firma agregada para asegurarse que los datos fueron originados por el presunto remitente y que no fueron alterados.

- \* Si está usando una aplicación de correo electrónico que es soportada por los complementos PGP, puede descifrar y verificar sus mensajes seleccionando las opciones apropiadas desde la barra de herramientas de su aplicación.
- \* Si su aplicación de correo electrónico no está soportada por los complementos PGP, puede copiar el mensaje al portapapeles y realizar las funciones apropiadas desde allí. Si desea descifrar y verificar los archivos adjuntos, puede hacerlo desde el Explorador de Windows. También puede descifrar archivos cifrados guardados en su equipo, y verificar archivos firmados para asegurarse que no han sido modificados.

## **Tachado irreversible de archivos**

Cuando necesite borrar permanentemente un archivo, puede usar la opción Tachar [Wipe] para asegurarse que el archivo sea irrecuperable. El archivo es entonces inmediatamente sobrescrito de modo que no pueda ser recuperado usando herramientas de recuperación de datos.

# Puesta en Marcha

Este Capítulo explica cómo hacer funcionar PGP, y proporciona una vista rápida a los procedimientos que usted normalmente sigue al usar el producto. También contiene una tabla de los iconos usados con PGPkeys.

## Requerimientos de sistema

Estos son los requerimientos de sistema para instalar PGP Versión 5.5:

- \* Windows 95 o NT
- \* 8 MB de RAM
- \* 15 MB de espacio en el disco duro

## Compatibilidad con otras versiones

PGP pasó por muchas revisiones desde que fue publicado como producto de dominio público por Phil Zimmermann en 1991. Aunque esta versión de PGP presenta una diferencia importante con el programa original e incorpora una interfaz de usuario completamente nueva, ha sido diseñada para ser compatible con las versiones anteriores de PGP. Esto significa que usted puede intercambiar correo electrónico seguro con personas que todavía están usando estas versiones más antiguas del producto:

- \* PGP 2.6 (Distribuidas por el MIT)
- \* PGP 2.7x para Macintosh (Publicada por Via Crypt)
- \* PGP 4.0 (Publicada por Via Crypt)
- \* PGP 4.5 (Publicada por PGP, Inc.)
- \* PGP for Personal Privacy, Versión 5.0



\* PGP for Business Security, Versión 5.5

## **PGP for Personal Privacy**

PGP for Personal Privacy Versión 5.5 soporta el uso de un tipo de clave: Diffie-Hellman/DSS. Usando PGP Versión 5.5 for Personal Privacy, usted solamente puede crear claves que usen tecnologías de cifrado Diffie-Hellman y de firma digital DSS. La porción DSS de la clave es usada para firmar, y la Diffie-Hellman para el cifrado.

No se pueden usar claves RSA existentes para descifrar y verificar mensajes o archivos cifrados o firmados, ni tampoco generar claves RSA nuevas. Usando esta versión de PGP para Privacidad personal, no puede usar claves ya existentes que fueron creados usando algoritmos de cifrado RSA. Si usted está intercambiado mensajes de correo electrónico o archivos con personas que usan una versión más antigua de PGP, deberían actualizarse a una de las versiones de PGP más nuevas para aprovecharse de las nuevas interfases de usuario y opciones.

[Nota de Traducción: La versión PGP Internacional 5.5.3i sí tiene la opción de generar, usar y administrar claves tipo RSA]

## **PGP for email and files**

PGP for email and files Versión 5.5 es un producto diseñado para ser usado en entorno empresarial. Usted debería estar al tanto de algunas características que contiene si piensa mantener correspondencia con personas que lo usan. PGP for email and files ofrece una Clave de Firma Corporativa y Claves de Descifrado Adicionales Entrante y Saliente.

Una Clave de Firma Corporativa es una clave pública que es diseñada como la clave de la empresa en la cual todos los usuarios pueden confiar para firmar otras claves.

Las Claves de Descifrado Adicionales son claves que permiten que bajo ciertas circunstancias el personal de seguridad descifre mensajes que hayan sido enviados por o hacia empleados de la empresa. La Clave de Descifrado Adicional Entrante hace que el correo cifrado enviado al personal de una empresa también sea cifrado a la Clave de Descifrado Adicional. La Clave de Descifrado Adicional Saliente hace que el correo enviado por personal de la empresa también sea cifrado con la Clave de Descifrado Adicional Saliente. Usted puede usar el menú Propiedades de Clave para determinar si una clave contiene una Clave de Descifrado Adicional asociada con ella, y será alertado si está cifrando a una clave que contiene una Clave de Descifrado Adicional.

## **PGP/MIME, su uso**

PGP/MIME es una norma para algunos de los complementos PGP que integran las funciones PGP directamente a las aplicaciones de correo electrónico populares. Si usted está usando una aplicación de correo electrónico que es soportada por uno de los complementos que ofrecen PGP/MIME, será capaz de cifrar y firmar, así como descifrar y autenticar automáticamente sus mensajes de correo electrónico y archivos adjuntos cuando envíe o reciba su correo electrónico.

Sin embargo, antes de enviar correo electrónico PGP/MIME verifique que los destinatarios estén usando una aplicación de correo electrónico que soporte esta norma, porque si no es así podrían tener dificultades para descifrar y autenticar sus mensajes. También puede cifrar mensajes y archivos sin usar PGP MIME. Para ello deje sin seleccionar esta opción en el menú Preferencias.

## Actualización desde una versión anterior

Si está actualizando desde una versión anterior de PGP (sea de PGP Inc. o Via Crypt), antes de instalar PGP podría desear borrar los archivos de programa antiguos para liberar espacio de disco. Sin embargo, deberá tener cuidado de no borrar los archivos de claves privadas y públicas usados para guardar cualquier clave que usted pudiera haber creado o recogido mientras usaba la versión anterior. Cuando usted instala PGP, tiene la opción de mantener sus archivos de claves públicas y privadas para evitarle la molestia de tener que importarlas desde sus archivos de claves antiguos. Para actualizar desde una versión anterior, siga los pasos indicados en esta sección:

### PGP Versión 2.6.2 o 2.7.1; actualización

1. Asegúrese de haber salido de todos los programas que hubiera estado usando en su equipo.
2. Haga copias de seguridad de sus archivos de claves PGP antiguos en otra unidad de volumen. Sus claves públicas están guardadas en `pubring.pgp` y sus claves privadas en `secring.pgp`.

**NOTA:**

Puede que usted desee hacer dos copias de seguridad separadas de sus archivos de clave en dos disquetes diferentes como para estar seguro. Sea especialmente cuidadoso en no perder su archivo de claves privadas, o nunca más podrá descifrar mensajes de correo electrónico o archivos adjuntos cifrados con las claves perdidas.

3. Cuando haya hecho una copia de seguridad de sus archivos de claves antiguos, borre o archive de su disco duro el programa PGP 2.6.2. Aquí tiene dos opciones:

Borrar manualmente el directorio PGP262 y todo su contenido.

Borrar manualmente el archivo de programa pgp.exe (2.6.2) y archivar los archivos restantes, especialmente los archivos de claves y config.txt.

**NOTA:**

Si obtiene una copia de la nueva versión actualizada PGP 2.6.4 del MIT, su antiguo software 2.6.x podrá leer las claves RSA en los nuevos archivos de claves 5.0, y no fallará cuando encuentre los nuevos formatos de claves DSS/Diffie-Hellman.

4. Instale PGP 5.5 usando el ejecutable InstallShield provisto.
5. Cuando el programa de instalación le pregunte si tiene archivos de claves existentes marque Sí, ubique sus archivos de claves 2.6.2 antiguos, y siga las instrucciones para copiar esas claves a sus archivos de claves PGP 5.5 nuevos.
6. Reinicie su equipo.

### **PGPmail 4.0; actualización**

Este proceso es el mismo que con PGP 2.6.2 (PGP Via Crypt debe ser borrado o archivado manualmente). Asegúrese de guardar copias de seguridad de sus archivos de claves. Vea también el archivo ReadMe de PGP 4.0.1 para Unix y DOS, los cuales describen la versión actualizada para leer los archivos de claves PGP 5.5 con el programa Via Crypt antiguo.

### **PGPmail 4.5; actualización**

1. Asegúrese de haber salido de todos los programas y procesos que estaba usando en su equipo.
2. Si el proceso PGP Enclyptor (enclrypt\_32.exe) está activo, finalícelo de modo que pueda ser desinstalado.

Para determinar si está activo el Enclyptor, busque su paleta flotante o su icono minimizado en la barra de tareas. También puede usar Control+Alt+Supr para desplegar el Administrador de Tareas, seleccionar el proceso The Enclyptor, y hacer clic sobre el botón Finalizar la tarea.

3. Desde el menú Inicio, seleccione Configuración, Panel de control.
4. Haga doble clic en Agregar o quitar programas.

5. Seleccione PGPmail 4.5
6. Haga clic sobre el botón Agregar/Quitar. La utilidad Desinstalar borra automáticamente todos los archivos necesarios, y actualiza su archivo de Registro de Windows.

**NOTA:**

Si durante la desinstalación se le pidiera borrar algunos archivos .dll, conteste Aceptar; es seguro quitarlos. El programa que instala PGP 5.5 instalará nuevas versiones de esos archivos.

7. Haga clic en Aceptar para completar la desinstalación y cerrar la ventana Agregar o quitar programas cuando esté completa.
8. Use la utilidad InstallShield para instalar el nuevo programa 5.5. Aunque no es obligatorio, se recomienda instalar en el directorio de instalación predeterminado.
9. Cuando el programa de instalación le pregunte si tiene archivos de claves existentes haga clic en Sí, localice sus archivos de claves PGP 4.5 antiguos, y siga las instrucciones para copiar esas claves a sus nuevos archivos de claves PGP 5.5.
10. Reinicie su equipo.

## **PGP Versión 5.0; actualización**

1. Asegúrese de haber salido de todos los programas y procesos que estaba usando en su equipo.
2. Finalice PGPtray si estuviera activo.

Para determinar si está activo PGPtray, busque en la barra de tareas un pequeño icono de un sobre PGP: si está presente, PGPtray está activo. Para finalizar la tarea, haga clic sobre el icono PGPtray y seleccione el comando Salir PGPtray al final del menú. También puede usar Control+Alt+Supr para desplegar el Administrador de Tareas, seleccionar el proceso PGPtray y hacer clic sobre el botón Finalizar la tarea.

3. Desde el menú Inicio, seleccione Configuración, Panel de control.
4. Haga doble clic en Agregar o quitar programas.
5. Seleccione PGP 5.0bNN

Haga clic sobre el botón Agregar/Quitar. Aparece el cuadro de diálogo Quitar archivo compartido. Se le pregunta Especificar el nombre de archivo y la ubicación.

**NOTA:**

Si durante la desinstalación se le pidiera borrar algunos archivos .dll, conteste Aceptar; es seguro quitarlos. El programa que instala PGP 5.5 instalará nuevas versiones de esos archivos.

6. Haga clic en Aceptar para completar la desinstalación y cerrar la ventana Agregar o quitar programas cuando esté completa.
7. Use la utilidad InstallShield para instalar el nuevo programa 5.5. Aunque no es obligatorio, se recomienda instalar en el directorio de instalación predeterminado.
8. Cuando el programa de instalación le pregunte si tiene archivos de clave existentes haga clic en Sí, localice sus archivos de claves PGP 5.0 antiguos, y siga las instrucciones para copiar esas claves a sus nuevos archivos de claves PGP 5.5.
9. Reinicie su equipo.

¡Ahora puede usar el nuevo software PGP5.5!

## PGP Versión 5.5; instalación

He aquí las formas de instalar PGP 5.5:

- \* Desde un CD ROM
- \* Desde el sitio Web de PGP.

**ALERTA:**

Si tiene instaladas versiones anteriores de PGP 5.5 debe quitar las versiones previas completamente. Vaya al menú Inicio, Configuración. Haga doble clic sobre Agregar o quitar programas. Seleccione PGP 5.5, haga clic sobre el botón Agregar o Quitar, y haga clic en Aceptar.

### Desde un CD ROM

1. Inicie Windows
2. Inserte el CD ROM
3. Ejecute el programa de instalación [Setup].
4. Siga las instrucciones de pantalla.

## **Desde el sitio Web de Network Associates**

1. Descargue el programa PGP en el disco duro de su equipo.
2. Haga doble clic sobre el icono del programa de instalación de PGP.
3. Siga las instrucciones de la pantalla.

## **Uso de PGP**

PGP funciona sobre los datos generados por otras aplicaciones. Por lo tanto, las funciones PGP apropiadas están diseñadas para estar inmediatamente disponibles para su uso según la tarea que usted esté realizando en un momento dado. Hay tres modos primarios de usar PGP:

- \* Desde la barra de tareas del sistema.
- \* Desde aplicaciones de correo electrónico soportadas [por PGP].
- \* Desde el menú del Explorador de archivos de Windows.

### **Barra de tareas de Windows; uso desde**

Usted puede acceder a muchas de las principales funciones de PGP haciendo clic sobre el icono de la llave y el candado que normalmente está ubicado en la barra de tareas del sistema, y eligiendo la opción apropiada del menú. (Si no puede encontrar este icono en la barra de tareas de su sistema, ejecute PGP desde el menú Inicio)

### **Portapapeles de Windows; uso desde**

Usted se dará cuenta que muchas de las opciones disponibles desde la barra de tareas se refieren a funciones PGP que se pueden realizar desde el portapapeles de Windows. Si está usando una aplicación de correo electrónico que no es soportada por los complementos de PGP, o si está trabajando con texto generado por alguna otra aplicación, realice sus funciones de cifrado/descifrado y firma/verificación mediante el portapapeles de Windows.

Por ejemplo, para cifrar o firmar texto, usted debe copiarlo desde su aplicación al portapapeles, lo cifra o firma usando las funciones PGP apropiadas, y luego lo pega nuevamente en su aplicación antes de enviarlo a los destinatarios. Cuando usted reciba un mensaje de correo electrónico cifrado o firmado, simplemente debe invertir el proceso y copiar el texto cifrado, [conocido como ciphertext en el idioma inglés] desde su aplicación al portapapeles, descifrarlo y

verificar la información, y luego leer el contenido. Después de leer el mensaje descifrado, puede decidir si guardar la información o mantenerla en su forma cifrada.

## **PGPkeys; cómo usar**

Cuando usted ejecuta PGPkeys, desde la ventana emergente PGP se abre la ventana PGPkeys, mostrando su par de claves, compuesto por la clave privada y la clave pública que usted ha creado, así como las claves públicas de otros usuarios que ha agregado a su archivo de claves (Si todavía no ha creado un nuevo par de claves, el Asistente de Claves PGP le guía a través de las etapas necesarias. Sin embargo, antes de atravesar el proceso de crear un nuevo par de claves, debería leer el Capítulo 3 por detalles completos sobre las diversas opciones).

Desde la ventana PGPkeys puede crear nuevos pares de claves, y administrar todas sus otras claves. Por ejemplo, aquí es donde usted examina los atributos asociados con una clave en particular, especifica cuánta confianza tiene usted en que la clave realmente pertenezca al verdadero propietario, e indica cuánto confía en el dueño de la clave para dar fe de la autenticidad de las claves de otros usuarios. Para una explicación más completa de las funciones de administración de claves que se realiza desde la ventana PGPkeys, vea el Capítulo 6.

## **Preferencias PGP; configuración**

Cuando usted elige Preferencias PGP desde la ventana emergente PGP, accede al cuadro de diálogo Preferencias PGP que especifica las configuraciones que afectan el funcionamiento del programa PGP de acuerdo al entorno de su sistema.

Haciendo clic en la ficha apropiada, puede avanzar a las configuraciones que desea modificar. Para una explicación más completa de estas configuraciones, vea el Capítulo 6.

## **Ayuda; cómo usar**

Cuando elige Ayuda desde el menú o ventana PGP, accede al sistema de Ayuda PGP, el cual proporciona una descripción general e instrucciones para todos los procedimientos que probablemente realice. Muchos de los cuadros de diálogos también tienen ayuda sensible al contexto a la que se accede haciendo clic sobre el signo de interrogación en el ángulo superior derecho de la ventana y apuntando luego al área de interés sobre la pantalla. Aparece luego una corta explicación.

## **Salir de PGP**

En forma predeterminada, el programa PGP funciona desde el momento que usted inicia su equipo, como se indica por el icono de la llave y el candado que se muestra en la barra de tareas del sistema. Si por alguna razón usted desea cerrar PGP desde la barra de tareas, puede hacerlo eligiendo Salir desde el menú emergente de PGP.

## Aplicaciones de Correo Electrónico, cómo usar PGP desde

Si tiene una de las aplicaciones de correo electrónico soportadas por los complementos PGP, puede acceder a las funciones PGP necesarias haciendo clic sobre los botones apropiados de la barra de tareas de su aplicación. Por ejemplo, haciendo clic sobre el icono del candado para cifrar su mensaje, y sobre el icono de la pluma estilográfica para firmarlo.



Cuando recibe correo electrónico de otro usuario PGP, usted descifra el mensaje y verifica la firma digital de la persona haciendo clic en el sobre abierto.



El botón de la llave y el sobre agrega cualquier clave incluida en el mensaje a su archivo de claves. También puede acceder a la ventana PGPkeys en cualquier momento mientras compone o recibe su correo haciendo clic sobre el botón PGPkeys.

Para simplificar aún más las cosas, si está usando una aplicación de correo electrónico con uno de los complementos que soportan la norma PGP/MIME, y está comunicándose con otro usuario cuya aplicación de correo electrónico también soporta la norma, ambos pueden cifrar y descifrar automáticamente sus mensajes de correo electrónico y archivos adjuntos cuando envíen o reciban su correo electrónico. Todo lo que se debe hacer es activar desde el cuadro de diálogo Preferencias PGP las funciones PGP/MIME de cifrado y firma.

Cuando recibe correo electrónico de alguien que use la norma PGP/MIME, el correo llega con un icono adjunto que indica que está cifrado con esa norma.

Para descifrar el texto y archivos adjuntos en el correo electrónico encapsulado PGP/MIME, y para verificar cualquier firma digital, simplemente debe hacer doble clic sobre el icono del sobre abierto.

## Explorador de Windows, uso de PGP desde



Usted puede cifrar y firmar o descifrar y verificar archivos tales como documentos de procesadores de texto, hojas de cálculo, e imágenes de vídeo directamente desde el Explorador de Windows. Si no está usando una aplicación de correo electrónico como el Eudora Qualcomm que soporta la norma PGP/MIME, o una aplicación como Exchange o Outlook que no requieren PGP para cifrar o firmar archivos, debe usar este método para adjuntar archivos que desea enviar junto con sus mensajes de correo electrónico. También podría desear cifrar y descifrar archivos que guarda en su propio equipo para evitar que otros puedan acceder a ellos.

Para acceder a las funciones PGP desde el Explorador de Windows, elija la opción apropiada desde el submenú PGP del menú Archivo. Las opciones que aparecen dependen del estado en que se encuentre el archivo que usted ha seleccionado. Si todavía no ha sido cifrado o firmado, en el menú aparecen las opciones para realizar estas funciones. Si el archivo ya ha sido cifrado o firmado, entonces se muestran las opciones para descifrar y verificar su contenido.

## **Destinatarios, cómo seleccionarlos**

Cuando envía correo electrónico a alguien cuya aplicación de correo electrónico está soportada por los complementos PGP, la dirección de correo electrónico del destinatario determina qué claves usar cuando se cifra el contenido. Sin embargo, si usted escribe un nombre de usuario o una dirección de correo electrónico que no corresponde con alguna de las claves de su archivo de claves públicas, o si está cifrando desde el portapapeles o desde el Explorador de Windows, debe seleccionar manualmente la clave pública del destinatario desde el cuadro de diálogo Selección de Clave PGP. Para seleccionar claves públicas de destinatarios, simplemente arrastre los iconos que representan sus claves dentro del cuadro de Destinatarios y luego haga clic en Aceptar.

Para las instrucciones completas sobre cómo cifrar/firmar, y descifrar/verificar correo electrónico, vea el Capítulo 4. Si desea cifrar archivos para guardarlos en su disco rígido o enviarlos como archivos adjuntos de correo electrónico, vea el Capítulo 5.














## **Atajos**







Aunque encontrará que PGP es fácil de usar, hay atajos para ayudarlo a realizar su tarea de cifrado aún más rápido. Por ejemplo, mientras usted administra sus claves en la ventana PGPkeys, puede apretar el botón derecho del ratón para realizar todas las funciones PGP necesarias, en vez de hacerlo desde la barra de menú. También puede arrastrar un archivo que contenga una clave dentro de la ventana PGPkeys para agregarla a su archivo de claves.

También están disponibles atajos de teclado para la mayoría de las operaciones de menú. Estos atajos de teclado se muestran en todos los menús PGP, y otros atajos son descritos en contexto a través de este manual.

## Iconos de PGPkeys, definiciones

La siguiente tabla muestra todos los mini-iconos usados en la ventana PGPkeys, junto a una descripción de lo que representan.

ICONO	QUÉ REPRESENTA
	Un par de llaves amarillas representa su par de claves Diffie-Hellman/DSS, que consta de su clave privada y su clave pública.
	Una sola llave amarilla representa una clave pública Diffie-Hellman/DSS.
	Un par de llaves azules representa su par de claves RSA, que consta de su clave privada y su clave pública.
	Una sola llave azul representa una clave pública RSA.
	Cuando un par de llaves está atenuado, temporalmente no está disponible para cifrar y firmar. Usted puede inhabilitar una clave desde la ventana PGPkeys, para evitar confusiones con las claves que usa siempre en el cuadro de diálogo Selección de Claves.
	Una llave atravesada por una línea roja indica que la clave ha sido revocada. Los usuarios revocan sus claves cuando no son más válidas o han sido comprometidas de algún modo. Una llave atravesada por una X roja indica que la clave es inválida.
	Una llave con un reloj indica que la clave ha caducado. La fecha de caducidad de la clave es establecida cuando es creada la clave.
	Un diamante representa al dueño de la clave y lista los nombres de usuario y direcciones de correo electrónicos asociados con la clave.
	Una llave con un reloj indica que la clave ha caducado. La fecha de caducidad de la clave es establecida cuando es creada la clave.
	Un sobre representa al dueño de la clave y lista los nombres de usuario y direcciones de correo electrónico asociados con la clave.
	Un círculo vacío indica que la clave es inválida.
	Un círculo verde indica que la clave es válida. Un círculo rojo indica que la clave tiene asociada una Clave de Descifrado Adicional.
	Un diamante verde indica que usted posee la clave, y que tiene confianza implícita.

ICONO	QUÉ REPRESENTA
	<p>Un lápiz o una estilográfica indica las firmas de los usuarios PGP que responden por la autenticidad de la clave. Una firma atravesada por una línea roja indica una firma revocada. Una firma atravesada por una X roja indica una firma mala o inválida. Una firma con una flecha azul próxima a ella indica que es exportable.</p>
	<p>Una pluma de ave indica la firma de los usuarios PGP que han garantizado la autenticidad de la clave. Una firma atravesada por una línea roja indica una firma revocada. Una firma atravesada por una X roja indica una firma mala o inválida.</p>
	<p>Una barra vacía indica una clave inválida, o desconfianza en el usuario.</p>
	<p>Una barra llena por la mitad indica una clave con validez marginal, o confianza marginal en el usuario.</p>
	<p>Una barra llena indica una clave con validez completa, o confianza completa en el usuario.</p>
	<p>Una barra con franjas indica una clave con validez implícita y confianza implícita en el usuario. Esta configuración está disponible solamente para los pares de claves creados por vd</p>

# Creación e Intercambio de Claves

Este Capítulo describe cómo generar el par de claves, pública y una clave privada que necesita para intercambiar correspondencia con otros usuarios de PGP. También explica cómo distribuir su clave pública y obtener las claves públicas de otros para poder empezar a intercambiar correo electrónico privado y autenticado.

## Conceptos clave

PGP está basado en un sistema de criptografía de clave pública ampliamente aceptado y confiable, por el cual usted y otros usuarios de PGP generan un par de claves, que consiste de una clave privada y una clave pública. Como su nombre indica, solamente usted tiene acceso a su clave privada, pero para poder mantener correspondencia con otros usuarios de PGP necesita una copia de las claves públicas de ellos, y ellos necesitan una copia de la clave pública suya. Usted usa su clave privada para firmar los mensajes de correo electrónico y archivos adjuntos que envía a otras personas, y para descifrar los mensajes y archivos que otras personas le envían a usted. Al contrario, usted puede usar las claves públicas de otras personas para enviarles mensajes de correo electrónico cifrado, y para verificar sus firmas digitales.

### NOTA:

Sin entrar en demasiados detalles técnicos, usted podría estar interesado en saber que no es realmente el contenido del mensaje de correo electrónico el que es cifrado usando el esquema de cifrado de clave pública. En vez de eso, los datos son cifrados usando un algoritmo de clave única mucho más rápido, y realmente es esta clave única la que está cifrada usando la clave pública del destinatario. El destinatario entonces usa su clave privada para descifrar esta clave, la cual le permite descifrar los datos.

## Par de claves

A menos que usted ya lo haya hecho mientras usaba otra versión de PGP, lo primero que necesita hacer antes de enviar o recibir mensajes de correo electrónico cifrados y certificados es crear un nuevo par de claves. Un par de claves consiste de dos claves: una clave privada que solamente usted posee y una clave pública que usted distribuye libremente a aquellos con quienes desea mantener correspondencia. Usted genera un nuevo par de claves desde la ventana PGPkeys usando el Asistente de Generación de Claves PGP, el cual lo guía a través del proceso.

**ALERTA:**

Si usted está actualizando desde una versión anterior de PGP, probablemente ya haya generado una clave privada, y distribuido la clave pública que la complementa a aquellos con quienes desea mantener correspondencia. En tal caso, no tiene que hacer un nuevo par de claves (como es descrito en la sección siguiente). En vez de eso, especifique la ubicación de sus claves cuando abre la ventana PGPkeys. Puede ir al menú Edición en la ventana PGPkeys y elegir Preferencias. Seleccione la ficha Archivo e introduzca la ruta correcta a sus claves existentes en cualquier momento.

**Creación de un nuevo par de claves**

1. Haga clic sobre el botón de inicio de Windows y elija PGPkeys desde el submenú PGP del menú Programas, o desde PGPtray. También puede abrir esta ventana haciendo clic sobre el icono de las llaves dobles ubicado en la barra de herramientas de su aplicación de correo electrónico.

Se abre la ventana PGPkeys.

2. Elija Nueva desde el Menú Claves.

El Asistente de Generación de Claves PGP proporciona alguna información introductoria en la primer pantalla.

3. Una vez leída esta información haga clic en Siguiente para avanzar a la pantalla siguiente.

El Asistente de Generación de Claves PGP le pide que escriba su nombre de usuario y dirección de correo electrónico.

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

No es absolutamente necesario escribir su nombre real o aún su dirección de correo electrónico. Sin embargo, usando su nombre real facilita que otros lo identifiquen como el dueño de su clave pública. También, usando su dirección de correo electrónico correcta, usted y los demás pueden aprovechar una característica del complemento PGP [plug-in], que automáticamente busca en su archivo de claves la clave apropiada, cuando dirige el correo a un destinatario en particular.

5. Haga clic en Siguiente para avanzar a la pantalla siguiente.

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

6. Elija un tamaño de clave entre 768 y 3072 bits, o escriba un tamaño personalizado entre 512 y 4096 bits.

**NOTA:**

Podría tomar un largo tiempo generar una clave de un tamaño personalizado, dependiendo del equipo que usted esté usando.

El tamaño de la clave corresponde al número de bits usado para construir su clave digital. Cuanto más grande es este número, menor es la posibilidad que alguien pueda descubrirla, pero mayor el tiempo que tomará realizar los procesos de cifrado y descifrado. Usted necesita buscar un balance entre la conveniencia de realizar las funciones PGP en forma rápida con una clave más pequeña, y el mayor nivel de seguridad provisto por una clave más grande. Usted está seguro si usa una clave compuesta de 1024 bits, a menos que intercambie información extremadamente sensible que interese lo suficiente como para que alguien esté dispuesto a montar un ataque criptográfico caro y lento.

7. Haga clic en **Siguiente** para avanzar a la pantalla siguiente.

El Asistente de Generación de Claves PGP le pedirá que indique cuándo debería caducar el par de claves.

8. Indique cuándo desea que caduquen sus claves. Puede aceptar la opción predeterminada que es **Nunca**, o poner un número específico de días después del cual las claves caducarán.

Una vez creado su par de claves y después de haber distribuido su clave pública al mundo, usted probablemente continuará usando las mismas claves a partir de entonces. Sin embargo, bajo ciertas condiciones usted probablemente desee crear un par de claves especiales con el propósito de usarlo solamente por un período limitado de tiempo. En este caso, cuando la clave pública caduca usted no puede usarla más para cifrar correo, pero todavía puede ser usada por otros para verificar su firma digital. Similarmente, cuando su par de claves caduca, todavía puede ser usado por usted para descifrar correo que le fue enviado antes que caducara su clave pública, pero no puede ser usado más para firmar correo a dirigido otros.

9. Haga clic en **Siguiente** para avanzar a la pantalla siguiente.

El Asistente de Generación de Claves le pide que escriba una contraseña.

10. En el cuadro de diálogo **Contraseña PGP**, escriba la secuencia de caracteres o palabras que desee usar para mantener acceso exclusivo a su clave privada. Para confirmar lo que ha escrito, avance a la siguiente línea con la tecla de **Tabulación**, y repita la contraseña.

Como seguridad adicional, los caracteres que usted escribe para la frase de contraseña normalmente no aparecen sobre la pantalla. Sin embargo, si usted está seguro que nadie

está mirando y desea ver los caracteres de su contraseña a medida que los escribe, desactive el casillero Ocultar Escritura.

**SUGERENCIA:**

Su frase de contraseña debería contener muchas palabras y puede incluir espacios, números, y caracteres de puntuación. Elija alguna que pueda recordar con facilidad, pero que otros no puedan adivinar. La frase de contraseña distingue entre letras mayúsculas y minúsculas. Cuanto más larga su frase de contraseña y mayor la variedad de caracteres que contiene, más segura es. Las frases de contraseñas seguras incluyen letras mayúsculas y minúsculas, números, signos de puntuación y espacios pero son olvidadas más fácilmente. Para más información, vea "Frase de contraseña, cómo recordarla", más adelante en este Capítulo.

La barra Calidad muestra la vulnerabilidad de su frase de contraseña comparada con la vulnerabilidad de la clave que está siendo generada. Una barra llena significa que son aproximadamente equivalentes.

11. Haga clic en **Siguiente** para empezar el proceso de generación de claves.

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

Si usted ha escrito una frase de contraseña inadecuada, aparece un mensaje de alerta antes que sean generadas las claves, y usted tiene la opción de aceptar la frase de contraseña mala o ingresar una más segura antes de continuar.

Si no hay suficiente información aleatoria sobre la cual construir la clave, aparece la pantalla Datos Aleatorios PGP. Como se instruye en la pantalla, mueva su ratón y efectúe una serie de pulsaciones aleatorias hasta que la barra de progreso se llene por completo. Sus movimientos del ratón y teclados generan la información aleatoria necesaria para crear un par de claves único.

**NOTA:**

PGP Versión 5.0 y posteriores están constantemente recogiendo datos aleatorios de muchas fuentes del sistema, incluyendo posición del ratón, temporización, y teclados. Si no aparece la pantalla Datos Aleatorios, significa que PGP ya ha recogido todos los datos que necesita.

Después de empezado el proceso de generación de claves, podría tomar algún tiempo la creación. De hecho, si usted especifica un tamaño distinto a los valores predeterminados para una clave Diffie-Hellman/DSS, la opción de generación rápida no es usada, y le podría llevar horas generar su clave para un tamaño de clave mayor. Al final, el Asistente de Generación de Claves PGP indicará que el proceso de generación de claves ha concluido.

12. Haga clic en **Siguiente** para avanzar a la pantalla siguiente.

Si está creando una clave con el mismo nombre de usuario o dirección de correo electrónico que una clave anterior, tiene la oportunidad de firmar la nueva clave con su clave anterior. Esto dota a su nueva clave con el mismo nivel de validez y confianza que su clave más antigua cuando es agregada al archivo de claves de alguien. La validez está basada en quiénes han firmado la clave en el pasado, pero en la clave nueva no se incorporan las demás firmas de su clave anterior.

13. Si corresponde, firme su nueva clave con la más vieja y escriba la frase de contraseña de la clave más vieja, y luego haga clic en Siguiente.

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

14. Especifique si desea que su nueva clave pública sea enviada al servidor de claves, y luego haga clic en Siguiente.

Cuando usted envía su clave pública al servidor de claves, quien tenga acceso al mismo puede obtener una copia de su clave cuando la necesite. Por detalles completos, vea "Distribución de su clave pública" más adelante en este Capítulo.

Cuando el proceso de generación está completo, aparece la pantalla final.

15. Haga clic en Terminar.

En la ventana PGPkeys aparece un par de llaves que representa su par de claves recientemente creado. Sepa que las claves RSA son las representadas por las llaves azules de tipo antiguo, y las claves más nuevas Diffie-Hellman/DSS por las llaves amarillas de tipo moderno.

## **Frase de contraseña, cómo recordarla**

Cifrar un archivo y luego encontrarse usted mismo imposibilitado de descifrarlo es una lección dolorosa, que le conduce a aprender cómo elegir una frase contraseña que usted recordará. Una palabra de contraseña es vulnerable a un "ataque de diccionario" que consiste en hacer que una PC pruebe todas las palabras del diccionario hasta encontrar su contraseña. Para protegerse de este tipo de ataques, es ampliamente recomendada la creación de una palabra que incluya una combinación de letras mayúsculas y minúsculas, números, signos de puntuación y espacios. Esto resulta en una contraseña de una palabra más segura pero oscura, que usted probablemente no recuerde fácilmente. No recomendamos que usted use una contraseña de una sola palabra.

Una frase de contraseña es menos vulnerable al ataque del diccionario. Se efectúa fácilmente usando múltiples palabras en su contraseña, en vez de intentar impedir un ataque de diccionario insertando arbitrariamente en su palabra de contraseña un montón de caracteres raros,



no alfabéticos, con el propósito de enmascararla, lo que puede hacerla demasiado fácil de olvidar, y llevarlo a una pérdida desastrosa de información si usted no puede descifrar sus propios archivos. Sin embargo, a menos que la frase de contraseña que usted elija sea alguna que pueda memorizar fácilmente por mucho tiempo, probablemente no la recuerde al pie de la letra.

Elegir una frase sin pensar, probablemente resulte en que la olvide por completo. Elija algo que ya se encuentre en su memoria. Busque profundamente dentro de su memoria tratando de recordar algún dicho inocente que usted haya escuchado hace algunos años y no olvida. No debe ser algo que usted haya repetido a otros recientemente, ni una frase famosa, porque lo que usted desea es que sea difícil atacarla o adivinarla con equipos sofisticados. Si ya está profundamente metida en su memoria, probablemente no la olvidará.

Por supuesto, si usted es lo suficientemente imprudente como para escribir su contraseña en un papel pegado a su monitor o dentro de su escritorio, no importa lo que elija.

## **Protección de la clave**

Una vez que haya generado un par de claves, es conveniente hacer una copia y ponerla en un lugar seguro para el caso que algo le suceda al original. Sus claves privadas y públicas son guardadas en archivos de claves separados, que usted puede copiar como cualquier archivo en otra ubicación de su disco duro, o en un disquete. En forma predeterminada, el archivo de claves privadas (`secring.skr`) y el archivo de claves públicas (`pubring.pkr`), son guardados junto a los demás archivos de PGP en el directorio que los contiene, pero usted puede guardar sus copias de seguridad donde guste. PGP crea copias de seguridad de sus claves públicas y privadas cuando genera estas claves. Estas copias son llamadas `pubring.pkr.bak` y `secring.skr.bak`.

Además de hacer copias de seguridad de sus claves, debería ser especialmente cuidadoso acerca de dónde guarda su clave privada. Aún cuando su clave privada está protegida por una contraseña que solamente usted debería conocer, es posible que alguien pudiera descubrir su contraseña y entonces usar su clave privada para descifrar sus mensajes de correo electrónico o firmar con su firma digital. Por ejemplo, alguien podría mirar por encima de su hombro y ver las teclas que usted pulsa para escribir su contraseña, o interceptar su contraseña desde otro equipo conectado en red, o capturarla de las emisiones de radiofrecuencia que emite su equipo.

Para prevenir que alguien que pudiera haber obtenido su contraseña use su clave privada, debería guardarla solamente en su equipo. Si su equipo está conectado a otros en una red, debe asegurarse que sus archivos no sean incluidos automáticamente en las copias de seguridad del sistema, donde otros pudieran tener acceso a su clave privada. Dada la facilidad con la que los equipos son accesibles a través de las redes, si está trabajando con información extremadamente sensible le convendría tener su clave privada en un disquete, que inserta al modo antiguo como si fuera una llave cuando desea leer o firmar su correo privado.

Como otra precaución de seguridad, considere asignar un nombre diferente a su archivo de claves privadas, y guárdelo en un lugar donde no sea fácil de ubicar, distinto al directorio que contiene los archivos de PGP.

## **Distribución de su clave pública**

Después de crear sus claves, necesita hacerlas disponibles a otros para que puedan enviarle correo electrónico cifrado y verifiquen su firma digital. Usted 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 a un archivo de texto.

Su clave pública se compone básicamente de un bloque de texto, así que resulta bastante fácil hacerla disponible a través de un servidor de claves público, incluirla en un mensaje de correo electrónico o exportarla/copiarla a un archivo. El destinatario puede entonces usar el método más conveniente para añadir su clave pública, a su propio archivo de claves públicas.

## **Servidor de claves, hacer disponible su clave pública**

El mejor método para hacer disponible su clave pública es ubicarla en un servidor de claves públicas donde cualquiera pueda accederla. De este modo, la gente puede enviarle mensajes de correo electrónico cifrado sin tener que pedirle explícitamente una copia de su clave. También le libera a usted y otros de tener que mantener un gran número de claves públicas que usted raramente usa. Hay un número de servidores de claves públicas en todo el mundo, incluyendo aquellos ofrecidos por Network Associates, Inc., en los que usted puede hacer disponible su clave para que cualquiera acceda a ella.

### **Envío de su clave pública a un servidor de claves**

1. Abra la ventana PGPkeys haciendo clic sobre el icono de la llave y el candado en la Barra de Tareas del sistema.
2. Seleccione el icono que representa la clave pública que desea publicar en el servidor.
3. Desde el menú Claves elija Enviar a Servidor. Como alternativa, puede apretar el botón derecho del ratón y elegir Enviar a Servidor de Claves desde el menú emergente.

4. Desde el submenú **Enviar a Servidor**, elija el servidor de claves al cual desea enviar sus claves. Dependiendo de su entorno PGP, puede tener varios para elegir.

Después de ubicar una copia de su clave pública en un servidor de claves, puede pedirle a la gente que desee enviarle mensajes de correo electrónico cifrado o verificar su firma digital, que obtenga una copia de su clave desde el servidor de claves. Aún si usted no les da todos los detalles de su clave, pueden obtener una copia buscando en el servidor de claves por su nombre o dirección de correo electrónico. Mucha gente incluye al final de sus mensajes de correo electrónico la dirección de Internet de sus claves públicas; el destinatario sólo tiene que hacer doble clic sobre la dirección para acceder a una copia de la clave en el servidor de claves.

Si alguna vez necesita cambiar su dirección de correo electrónico, o si adquiere nuevas firmas, todo lo que tiene que hacer para reemplazar su clave antigua es enviar una nueva copia al servidor de claves, y toda la información es automáticamente actualizada. Sin embargo, tenga en mente que los servidores de claves solamente son capaces de agregar información, y no permiten eliminar nombres y firmas de usuarios. Si alguna vez su clave queda comprometida puede revocarla, lo cual dice al mundo que no confíe más en esa versión de su clave. Vea el Capítulo 6 para más detalles sobre cómo revocar una clave.

## **Inclusión de 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.

### **Incluir su clave pública en un mensaje de correo electrónico**

1. Abra la ventana PGPkeys haciendo clic sobre el icono del candado y la llave en la Barra de Tareas del sistema.
2. Seleccione su par de claves y luego elija Copiar desde el menú Edición.
3. Abra el editor que usted usa para componer sus mensajes de correo electrónico, ubique el cursor en el área deseada, y luego desde el menú Edición elija Pegar. En las aplicaciones de correo electrónico más nuevas, sólo tiene que arrastrar su clave desde la ventana PGPkeys al texto de su mensaje de correo electrónico para transferir la información de la clave.

Cuando usted envía a alguien su clave pública, asegúrese de firmar el mensaje de correo electrónico. De ese modo el destinatario puede verificar su firma y asegurarse que nadie haya modificado la información a lo largo de su recorrido. Por supuesto, la única manera de asegurarse con certeza que la firma proviene de usted es verificando la huella de su clave si su clave no ha sido firmada por un presentador de confianza.

## Exportación de su clave pública a un archivo

Otro método de distribuir su clave pública es copiarla a un archivo y hacerlo disponible a la persona con quien desea comunicarse. Hay tres maneras de copiar su clave pública a un archivo:

- \* Seleccione el icono que representa su par de claves desde la ventana PGPkeys, luego elija Exportar desde el menú Claves, y escriba el nombre del archivo con el cual desea guardar su clave.
- \* Arrastre el icono que representa su par de claves desde la ventana PGPkeys y suéltelo en la ubicación deseada dentro de la ventana del Explorador de Windows.
- \* Seleccione el icono que representa su par de claves desde la ventana PGPkeys, elija Copiar desde el menú Edición y luego elija Pegar para insertar la información de la clave en un documento de texto.

## Obtención de las claves públicas de otros

Del mismo modo que usted necesita distribuir su clave pública a aquellos que desean enviarle correo cifrado o verificar su firma digital, usted necesita obtener las claves públicas de otros a quienes desee enviar correo cifrado o verificar sus firmas digitales. Usted tiene tres alternativas para obtener la clave pública de alguien:

- \* Obtener la clave de un servidor de claves público.
- \* Agregar la clave pública directamente desde un mensaje de correo electrónico.
- \* Importar la clave pública desde un archivo.

Las claves públicas son en realidad bloques de texto, de modo que son bastante fáciles de agregar a su archivo de claves importándolas desde un archivo o copiándolas desde un mensaje de correo electrónico y luego pegándolas a su archivo de claves públicas. Aquí está un ejemplo de un bloque de texto de una clave pública:

-----BEGIN PGP PUBLIC KEY BLOCK-----

```
mQENAjMCpkOAAEIALQiOUPrbStLJYfU7GGOX1QwrEkunvibLB8csCdfen9qPzKg
UZolEgBTE6RstgNyYEPQjMxmYozUBvRuag6WJdlJlpJ8/AFWVVOUACYUbxq8Vro4b
4RnMD7bjvy68MalGvV07vC2+jx0yx9FeOx1M4BURYxrfzLt9B8eP85CEjfcYAgCOcc/
6CW8iZWUlwwpNtVuirDdF6TCKmQ/K3gdbmUwHByxSo2PInG9jva+4vhUOKk71wQx
4k/1Tv68hKlqieGqnLonNWvQrPK2yv2BOKQ4Waf2xx25b5Cel7uNJDIEhp996nf2jnzG7
xkhdv3amXNODO2Gs4m3gTXWWEABRGOIk1pY2hhZUugSi4gSWFubmFtaWNvMDxta
malcGdwLmNvbT6JARUDBRAzX1b1Gs4m3gTXWWEBASP1B/4xAf+8HfUSRbq6XMx
MMVYNdVHGw+2bW9AG4JKwM/T8hmSq+Lj8VMpOMN1XzZmXVjxQ5Ln2HSgNAC
XtsA+sqCVd7xsXjIG72i+bioJtS4xQJHVsQ+mOmBYHlc67gobUSGO3iuqjDrJrB3P1
+4CwtFPTcE6mkfIYoKor20GAppJVbrpEAm3Fjs20+gDUC9NvogKzvOE1XOco6RQmZ
M7BMT3kDZe44UOp/JsxTBEzxpARxBCgKVXcQ08VXFbA/+oDdJ8EqLd/OckGunw31
2Nfd+fvGv5MKdva+JdsJzOK75xH3YHmQrpB/QUP8gMB/nnhclP2x1JbW/NcxXV0V9
riQEVAwUQMwQn4TP6oFK2L9UBAQEk7gf+IKstUhaBL9BRbF9RbMje9bdiHCEt8KR
x0A912/+IZG2ckY2rypBP7A3mPOTfs6MQWD9/A4fb5locld833GiOjEww/Uu2VBCZbZ
TR74PwuhJc6n2dsMvq01T6rql4SidCxwskaAveaf9qkKGbWapJF1G3gzl2dgsvKh26pA
ohD9NTvo13xj4aEL2xAvtcbjgVhXqW4Yk0YjHDci3TyelrEpkeJ5qjwEMX8HTnJRsVjX1pM
lIOEaZmrODk4AFbstRHwH2PbhRRkjtZg8CZn3F5WxzKwafjwM3aeTLt+Y2qtEwjnEr
ct6OIZA8Je/IDokt19XoOn20EWxjiOw+Hlka1QMFEDMOF4dleYS4x61m3QEBejOD/l
bJLL3Kuek9rOK/fwUdIRx/TZyVBUo3JCpiOEZVF7VhZo3GOWMuNYNSwmSoMMgs+
gyB8qOWsPldnugL4XpGlicvNLBP7Fbuw4iUN8coxXFOQP16RQ60Suu9r/SX3Qdcu39
HhzzzZVLYks+6AwtDmOuoOttzqpcgAd+3R9mWWm
=pz/6
-----END PGP PUBLIC KEY BLOCK-----
```

## Obtención de claves públicas mediante un servidor de claves

Si la persona a quien usted desea enviar correo cifrado es un usuario de PGP con experiencia, es posible que haya ubicado una copia de su clave pública en un servidor de claves públicas. En PGP Versión 5.5, usted puede buscar en el servidor de claves que es especificado en Preferencias PGP. Esto lo hace muy conveniente para que pueda obtener una copia de la clave más actualizada de esa persona cuando desee enviarle correo y también le libera de tener que guardar un montón de claves en su archivo de claves públicas.

Con PGP Versión 5.5, usted puede buscar una clave en el servidor de claves usando los siguientes métodos:

- \* Identificador de usuario [User ID]
- \* Identificador de Clave [Key ID]
- \* Tipo de Clave (Diffie-Hellman o RSA)
- \* Fecha de creación
- \* Fecha de caducidad
- \* Claves Revocadas

\* Claves Inhabilitadas

\* Claves firmadas por una clave en particular

La negación de estas operaciones también está disponible. Por ejemplo, si usted sabe que el identificador de usuario no es Roberto, puede buscar "ID Usuario" no es "Roberto".

### **Obtención de la clave pública de alguien de un servidor de claves públicas**

1. Abra la ventana PGPkeys haciendo clic sobre el icono del candado y la llave en la Barra de Tareas del sistema.
2. Desde la ventana PGPkeys, menú Ver, elija Buscar Clave.  
  
Aparece la pantalla Buscar.
3. Use el menú para introducir el criterio de búsqueda para localizar los usuarios de claves públicas.

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

### **Adición de claves públicas desde sus mensajes de correo electrónico**

Una manera conveniente de obtener 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 que es soportada por los complementos PGP, puede agregar la clave pública del remitente haciendo clic sobre un botón de la barra de herramientas de la aplicación. Por ejemplo, cuando un mensaje de correo electrónico llega con un bloque de texto que contiene la clave pública de alguien, haga clic sobre el botón de la llave y el sobre para guardar la clave en su archivo de claves públicas.

Si usted está usando una aplicación de correo electrónico que no está soportada por los complementos PGP, puede agregar la clave pública al archivo de claves copiando el bloque de texto que representa la clave pública y pegándolo en la ventana PGPkeys.

### **Importación de 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 la pueda importar, o copiar y pegar en su archivo de claves públicas. Hay tres métodos para extraer la clave pública de alguien y agregar a su archivo de claves públicas:

- \* Desde el menú Claves elija Importar y luego seleccione el archivo.
- \* Arrastre el archivo que contiene la clave pública desde el Explorador de Windows a la ventana PGPkeys.
- \* Abra el documento de texto donde se guarda la clave pública, seleccione el bloque de texto que representa la clave, y luego elija Copiar desde el menú Edición. Vaya a la ventana PGPkeys y elija Pegar desde el menú Edición para copiar la clave. La clave aparecerá como icono en la ventana PGPkeys

## **Verificación de la autenticidad de una clave**

Cuando usted intercambia claves públicas con alguien, algunas veces es difícil de saber si la clave realmente pertenece a esa persona. PGP proporciona un conjunto de salvaguardas que le permiten a usted verificar la autenticidad de una clave y certificar que la clave pertenece a un usuario en particular. El programa PGP lo alerta si intenta usar una clave que no es válida, y también en forma predeterminada lo alerta cuando usted está por usar una clave de validez marginal.

Una de las mayores vulnerabilidades del sistema de cifrado por clave pública, es la habilidad de algunos fisgones para montar un ataque "hombre del medio" [man-in-the-middle], reemplazando la clave pública de una persona por una que les pertenezca. De ese modo pueden interceptar cualquier mensaje de correo electrónico cifrado dirigido a esa persona, descifrarlo usando su propia clave, cifrarlo de nuevo con la clave real de esa persona, y luego enviarlo como si nada hubiera sucedido. En realidad, esto podría hacerse automáticamente a través de un sofisticado programa de computadora que se ubica en el medio y descifra toda la correspondencia dirigida a usted.

Basado en este escenario, usted y aquellos con quienes intercambia mensajes de correo electrónico necesitan una manera para determinar si de veras tienen copias legítimas de las claves de los demás. La mejor manera de estar completamente seguro que una clave pública realmente pertenece a una persona en particular es que la copie en un disquete y le entregue en mano a usted. Sin embargo, raramente estará usted lo suficientemente cerca de alguien como para entregarle un disquete en mano, y generalmente va a intercambiar claves públicas a través de mensajes de correo electrónico o las obtendrá de un servidor de claves público.

Aún cuando estos métodos de intercambiar claves a prueba de modificaciones son algo menos seguros, usted todavía puede determinar si una clave realmente pertenece a una persona en particular verificando su huella, una serie única de números generados cuando la clave es creada. Usted puede estar absolutamente seguro que tiene una copia válida de la clave pública de una persona comparando la huella de su copia de la clave con la huella de la clave original. Para encontrar la huella de una clave, seleccione la clave en la ventana PGPkeys, y luego desde el menú Claves elija Propiedades de la Clave.

El modo más eficaz de verificar la huella de la clave de una persona es llamarla por teléfono y pedirle que le lea la huella. El segundo mejor modo es el impreso. Muchas personas han impreso la huella de su clave en sus tarjetas personales y de negocios, pero el único modo de asegurar que la tarjeta es legítima es que le haya sido entregada por su titular.

Una vez que usted está absolutamente convencido que tiene una copia legítima de la clave pública de una persona, la firma. Al firmarla con su clave privada, usted certifica al mundo que está seguro que de la clave pertenece al pretendido usuario. En forma predeterminada, las firmas que usted hace sobre otras claves no serán exportadas, lo cual significa que solamente se aplican a la clave cuando están en su archivo de claves.

## **Obtención de claves a través de presentadores de confianza**

Los usuarios PGP a menudo hacen firmar sus claves públicas por otros usuarios de confianza para que atestigüen su autenticidad. Por ejemplo, usted podría enviar a un colega de confianza una copia de su clave pública con una petición de que la certifique y la devuelva, de modo que usted pueda incluir esa firma cuando publique su clave en un servidor de claves público. Usando PGP, cuando una persona obtiene una copia de la clave pública suya, no tiene que verificar la autenticidad de la clave por sí misma, sino basarse en lo mucho que confía en las personas que firmaron su clave. PGP proporciona las maneras para establecer este nivel de validez para cada una de las claves públicas que usted agregue a su archivo de claves públicas y muestra el nivel de confianza en la validez asociada con cada clave en la ventana PGPkeys. Esto significa que cuando usted obtiene una clave de alguien cuya clave está firmada por un presentador de confianza, puede estar medianamente seguro de que la clave pertenece al pretendido usuario. Para más detalles sobre cómo firmar claves y validar usuarios vea "Firma de la clave pública de una persona" en el Capítulo 6.



# Envío y Recepción de Correo Electrónico Privado

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

## Cifrado y firma de mensajes de correo electrónico

La manera más rápida y fácil de cifrar y firmar mensajes de correo electrónico es con una aplicación soportada por los complementos PGP [plug-ins]. Aunque el procedimiento varía ligeramente entre las diferentes aplicaciones de correo electrónico, usted realiza los procesos de cifrado y firma haciendo clic sobre los botones apropiados en la barra de herramientas de la aplicación. Además, si está usando una aplicación que soporta o que no requiere la norma PGP/MIME, puede cifrar y firmar sus mensajes de correo electrónico así como archivos adjuntos cuando envía o recibe su correo electrónico.

Si usted está usando una aplicación de correo electrónico que no es soportada por los complementos PGP, puede cifrar y firmar sus mensajes de correo electrónico por medio del portapapeles de Windows seleccionando la opción apropiada luego de hacer clic sobre el icono del candado y la llave ubicado en la barra de tareas del sistema. Para incluir archivos adjuntos, previamente debe cifrarlos desde el Explorador de Windows.

**SUGERENCIA:** Si está enviando un mensaje de correo electrónico sensible, considere dejar en blanco el renglón Asunto, o llénelo con algo que no revele el contenido de su mensaje cifrado.

Si su aplicación de correo electrónico no es soportada por PGP, vea el Capítulo 5 para más información sobre cómo cifrar archivos.

## Cifrado y firma con aplicaciones soportadas de correo electrónico

Cuando usted cifra y firma con una aplicación de correo electrónico que es soportada por los complementos PGP, tiene dos opciones, que dependen del tipo de aplicación de correo electrónico que está usando el destinatario. Si usted se está comunicando con otros usuarios de

PGP con una aplicación de correo electrónico que soporta la norma PGP/MIME, puede aprovechar las ventajas de esa norma para cifrar y firmar sus mensajes de correo electrónico y archivos adjuntos automáticamente cuando los envía. Si usted está intercambiando correspondencia con alguien que tiene una aplicación que no cumple con la norma PGP/MIME, debería cifrar sus mensajes de correo electrónico con PGP/MIME desactivado para evitar cualquier problema de incompatibilidad. La desventaja de este método es que debe cifrar por separado cualquier archivo adjunto que desee enviar con el mensaje de correo electrónico, a menos que esté usando una aplicación como Exchange, que le permite cifrar y firmar adjuntos sin usar PGP/MIME.

**NOTA:**

Si usted no envía su mensaje de correo electrónico inmediatamente después de redactarlo, y en vez de eso lo guarda en su buzón de salida, debería saber que en algunas aplicaciones de correo electrónico la información no es cifrada hasta que el mensaje sea verdaderamente transmitido. Antes de poner mensajes cifrados en la cola de transmisión debería fijarse si su aplicación cifra los mensajes en su buzón de salida. Si no los cifra, usted podría considerar cifrar sus mensajes por medio del portapapeles de Windows antes de ponerlos en la cola de transmisión del buzón de salida. Vea el Capítulo 5 para más información.

### **Cifrar y firmar con aplicaciones soportadas de correo electrónico.**

1. Use su aplicación de correo electrónico para componer su mensaje de correo electrónico del modo que lo haría normalmente.
2. Cuando usted haya terminado de componer el texto de su mensaje de correo electrónico, especifique si desea cifrar y firmar el texto de su mensaje haciendo clic sobre los botones del candado y la pluma de ave.
3. Envíe su mensaje de correo electrónico como lo hace normalmente.

Si ha elegido firmar los datos cifrados, aparece el cuadro de diálogo Contraseña pidiéndole su contraseña antes que el mensaje sea enviado.

4. Escriba su contraseña y luego haga clic en Aceptar.

Si usted tiene una copia de las claves públicas de cada uno de los destinatarios, son usadas las claves apropiadas. Sin embargo, si usted especifica un destinatario para el que no existe una clave pública correspondiente, aparece el cuadro de diálogo Selección de PGPkeys de modo que pueda especificar la clave correcta.

5. Arrastre las claves públicas de quienes van a recibir una copia del mensaje de correo electrónico cifrado dentro del cuadro que lista los "Destinatarios". También puede hacer

doble clic sobre cualquiera de las claves para moverlas desde un área de la pantalla al otro.

Los botones Validez indican el nivel mínimo de confianza para que sean válidas las claves públicas de la lista Destinatarios. Esta validez está basada en las firmas asociadas con la clave, y la confianza indica cuánta deposita usted en el dueño de la clave para garantizar la autenticidad de otra clave de usuario. Vea el Capítulo 6 para más detalles.

**NOTA:** Si usted no está usando PGP/MIME o está usando una aplicación de correo electrónico que no requiere PGP/MIME, antes de enviar cualquier archivo como archivo adjunto, debe cifrarlo desde el Explorador de Windows.

6. Haga clic en Aceptar para enviar su mensaje.

## **Descifrado y verificación de mensajes de correo electrónico.**

La manera más fácil y rápida para descifrar y verificar los mensajes que le envían es con una aplicación soportada por los complementos PGP. Aunque el procedimiento varía ligeramente entre las diferentes aplicaciones de correo electrónico, cuando usted está usando una aplicación de correo electrónico soportada por los complementos PGP, puede realizar los procesos de descifrado y verificación haciendo clic sobre un botón de la barra de herramientas de su aplicación. Además, si está usando una aplicación que soporta la norma PGP/MIME o no requiere PGP/MIME, puede descifrar y verificar sus mensajes de correo electrónico así como los archivos adjuntos con el simple clic sobre un icono adjunto a su mensaje de correo electrónico.

Si usted está usando una aplicación de correo electrónico que no es soportada por los complementos PGP, descifrará y verificará sus mensajes de correo electrónico por medio del portapapeles de Windows. Además, si el mensaje de correo electrónico incluye archivos adjuntos cifrados, debe descifrarlos separadamente desde el Explorador de Windows.

## **Descifrado y Verificación con aplicaciones soportadas de correo electrónico.**

Si usted se está comunicando con otros usuarios de PGP, y ellos han cifrado y firmado sus mensajes usando la norma PGP/MIME, aparece un icono de un sobre con llave cuando usted abre su mensaje de correo electrónico.



En tal caso, puede descifrar y verificar el mensaje y archivos adjuntos con sólo hacer doble clic sobre este icono.

Si está recibiendo mensajes de correo electrónico de alguien que no está usando una aplicación de correo electrónico que cumple la norma PGP/MIME, puede descifrar los mensajes de correo electrónico haciendo clic sobre el icono del sobre abierto en la barra de tareas de su aplicación. También, si hay archivos adjuntos, los puede descifrar desde el Explorador de Windows haciendo doble clic sobre ellos.

### **Descifrar y verificar desde aplicaciones de correo electrónico soportadas.**

1. Abra su mensaje de correo electrónico como lo hace normalmente.  
  
Verá un bloque de texto cifrado, ininteligible, en el cuerpo de su mensaje de correo electrónico.
2. Para descifrar y verificar el contenido del mensaje de correo electrónico, haga clic sobre el botón del sobre abierto en la barra de herramientas de su aplicación.  
  
Aparece el cuadro de diálogo Contraseña PGP, pidiéndole que escriba su contraseña.
3. Escriba su contraseña y luego haga clic en Aceptar.  
  
El mensaje es entonces descifrado. Si ha sido firmado, aparece un panel que indica si la firma es válida.
4. Después que usted haya leído el mensaje, puede guardarlo en su estado descifrado, o puede guardar la versión original cifrada para que permanezca segura.

## **PGPlog**

La ventana PGPlog aparece cuando usted verifica un mensaje firmado. Muestra la siguiente información:

- \* El nombre del archivo o la aplicación que está verificando el mensaje
- \* Un icono indica que la firma fue verificada (un guión rojo indica que la firma no fue verificada)
- \* El nombre de la clave firmante, si la clave está en su archivo de claves.
- \* La fecha de la firma.

En algunas circunstancias se muestra información adicional:

- \* No se encuentra la clave firmante
- \* Firma Mala
- \* Clave Revocada
- \* Clave Caducada
- \* Clave Inhabilitada
- \* Clave Inválida

## Grupos de destinatarios

Usted puede usar PGP para usar grupos de destinatarios. Por ejemplo, si desea enviar mensajes de correo cifrados a 10 personas en ingenieria@xyz.com, podría crear un grupo con ese nombre. El menú Grupos contiene un ítem Mostrar Grupos que activa la lectura de la sección Grupos de la ventana PGPkeys.

Después de haber creado un grupo, usted puede usar el menú emergente Grupos cuando trabaje con grupos. Para acceder al menú emergente Grupos, seleccione un grupo y presione el botón derecho del ratón. Puede pegar dentro de Grupos, borrar Grupos, obtener claves desde un servidor de claves público, y examinar Propiedades de Grupo.

### Creación de un grupo

1. Elija Nuevo Grupo desde el menú Grupos
2. Escriba el nombre del Grupo.
3. Si lo desea, puede escribir una descripción del grupo, la cual aparece como Propiedades de Grupo.

### Adición de miembros a un grupo

1. Seleccione la clave de la persona a ser incluida en un grupo, desde la ventana PGPkeys.
2. Arrastre el nombre de usuario desde la ventana PGPkeys al grupo deseado en el cuadro Grupos.

### **Eliminación de un grupo**

1. Seleccione el grupo desde el cuadro Grupos de la ventana PGPkeys.
2. Presione la tecla Supr o elija Eliminar Grupos desde el menú emergente.

### **Agregación de un grupo a otro grupo**

1. Seleccione el grupo que usted desea ubicar dentro de otro grupo.
2. Arrastre el grupo seleccionado dentro del otro grupo.

### **Eliminación de miembros de un grupo**

1. Seleccione el miembro del grupo a ser eliminado.
2. Elija Eliminar desde el menú emergente.  
PGP le pide que confirme la acción.
3. Confirme la acción presionando Sí.

### **Envío de mensajes cifrados de correo electrónico a grupos**

1. Dirija el mensaje a su grupo de correo

El nombre del grupo al que va a cifrar debe corresponderse con el nombre del grupo de correo electrónico. Su administrador de correo electrónico puede haber configurado grupos de correo electrónico, como ingeniería o finanzas.

2. Cifre el mensaje.
3. Envíe el mensaje.

# Uso de PGP para Almacenamiento Seguro de Archivos

Este Capítulo describe cómo usar las funciones PGP sin usar los complementos PGP [plugins]. Describe cómo usar PGP para cifrar y descifrar, y cómo firmar y verificar archivos por medio del portapapeles y desde el Explorador de Windows usando PGTools o el menú PGP, de modo que usted pueda cifrar y firmar archivos para enviarlos por correo electrónico o para guardarlos en forma segura en su equipo o en un servidor de archivos. También describe la función Tachar [Wipe] PGP, la cual borra de manera irreversible archivos, eliminándolos por completo de su equipo.

## Uso de PGP para cifrar y descifrar archivos

Usted puede usar PGP para cifrar y firmar archivos sin utilizar uno de los complementos PGP de correo electrónico, de modo que pueda enviar archivos cifrados o firmados como adjuntos de mensajes de correo electrónico. También puede usar las técnicas descritas en este Capítulo para cifrar y firmar archivos que guarda en su equipo o servidor de archivos.

### Cifrado y firma por medio del portapapeles

Si usted está usando una aplicación de correo electrónico que no es soportada por los complementos PGP, puede cifrar y firmar sus archivos por medio del portapapeles. Esto se hace mediante un clic sobre el icono del candado y la llave ubicado en la barra de tareas del sistema, y seleccionando luego la opción apropiada. En esencia, usted copia el contenido de su mensaje o archivo al portapapeles, y cifra y/o firma su contenido. Luego lo pega en su editor de mensajes de correo electrónico antes de enviarlo, lo guarda como un archivo firmado o cifrado. Si piensa enviar archivos adjuntos con su mensaje, debe antes cifrarlos desde el Explorador de Windows.

### Cifrar y firmar por medio del portapapeles

1. Use el editor suministrado con su aplicación de correo electrónico o su procesador de textos favorito para crear el archivo.

2. Cuando está listo para enviar el mensaje, seleccione el área de texto que desea cifrar, o elija Seleccionar Todo desde el menú Edición.

**NOTA:** Usted probablemente perderá cualquier formato específico del procesador de textos cuando cifre el mensaje.

3. Elija Copiar desde el menú Edición para copiar el contenido de su mensaje al portapapeles.

**SUGERENCIA:** Cada vez que usted copie o corte texto en su aplicación, es guardado temporalmente en el portapapeles.

4. Haga clic sobre el icono del candado y la llave en la barra de tareas del sistema y elija Cifrar Portapapeles, Firmar Portapapeles, o Cifrar y Firmar Portapapeles.

Si usted indica que desea cifrar el contenido del portapapeles, aparece el cuadro de diálogo Selección de Clave PGP.

5. Arrastre las claves públicas de quienes van a recibir una copia del mensaje de correo electrónico en el cuadro que lista los Destinatarios.

Si está cifrando un archivo para guardarlo en forma segura, selecciónese usted mismo como el destinatario.

El botón Validez indica el nivel mínimo de confianza que sean válidas las claves públicas en la lista Destinatarios. Esta validez está basada en las firmas asociadas con la clave.

6. Haga clic en Aceptar.

Si usted ha elegido firmar el mensaje, aparece el cuadro de diálogo Contraseña de Firma PGP, pidiéndole su contraseña personal para su clave privada predeterminada. Si usted tiene otras claves privadas y quiere usar una distinta a la predeterminada, haga clic en la flecha y seleccione la clave apropiada.

7. Escriba su contraseña, y luego haga clic en Aceptar.

8. Si usted está enviando el archivo cifrado en un mensaje de correo electrónico, copie el mensaje cifrado en su aplicación de correo electrónico.

9. Envíe su correo electrónico o guarde el archivo cifrado en su disco duro o servidor de archivos.



## **Descifrado y verificación por medio del portapapeles**

Si su aplicación de correo electrónico no es soportada por los complementos PGP, o si usted tiene archivos cifrados o firmados que desea guardar en forma segura, debe copiar el contenido de su mensaje al portapapeles para descifrarlo o para verificar cualquier firma digital. Si el mensaje de correo electrónico contiene archivos adjuntos, debe descifrarlos y verificarlos a través del Explorador de Windows.

### **Para descifrar y verificar por medio del portapapeles**

1. En el editor suministrado con su aplicación, seleccione el texto cifrado y luego cópielo al portapapeles.

En la mayoría de las aplicaciones, elija Copiar desde el menú Edición para copiar el texto al portapapeles de Windows.

2. Haga clic sobre el icono del candado y la llave en la barra de tareas del sistema para abrir el menú emergente PGP. Elija Descifrar/Verificar Portapapeles para iniciar el proceso de descifrado y verificación.

Aparece el cuadro de diálogo Contraseña PGP pidiéndole que escriba su contraseña.

3. Escriba su contraseña y haga clic en Aceptar.

El mensaje es descifrado. Si ha sido firmado, aparece un mensaje indicando si la firma es válida.

4. Para ver el contenido descifrado del mensaje de correo electrónico, elija Editar Portapapeles desde el menú emergente PGP. Usted puede entonces copiar el contenido del portapapeles de vuelta en su editor de texto y guardarlo si lo desea.

## **Cifrado y firma desde el Explorador de Windows**

Si usted piensa enviar un archivo cifrado como adjunto de su mensaje de correo electrónico, o si desea cifrar un archivo para protegerlo en su equipo o servidor de archivos, puede hacerlo desde el Explorador de Windows.

### **Para cifrar y firmar desde el Explorador de Windows**

1. Abra el Explorador de Windows desde el menú Inicio.
2. Seleccione el archivo (o archivos) que desea cifrar.
3. Elija la opción deseada desde el submenú PGP del menú Archivo o desde el menú emergente al cual accede presionando el botón derecho del ratón.

Aparece el cuadro de diálogo Selección de Clave PGP, en el cual puede seleccionar las claves públicas de los destinatarios de los archivos que usted está cifrando o firmando. Usted tiene varias opciones:

- \* Cuando envía archivos como adjuntos en algunas aplicaciones de correo electrónico, podría necesitar marcar el casillero Salida Texto para hacer que el archivo sea guardado como texto ASCII. Algunas veces esto es necesario para poder enviar un archivo binario usando aplicaciones de correo electrónico más antiguas.
- \* Si desea que la salida cifrada del archivo sea guardada en un formato de texto que pueda ser manejado por todas las aplicaciones de correo electrónico, marque el casillero Salida Texto. La selección de esta opción aumenta el tamaño del archivo cifrado en alrededor de un 30 por ciento.
- \* Con Cifrado Convencional usted trabaja con una sola clave simétrica, lo cual significa que utiliza una sola clave, en vez de criptografía de clave pública. El archivo es cifrado usando una clave de sesión, la cual es cifrada usando una contraseña cuya creación le es pedida.
- \* Tachar Original sobrescribe el documento original que usted está cifrando o firmando, de modo que su información sensible no sea legible por alguien que pueda acceder a su disco duro.

**ALERTA:**

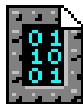
Aún en sistemas con memoria virtual, PGP sobrescribe correctamente todo el contenido del archivo. Es importante notar que programas de aplicación que pudieran haber guardado el archivo antes de cifrarlo, pueden haber dejado fragmentos del archivo en ubicaciones de su disco que ya no son consideradas partes del archivo. Lea "Vulnerabilidades" en el Capítulo 8 sobre Memoria Virtual. Considere la posibilidad de usar un programa utilitario de terceros para tachar todo el espacio libre de su disco para resolver este problema. PGP [esta versión] no tiene esta característica actualmente.

- \* Si usted ha firmado archivos, se le pide suministre su contraseña.
  - \* Si usted está agregando su firma al archivo cifrado y desea que la firma sea guardada en un archivo separado, seleccione el casillero Archivo de Firma Separado.
4. Seleccione las claves públicas arrastrándolas a la lista Destinatarios y luego haga clic en Aceptar.

Aparece el cuadro de diálogo Guardar Archivo Cifrado Como.

5. Especifique la ubicación y escriba el nombre del archivo donde usted desea guardar la versión cifrada del mismo. La extensión .pgp es automáticamente agregada al nombre del archivo, a menos que usted haya activado la opción Armadura ASCII, en cuyo caso es usada la extensión .asc.
6. Haga clic en Guardar para guardar el archivo en la ubicación especificada.

Si usted mira en el directorio donde ha guardado el archivo, encontrará un archivo con el nombre especificado representado por uno de estos dos iconos:



.pgp

Cifrado con salida normal



.asc

Cifrado con salida de texto

## Descifrado y verificación desde el Explorador de Windows

Si el mensaje de correo electrónico que usted recibe contiene archivos adjuntos, y está usando una aplicación de correo electrónico no compatible con la norma PGP/MIME, o que no requiere PGP/MIME, debe descifrarlo desde el Explorador de Windows.

### Descifrar y verificar desde el Explorador de Windows

1. Abra el Explorador de Windows desde el menú de inicio.
2. Seleccione el archivo (o archivos) que desea descifrar y verificar.
3. Elija Descifrar/Verificar desde el submenú PGP del menú Archivo, o presione el botón derecho del ratón para abrir el menú emergente PGP y luego elija Descifrar/Verificar.

Aparece el cuadro de diálogo Contraseña PGP pidiéndole que escriba su contraseña.

4. Escriba su contraseña y luego haga clic en Aceptar.

Si el archivo ha sido firmado, aparece un mensaje que indica si la firma es válida.

5. Haga clic en Aceptar.

Aparece el cuadro de diálogo Guardar Archivo Descifrado Como.

6. Especifique la ubicación y escriba el nombre del archivo donde desea guardar la versión descifrada del mismo.

Si usted no escribe un nombre en forma explícita, se usa el nombre original.

7. Haga clic sobre el botón Guardar para guardar el archivo.

El archivo descifrado es guardado en la ubicación especificada.

## Funciones PGP desde el Explorador de Windows

PGPtools y PGPtray proporcionan otro modo de usar las funciones de PGP sobre archivos y carpetas. Para acceder a estas funciones, seleccione un archivo y presione el botón derecho del ratón para abrir el menú emergente PGP que contiene las siguientes opciones:

- \* Cifrar
- \* Firmar
- \* Cifrar y Firmar
- \* Tachar

Para acceder a PGPtools, haga clic sobre el icono del sobre con el candado en la barra de tareas del sistema, o seleccione PGPtools desde el directorio PGP. Además de las funciones listadas en el menú emergente PGP, PGPtools incluye las funciones Descifrar y Verificar.

Vea "Cifrado y firma desde el Explorador de Windows" más atrás en este Capítulo por explicaciones sobre cómo cifrar y firmar archivos.

Tachar sobrescribe archivos y sus contenidos y los borra de su equipo. La característica Tachar es una manera segura de borrar permanentemente del disco duro de su equipo un archivo y su contenido. En el sistema operativo Windows, cuando usted borra un archivo, se elimina el nombre del archivo de la lista de archivos. Tachar borra toda traza de los datos del archivo, de modo que nadie pueda recuperarlo usando herramientas de recuperación de datos.

### Tachado de archivos

1. Abra el Explorador de Windows desde el menú Inicio.

2. Seleccione el archivo o los archivos que desea tachar.
3. Abra el menú emergente PGP o acceda a PGPtools.

Para abrir el menú PGP, seleccione el archivo y presione el botón derecho del ratón. Elija PGP. Aparece un submenú que contiene los comandos Cifrar, Firmar, Cifrar y Firmar, y Tachar.

4. Elija Tachar.

**ALERTA:**

Si usted usa Tachar PGP para borrar un acceso directo a una aplicación Windows, también borra la aplicación.

5. Seleccione el archivo o elija Abrir desde el cuadro de diálogo Seleccionar Archivos para tachar el archivo.

Aparece un cuadro de diálogo Confirmar que le pregunta si está seguro que desea borrar los archivos de manera irreversible.

6. Haga clic en Aceptar para tachar el o los archivos.

**ALERTA:**

Aún en sistemas con memoria virtual, PGP sobrescribe correctamente todo el contenido del archivo. Es importante notar que programas de aplicación que pudieran haber guardado el archivo antes de cifrarlo, pueden haber dejado fragmentos del archivo en ubicaciones de su disco que ya no son consideradas partes del archivo. Lea "Archivos de Intercambio o Memoria Virtual" en el Capítulo 8. Asimismo, no olvide que muchos programas guardan automáticamente los archivos mientras los procesan, de modo que pueden haber copias de seguridad del archivo que usted desea borrar. Considere usar un programa utilitario de terceros para tachar todo el espacio libre de su disco para resolver este problema. PGP [esta versión] no tiene esta característica actualmente.

# Administración de Claves y Configuración de Preferencias

Este Capítulo explica cómo examinar y administrar las claves guardadas en sus archivos de claves. También describe cómo establecer sus preferencias para ajustarlas a su sistema en particular.

## Administración de sus claves

Las claves que usted crea, así como las que recoge de otras personas, se almacenan en archivos de claves, que esencialmente son archivos guardados en su disco duro o en un disquete. Normalmente, sus claves privadas son guardadas en un archivo llamado `secring.skr` y sus claves públicas son guardadas en otro archivo llamado `pubring.pkr`. Estos archivos están ubicados usualmente en el mismo directorio que los demás archivos de PGP. Los siguientes iconos son usados para representar a su archivo de claves privadas y su archivo de claves públicas respectivamente, haciéndolas fáciles de distinguir cuando está trabajando con sus archivos.



Archivo de Claves Privadas



Archivo de Claves Públicas

**NOTA:**

Si no se siente cómodo guardando sus claves en el lugar habitual, puede elegir un nombre de archivo o una ubicación diferentes. Para más detalles, vea "Establecer sus preferencias" más adelante en este Capítulo.

En ocasiones usted podría desear examinar o cambiar los atributos asociados a sus claves. Por ejemplo, cuando obtiene la clave pública de alguien, quizá quiera identificar el tipo (RSA o Diffie-Hellman/DSS), comprobar su huella, o determinar su validez basándose en alguna de las firmas digitales incluidas con la clave. También podría desear firmar la clave pública de alguien para indicar que cree en su validez, asignar un nivel de confianza al propietario de la clave, o cambiar la contraseña de su clave privada. Toda búsqueda en un servidor de claves añade funciones de administración de claves desde la ventana PGPkeys.

## La ventana de PGPkeys

Para abrir la ventana PGPkeys, presione el icono del candado y la llave en la barra de tareas del sistema y elija Ejecutar PGPkeys, o haga doble clic sobre el icono PGPkeys.

La ventana PGPkeys muestra las claves que usted ha creado para sí mismo, así como toda clave pública que haya añadido a su archivo de claves públicas.

Las llaves dobles representan los pares de claves que ha creado para usted, estando cada par compuesto por una clave privada y una clave pública, y las llaves simples representan las claves públicas que ha recogido de otros. Si tiene más de un tipo de clave, notará que las claves RSA están representadas por llaves azules de tipo antiguo, y las Diffie-Hellman/DSS por llaves amarillas modernas.

Haciendo clic en la casilla situado a la izquierda del icono correspondiente a la llave, podrá expandir y revelar el identificador del usuario [User ID], junto con la dirección de correo electrónico del propietario de la clave, tal como es representada por los iconos de sobre. Haciendo clic sobre el signo más que está al lado de un icono del sobre, puede ver las firmas de los usuarios que han certificado la clave, las cuales vienen representadas por el icono de una pluma de ave. Si no quiere hacer doble clic para obtener todos los niveles de información de todas las claves, simplemente seleccione la clave de su interés y elija Expandir Selección desde el menú Edición.

### Ventana PGPkeys, Configuración de la Presentación

1. Elija Seleccionar Columnas desde el menú Claves

Aparece el cuadro de diálogo Seleccionar Columnas, mostrando 'Campos Disponibles' con los atributos de clave que no están siendo mostrados, y 'Mostrar Estas Columnas', con los atributos de clave que sí están siendo mostrados. Las columnas mostradas en forma predeterminada son Validez, Tamaño y Descripción.

2. Para añadir a los atributos mostrados en la ventana PGPkeys, haga clic sobre el atributo desde Campos Disponibles y luego sobre el botón Añadir.
3. Para quitar un atributo que está siendo mostrado en la ventana PGPkeys, haga clic sobre el atributo y luego sobre el botón Eliminar.
4. Haga clic en Aceptar para mostrar la nueva presentación, o en Cancelar para volver a la presentación previa.

## Atributos en PGPkeys, definiciones

En la parte superior de la ventana hay lengüetas que se corresponden con los atributos asociados con cada clave.

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

**Validez** Indica el nivel de confianza acerca de si la clave realmente pertenece a su supuesto dueño. La validez se basa en quién ha firmado la clave y cuánto confía usted en los firmantes que dan fe de la autenticidad de la clave. Las claves públicas que usted mismo firma tienen el mayor grado de validez, basado en la suposición que solamente firmará la clave de alguien si está totalmente convencido que es válida. La validez de cualquier otra clave que usted no haya firmado personalmente depende del nivel de confianza que haya otorgado a otros usuarios que han firmado la clave. Si no hay firmas asociadas con la clave, no es considerada válida, apareciendo un mensaje que indica este hecho cada vez que usted use la clave.

La validez es indicada por iconos de círculos o barras, dependiendo de su configuración de "Mostrar nivel de validez marginal" en Preferencias Avanzadas (vea "Preferencias Avanzadas" más adelante en este Capítulo). Si está configurado, entonces la validez aparece como

- una barra vacía para claves inválidas
- una barra medio llena para claves de validez marginal
- una barra llena para claves válidas que no le pertenecen
- una barra con franjas para claves válidas que le pertenecen

Si no está configurado, entonces la validez aparece como

- un círculo gris para claves inválidas y de validez marginal, si está configurado "Tratar claves de validez marginal como inválidas" en Preferencias Avanzadas
- un círculo verde para claves válidas que no le pertenecen.
- un diamante verde para claves válidas que sí le pertenecen.

**Confianza** Indica el nivel de confianza que usted ha otorgado al propietario de la clave para que éste sirva como introductor de las claves públicas de otros. Esta confianza



entra en juego cuando usted es incapaz de verificar la validez de la clave pública de otro por sí mismo, y en su lugar confía en el buen juicio de otros usuarios que han firmado la clave. Cuando usted crea un par de claves, éste es considerado de confianza implícita, como es mostrado por las franjas en las barras de confianza y validez, o por un diamante indicador de validez.

Cuando usted recibe una clave pública de alguien, que ha sido firmada por otra de las claves de usuario existentes en su archivo de claves públicas, el nivel de autenticidad está basado en la confianza que ha otorgado al firmante de esa clave. Usted asigna un nivel de confianza, que puede ser Completa, Marginal o Sin confianza en el cuadro de diálogo Propiedades de Clave.

En la presentación de PGPkeys, inicialmente no es mostrada la confianza. Usted puede mostrar la columna de Confianza eligiendo Columnas desde el menú Ver.

**Creación** Muestra la fecha en la que la clave fue creada originariamente. A veces puede hacer una suposición sobre la validez de una clave basándose en cuánto tiempo ha estado en circulación. Si la clave ha sido usada durante algún tiempo, es menos probable que alguien intente reemplazarla porque hay muchas otras copias en circulación. No debería usted confiar en la fecha de creación como único indicador de validez.

**Caducidad** Muestra la fecha en que la clave caducará. La mayoría de las claves la tienen configurada en Nunca; sin embargo, pueden haber situaciones en las que usted quiera usar una clave durante un período fijo de tiempo.

#### **Clave de Descifrado Adicional**

Muestra si la clave tiene asociada una Clave de Descifrado adicional (ver Capítulo 2 para una explicación).

**Tamaño** Muestra el número de bits usados para construir la clave. Por lo general, cuanto más grande es la clave, menor es la posibilidad de que se vea comprometida. Sin embargo, las claves grandes requieren más tiempo que las claves más pequeñas para cifrar y descifrar datos. Cuando crea usted una clave Diffie-Hellman/DSS, hay un número para la parte Diffie-Hellman y otro número para la parte DSS. La parte DSS de la clave es usada para firmar y la parte Diffie-Hellman es usada para cifrar.

## **Propiedades de una clave**

Además de los atributos generales mostrados en la ventana PGPkeys, puede examinar y cambiar otras propiedades de una clave. Para acceder a las propiedades de una clave en particular, seleccione la clave deseada y elija Propiedades de Clave desde el menú Claves.

**ID de clave** Es un número de identificación único asociado con cada clave. Este número de identificación resulta útil para distinguir entre dos claves que comparten el mismo nombre de usuario y dirección de correo electrónico.

**Creada** Fecha en la que fue creada la clave.

**Tipo de clave** Tipo de clave, RSA o Diffie-Hellman/DSS.

**Cifrado** CAST, TripleDES o IDEA. Este es el cifrado preferido, y es el cifrado por el cual el dueño de la clave le solicita que cifre la clave pública de él. Si el algoritmo está habilitado en Preferencias Avanzadas, puede ser usado cuando se cifre a esta clave, y este cifrado será utilizado cuando se use cifrado convencional.

**Caduca** Fecha en la cual caduca la clave. El propietario especifica esta fecha cuando crea sus claves, y usualmente el valor es configurado en Nunca. Sin embargo, algunas claves son configuradas para caducar en una fecha determinada si el propietario desea que ellas sean usadas por un período limitado de tiempo.

**Confianza** Indica la validez de la clave basándose en su certificación y el nivel de confianza que usted tiene en el propietario para garantizar la autenticidad de la clave pública de otro. Usted configura el nivel de confianza deslizando la barra al nivel apropiado (Completa, Marginal, o Sin Confianza). La barra no es mostrada para claves revocadas, caducadas y de confianza implícita (como su propia clave).

**Huella** Un número de identificación único que es generado cuando es creada la clave. Este es el procedimiento principal por el cual usted puede comprobar la autenticidad de una clave. Una buena manera de comprobar una huella es hacer que el propietario la lea por teléfono de modo que usted pueda compararla con la correspondiente a su copia de esa clave pública. También puede comprobar la autenticidad de la clave de otros comparando la huella que hay en su copia de la clave con la ubicada en un servidor de claves, porque se supone que el propietario controla periódicamente para asegurarse que sigue siendo válida.

**Habilitada** Indica si actualmente la clave está habilitada. Cuando una clave es inhabilitada, aparece atenuada en la ventana PGPkeys, y no está disponible para efectuar ninguna función de PGP excepto descifrar y verificar. Sin embargo, la clave permanece en su archivo de claves y usted puede habilitarla de nuevo en cualquier momento. Para habilitar o inhabilitar una clave, marque o quite la marca en la casilla Habilitar, o elija Habilitar o Inhabilitar desde el menú Claves. Esta característica es útil para

evitar confundir claves en la ventana PGPkeys cuando usted envía correo electrónico cifrado.

### **Cambiar Contraseña**

Cambia la contraseña de una clave privada. Si piensa que su contraseña ya no es más secreta, haga clic en este botón para entrar una nueva contraseña. Es una buena idea cambiar cada seis meses la contraseña. Vea "Cambio de Contraseña" en este Capítulo.

### **Par de claves predeterminado**

Cuando usted firma un mensaje o la clave pública de alguien, es usado su par de claves predeterminado. Si tiene más de un par de claves, podría designar específicamente un par como su par predeterminado. El par de claves predeterminado en uso es mostrado en negrita para distinguirlo de sus otras claves.

#### **Par de claves predeterminado, especificación**

1. Seleccione el par de claves que quiere designar como predeterminado.
2. Elija Establecer como Clave Predeterminada desde el menú Claves.

La selección es mostrada en negrita, lo que indica que ahora es su par de claves predeterminado.

#### **Nuevo nombre o dirección de usuario, añadir**

Usted podría tener más de un nombre de usuario o dirección de correo electrónico para los cuales quiera usar el mismo par de claves. Después de crear un nuevo par de claves, puede añadir nombres y direcciones alternativas a la clave. Solamente si tiene ambas claves del par, la privada y la pública, puede añadir un nuevo nombre o dirección de correo electrónico.

#### **Nuevo nombre o dirección de usuario, procedimiento para añadir a una clave existente**

1. Seleccione el par de claves para el que quiera añadir otro nombre o dirección de usuario.
2. Elija Añadir Nombre desde el menú Claves

Aparece el cuadro de diálogo Nuevo Nombre de Usuario PGP.

3. Escriba el nuevo nombre y luego presione el tabulador para ir al siguiente campo.
4. Escriba la nueva dirección de correo electrónico y luego haga clic sobre Aceptar.

Aparece el cuadro de diálogo Contraseña PGP pidiéndole que escriba su contraseña.

5. Escriba su contraseña y luego haga clic sobre Aceptar.

El nuevo nombre es añadido al final de la lista de nombres de usuario asociada con la clave. Si quiere establecer este nuevo nombre y dirección de usuario como el identificador primario para su clave, seleccione el nombre y dirección, y desde el menú Claves haga clic en Establecer Como ID de Usuario Primario.

## **Huella de una clave, comprobación**

A menudo resulta difícil saber con seguridad si una clave pertenece a una persona en particular, a menos que esa persona se la entregue en un disquete personalmente en su mano. Intercambiar claves de esta manera no suele ser práctico, especialmente para los usuarios que están separados por una gran distancia, pero usted puede confiar en la huella única asociada con cada clave para comprobar que una clave realmente pertenece al supuesto propietario. Hay varias maneras para comprobar la huella de una clave, pero la forma más segura es llamar por teléfono al propietario y pedirle que le lea la huella. Es altamente improbable que alguien pueda interceptar esta llamada al azar e imite al propietario de la clave. También puede comparar la huella de su copia de una clave pública con la huella de la clave original listada en un servidor de claves público.

### **Huella de una clave, Procedimiento de Comprobación**

1. Seleccione la clave cuya huella quiera comprobar.
2. Elija Propiedades de Clave desde el menú Claves.
3. Anote la huella y compárela con la original.

## **Firmar una clave pública**

Cuando usted crea un par de claves, esta es automáticamente certificada usando su clave pública. Del mismo modo, si está seguro que una clave pertenece a una determinada persona, puede firmar esa clave pública para indicar que está seguro que es una clave válida. Cuando usted firma la clave pública de alguien, es mostrado para esa clave un icono asociado con su nombre de usuario.

## **Firma de una clave pública, Procedimiento**

1. Seleccione la clave que desea firmar.

2. Elija Firmar desde el menú Claves.

Aparece el cuadro de diálogo Firmar Claves.

3. Se le pregunta si permite que la firma pueda ser exportada. Otros pueden confiar en su firma.

Marque esta casilla si desea que su firma pueda ser exportada.

4. Si quisiera enviar la clave con su firma a un servidor de claves, marque la casilla Enviar Firma a Servidor de Claves. La clave pública en el servidor es actualizada para reflejar la inclusión de su firma. La mayoría de los usuarios prefieren usar su propio criterio cuando permiten a otros que firmen sus claves, de modo que siempre es una buena idea hablar con el propietario de la clave antes de añadir su firma a la copia en el servidor.

Aparecerá una casilla que dice "Permitir que la firma sea exportada. Otros pueden confiar en su firma". Una firma exportable es una que puede ser vista con la clave pública de un usuario en el servidor de claves y a la que le es permitida ser enviada a servidores de claves y viajar con la clave cuando es copiada al ser arrastrada a un mensaje de correo electrónico.

5. Haga clic en Aceptar para indicar su certeza que la clave realmente pertenece al supuesto dueño.

6. Aparece el cuadro de diálogo Contraseña de Firma PGP. Se le pide que escriba la contraseña para su par de claves predeterminado.

7. Cuando firme la clave pública de otra persona, es mostrado para esa clave un icono asociado a su nombre de usuario.

## **Nivel de confianza para validaciones de clave**

Además de certificar que una clave pertenece a alguien, usted puede asignar un nivel de confianza al propietario, indicando cuánto confía en él como introductor de otros usuarios cuyas claves usted podría obtener en el futuro. Esto significa que si alguna vez obtiene una clave que ha

sido firmada por una persona a quien usted haya designado como de confianza, la clave será considerada válida aunque usted no haya hecho la comprobación personalmente.

### **Nivel de confianza para validaciones de clave, procedimiento de asignación**

1. Seleccione la clave cuyo nivel de confianza desea cambiar. Elija Propiedades de Clave desde el menú Claves.

Aparece el cuadro de diálogo Propiedades.

2. Use la barra deslizante para establecer el nivel de confianza apropiado para la clave: Sin Confianza, Marginal o Completa.
3. Haga clic sobre Aceptar para activar la nueva configuración.

### **Inhabilitación y habilitación de claves**

A veces usted podría desear inhabilitar temporalmente una clave. La capacidad de inhabilitar claves es útil cuando desea conservar una clave pública para usos futuros sin desordenar la lista de Destinatarios cada vez que envía correo.

#### **Inhabilitación de una clave, procedimiento**

1. Seleccione la clave que quiera inhabilitar
2. Elija Inhabilitar desde el menú Claves

La clave es atenuada y está temporalmente no disponible para su uso.

#### **Habilitación de una clave, procedimiento**

1. Elija la clave que quiera habilitar
2. Elija Habilitar desde el menú Claves.

La clave se vuelve visible y puede ser usada como antes.

### **Eliminación de una clave o firma**

En algún momento usted podría desear eliminar una clave, una firma, o un identificador de usuario asociado a una clave determinada.

### **Eliminación de una clave, firma, o ID de usuario, procedimiento**

1. Seleccione la clave, firma o ID de usuario que quiera eliminar.
2. Elija Borrar desde el menú Edición.

### **Cambio de contraseña**

Es una buena idea cambiar la contraseña cada seis meses.

### **Cambio de contraseña, procedimiento**

1. Seleccione el par de claves cuya contraseña quiere cambiar.
2. Elija Propiedades de Clave desde el menú Claves.  
  
Aparece el cuadro de diálogo Propiedades.
3. Haga clic sobre Cambiar Contraseña.  
  
Aparece el cuadro de diálogo Cambiar Contraseña.
4. Escriba la contraseña a ser cambiada en el campo superior y avance al campo siguiente con el tabulador.
5. Escriba su nueva contraseña en el campo central y avance al campo siguiente con el tabulador.
6. Confirme su nueva contraseña escribiéndola de nuevo.
7. Haga clic en Aceptar.

### **Importación y exportación de claves**

Aunque usted suela distribuir su clave pública y obtener las claves públicas de otros cortando y pegando el texto desde un servidor de claves público o corporativo, también puede intercambiar claves importándolas y exportándolas como archivos separados de texto. Por

ejemplo, una persona podría entregarle en mano un disco que contenga la clave pública que le pertenezca, o usted podría hacer que su propia clave pública esté disponible en un servidor FTP.

### **Importación de una clave desde un archivo, procedimiento**

1. Elija Importar desde el menú Claves.

Aparece el cuadro de diálogo Seleccionar Archivo con la Clave.

2. Seleccione el archivo que contiene la clave que quiere importar y haga clic en Abrir.

La clave importada aparecerá en la ventana PGPkeys, donde podrá usarla para cifrar datos y para verificar la firma digital de alguien.

### **Exportación de una clave a un archivo**

1. Seleccione la clave que desea exportar a un archivo.

2. Elija Exportar desde el menú Claves.

Aparece el cuadro de diálogo Exportar Clave a Archivo.

3. Escriba el nombre del archivo al cual desea exportar la clave y luego haga clic sobre Guardar.

La clave exportada es guardada en el archivo especificado.

### **Adición de una clave desde un mensaje de correo electrónico**

Si alguien le envía un mensaje de correo electrónico con su clave incluida como un bloque de texto, puede añadirla a su archivo de claves.

1. Con el mensaje de correo electrónico abierto, abra la ventana PGPkeys.

2. Ajuste las dos ventanas de modo que pueda ver parte de la ventana PGPkeys detrás de la ventana del mensaje.

3. Seleccione el texto de la clave, comprendido entre BEGIN PGP PUBLIC KEY BLOCK [COMIENZO DEL BLOQUE DE CLAVE PÚBLICA PGP] y END PGP PUBLIC KEY BLOCK [FIN DEL BLOQUE DE CLAVE PÚBLICA PGP] inclusive.



4. Aparece el cuadro de diálogo 'Seleccionar Claves para Importar', mostrando las claves incluidas en el mensaje. Elija las claves que desea copiar eligiendo Seleccionar Todo, Anular Selección, Importar o Cancelar.
5. Las claves nuevas aparecerán en la ventana PGPkeys.

## **Revocación de una clave**

Si ya no confía en su par de claves personal, puede librar una revocación diciendo a todos que paren de usarla. La mejor manera de hacer circular una clave revocada es ubicarla en un servidor de claves públicas.

### **Revocación de una clave, procedimiento**

1. Seleccione el par de claves que va a revocar.
2. Elija Revocar desde el menú Claves.

Aparece un mensaje con una información breve sobre las consecuencias de revocar una clave, y pidiéndole especifique si realmente desea revocar la clave seleccionada.

3. Haga clic sobre Sí para confirmar su intención de revocar la clave seleccionada.

Aparece el cuadro de diálogo Contraseña PGP, pidiéndole que escriba la contraseña.

4. Escriba su contraseña y haga clic sobre Aceptar.

Cuando usted revoca una clave, ésta aparece cruzada con una línea roja para indicar que ya no es válida.

5. Envíe la clave revocada al servidor de claves para que todos sepan que no deben usar su clave antigua.

Podría suceder que algún día usted olvide su contraseña. En ese caso nunca podría volver a usar su clave, y no tendría manera de revocarla al crear una nueva. Para protegerse contra esa posibilidad, puede crear una clave de revocación haciendo una copia de su clave privada, revocando esa copia, y guardándola en un lugar seguro. Si alguna vez olvida su contraseña puede entonces enviar la copia revocada a un servidor de claves público. Sin embargo, debería ser muy cuidadoso sobre dónde guarda la versión revocada de su clave. Alguien que tuviera acceso a la clave revocada, podría revocar su clave sin su consentimiento.

## Configuración de sus preferencias

PGP está configurado para acomodarse a las necesidades de la mayoría de los usuarios, pero usted tiene la opción de ajustar algunos parámetros para adaptarlo a su entorno de trabajo en particular. Puede especificar estas opciones por medio del cuadro de diálogo Preferencias, al cual puede acceder usando uno de los siguientes métodos:

- \* Haciendo clic sobre el icono de la llave y el candado, y eligiendo Preferencias.
- \* Eligiendo Preferencias desde el menú Edición en la ventana PGPkeys.

### Preferencias generales

Puede especificar la configuración general de cifrado desde el panel General.

#### Cifrar también a la clave predeterminada

Cuando es seleccionada esta casilla, todos los mensajes de correo electrónico y archivos adjuntos que cifre con la clave pública del destinatario también son cifrados con su clave pública predeterminada. Es útil dejar activada esta opción para que usted tenga la posibilidad de descifrar el contenido de cualquier mensaje o archivo que haya cifrado con anterioridad.

#### Permanencia de Contraseña de cifrado en memoria caché

Esta opción especifica el intervalo de tiempo (en horas: minutos: segundos) durante el cual su contraseña de cifrado queda almacenada en la memoria del sistema. Si habitualmente compone o lee varios mensajes de correo electrónico en sucesión, podría desear aumentar el intervalo de tiempo en el cual su contraseña permanezca en la memoria caché de modo de no tener que escribirla repetidamente una y otra vez hasta procesar todo su correo. Sin embargo, recuerde que cuanto más tiempo esté almacenada su contraseña en la memoria de su equipo, más tiempo tiene un fisgón sofisticado para capturarla. En forma predeterminada se establece en dos minutos, lo que probablemente sea suficiente para efectuar la mayoría de las tareas de PGP sin tener que escribir su contraseña demasiadas veces, pero no lo bastante como para que un atacante la encuentre en la memoria de su equipo en un descuido.

#### Permanencia de Contraseña de firma en memoria caché

Esta opción especifica el intervalo de tiempo (en horas: minutos: segundos) durante el cual su contraseña de firmado queda almacenada en la memoria del sistema. Si habitualmente compone o lee varios mensajes de correo electrónico en sucesión, podría desear aumentar el intervalo de tiempo en el cual su contraseña permanezca

en la memoria caché de modo de no tener que escribirla repetidamente una y otra vez hasta procesar todo su correo.

Usar su frase clave para firmar es considerado una amenaza mayor en algunos casos, ya que un atacante podría intentar hacerse pasar por usted, motivo por el cual la Permanencia de la contraseña de Firma en memoria Caché es manejada separadamente del cifrado. El tiempo empieza a contarse y es reestablecido cada vez que se firma un mensaje, y la contraseña es borrada de la memoria inmediatamente después de vencido el plazo. En forma predeterminada este caché está desactivado, debido a las complejas implicaciones de seguridad.

### **Bloque de comentario**

Cuando esta opción es seleccionada, siempre será incluido su texto de comentario en los mensajes y archivos que usted cifre o firme. PGP recomienda activar esta opción.

### **Generación rápida de claves**

Cuando es seleccionada esta opción se necesita menos tiempo para generar un nuevo par de claves Diffie-Hellman/DSS. Este proceso se acelera usando un conjunto de números primos previamente calculado en vez de pasar por el lento proceso de su creación cada vez que se genera una nueva clave. Sin embargo, recuerde que la generación rápida de claves solamente es posible para los tamaños fijos de clave entre 1024 y 4096 [bits] que se muestran como opción cuando se crea una clave, y no es usada si se trabaja con otro valor. Aunque sería prácticamente imposible que alguien descubra su clave basándose en el conocimiento de estos números primos precalculados, usted podría desear perder un poco más de tiempo para crear un par de claves con el máximo nivel de seguridad. La mayoría de los criptógrafos creen que usar "primos precalculados" no plantea mayores riesgos a la seguridad.

### **Mostrar confirmación de Tachar**

Cuando es seleccionada esta opción, antes de Tachar [borrar de manera irreversible] un archivo, aparece un cuadro de diálogo para darle la última oportunidad de cambiar de idea antes que PGP sobrescriba de modo seguro el contenido del archivo y lo elimine de su equipo.

### **Preferencias de archivos**

Haga clic sobre la ficha Archivos para avanzar al panel en el cual usted especifica la ubicación de los archivos de clave usados para guardar sus claves privadas y públicas.

### **Archivo de claves públicas**

Muestra la actual ubicación y nombre del archivo donde el programa PGP espera encontrar su archivo de claves públicas. Si usted piensa guardar sus claves públicas en un archivo con un nombre diferente o en otra ubicación, aquí donde especifica esa información. Puede usar el botón Buscar para buscar entre tus archivos, en vez de tener que escribir toda la ruta del archivo. Esta es también la ubicación donde son guardadas todas las copias de seguridad que se hacen automáticamente.

### **Archivo de claves privadas**

Muestra la actual ubicación y nombre del archivo donde el programa PGP espera encontrar su archivo de claves privadas. Si usted piensa guardar sus claves públicas en un archivo con nombre diferente o en otra ubicación, aquí es donde especifica esa información. Algunos usuarios prefieren guardar su archivo de claves privadas en un disquete, que insertan como una llave cuando necesitan firmar o descifrar correo. Esta es también la ubicación donde son guardadas todas las copias de seguridad que se hacen automáticamente.

### **Archivo de datos aleatorios**

Muestra la ubicación del archivo randseed.bin. Este archivo almacena datos aleatorios usados durante el cifrado y la generación de claves. Algunos usuarios podrían desear mantener su Archivo de Datos Aleatorios en un lugar seguro para evitar su alteración. Este ataque es muy difícil y PGP tiene muchas diferentes protecciones contra él.

## **Preferencias de correo electrónico**

Haga clic sobre la ficha Correo para avanzar al panel en el cual usted especifica las preferencias que afectan a la manera en que son implementadas las funciones PGP en aquellas aplicaciones de correo electrónico que utilizan los complementos PGP [plug-ins]. Recuerde que la opción PGP/MIME no es aplicable para todas las aplicaciones de correo electrónico

### **Uso de PGP/MIME al enviar correo electrónico**

Cuando es seleccionada esta casilla no necesita activar explícitamente PGP/MIME cada vez que envía correo electrónico. Si está usando Eudora y activa esta opción, todos sus mensajes y archivos adjuntos son automáticamente cifrados y firmados con la clave del destinatario. Esta opción no tiene efecto sobre otros cifrados que usted realice desde el portapapeles o con el Explorador de Windows. No use esta opción si piensa enviar correo electrónico a destinatarios que usan aplicaciones de correo electrónico no soportadas por la norma PGP/MIME. Usando Eudora los archivos adjuntos son siempre cifrados sin importar cómo está configurada esta opción, pero si el destinatario no tiene PGP/MIME, deberá usar PGTools para descifrar los mensajes.

### **Ajuste de línea [Word-Wrap] para mensajes firmados en columna []**

Esta opción especifica el número de columna donde es forzado un retorno de carro para ajustar [wrap] el texto en su firma digital. Esto es necesario porque no todas las aplicaciones manejan el ajuste de línea de la misma manera, lo que podría causar que las líneas en sus mensajes firmados digitalmente sean cortadas de una manera que no puedan ser leídas fácilmente. La configuración predeterminada es 70, que evita problemas con la mayoría de las aplicaciones.

#### **ALERTA:**

Si cambia la configuración del ajuste de línea en PGP, asegúrese que sea a un valor menor que la configuración del ajuste de línea de su aplicación de correo electrónico. Si lo establece a un valor igual o mayor podrían añadirse retornos de carro que invaliden su firma PGP.

### **Cifrar en forma predeterminada los mensajes nuevos**

Cifra todos sus mensajes de correo electrónico. El icono del candado aparece presionado para indicar que la función cifrado está activa.

### **Firmar en forma predeterminada los mensajes nuevos**

Firma todos sus mensajes de correo electrónico. El icono de la pluma de ave usada para escribir aparece presionado para indicar que la función firmado está activa.

### **Descifrar automáticamente al abrir mensajes**

Descifra automáticamente sus mensajes de correo electrónico cuando usted abre un mensaje.

## Preferencias del servidor de claves

Haga clic sobre la ficha Servidor de Claves para avanzar al panel que especifica la configuración para el servidor de claves que está usando.

**Servidor** Especifica la dirección de Internet, por ejemplo `www.company.com`, para el servidor de claves que es usado por PGP para enviar y obtener claves públicas. Esta dirección será usada al enviar claves a un servidor, para consultar el servidor apropiado.

**Puerto** Dirección de puerto para el servidor de claves públicas. Debe escribirse en formato URL completo, como `http://pgpkeys.mit.edu:11371`. También es admitido el protocolo LDAP.

Use las siguientes opciones para elegir el servidor con el cual sincronizará las claves automáticamente.

**Nuevo:** Elija un nuevo servidor de claves. Escriba el dominio del servidor de claves y elija una dirección HTTP o LDAP.

**Quitar:** Quite un servidor de claves que está listado como uno de los servidores de claves que usted usa.

### Establecer predeterminado:

Elija cuál de los servidores de claves es su servidor de claves predeterminado. Consulte a su oficina de seguridad informática para determinar si hay un servidor de claves predeterminado que usted debiera usar.

## Preferencias avanzadas

Haga clic sobre la ficha Avanzados para hacer las siguientes elecciones:

### Algoritmo de cifrado

Puede seleccionar el algoritmo de cifrado para sus claves PGP: CAST (predeterminado), IDEA o Triple-DES. Si desea usar IDEA o Triple-DES, debe marcar esta opción antes de generar sus claves.

CAST es un nuevo algoritmo que PGP cree es seguro, y Triple-DES es un algoritmo gubernamental que ha soportado la prueba del tiempo. IDEA es el algoritmo usado tradicionalmente en PGP. Para más información sobre estos algoritmos, ver "Los algoritmos simétricos de PGP" en el Capítulo 8.

Hay dos razones por las que PGP le da la opción de cambiar el algoritmo de cifrado:

\* Al usar cifrado convencional, el cifrado aquí seleccionado es el usado para encriptar.

\* Al crear una clave, el método de cifrado es registrado como parte de la clave, de modo que otras personas usen ese algoritmo al cifrarle mensajes a usted.

**ALERTA:**

Use las casillas de elección solamente si ha decidido que un algoritmo particular es inseguro. Si se da cuenta que Triple-DES ha sido descubierto, puede simplemente deseleccionar esa casilla y sus mensajes serán cifrados usando un algoritmo seguro. Todas las nuevas claves generadas desde ese momento tendrán un registro que Triple-DES no puede ser usado cuando le cifren mensajes a usted.

### **Mostrar nivel de validez marginal**

Seleccione esta casilla para mostrar claves con validez marginal o simplemente para mostrarlas como válidas o inválidas. Los círculos verdes indican que una clave es válida; los grises indican que la clave no ha sido validada porque no fue firmada por un introductor de confianza o por usted; o que es de confianza implícita porque es una clave que usted generó.

### **Tratar claves de validez marginal como inválidas**

Seleccione esta casilla para tratar todas las claves de validez marginal como inválidas. Si usted cifra con claves de validez marginal y esta casilla está seleccionada, aparece el cuadro de diálogo Selección de Claves

### **Avisar al cifrar a claves con una Clave de Descifrado Adicional**

Fuerza la presentación del cuadro de diálogo Destinatario si la clave con la que está cifrando tiene asociada una Clave de Descifrado Adicional.

## Acerca de la búsqueda de claves

Usted puede buscar la clave de otro usuario en archivos de claves locales y en servidores de claves remotos.

### Búsqueda de la clave de un usuario, procedimiento

1. Abra la ventana PGPkeys

2. Elija Buscar desde el menú Claves

Aparece la ventana Búsqueda de Claves PGP. En ella hay varios menús, en los cuales usted puede especificar criterios de búsqueda.

3. En el menú Buscar Claves, elija la ubicación desde la cual usted desea buscar claves.

Puede elegir la ruta de búsqueda del buscador de claves predeterminado, o usar el menú para elegir una ubicación diferente.

4. Especifique su objeto de búsqueda.

El objeto predeterminado es ID Usuario, pero puede hacer clic en el menú para seleccionar ID Clave, Tipo de Clave, Fecha de Creación, Fecha de Caducidad, Estado de Clave y Tamaño de Clave. Por ejemplo, podría buscar todas las claves con el ID Usuario de Alfredo.

5. Especifique las condiciones que está buscando.

Puede elegir criterios de búsqueda con las siguientes condiciones:

\* Es

\* No es

\* Contiene

\* No contiene

\* Está firmada por

\* No está firmada por

\* Está activa (para fechas de creación o caducidad)



\* Activada Antes o Hasta (para fechas de creación o caducidad)

\* Activada Desde o Después (para fechas de creación o caducidad)

6. Escriba los criterios de búsqueda.

Estos criterios deben corresponder al objeto de búsqueda que usted especificó.

El botón de Más Criterios le permite buscar de acuerdo con un segundo criterio, por ejemplo, IDs de clave con el nombre Alfredo creadas antes o hasta el 6 de Octubre de 1997.

7. Haga clic en Buscar para comenzar la búsqueda.

Una barra de progreso muestra que se está efectuando la búsqueda. Haga clic en Parar Búsqueda si la búsqueda está demorando demasiado o si ya ha encontrado las claves que buscaba. Los resultados de la búsqueda aparecen en la ventana.

8. Haga clic en Limpiar Búsqueda para vaciar la ventana de búsqueda y limpiar los criterios de búsqueda.

# Solución de Problemas

Este Capítulo presenta información sobre los posibles problemas, y sus soluciones.

Error	Causa Posible	Solución
No se puede realizar la operación solicitada porque el búfer de salida es demasiado pequeño.	Hay más datos de salida que los que los búferes internos pueden manejar.	Si usted está cifrando o firmando, podría tener que dividir el mensaje en partes más pequeñas y cifrar/firmar por separado. Si usted está descifrando o verificando, pídale al remitente que cifre o firme partes de datos más pequeñas, y se las envíe.
No se puede usar la clave solicitada para esta operación porque no existe confianza suficiente en la clave.	La operación no puede usar una clave en la que no se confía.	Firme la clave con su propia clave para que aquélla pueda ser de confianza, e inténtelo de nuevo.
No se pudo cifrar con la clave especificada porque es una clave sólo para firmar.	La clave seleccionada puede ser usada solamente para firmar.	Elija una clave diferente, o genere una clave nueva que pueda cifrar datos.
No se pudo firmar con la clave especificada porque es una clave solamente para cifrar.	La clave seleccionada solamente puede usarse para cifrar.	Elija una nueva clave, o genere una nueva clave que pueda firmar datos.
No se encontraron claves secretas en su archivo de claves.	No hay claves secretas en su archivo de claves.	Genere su propio par de claves en PGPkeys.

<b>Error</b>	<b>Causa Posible</b>	<b>Solución</b>
La acción no se pudo completar debido a una operación inválida de archivo .	El programa falló al intentar leer o escribir datos en un cierto archivo. El archivo probablemente esté dañado.	Pruebe usar un archivo diferente. Si es necesario modifique sus Preferencias PGP.
La clave ya está firmada por la clave de firmado especificada.	Usted no puede firmar una clave que ya ha firmado anteriormente.	Usted podría haber tomado accidentalmente una clave equivocada. Si es así, elija una clave diferente para firmar.
El archivo de claves contiene un paquete PGP dañado.	El mensaje PGP con el que usted está trabajando ha sido dañado, o sus archivos de claves han sido dañados.	Pida al remitente que envíe el mensaje de nuevo para saber si es el mensaje el que ha sido dañado, o si son sus archivos de claves los dañados. Restaure sus archivos de claves desde su copia de seguridad y pruebe nuevamente.
El archivo de claves está dañado.	El programa no pudo leer o escribir datos en un cierto archivo. Hay un archivo que probablemente falta o está dañado, que puede o no ser el archivo de claves.	Pruebe usar un nombre o una ruta diferentes, si es posible.
El mensaje o datos contiene una firma separada.	La firma para el mensaje o archivo está ubicado en un archivo separado.	Primero, haga doble clic sobre el archivo de firma separado.
La contraseña que ha escrito no coincide con la contraseña de la clave.	La contraseña que usted escribió es incorrecta. Puede que usted haya activado la opción Mayúsculas, o que simplemente haya escrito mal la contraseña.	Inténtelo de nuevo.
La librería PGP se ha quedado sin memoria.	El sistema operativo se ha quedado sin memoria.	Cierre otros programas que se estén ejecutando. Si eso no funciona, podría necesitar más memoria en su máquina.

<b>Error</b>	<b>Causa Posible</b>	<b>Solución</b>
La clave especificada no pudo ser encontrada en su archivo de claves.	La clave necesaria para descifrar el corriente mensaje no está en su archivo de claves.	Pídale al remitente del mensaje que le envíe el mensaje de nuevo y asegúrese que cifre el mensaje con clave pública suya.
El archivo de entrada especificado no existe.	El nombre del archivo escrito no existe.	Use el Explorador de Windows para encontrar el nombre y ruta exactos del archivo que usted desea.
El ID de usuario especificado no se añadió porque ya existía en la clave seleccionada.	No puede añadir un ID de Usuario idéntico a un ID de usuario existente en la clave.	Pruebe a añadir un ID de usuario diferente, o borre antes el ya existente.
Hubo un error al abrir o escribir el archivo de claves o el archivo de salida.	Un archivo que se necesitaba no pudo ser abierto.	Asegúrese que sea correcta la configuración en PGP Preferencias. Si ha borrado recientemente archivos del directorio que instaló PGP, podría necesitar reinstalar el programa.
No hay suficientes datos aleatorios disponibles.	El generador de números aleatorios necesita más datos para generar buenos números aleatorios.	Cuando se le solicite, mueva el ratón o pulse teclas al azar, para generar datos de entrada.
Incapaz de realizar la operación porque el archivo es de sólo lectura o está protegido de algún modo.	Si usted guarda sus archivos de claves en discos extraíbles, puede que el disco no esté insertado. Un archivo que es necesario está con el atributo de sólo lectura o está siendo usado por otro programa.	Cierre otros programas que puedan estar accediendo a los mismos archivos que el programa que usted está ejecutando. Si usted tiene sus archivos de claves en un disquete, compruebe de que el disquete está en la unidad de disco correspondiente.

# Aspectos de Seguridad y Vulnerabilidades

Este Capítulo contiene información introductoria y de fondo sobre criptografía, escrita por Phil Zimmermann.

"Lo que sea que hagas será insignificante, pero es muy importante que lo hagas."  
-Mahatma Gandhi.

## Por qué escribí PGP

Es personal. Es privado. Y no depende de nadie más que de usted. Usted podría estar planificando una campaña política, discutiendo sus impuestos, o teniendo un romance secreto. O podría estar comunicándose con un disidente político en un país represivo. Lo que quiera que sea, usted no desea que su correo electrónico privado (email) o documentos confidenciales sean leídos por nadie más. No hay nada malo con resguardar su privacidad. La privacidad es un derecho natural.

El derecho a la privacidad está implícitamente expresada en la Carta de Derechos. Pero cuando fue redactada la Constitución de los Estados Unidos, no se consideró necesario enunciar explícitamente el derecho a tener una conversación privada. Eso no hubiera tenido sentido. Hace doscientos años todas las conversaciones eran privadas. Si alguien podía escuchar, usted simplemente se alejaba hasta detrás del granero y conversaba allí. Nadie podía escuchar sin su conocimiento. El derecho a una conversación privada era un derecho natural, no sólo en un 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, iniciada con la invención del teléfono, todo eso cambió. Ahora la mayoría de nuestras conversaciones son conducidas electrónicamente. Esto permite que nuestras conversaciones más íntimas sean expuestas sin nuestro conocimiento. Las llamadas de telefonía celular móvil pueden ser vigiladas por cualquiera que tenga una radio. El correo electrónico, enviado por Internet, no es más seguro que las llamadas de telefonía móvil. El correo electrónico está reemplazando rápidamente al correo postal volviéndose la norma para todos, dejando de ser la novedad que fue en el pasado. Y el correo electrónico puede ser revisado a gran escala en forma rutinaria, automática y sin detección, en búsqueda de palabras de interés. Es como pescar con una red.

Tal vez usted piense que su correo electrónico es lo suficientemente legítimo que no se justifica cifrarlo. ¿Por qué entonces no escribe sus cartas en tarjetas postales y las envía sin sobres si es que realmente es un ciudadano cumplidor de la ley sin nada que ocultar? ¿Por qué no se somete a exámenes sobre consumo de sustancias prohibidas a pedido de cualquiera? ¿Por qué exige una orden judicial para que la policía pueda registrar su casa? ¿Está intentando esconder algo? Si envía sus cartas dentro de sobres, tal vez se deba a que usted sea un subversivo, un traficante de drogas, o un loco con delirios de persecución. ¿Es que acaso tienen alguna necesidad de cifrar su correo electrónico los ciudadanos cumplidores de la ley?

¿Qué pasaría si todos creyesen que los ciudadanos cumplidores de la ley debieran usar tarjetas postales para su correo? Si un inconformista intentase proteger su privacidad usando sobres para sus cartas, su actitud despertaría sospechas. Tal vez las autoridades abrirían sus cartas para ver qué está ocultando. Afortunadamente, no vivimos en ese tipo de mundo, porque todos cubrimos con sobres la mayoría de nuestras cartas. Así nadie despierta sospechas al proteger su privacidad con un sobre. Hay seguridad en los números. Análogamente, sería bueno que todos usemos rutinariamente el cifrado para todo correo electrónico inocente o no, de modo que nadie resulte sospechoso por proteger con el cifrado la privacidad de su correo electrónico. Piénselo como una forma de solidaridad.

Hasta ahora, si el gobierno quería violar la privacidad de los ciudadanos comunes tenía que gastar dinero y emplear personal para interceptar y abrir los sobres al vapor. O tenía que escuchar y posiblemente transcribir conversaciones telefónicas, al menos antes que estuviera disponible el reconocimiento automático de la voz. Esta clase de onerosas escuchas no eran prácticas a gran escala. Solamente se hacía en los casos importantes cuando parecía que valía la pena.

El proyecto de ley 266/91 del Senado de los EEUU, que proponía varias medidas anticrimen, tenía una inquietante medida escondida en su interior. Si este proyecto se hubiera convertido en ley, habría forzado a los fabricantes de equipos para comunicaciones seguras a insertar "puertas trampa" especiales en sus productos de modo que el gobierno pudiera leer los mensajes cifrados de cualquiera. El proyecto decía: "Es el sentimiento del Congreso que los que proporcionan de servicios de comunicaciones electrónicas y los fabricantes de equipos para servicios de comunicaciones electrónicas se aseguren 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". Fue este proyecto de ley el que me llevó a publicar PGP electrónicamente y gratis aquel año, poco antes que esa medida fuera derrotada después de vigorosas protestas de grupos por las libertades civiles y de la industria.

El proyecto de ley de Telefonía Digital de 1994 obligaba a las compañías telefónicas a instalar extensiones de las líneas de sus abonados en los conmutadores de las centrales telefónicas digitales, creando una nueva infraestructura tecnológica para las escuchas donde sólo había que presionar un botón, con lo cual los agentes federales ya no tendrían que salir y aplicar pinzas de cocodrilo a las líneas telefónicas. Ahora, desde sus oficinas centrales en Washington podrían escuchar las conversaciones de los teléfonos intervenidos. Por supuesto, la ley todavía requiere una orden judicial para una escucha. Pero mientras la infraestructura tecnológica puede persistir

durante generaciones, las leyes y las políticas pueden cambiar de la noche a la mañana. Una vez que se ha establecido una infraestructura de comunicaciones optimizada para la vigilancia, un cambio en las condiciones políticas podría llevar a un abuso de este nuevo poder. Las condiciones políticas podrían variar con la elección de un nuevo gobierno, o quizá más abruptamente desde el atentado contra un edificio federal.

Un año después que el proyecto de 1994 fuera aprobado como ley de Telefonía Digital, el FBI reveló unos planes para obligar a las compañías telefónicas a incorporar en su infraestructura la capacidad de interceptar simultáneamente un uno por ciento de todas las llamadas telefónicas en todas las grandes ciudades de EEUU. Esto representaría un aumento del número de teléfonos que podrían ser intervenidos de más de mil veces respecto a los niveles anteriores. En años anteriores hubieron alrededor de solamente un millar de escuchas mediante orden judicial por año en EEUU, sumados los casos federales, estatales y locales. Es difícil imaginarse 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 posible de procesar ese volumen de tráfico es una aplicación masiva, estilo Orwell, de tecnología automatizada de reconocimiento de voz, buscando palabras clave intesantes o buscando la voz de una persona 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 sea encontrado, o hasta que todas las líneas telefónicas hayan sido registradas en busca de tráfico subversivo. El FBI dice que necesita esta capacidad para planificar para el futuro. Este plan provocó tal indignación que fue derrotado en el Congreso de EEUU, al menos esta vez, en 1995. Pero el mero hecho de que el FBI siquiera pidiese estos amplios poderes es revelador de su programa. Y la derrota de este plan no es tan tranquilizador si se considera que el proyecto de ley sobre Telefonía Digital de 1994 también fue derrotado la primera vez que fue presentado en 1993.

Los avances tecnológicos no permitirán el mantenimiento de la situación actual en lo que concierne a la privacidad. La situación actual es inestable. Si no hacemos nada, las nuevas tecnologías darán al gobierno nuevos instrumentos de vigilancia automática que ni Stalin habría soñado. La única manera de resguardar la privacidad en la era de la información es la criptografía fuerte.

Usted no tiene que desconfiar del gobierno para desear 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 EEUU a la criptografía han debilitado las defensas de las empresas norteamericanas contra el espionaje extranjero y el crimen organizado.

El gobierno de EEUU 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 reveló una audaz nueva política de encriptación, la cual había estado siendo desarrollada en la Agencia de Seguridad Nacional [NSA, National Security Agency] desde el comienzo de la administración

Bush. La pieza central de esta iniciativa es un dispositivo de cifrado construido por el gobierno, un chip llamado Clipper, que contiene un nuevo y secreto algoritmo de cifrado de la NSA. El gobierno de EEUU 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 sería cargada con su propia clave única y el gobierno guardaría una copia sellada [key escrow]. No hay que preocuparse, puesto que el gobierno promete que solamente usará esas claves para leer sus mensajes solamente "cuando esté debidamente autorizado por la ley". Por supuesto, para hacer al Clipper completamente efectivo, el siguiente paso lógico sería prohibir otras formas de criptografía.

El gobierno de EEUU afirmó inicialmente que usar Clipper sería voluntario, que nadie sería obligado a usarlo en vez de otras formas de criptografía. Pero la reacción popular contra el chip Clipper ha sido más fuerte que lo que el gobierno había previsto. La industria informática 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 eran neutralizadas por criptografía no controlada 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 criptografía fuerte debe estar controlada por el gobierno (aunque nadie había sugerido que hubiese sido usado criptografía por los terroristas).

El Centro de Información sobre Privacidad Electrónica [EPIC, Electronic Privacy Information Center] obtuvo documentos reveladores gracias al Acta de Libertad de Información. En un documento titulado "Encriptación: Amenaza, Aplicaciones y Soluciones Potenciales", enviado al Consejo de Seguridad Nacional en Febrero de 1993, el FBI, la NSA y el Departamento de Justicia de EEUU concluían que "Las soluciones técnicas, tal como están, sólo funcionarán si se incorporan en todos los productos criptográficos. Para asegurarse 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".

En EEUU el gobierno tiene un historial que no inspira confianza acerca de respetar las libertades civiles. El programa COINTELPRO del FBI actuaba sobre grupos que se oponían a las políticas del gobierno. Espiaron al movimiento antiguerra y al movimiento de derechos civiles. Intervinieron el teléfono de Martin Luther King. Nixon tenía su lista de enemigos. Y luego sucedió el escándalo de Watergate. Ahora el Congreso parece empeñado en aprobar leyes para limitar las libertades civiles en Internet. En ningún momento del último siglo el público ha desconfiado tanto del gobierno y de cualquier tendencia política como ahora.

Si deseamos resistir esta inquietante tendencia de prohibir los sistemas criptográficos, una medida que podemos tomar es usar la criptografía tanto como podamos ahora mientras es legal. Cuando el uso de la criptografía fuerte se vuelva popular, será más difícil para el gobierno ilegalizarlo. Por lo tanto, usar PGP es bueno para preservar la democracia.



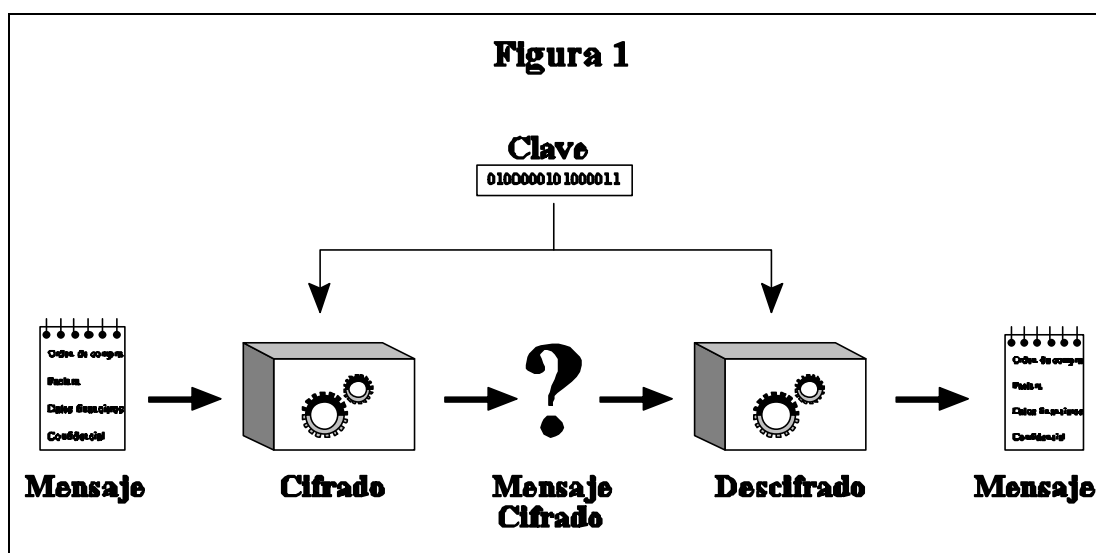
Si la criptografía es ilegalizada, solamente los fuera de la ley tendrán privacidad. Las agencias de inteligencia tienen acceso a buena tecnología criptográfica. También la tienen los grandes traficantes de armas y de drogas. Pero la gente común y las organizaciones políticas de base casi no han tenido acceso a una tecnología criptográfica de clave pública accesible de tipo militar. Hasta ahora.

PGP faculta a la gente para tomar en sus propias manos la responsabilidad de cuidar su privacidad. Hay una creciente demanda social por ella. Por eso lo creé.

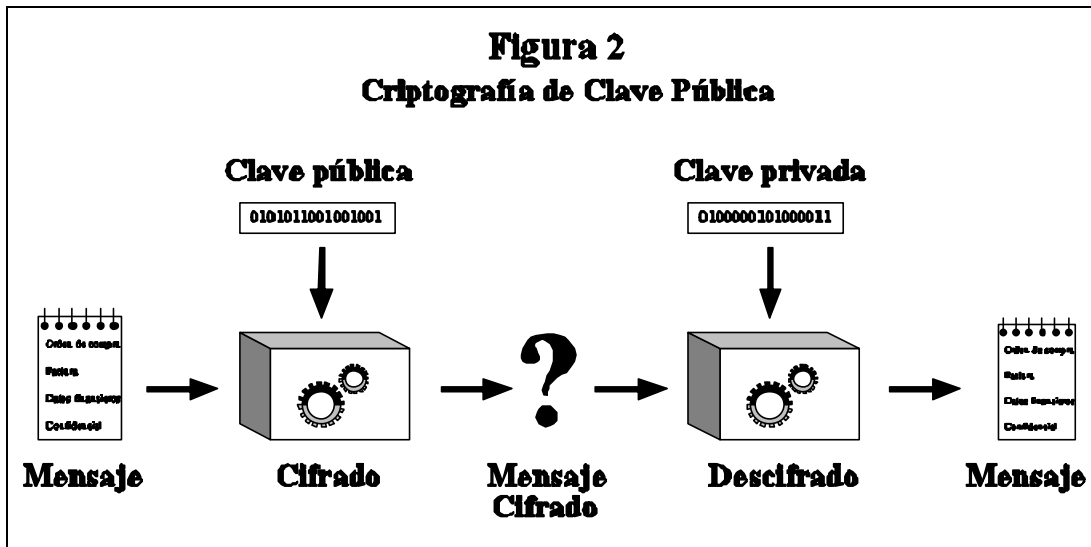
## Fundamentos del cifrado

Primero, alguna terminología elemental. Supóngase que desea enviar un mensaje a una colega, a quien llamaremos Alicia, y no desea que nadie más que Alicia sea capaz de leerlo. Como es mostrado en la Figura 1, usted puede encriptar o cifrar el mensaje, lo que significa desorganizarlo de una manera complicada, haciéndolo ilegible para cualquiera excepto usted y Alicia. Usted usa una clave criptográfica para cifrar el mensaje, y Alicia debe usar la misma clave para descifrarlo o descifrarlo. Al menos así es como funciona en el cifrado de "clave secreta" convencional.

Es usada una clave única para el cifrado y el descifrado. Esto significa que esta clave debe ser transmitida inicialmente por medio de canales de comunicación seguros de modo que ambas partes puedan conocerla antes que los mensajes cifrados sean enviados por canales inseguros. Esto puede ser un inconveniente. ¿Para qué necesita criptografía, si para empezar usted tiene un canal seguro para intercambiar claves?



## Cómo funciona la criptografía de clave pública



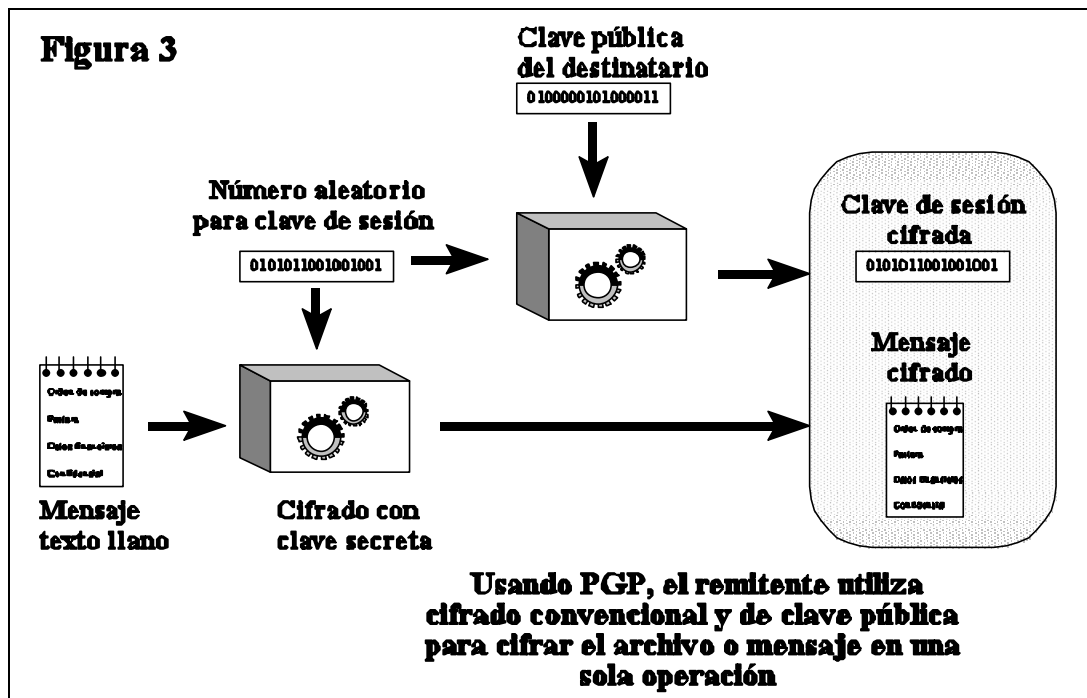
En la criptografía de clave pública, como es mostrado en la Figura 2, todos tienen dos claves complementarias relacionadas, una clave pública y una clave privada. Cada clave destraba el código que genera la otra clave. Conocer la clave pública no lo ayuda a deducir la clave privada correspondiente. La clave pública puede ser publicada y distribuída ampliamente a través de una red de comunicaciones.

Este protocolo proporciona privacidad sin la necesidad de los canales seguros que requiere la criptografía de clave secreta convencional.

Cualquiera puede usar la clave pública del destinatario para cifrar un mensaje a esa persona, y el destinatario usa su propia clave privada correspondiente 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.

## Cómo se cifran archivos y mensajes

Debido a que el algoritmo de cifrado con clave pública es mucho más lento que el cifrado convencional de clave única, se logra un mejor cifrado usando el proceso mostrado en la Figura 3.



Para cifrar el mensaje es usado un algoritmo rápido y de alta calidad de cifrado convencional mediante clave secreta. El mensaje original sin cifrar es llamado "texto llano". En un proceso invisible para el usuario, una clave aleatoria temporal creada solamente para esta "sesión", es usada para cifrar convencionalmente el archivo de texto llano. Luego es usada la clave pública del destinatario para cifrar esta clave convencional aleatoria temporal. Esta "clave de sesión" convencional, cifrada mediante clave pública, es enviada junto con el texto cifrado al destinatario.

## Los algoritmos simétricos de PGP

PGP ofrece una selección de diferentes algoritmos de clave secreta para cifrar el mensaje real. Cuando decimos algoritmo de clave secreta, nos referimos a un sistema de cifrado en bloque convencional, o simétrico, que usa la misma clave para cifrar y descifrar. Los tres cifrados en bloque simétricos ofrecidos por PGP son CAST, Triple-DES e IDEA. No son algoritmos caseros. Todos fueron desarrollados por equipos de criptógrafos de conocida reputación.

Para los curiosos en criptografía, los tres métodos de cifrado operan en bloques de 64 bits de textos llano y cifrado. Las claves CAST e IDEA tienen un tamaño de 128 bits, mientras que Triple-DES usa una clave de 168 bits. Al igual que la Norma de Cifrado de Datos [DES, Data Encryption Standard], cualquiera de estos tres métodos pueden ser usados en los modos de Realimentación 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 promete ser un buen sistema de cifrado en bloques con una clave de 128 bits, es muy rápido, y es gratuito. Su nombre se deriva de las iniciales de sus autores, Carlisle Adams y Stafford Tavares, de la empresa Northern Telecom (Nortel). Nortel ha solicitado una patente para CAST, pero ha hecho un compromiso por escrito para poner CAST a disposición de cualquiera en forma gratuita. 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, exhibiendo buenas razones para creer que probablemente se necesite agotar todas las combinaciones posibles para destrabar su clave de 128 bits. CAST no tiene claves débiles o semidébiles. Hay fuertes argumentos acerca 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 burlar 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 palpito 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 (International Data Encryption Algorithm, Algoritmo de Cifrado de Datos Internacional), está basado en el concepto de diseño de "mezclar operaciones desde grupos algebraicos diferentes". Fue desarrollado en la ETH de Zurich por James L. Massey y Xuejia Lai, y publicado en 1990. Trabajos publicados anteriormente sobre el algoritmo lo llamaban IPES (Improved Proposed Encryption Standard, Norma de Cifrado Mejorada Propuesta), pero posteriormente le cambiaron el nombre a IDEA. Hasta ahora, IDEA ha resistido mucho mejor los ataques que otros métodos de cifrado como FEAL, REDOC-II, LOKI, Snefru y Khafre. Además IDEA es mucho más resistente que DES al ataque altamente exitoso mediante criptoanálisis diferencial de Biham y Shamir, así como ataques de criptoanálisis lineal. Conforme este sistema de cifrado continúa atrayendo los esfuerzos de ataque de los más formidables miembros del mundo criptográfico, la confianza en IDEA está creciendo con el paso del tiempo. Lamentablemente, el mayor obstáculo para la aceptación de IDEA como una norma ha sido el hecho de que Ascom Systec tiene una patente sobre su diseño y, a diferencia de DES y CAST, IDEA no ha sido puesto libre de derechos a disposición de cualquiera.

Como una protección, PGP incluye Triple-DES de 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 ha sido bien estudiado por muchos años, así que podría ser una

apuesta más segura que los cifrados más nuevos como CAST e IDEA. Triple-DES es el 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 e IDEA, usualmente la velocidad no suele ser algo crítico para aplicaciones de correo electrónico. Aunque Triple-DES usa un tamaño de clave de 168 bits, parece tener una fortaleza efectiva de al menos 112 bits frente a un atacante con una capacidad de almacenamiento de datos imposiblemente inmensa para usar en el ataque. 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 quebrar 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 incluyen dentro de sí información que cuenta a un remitente qué métodos de cifrado en bloque son comprendidos por el software del destinatario, de modo que el software del remitente sepa qué método de cifrado puede ser usado para cifrar. Las claves públicas DSS/Diffie-Hellman aceptan CAST, IDEA o Triple-DES como métodos de cifrado en bloque, con CAST como opción predeterminada. 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 normalmente comprime el texto llano antes de cifrarlo porque sería demasiado tarde hacerlo después: 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 del cifrado. La mayoría de las técnicas de criptoanálisis explotan las redundancias que se encuentran en el texto llano, para quebrar 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, no son comprimidos por PGP. Además, 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 ha sido comprimido.

Para los curiosos de los aspectos técnicos, el programa usa las rutinas de compresión ZIP de dominio público escritas por Jean-Loup Gailly, Mark Adler y Richard B. Wales. Este software ZIP usa algoritmos de compresión que son 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 realmente buena y porque es rápido.

## **Acerca de los números aleatorios usados como claves de sesión.**

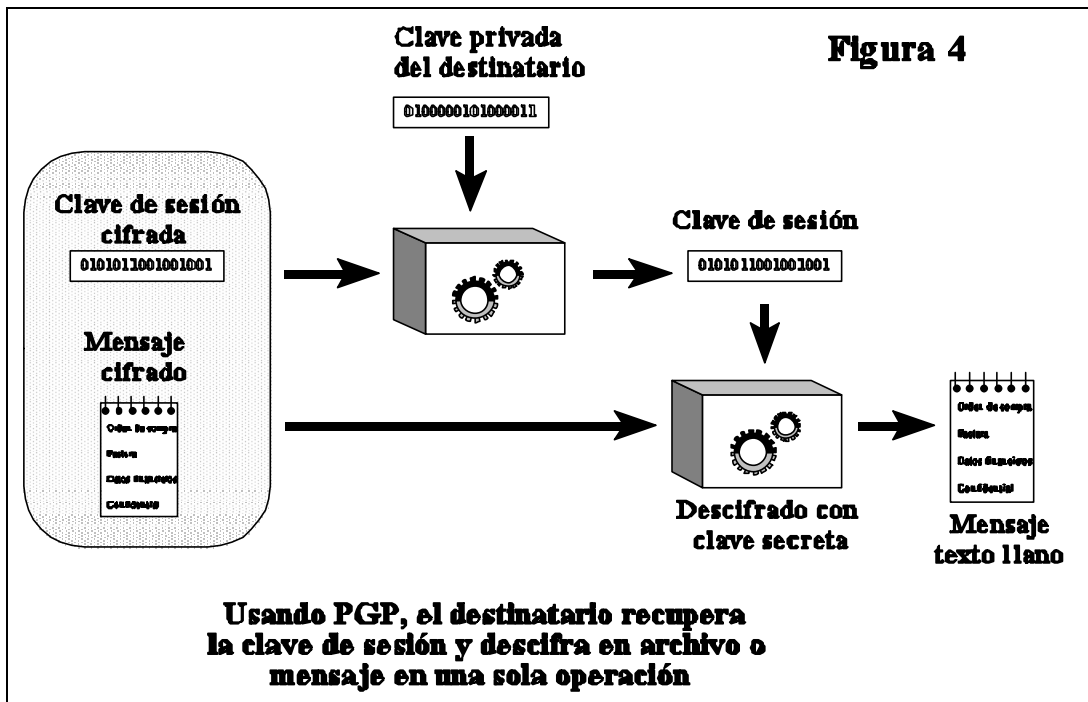
PGP utiliza un generador de números pseudoaleatorios criptográficamente fuerte para crear claves de sesión temporales. Si el archivo de números aleatorios no existe, es creado automáticamente y alimentado con números verdaderamente aleatorios derivados de sus eventos aleatorios recogidos por el programa PGP a partir de los tiempos entre pulsaciones de teclado y movimientos del ratón.

Este generador recarga el archivo de números aleatorios cada vez que es usado, mezclando material nuevo derivado parcialmente de la hora del día con otras fuentes verdaderamente aleatorias. Usa el algoritmo de cifrado convencional como un motor para el generador números aleatorios. El archivo de números aleatorios contiene material generado aleatoriamente y material de clave aleatorio usado para la clave convencional de sesión.

Este archivo de números aleatorios debería estar protegido para evitar que sea descubierto, y así reducir el riesgo que un atacante deduzca sus claves de sesión siguiente o anterior. El atacante tendría que esforzarse para obtener algo útil a partir de este archivo de números aleatorios, porque el archivo es lavado criptográficamente antes y después de cada uso. No obstante, parece prudente intentar evitar que caiga en manos equivocadas. Si es posible, haga que el archivo solamente pueda ser leído por usted. Si no es posible, no permita que otros copien discos indiscriminadamente desde su equipo.

## **Cómo funciona el descifrado**

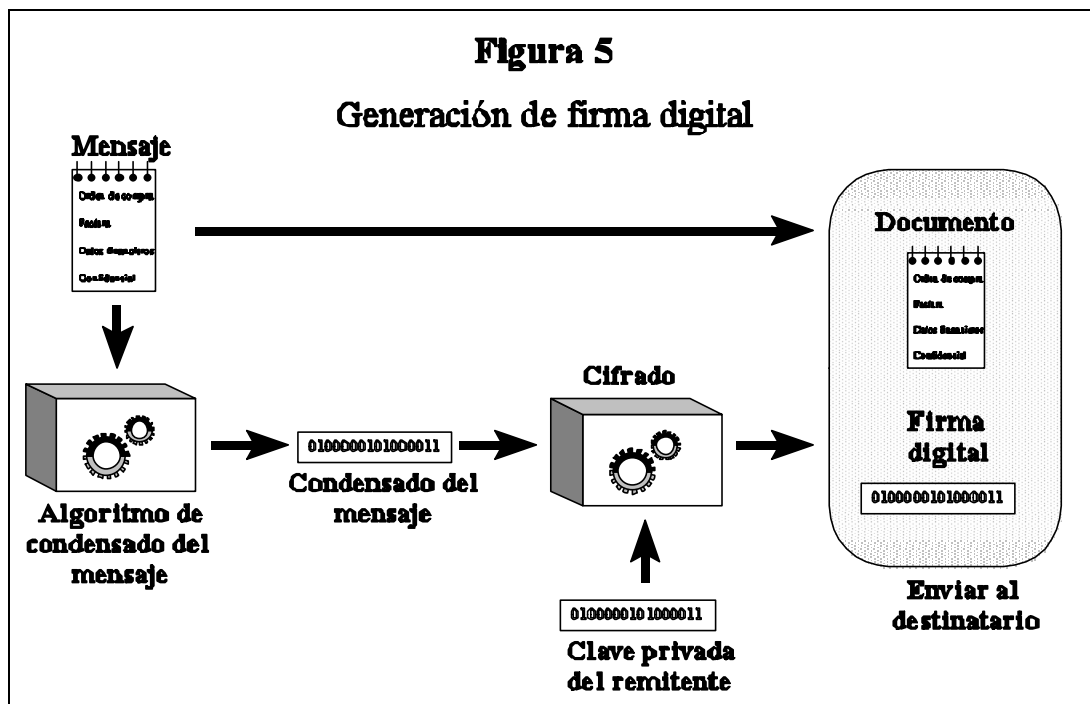
Como es mostrado en la Figura 4, el proceso de descifrado es simplemente el opuesto al cifrado. La clave privada del destinatario es usada para recuperar la clave de sesión temporal, y luego esa clave de sesión es usada para activar el algoritmo de clave secreta convencional rápido para descifrar el verdadero mensaje cifrado.



## Cómo funciona la firma digital

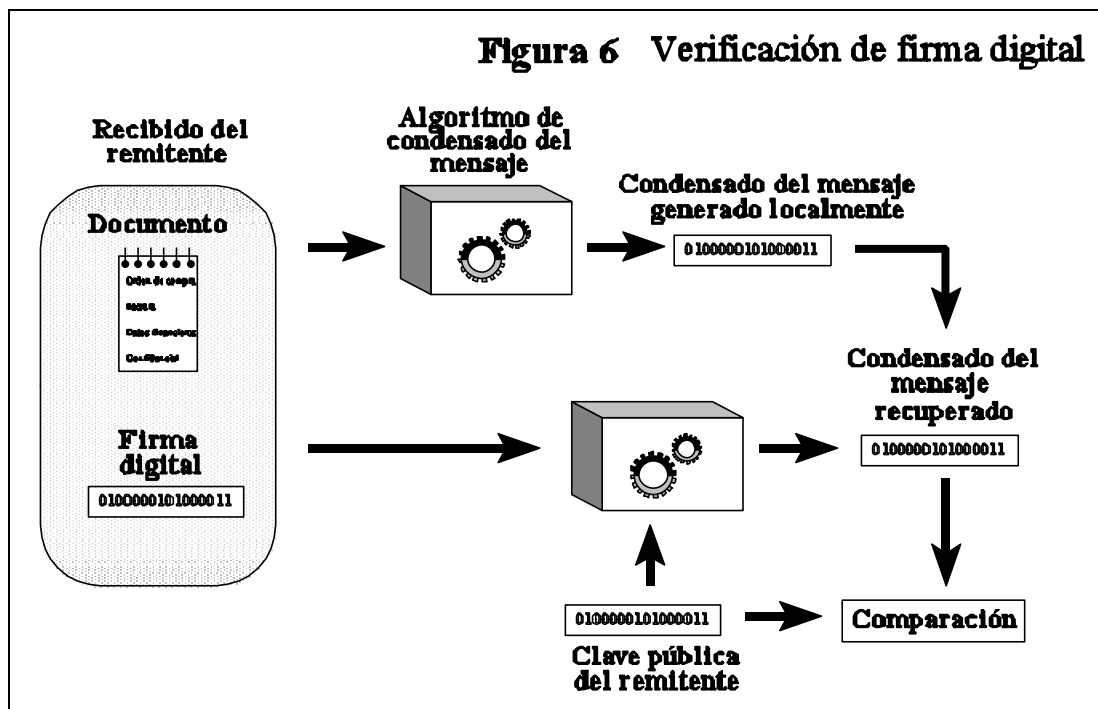
PGP usa firmas digitales para autenticar mensajes. La propia clave privada del remitente puede ser usada para cifrar un condensado del mensaje, "firmando" así el mensaje. Un condensado de mensaje [message digest] es una función hash [resumen del mensaje], unidireccional, criptográficamente fuerte, de 160 o 128 bits. Es análogo a una "suma de control" [checksum] o a un código de control de errores CRC [Cyclic Redundancy Checksum, Suma de Control de Redundancia Cíclica], en el sentido que representa de modo compacto el mensaje y es usado para detectar cambios en el mismo. Sin embargo, a diferencia de CRC, se cree que es computacionalmente inviable que un atacante consiga hacer un mensaje sustituto que produzca un condensado de mensaje idéntico. El condensado de mensaje se cifra con la clave privada del remitente, creando una firma digital del mensaje.

La Figura 5 muestra cómo es generada una firma digital.



El destinatario (o cualquier otro) puede verificar la firma digital usando la clave pública del remitente para descifrarla, como es mostrado en la Figura 6. Esto comprueba que fue el remitente quien verdaderamente originó del mensaje, y que el mensaje no ha sido alterado posteriormente por nadie, porque solamente el remitente posee la clave privada que hizo esa firma. No es posible la falsificación de un mensaje firmado, y el remitente no puede más tarde negar que lo firmó.





### Acerca del condensado de mensaje

El condensado de mensaje es un "destilado" compacto (160 bits o 128 bits) del mensaje o una suma de control del archivo. Usted puede imaginarlo como una "huella dactilar" del mensaje o archivo. El condensado del mensaje "representa" su mensaje de tal modo, que si de alguna manera el mensaje fuera alterado, resultaría un condensado de mensaje diferente. Esto hace posible detectar cualquier cambio hecho al mensaje por un falsificador. Un condensado de mensaje es calculado usando una función hash unidireccional, criptográficamente fuerte. Debería ser computacionalmente inviable para un atacante 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 control [CRC], porque es fácil hacer un mensaje diferente que produzca la misma suma de control. Pero, al igual que una suma de control, usted no puede deducir el mensaje original partiendo del condensado de mensaje.

El algoritmo para el condensado de mensaje usado ahora en PGP (versión 5.0 y posterior) es llamado SHA [Secure Hash Algorithm, Algoritmo Hash Seguro], diseñado por la NSA para el Instituto Nacional de Normas y Tecnología, NIST [National Institute of Standards and Technology]. SHA es un hash de 160 bits. Algunas personas pueden considerar con suspicacia cualquier cosa que provenga de la NSA porque la NSA está a cargo de interceptar comunicaciones y romper códigos. Pero tengamos en mente que la NSA no tiene interés en falsificar firmas, y el gobierno se beneficiaría de una buena norma de firma digital infalsificable

que evitaría que alguien desconociera su firma. Esto tiene distintos beneficios para el refuerzo de la ley y recopilación de información mediante espionaje.

Asimismo, el SHA ha sido publicado sin limitaciones y ha sido extensamente revisado por la mayoría de los mejores criptógrafos del mundo que se especializan en funciones de fragmentos mezclados, y la opinión unánime es que SHA está extremadamente bien diseñado. Tiene algunas innovaciones de diseño que corrige todas las debilidades observadas en los algoritmos de condensado de mensaje publicados previamente 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 la Norma de Firma Digital [Digital Signature Standard] del NIST. Por razones de compatibilidad, las nuevas versiones de PGP todavía usan MD5 para las firmas RSA, porque era lo usado por las versiones más antiguas de PGP.

El algoritmo de condensado de mensaje usado por las versiones más antiguas de PGP es el Algoritmo de Condensado de Mensaje [Message Digest Algorithm] MD5, puesto a disposición en el público por RSA Data Security, Inc. MD5 es un algoritmo hash de 128 bits. En 1996 casi fue quebrado el MD5 por un criptógrafo alemán, Hans Dobbertin. Aunque en ese momento el MD5 no fue quebrado completamente, se descubrió que tiene tan serias debilidades que nadie debería seguir usándolo para generar firmas. Trabajos posteriores en este campo podrían quebrarlo completamente, permitiendo que las firmas sean falsificadas. Si no desea encontrar algún día su firma digital PGP en una falsa confesión, sería un buen consejo el migrar a las nuevas claves PGP DSS como su método preferido para hacer firmas digitales, porque DSS usa SHA como algoritmo hash seguro.

## **Claves públicas, cómo protegerlas contra alteraciones**

En un criptosistema de clave pública, usted no tiene que proteger sus claves públicas contra la exposición. De hecho, es mejor si están 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 "Protección de la clave" en el Capítulo 3 por los procedimientos adecuados. Veamos primero un desastre potencial, y luego describamos cómo evitarlo de una manera segura con PGP.

Supongamos que desea enviar un mensaje privado a Alicia. Usted obtiene el certificado de clave pública de Alicia desde un servicio de boletines electrónicos [BBS, Bulletin Board System]. Cifra su carta a Alicia con esta clave pública y se la envía por correo electrónico a través del BBS.

Desafortunadamente, y sin que lo sepa usted o Alicia, otro usuario llamado Carlos se ha infiltrado en el BBS y ha generado una clave pública para sí con el identificador de usuario de Alicia. Substituye furtivamente la clave pública verdadera de Alicia por su clave falsa. Sin saberlo, 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 identificador de usuario de Alicia. Ahora Carlos puede descifrar el mensaje destinado a Alicia porque él tiene la clave privada correspondiente. Puede incluso volver a cifrar el mensaje descifrado usando la clave pública verdadera de Alicia, y enviarle a ella de modo que nadie sospeche ninguna irregularidad. Más aún, puede incluso hacer firmas aparentemente buenas de Alicia con esta clave privada porque todos usarán la clave pública falsa para comprobar la firma de Alicia.

El único modo de evitar este desastre es evitar que alguien altere las claves públicas. Si usted obtuvo la clave pública de Alicia directamente de Alicia, no hay problema. Pero eso puede resultar difícil si Alicia está a mil kilómetros de distancia o no se encuentra disponible.

Tal vez usted podría obtener la clave pública de Alicia de un amigo en común de confianza, David, quien sabe que tiene una buena copia de la clave pública de Alicia. David podría firmar la clave pública de Alicia, garantizando 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 ha sido alterada. Esto requiere que usted tenga una copia buena de la clave pública de David para comprobar su firma. Quizá David podría entregar a Alicia una copia firmada de su clave pública también. David sirve así como un "presentador" entre Alicia y usted.

Este certificado de clave pública firmado para Alicia podría ser cargado por David o Alicia al BBS, y usted podría descargarlo más tarde. Podría entonces comprobar la firma por medio de la clave pública de David y así asegurarte que esa es realmente la clave pública de Alicia. Ningún impostor pueden engañarle haciéndole aceptar su clave falsa como si fuese de Alicia, porque nadie puede falsificar firmas hechas por David.

Una persona de confianza para muchas personas podría incluso especializarse en proporcionar este servicio de "presentador" entre usuarios proveyendo firmas para sus certificados de clave pública. Esta persona de confianza podría ser considerada una "Autoridad de Certificación". Cualquier certificado de clave pública que lleve la firma de esta Autoridad de Certificación podría ser considerado con confianza como realmente perteneciente a la persona a quien parece pertenecer. Todos los usuarios que desearan participar necesitarían una copia de validez reconocida solamente de la clave pública de la Autoridad de Certificación, de modo que la firma de la Autoridad de Certificación pudiera ser verificada. En algunos casos, la Autoridad de Certificación puede también actuar como un 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 también deba 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 de confianza para sus amigos podría probablemente funcionar mejor que una autoridad de certificación de claves centralizada.

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

El problema más difícil en las aplicaciones prácticas de clave pública es el de proteger a las claves públicas contra alteraciones. Es el "talón de Aquiles" de la criptografía de clave pública, y mucha complejidad de software está dedicado a resolver este problema.

Usted debería usar una clave pública solamente después de asegurarse que es una buena clave pública, que no ha sido alterada, y que realmente pertenece a la persona a quien se supone que está asociada. Puede asegurarse de esto si obtuvo este certificado de clave pública directamente de su propietario, o si lleva la firma de alguien en quien confía, de quien usted ya tiene una clave pública buena. Asimismo, el identificador de usuario debería llevar el nombre completo del propietario de la clave, no solamente el primer nombre.

No importa lo tentado que esté, usted nunca debería ceder a lo más cómodo y confiar en una clave pública descargada de un servicio de boletines electrónico, a no ser que esté firmada por alguien en quien confíe. Esa clave pública no certificada podría haber sido manipulada por cualquiera, hasta por el mismo administrador del sistema.

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

Para firmar una clave pública, debe estar más que seguro de la propiedad de esa clave respecto a si simplemente desea usarla para cifrar un mensaje. Para convencerse suficientemente de la validez de una clave para usarla, deberían bastar las firmas de certificación de presentadores de confianza. Pero para firmar una clave usted mismo, debería exigir información independiente y de primera mano de quien posee esa clave. Tal vez podría llamar por teléfono al propietario de la clave y leerle la huella de ésta para confirmar que la clave que tiene es realmente suya ... y asegúrese que realmente está hablando con la persona correcta.

Tenga en mente 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 completamente que la clave realmente le pertenece. Otras personas aceptarían esa clave

como perteneciente a él porque usted la firmó (suponiendo que confíen en usted), pero no deberían confiar en el dueño de la clave. Confiar en una clave no es lo mismo que confiar en su dueño.

Sería una buena idea que su propia clave pública contenga una colección de firmas de certificación de un conjunto de "presentadores", con la esperanza de que la mayoría de la gente confíe en al menos uno de los presentadores que responda por la validez de su clave pública. Podría publicar su clave, con su colección de firmas de certificación, en varios servicios de boletines electrónicos. Si firma la clave pública de alguien, devuélvasela con su firma para que pueda añadirla a su propia colección de credenciales para su propia clave pública.

Asegúrese que nadie más pueda manipular su propio archivo de claves públicas. Comprobar un nuevo certificado de clave pública firmado recientemente, al final dependerá de las claves públicas de confianza que ya están en su propio archivo de claves. Mantenga un control físico de su propio archivo de claves públicas, preferentemente en su propio equipo en vez de hacerlo en un sistema compartido de acceso remoto, igual como lo haría para su archivo de claves privadas. Esto es para protegerlo contra alteraciones, no contra su exposición. Mantenga una copia de seguridad fiable de su archivo de claves públicas y de su clave privada en medios protegidos contra escritura.

Puesto que su propia clave pública fiable es usada 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 modificaciones. Debería conservar una copia de seguridad en un disquete protegido contra escritura.

PGP generalmente supone que usted mantendrá control físico sobre su sistema y sus archivos de claves, así como sobre su copia de PGP en sí. Si un intruso puede manipular su disco, entonces en teoría podría modificar el propio programa, burlando así las salvaguardias que el programa pueda tener para detectar las modificaciones de claves.

Un modo algo complicado de proteger su archivo de claves públicas en su totalidad contra modificaciones es firmarlo con su propia clave privada. Puede hacerlo mediante un certificado de firma separado del archivo de claves público.

## **¿Cómo controla PGP qué claves son válidas?**

Antes de leer esta sección, debería leer la sección anterior, "Claves Públicas, cómo protegerlas contra alteraciones".

PGP hace un seguimiento de qué claves de su archivo de claves públicas están apropiadamente certificadas con firmas de presentadores de su confianza. Todo lo que tiene que hacer es decirle a PGP en quiénes confía como presentadores, y certificar usted mismo sus claves con su propia clave de confianza total. Desde ahí PGP puede validar automáticamente cualquier

otra clave que haya sido firmada por sus presentadores designados. Y por supuesto, usted mismo puede firmar más claves.

Hay dos criterios completamente diferentes que PGP usa para juzgar la utilidad de una clave pública ... no los confunda:

1. ¿Realmente pertenece la clave a la persona a quien parece pertenecer? En otras palabras, ¿ha sido certificada con una firma fiable?
2. ¿Pertenece a alguien en quien usted pueda confiar para certificar otras claves?

PGP puede calcular la respuesta a la primera pregunta. Para responder a la segunda pregunta debe formularla explícitamente a PGP. Cuando usted suministra la respuesta a la pregunta 2, PGP luego puede calcular la respuesta a la pregunta 1 para otras claves firmadas por el presentador que usted ha designado como de confianza.

Las claves que han sido certificadas por presentadores de confianza son consideradas válidas por PGP. Las claves pertenecientes a presentadores de confianza deben estar certificadas ellas en sí, ya sea por usted o por otros presentadores de confianza.

PGP también permite la posibilidad que usted tenga varios grados de confianza para que la gente actúe como presentadores. Su confianza en el propietario de una clave para actuar como un presentador no solamente refleja su estimación de su integridad personal--debería también reflejar cuán competente cree que él es para comprender la administración de claves y si usa buen juicio para firmar claves. Usted puede designar una persona como sin confianza, de confianza marginal o de confianza total para certificar las claves públicas de otros. Esta información de confianza es guardada en su archivo de claves junto con la clave de ella, pero cuando le dice a PGP que copie una clave fuera de su archivo de claves, PGP no copia la información de confianza junto a la clave, porque sus opiniones personales sobre confianza son consideradas como confidenciales.

Cuando PGP está calculando la validez de una clave pública, examina el nivel de confianza de todas las firmas certificadoras adosadas. Calcula un grado de validez--por ejemplo, dos firmas de confianza marginal son consideradas tan creíbles como una firma de confianza total. El escepticismo del programa es configurable--por ejemplo, puede configurar PGP para que exija dos firmas de confianza total o tres firmas de confianza marginal para juzgar una clave como válida.

Su propia clave es "axiomáticamente" válida para PGP, no necesitando firmas de presentadores para probar su validez. PGP reconoce cuáles claves públicas son suyas mirando las claves privadas correspondientes del archivo de claves privadas. PGP también supone que usted confía completamente en usted mismo para certificar otras claves.

Con el tiempo, usted acumulará claves de otras personas a quienes podría desear designarlas como presentadores de confianza. Cada persona elegirá sus propios presentadores de confianza. Y además cada persona acumulará y distribuirá gradualmente con sus claves una colección de firmas de certificación de otras personas, con la esperanza que quien la reciba

confiará en al menos una o dos de las firmas. Esto originará el surgimiento de una red de confianza descentralizada y tolerante a fallos para todas las claves públicas.

Esta estructura de aproximación desde las bases contrasta con los esquemas de administración de claves públicas normales desarrollados por el gobierno y otras instituciones monolíticas, tales como el Correo de Privacidad Acrecentada de Internet [PEM, Internet Private Enhanced Mail], el cual está basado en un control centralizado y confianza centralizada obligatoria. Los esquemas normales confían en una jerarquía de Autoridades de Certificación que dictaminan en quién usted debe confiar. El método probabilístico descentralizado del programa para determinar la legitimidad de una clave pública es la pieza central de su arquitectura de administración de claves. PGP solamente le permite a usted elegir en quién confía, poniéndole en la cima de su propia pirámide de certificación privada. PGP es para gente que prefieren ser ellos mismos quienes empaquen sus propios paracaídas.

Nótese que aunque aquí es enfatizada la aproximación desde las bases descentralizada, ello no significa que PGP no se comporte igualmente bien en los esquemas de administración de claves públicas centralizados, más jerárquicos. Por ejemplo, los usuarios de grandes empresas probablemente desearán una figura o persona central que firme las claves de todos los empleados. PGP maneja esa estructura centralizada como un caso especial derivado del modelo de confianza más generalizado de PGP.

## **Cómo evitar la exposición de sus claves privadas**

Proteja muy cuidadosamente su propia clave privada y su contraseña. Si su clave privada alguna vez es comprometida, mejor será que avise rápidamente a todas las partes interesadas antes de que alguien la use para firmar en su nombre. Por ejemplo, alguien podría usarla para firmar certificados falsos de clave pública, lo que podría crear problemas a mucha gente, especialmente si su firma goza de amplia confianza. Y por supuesto, un compromiso de su propia clave privada podría exponer todos los mensajes que le envíen.

Para proteger su clave privada, puede empezar por mantener siempre un control físico sobre ella. Dejarla en el equipo de su casa está bien, o guardarla en su equipo portátil que puede llevar con usted. Si debe usar un equipo de la oficina cuyo control físico no siempre tiene, mantenga sus archivos de claves públicas y privadas en un disquete protegido contra escritura, y cuando salga no lo deje en la oficina. No sería buena idea permitir que su clave privada residiera en un sistema compartido de acceso remoto, como un sistema UNIX de acceso remoto. Alguien podría observar a escondidas su línea de modem, capturar su contraseña, y obtener su clave privada desde el sistema remoto. Solamente debería usar su clave privada en una máquina que esté bajo su control físico. Vea el Capítulo 8 por información adicional.

No guarde su contraseña en ningún lugar del equipo que tenga su archivo de claves privadas. Almacenar la clave privada y la contraseña en el mismo equipo es tan peligroso como guardar su contraseña del cajero automático en la misma billetera que su tarjeta de crédito. Usted

no desea que alguien ponga sus manos en su disco conteniendo tanto la contraseña como el archivo de claves privadas. Sería más seguro si usted solamente memoriza la contraseña y no la guarda en ningún otro lugar excepto su cerebro. Si cree que debe escribir su contraseña, manténgala bien protegida, si es posible aún 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 usted haya distribuido por el mundo.

El esquema no institucional descentralizado que PGP admite para la administración de claves públicas tiene sus beneficios, pero desafortunadamente también significa que usted no puede confiar en una única lista centralizada de claves comprometidas. Esto hace un poco más difícil contener el daño de una clave privada comprometida. Usted tiene que avisar al mundo y esperar que todos lo escuchen.

Si sucede lo peor--que tanto su clave privada como su contraseña hayan sido comprometidas (esperemos que de alguna manera se haya dado cuenta), tendrá que emitir un certificado de "clave comprometida". Este tipo de certificado es usado para alertar a la gente a que dejen de usar su clave pública. Puede usar PGP para crear tal certificado, usando el comando Revocar desde el menú Claves. Luego, debe de alguna manera enviar este certificado de compromiso a cada persona del planeta, o al menos a todos sus amigos y los de éstos, etc. El software PGP de ellos instala este certificado de clave comprometida en sus archivos de claves públicas y automáticamente evita que su clave pública sea nuevamente usada por accidente. Usted puede entonces generar un nuevo par de claves privada/pública y publicar la nueva clave pública. Podría enviar un paquete conteniendo tanto su nueva clave pública como el certificado de clave comprometida para su vieja clave.

### **¿Y si pierde su clave privada?**

Normalmente, si desea revocar su propia clave privada puede usar el comando Revocar desde menú Claves 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 es destruida? No puede revocarla, porque debe usar su propia clave privada para revocarla, y ya no la tiene. Puedes pedir a cada persona que firmó su clave que retire su certificación. Entonces, quien intente usar su clave basándose en la confianza en uno de los presentadores sabrá que no debe confiar en su clave pública.

## **Cuidado con el aceite de serpiente**

Cuando se examina un paquete de software criptográfico, siempre queda la misma pregunta: ¿por qué se debería confiar en este producto? Aún si examinó el código fuente usted



mismo, no todos tienen la experiencia criptográfica para juzgar la seguridad. Aunque sea usted un experimentado criptógrafo, podrían pasársele por alto sutiles debilidades en los algoritmos.

Cuando yo estaba en la Universidad a comienzos de los setenta, diseñé lo que creí era un brillante esquema de cifrado. Un simple conjunto de números pseudoaleatorios era añadido al texto llano para crear texto cifrado. Esto parecía frustrar cualquier análisis del texto cifrado basado en la frecuencia de repetición de letras, y sería imposible de quebrar incluso por las agencias de inteligencia gubernamentales con más recursos. Me sentí bastante vanidoso por mi hazaña.

Años más tarde, descubrí este mismo esquema en varios textos de introducción a la criptografía y en trabajos académicos. Qué placer. Otros criptógrafos habían pensado en el mismo esquema. Desafortunadamente, el esquema fue presentado como un simple ejercicio sobre cómo usar técnicas criptoanalíticas elementales para quebrarlo de manera trivial. Ahí terminó mi brillante esquema.

De esta humillante experiencia aprendí cuán fácil es caer en una falsa sensación de seguridad cuando se diseña un algoritmo de cifrado. La mayoría de la gente no se da cuenta de lo infernalmente difícil que es diseñar un algoritmo 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 ingenuos (a menudo incluso el mismo esquema de cifrado), y algunos de ellos han sido incorporados en paquetes comerciales de software de cifrado y vendidos a buen precio a miles de usuarios desprevenidos.

Esto es como vender cinturones de seguridad para automóviles, que lucen bien y son cómodos, pero que se abren en la más ligera prueba de choque. Dependiendo de ellos puede ser peor que no llevar cinturones de seguridad. Nadie sospecha que son malos hasta un choque verdadero. Dependiendo de software criptográficamente débil podría causar que usted sin saberlo arriesgue información sensible, cuando ésta no habría sido nunca expuesta en caso de ausencia de software criptográfico. Quizá incluso nunca descubra que sus datos habían sido comprometidos.

Algunas veces los paquetes comerciales usan la Norma de Cifrado de Datos Federal [DES, Data Encryption Standard], un algoritmo convencional bastante bueno recomendado por el gobierno para uso comercial (pero curiosamente no para información secreta--Hummm). 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 recomienda los modos más fuertes y complejos de Realimentación de Cifrado [CFB, Cipher Feedback] y de Encadenado de Bloques de Cifrado [CBC, Cipher Block Chaining].

Desafortunadamente, la mayoría de los paquetes comerciales de cifrado que he visto usan el modo ECB. Cuando hablé con los autores de varias de estas implementaciones, me dijeron que nunca habían oído hablar de los modos CBC o CFB, y que no sabían nada acerca de las debilidades del modo ECB. El mismo hecho que ni siquiera hubieran aprendido suficiente criptografía para conocer estos conceptos elementales resulta poco alentador. Y algunas 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 ser usado en lugar del DES, que es más lento. El autor del programa piensa a menudo que el algoritmo más rápido, que le pertenece, es tan seguro como DES, pero después de interrogarle suelo descubrir que solamente es una variación de mi brillante esquema de mis días de universidad. O tal vez ni siquiera revelará como funciona el esquema de cifrado de su propiedad, pero me asegura que es un esquema brillante y que debería confiar en él. Estoy seguro que él cree que su algoritmo es brillante, pero ¿cómo puedo saberlo yo sin verlo?

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

Aún los programas realmente buenos que usan DES en los modos correctos de operación tienen problemas. El DES normal usa una clave de 56 bits, que es demasiado pequeña para las normas actuales, y puede ser fácilmente quebrada mediante búsquedas exhaustivas de clave en máquinas especiales de alta velocidad. DES ha llegado al fin de su vida útil y en consecuencia 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 por 185 dólares vende un paquete de software que quiebra los esquemas de cifrado incluidos dentro de WordPerfect, Lotus 1-2-3, MS Excel, Symphony, Quattro Pro, Paradox, MS Word y PKZIP. No hace simplemente adivinanza de contraseñas--hace verdadero criptoanálisis. Algunas personas lo compran cuando olvidan la contraseña de acceso a sus propios archivos. Las fuerzas de seguridad también lo usan para poder leer los archivos que capturan. Hablé con Eric Thompson, el autor, y me dijo que a su programa le toma solamente una fracción de segundo para quebrarlos, pero puso algunos lazos de retardo para volverlo más lento de modo que no le pareciese tan fácil al cliente.

En el campo de la telefonía segura, sus opciones son desoladoras. El competidor líder es el STU-III (Secure Telephone Unit = Unidad Telefónica Segura), fabricado por Motorola y AT&T por entre 2.000 y 3.000 dólares, y usado por el gobierno en aplicaciones clasificadas secretas. Tiene criptografía fuerte, pero necesita una especie de licencia especial del gobierno para comprar esta versión fuerte. Existe una versión comercial del STU-III que está debilitada por conveniencia de la NSA, y hay una versión para exportación que está aún más debilitada. Luego está el AT&T Surity 3600 de 1.200 dólares, que usa el polémico chip Clipper del gobierno para cifrar, con copias de las claves guardadas selladas en depósitos del gobierno [escrow], para facilitar la tarea de los escuchas si fuera ordenado. Y por supuesto, luego están los perturbadores de voz analógicos (no digitales) que puede comprar en los catálogos de aspirantes a espía, y que realmente son juguetes inútiles en lo que respecta a criptografía, pero que son vendidos como productos de comunicaciones "seguros" a clientes que simplemente no conocen nada mejor.

En cierta forma los productos criptográficos son como los farmacéuticos. Su integridad es crucial. La mala penicilina tiene el mismo aspecto que la buena penicilina. Usted puede saber si su programa de hoja de cálculo es malo, pero ¿cómo saber si su programa criptográfico es débil? El texto cifrado producido por un algoritmo de cifrado débil luce igual que el producido por un

algoritmo de cifrado fuerte. Hay mucho aceite de serpiente por ahí. Muchas curas de charlatán. A diferencia de los vendedores ambulantes de medicina patentada de antaño, estos implementadores de software ni siquiera saben que sus productos son aceite de serpiente. Tal vez sean buenos ingenieros de software, pero usualmente ni siquiera han leído nada de la bibliografía académica sobre criptografía. Pero ellos piensan que pueden escribir buen software de criptografía. ¿Y por qué no? Después de todo, parece intuitivamente fácil hacerlo. Y su software parece funcionar bien.

Cualquiera que piense haber diseñado un esquema de cifrado imposible de quebrar, o es un raro genio increíble, o un ingenuo e inexperto. Desafortunadamente, algunas veces tengo que tratar con aprendices de criptógrafos que desean hacer "mejoras" a PGP añadiéndole algoritmos 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 no se hubiese "ganado sus galones" pasando antes un montón de tiempo quebrando códigos. Eso tenía mucho sentido. Le hice notar que según ese criterio prácticamente nadie está cualificado en el mundo de la criptografía comercial. "Sí", dijo con una sonrisa de suficiencia. "y eso hace nuestro trabajo en la NSA mucho más fácil". Un pensamiento estremecedor. Yo tampoco estaba cualificado.

También el gobierno ha tratado con aceite de serpiente. Después de 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 quebraron el código Enigma durante la guerra, un hecho que permaneció clasificado secreto por muchos años. Aún hoy muchos sistemas UNIX de todo el mundo usan el cifrado Enigma para el cifrado de archivos, en parte debido a que el gobierno ha creado obstáculos legales contra el uso de mejores algoritmos. Hasta intentaron evitar la publicación inicial del algoritmo RSA en 1977. Y durante muchos años han frenado 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 EEUU es reunir información, principalmente mediante escuchas encubiertas de las comunicaciones privadas de la gente (lea el libro 'The Puzzle Palace', de James Bamford). La NSA ha acumulado considerables habilidades y recursos para quebrar códigos. Cuando la gente no puede obtener buenos productos criptográficos para protegerse, el trabajo de la NSA se hace mucho más fácil. La NSA también tiene la responsabilidad de aprobar y recomendar algoritmos de cifrado. Algunos críticos afirman que esto es un conflicto de intereses, como poner al zorro a cuidar el gallinero. En los años 80, la NSA había estado promoviendo un algoritmo de cifrado convencional que había diseñado (el Programa de Adhesión COMSEC), y no le contaban a nadie cómo funcionaba porque eso era secreto. Querían que otros confiaran en él y lo usaran. Pero cualquier criptógrafo puede decirle que un algoritmo de cifrado bien diseñado no tiene que ser secreto para permanecer seguro. Solamente las claves deberían necesitar protección. ¿Cómo podría alguien realmente saber si el algoritmo secreto de la NSA es seguro? No sería tan difícil para la NSA diseñar un algoritmo de cifrado que solamente ellos pudiesen quebrar, 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 deliberadamente vendiendo aceite de serpiente?

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

- \* El primero es la virtual universal falta de competencia de los implementadores de software para cifrado comercial (aunque esto está empezando a cambiar desde la publicación de PGP). Todo ingeniero de software se considera criptógrafo, lo que ha llevado a la proliferación de criptosoftware realmente malo.
- \* El segundo es la supresión deliberada y sistemática por parte de la NSA de toda tecnología comercial buena de cifrado, por medio de intimidación legal y presión económica. Parte de esta presión se manifiesta en la forma de controles estrictos a la exportación de software de cifrado, que por las características que tiene el mercado del 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 monopolio de patentes de criptografía se rompió a fines de 1995).

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

No estoy tan seguro sobre la seguridad de PGP como una vez lo estuve sobre mi brillante software de cifrado de la universidad. Si lo estuviera, sería una mala señal. Pero no creo que PGP contenga debilidades claras (aunque estoy casi seguro que contiene algunas fallas menores). He seleccionado los mejores algoritmos de la bibliografía publicada sobre criptología civil. En su mayor parte, estos algoritmos han estado individualmente sometidos a extensas revisiones por parte de colegas de sus autores. Conozco a muchos de los principales criptógrafos del mundo, y he discutido con algunos de ellos muchos de los algoritmos y protocolos usados en PGP. Está bien investigado, 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 1991 que por primera vez desarrollé y distribuí gratuitamente PGP, pasé tres años bajo una investigación criminal de Aduanas de EEUU por la distribución de PGP fuera de EEUU, con riesgo de proceso criminal y años de encarcelamiento. Por cierto, no habrá visto que el gobierno se molestara por otros programas de cifrado--es PGP el que realmente les molestó. ¿Qué le indica eso acerca de 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 privacidad, por la 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 ser burlado de diversas maneras. En cualquier sistema de seguridad para datos, usted tiene que preguntarse si la información que está intentando proteger es más valiosa para su atacante que el costo del ataque. Esto le llevaría a protegerse de los ataques más baratos, sin preocuparse por los ataques más caros.

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

"Si la totalidad de PCs del mundo -260 millones- trabajasen en un sólo mensaje cifrado con PGP, en forma estimada les tomaría 12 millones de veces la edad del Universo, como promedio, para quebrar el mensaje." William Cromwell, Vicedirector, Agencia de Seguridad Nacional, 20 de Marzo de 1997.

## Contraseña y clave privada comprometidas

Probablemente el ataque más simple ocurre si deja la contraseña de su clave privada escrita en cualquier lugar. Si alguien la consigue, y también consigue su archivo de clave privada, puede leer sus mensajes y firmar en su nombre.

He aquí algunas recomendaciones para proteger su contraseña:

1. No use contraseñas obvias que puedan ser fácilmente adivinadas, como los nombres de sus niños o cónyuge.
2. Use espacios y una combinación de números y letras en su contraseña. Si hace que su contraseña sea una única palabra, puede ser fácilmente adivinada haciendo que un equipo pruebe todas las palabras en el diccionario hasta que encuentre su contraseña. Es por eso que una frase de contraseña es mucho mejor que una palabra de contraseña. Un atacante más sofisticado podría hacer que su equipo rastrease un libro de citas famosas para encontrar su frase de contraseña.
3. Sea creativo. Use una frase de contraseña fácil de recordar pero difícil de adivinar; puede construirla fácilmente usando algunos dichos sin sentido o citas literarias obscuras.

## Alteración de claves públicas

Existe una vulnerabilidad grave si las claves públicas son alteradas. Ésta podría ser la vulnerabilidad más importante de un criptosistema de clave pública, en parte porque muchos novatos no la reconocen de inmediato. La importancia de esta vulnerabilidad, y las contramedidas higiénicas apropiadas, son detalladas en "Claves Públicas, cómo protegerlas contra alteraciones.

Resumiendo: cuando use la clave pública de alguien, asegúrese que no haya sido alterada. Solamente debería tener confianza en una clave pública nueva de otra persona si la obtuvo directamente de su propietario, o si ha sido firmada por alguien en quien confía. Asegúrese que nadie pueda alterar su propio archivo de claves públicas. Mantenga un control físico tanto de su archivos de claves públicas como de su clave privada, preferentemente en su propio equipo en vez de un sistema compartido de acceso remoto. Guarde una copia de seguridad de ambos archivos de claves.

## **Archivos no del todo borrados**

Otro problema potencial de seguridad es causado por cómo la mayoría de los sistemas operativos borran los archivos. Cuando cifra un archivo y luego 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 sea reutilizado más tarde. Es algo así como tirar al cesto de papeles documentos que contienen datos importantes, en vez de pasarlos por la trituradora de papel. Los bloques del disco aún contienen los datos sensibles que usted deseaba borrar, y probablemente serán sobrescritos por nuevos datos en algún momento del futuro. Si un atacante lee esos bloques de disco borrados inmediatamente después de haber sido desasignados, podría recuperar su texto llano.

En realidad, esto incluso podría suceder accidentalmente, si se produjera una falla en el disco y algunos archivos hubieran sido borrados o dañados accidentalmente. Podría usarse un programa de recuperación de disco para recuperar los archivos dañados, pero esto a menudo significa que junto con todo lo demás, resuciten algunos archivos previamente borrados. Sus archivos confidenciales, que usted pensó que habían desaparecido para siempre, podrían reaparecer y ser inspeccionados por quienquiera que estuviera intentando recuperar su disco dañado. Incluso mientras está creando el mensaje original con un procesador o editor de textos, el programa 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 son borradas por el procesador de textos cuando termina, pero esos fragmentos sensibles todavía están 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 borrados sean sobrescritos. A menos que sepa con seguridad que todos los bloques borrados del disco serán prontamente reutilizados, debe tomar medidas para sobrescribir el archivo de texto llano, y también cualquier fragmento del mismo que haya quedado en el disco, dejado por su procesador de textos. Puede ocuparse de cualquier fragmento del texto llano dejado en el disco usando la opción Tachado Seguro [Wipe] de PGP.

## **Virus y caballos de Troya**

Otro ataque puede involucrar a un virus informático o un 'gusano' hostil especialmente diseñado que podría infectar PGP o su sistema operativo. Este hipotético virus podría ser diseñado para capturar su contraseña, su clave privada, o sus mensajes descifrados, y furtivamente escribir la información capturada en un archivo o enviarla a través de una red a quien implantó el virus. O podría alterar el funcionamiento de PGP para que las firmas no sean correctamente comprobadas. Este ataque es más económico que los ataques criptoanalíticos.

La defensa contra este tipo de ataques cae en la misma categoría que la defensa contra infecciones virales en general. Existen productos antivirales comerciales bastante buenos, y se deben seguir procedimientos higiénicos para reducir en gran medida las probabilidades de una infección viral. Un tratamiento completo de medidas contra virus y gusanos está más allá del alcance de este documento. PGP no tiene defensas contra virus, y supone que su equipo está 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 alguien que haya creado una buena imitación de PGP que se comporte como PGP en muchos casos, pero que no funciona como se supone que deba. Por ejemplo, podría estar debilitado deliberadamente para que no compruebe adecuadamente las firmas, permitiendo la aceptación de certificados de clave falsos. Usted debería hacer un esfuerzo para obtener su copia de PGP directamente de Pretty Good Privacy.

Hay otras maneras de comprobar si PGP fue alterado, y es 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 ayudaría del todo si su sistema operativo está infectado, ni detectará si su copia original de `pgp.exe` ha sido maliciosamente alterada de tal modo que comprometa su propia habilidad para comprobar firmas. Esta prueba también supone que usted tiene una buena copia de la clave pública que usa para comprobar la firma de los archivos ejecutables de PGP.

## **Archivos de intercambio o memoria virtual**

Originalmente PGP fue desarrollado para MS-DOS, un sistema operativo primitivo para las normas de hoy. Pero al migrar a sistemas operativos más complejos, como Microsoft Windows y Macintosh OS, surgió una nueva vulnerabilidad. Esta vulnerabilidad proviene del hecho que estos refinados sistemas operativos usan una técnica llamada memoria virtual.

La memoria virtual le permite ejecutar programas inmensos, mucho más grandes que la memoria física instalada en su equipo. Esto es útil porque el software se ha vuelto cada vez más voluminoso desde que las interfaces gráficas de usuario se convirtieron en la norma y los usuarios empezaron a ejecutar varias aplicaciones grandes al mismo tiempo. El sistema operativo usa el disco duro para almacenar porciones de su software que no están siendo usadas en ese momento. Esto significa que sin su conocimiento el sistema operativo podría escribir al disco algunas cosas que usted suponía estaban solamente en la memoria principal [física]--cosas como claves, contraseñas, y texto llano descifrado. PGP no guarda esa clase de datos sensibles en memoria más

tiempo del necesario, pero siempre existe alguna posibilidad que todas formas el sistema operativo lo escriba al disco.

Los datos son escritos en alguna zona no usada del disco, conocida como archivo de intercambio [swap file]. A medida que son necesitados, los datos son vueltos a leer desde el archivo de intercambio, de modo que solamente parte de su programa o datos están en la memoria física en un momento dado. Toda esta actividad es invisible al usuario, quien simplemente percibe el trabajo del disco. Microsoft Windows intercambia trozos de memoria, llamados páginas, usando un algoritmo de reemplazo de páginas Menos Usado Recientemente [LRU, Least Recently Used]. Esto significa que las páginas que no han sido accedidas por el período más largo de tiempo son las primeras en ser pasadas al archivo de intercambio del disco. Esta idea sugiere que en la mayoría de los casos el riesgo que los datos sensibles sean pasados al disco es relativamente bajo, ya que PGP no los deja en memoria mucho tiempo. Pero no damos garantías al respecto.

Este archivo de intercambio puede ser accedido por cualquiera que pueda tener acceso físico a su equipo. Si está preocupado por este problema, puede resolverlo obteniendo un software especial que sobrescribe 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 Mac OS. Desactivar la memoria virtual podría significar que necesite más chips de memoria física RAM instaladas para que todo quepa en la RAM.

## **Fugas en la seguridad**

Una fuga en la seguridad podría permitir a alguien obtener físicamente sus archivos de texto llano o mensajes impresos. Un oponente obstinado podría conseguirlo por medio del hurto, revisando la basura, por registro y captura, o por medio de soborno, extorsión o infiltrándose entre sus empleados. Algunos de estos ataques pueden ser especialmente posibles contra organizaciones políticas de base que dependen de un personal en su mayoría voluntario.

No caiga 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 incluso pueden comprometer datos en texto llano o información escrita o hablada.

Este tipo de ataques es más económico 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 equipo. Este ataque, caro y muy laborioso, probablemente sea más económico que un ataque criptoanalítico directo. Una furgoneta equipada con instrumental



apropiado puede estacionarse cerca de su oficina y captar desde lejos toda la actividad del teclado y los mensajes mostrados en la pantalla de su equipo. Esto comprometería todas sus contraseñas, mensajes, etc. Este ataque puede ser evitado apantallando adecuadamente todo el equipo instalado y el cableado de la red para que no irradie esas señales. Esta tecnología de apantallamiento, conocida como "Tempest", es usada por algunas agencias del gobierno y contratistas de defensa. Existen vendedores de hardware que suministran comercialmente apantallamientos Tempest.

## **Protección contra fechados falsos**

Una vulnerabilidad algo oscura de PGP involucra a los usuarios deshonestos que crean fechados [timestamp] falsos en sus propios certificados de clave pública y firmas. Puede omitir esta sección si es un usuario casual y no está compenetrado en oscuros protocolos de clave pública.

No hay nada que evite que un usuario deshonesto modifique la configuración de día y hora del reloj de su propio sistema, y genere firmas y certificados de clave pública propios que parezcan haber sido creados en un momento diferente. Puede aparentar que firmó algo antes o después de cuando realmente lo hizo, o que su par de claves pública/privada fue creado con anterioridad o posterioridad. Con ello podría obtener beneficios legales o financieros, por ejemplo para crear algún tipo de vacío legal que le permita repudiar una firma.

Creo que este problema fechados falsos en firmas digitales no es peor que el de las firmas manuscritas. Cualquiera puede escribir cualquier fecha al lado de su firma manuscrita en un contrato, pero nadie parece estar alarmado ante este estado de cosas. En algunos casos, una fecha "incorrecta" en una firma manuscrita no tiene por qué estar asociada con un fraude real. La fecha podría ser aquella en la que el firmante confirma que firmó un documento, o aquella en la que desea que la firma tenga validez.

En situaciones donde es crítico que una firma tenga una fecha correcta, la gente se limita a usar notarios (escribanos) para dar fe y fechar una firma manuscrita. El análogo a esto en las firmas digitales es conseguir que una tercera parte de confianza firme un certificado de firma, estampando una fecha confiable. Para ello no se necesitan protocolos exóticos o demasiado formales. Las firmas con testigos han sido reconocidas desde hace bastante tiempo como un modo legítimo de determinar cuándo fue firmado un documento.

Una Autoridad de Certificación confiable o un notario podría crear firmas notariales con una fecha confiable. Esto no necesariamente requeriría una autoridad centralizada. Tal vez cualquier presentador de confianza o parte no interesada podría servir al efecto, del mismo modo que lo hacen los notarios públicos reales. Cuando una autoridad firma las firmas de otras personas, crea un certificado de firma de un certificado de firma. Esto sirve como testigo de la firma del mismo modo que lo hacen los notarios reales al atestiguar en firmas manuscritas.

El notario podría introducir el certificado de firma separado (sin el documento real que había sido firmado) en un registro especial controlado por el notario. Cualquiera podría leer este registro. La firma del notario tendría una fecha confiable, lo que le daría mayor credibilidad o importancia legal que la fecha estampada en la firma original.

Hay un buen tratamiento de este tema en el artículo de 1983 en IEEE Computer por Denning. Futuras mejoras de PGP podría contener opciones para facilitar la administración de certificaciones notariales de firmas, con fechados estampados confiables.

## **Exposición en sistemas multiusuario**

Originalmente PGP fue diseñado para un PC monousuario, bajo su control físico directo. Si ejecuta PGP en su casa en su propio PC, sus archivos cifrados están generalmente seguros, a menos que alguien robe su PC y le persuada para que le entregue su contraseña (o si su contraseña es lo bastante fácil como para ser adivinada).

PGP no está diseñado para proteger sus datos mientras está en la forma de texto llano en un sistema comprometido. Ni tampoco puede evitar que un intruso use medidas sofisticadas para leer su clave privada mientras está siendo usada. Usted tendrá que reconocer estos riesgos en sistemas multiusuario, y en consecuencia ajustar sus expectativas y comportamiento. Tal vez tu situación sea tal que debiera considerar ejecutar PGP solamente en un sistema monousuario aislado, bajo su control físico directo.

## **Análisis de tráfico**

Aún si el atacante no puede leer el contenido de sus mensajes cifrados, podría ser capaz de deducir al menos alguna información útil observando desde dónde vienen los mensajes y hacia adónde van, el tamaño de los mensajes y el día y la hora en que se envían. Esto es análogo a si el atacante mirase su factura telefónica de larga distancia para ver a quién llamó usted, cuándo y durante cuánto tiempo habló, aunque desconozca el atacante el contenido real de sus llamadas. Esto es llamado análisis de tráfico. PGP por sí sólo no protege contra los análisis de tráfico. Resolver este problema requeriría protocolos especializados de comunicaciones 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 formidable podría ser montado por alguien con grandes recursos económicos y equipos sofisticados, tal como una agencia de inteligencia del gobierno. Podrían quebrar su clave RSA usando algún nuevo avance de factorización secreto. Pero la comunidad académica civil ha estado atacándolas sin éxito activamente desde 1978.

Tal vez el gobierno tenga algunos métodos secretos para quebrar 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 están entre los mejores criptógrafos de Europa. Ha sufrido extensos análisis de seguridad y revisiones por los mejores criptógrafos del mundo no secreto. Parece tener algunas ventajas de diseño sobre DES respecto al criptoanálisis diferencial.

Además, aún si este algoritmo tuviera alguna sutil debilidad desconocida, PGP comprime el texto llano antes del cifrado, lo cual reduciría grandemente esas debilidades. La carga computacional de trabajo necesaria para quebrarla será con toda probabilidad mucho más onerosa que el valor del mensaje.

Si su situación justifica que se preocupe acerca de ataques de este calibre muy formidable, entonces tal vez deba contactar a un consultor en seguridad de datos para obtener seguridad de datos adaptada a tus necesidades especiales.

Resumiendo, sin una buena protección criptográfica de sus comunicaciones de datos, podría ser sencillo e incluso rutinario para un oponente el interceptar sus mensajes, especialmente aquellos enviados a través de un modem o sistema de correo electrónico. Si usted usa PGP y sigue algunas precauciones razonables, el atacante tendrá que dedicar muchos más esfuerzos y gastos para violar su privacidad.

Si usted se protege contra los ataques más simples, y se siente confiado en que su privacidad no va a ser violada por un atacante resuelto y de grandes recursos, probablemente estará seguro usando PGP. PGP le da Privacidad Bastante Buena [Pretty Good Privacy].

# Transferencia de Archivos entre MacOS y Windows usando PGP

La dificultad para transferir archivos hacia y desde el sistema operativo MacOS es un problema clásico que se presenta al usar casi cualquier clase de software de intercambio de datos, tales como aplicaciones de correo electrónico, FTP, utilidades de compresión y PGP. Este apéndice está orientado a documentar cómo este problema es finalmente resuelto por PGP versión 5.5, y a discutir cómo comunicarse con versiones previas de PGP.

MacOS almacena archivos de manera diferente a otros sistemas operativos. Hasta el formato de los archivos de texto de MacOS es distinto. Los archivos MacOS son realmente dos archivos, uno de Datos y uno de Recursos. Para enviar un archivo MacOS a Windows sin perder datos deben fusionarse ambos segmentos. El método normal por el que un archivo MacOS se convierte en un archivo único para que pueda ser transferido a otro Macintosh o PC sin perder ninguna de sus mitades se llama MacBinary.

El problema es que, a menos que use un software especial, Windows y otras plataformas no pueden entender el formato MacBinary. Si sucede que el software receptor no consigue convertir un archivo de formato MacBinary en un archivo Windows, el archivo resultante es inutilizable. Existen utilidades Windows de terceros que pueden repararlo y convertirlo en un archivo utilizable, pero eso no conviene.

Las versiones anteriores de PGP y la mayoría de las utilidades disponibles hoy en el mercado generalmente intentan ignorar este problema tanto como sea posible y dejar que el usuario tome todas las decisiones sobre si codificar o no con MacBinary un archivo cuando lo envía desde MacOS. Esto plantea al usuario el dilema de tener que decidir entre enviar con MacBinary sin ningún riesgo de perder datos y enviar sin MacBinary con la esperanza de que no se pierdan datos importantes, al usuario que usualmente no tiene idea de cuál es la decisión correcta. La decisión debería basarse en si el fichero 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 las versiones anteriores de PGP y muchas otras utilidades. Esto ha resultado en una gran confusión e inconvenientes a los usuarios.

El caso opuesto, enviar un archivo desde Windows a MacOS, también ha sido un problema. Windows usa extensiones de nombres de archivos, como .doc, para identificar el tipo de archivo. Esto no tiene sentido en MacOS. Estos archivos son enviados a un equipo Macintosh sin ninguna información sobre el tipo de archivo y la aplicación que lo creó. El proceso de

hacerlos legibles después de la recepción generalmente involucra varias acciones en el diálogo Abrir de la aplicación que creó el archivo, y en muchos casos exige que el usuario entienda la jerga MacOS de códigos de tipo de archivo y aplicación que lo creó, y los especifique manualmente en una utilidad de terceros.

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

## **Envío desde MacOS a Windows**

Dentro de MacOS, en PGP 5.5 hay tres opciones 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 PGP versión 5.5 o superior en cualquier plataforma. Esto significa que los usuarios de MacOS recibirán el archivo exacto que habían querido, y la versión de Windows decodificará automáticamente el MacBinary, e incluso agregará la extensión apropiada al nombre de archivo, como .doc para Microsoft Word o .ppt para Microsoft PowerPoint. PGP incluye información sobre la mayoría de las extensiones de nombre de archivos y códigos creadores de las aplicaciones Macintosh más comunes. En los casos donde el tipo de archivo es desconocido o se sepa que se trata de un archivo sólo para MacOS, tal como una aplicación MacOS, el archivo permanece en formato MacBinary para que posteriormente pueda ser enviado completamente intacto a un equipo Macintosh.

### **MacBinary: No**

Si usted se está comunicando con usuarios que tienen una versión más antigua de PGP, la decisión de enviar con MacBinary generalmente termina en las manos de quien envía, como en la mayoría de los otros programas y en las versiones anteriores de PGP para MacOS. Al enviar a un equipo que tiene instalada una versión anterior, si sabe que el archivo que está enviando puede ser leído por aplicaciones Windows cuando no es usado MacBinary, seleccione esta opción. Esto incluye a la mayoría de los archivos de aplicaciones generalmente multiplataforma tales como aquellos creados por las aplicaciones Microsoft Office, archivos de gráficos, archivos

comprimidos y muchos otros. El remitente o el destinatario tendrán que renombrar manualmente el 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 pocos casos donde esta opción puede ser útil para 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. El archivo no será codificado con MacBinary, haciéndolo con ello legible en un PC con cualquier versión de PGP si pertenece a uno de los siguientes tipos:

- \* 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 com Compactor
- \* Archivos comprimidos con Arc
- \* Archivos de gráficos JPEG

Como se ve, solamente una selección limitada de archivos resultará en un archivo legible por versiones anteriores de PGP en otras plataformas, usando la opción Inteligente. Cualquier otro archivo recibido en un PC con una versión anterior de PGP será ilegible si antes no se quita la codificación MacBinary con un programa de terceros. Además, el archivo no tendrá la extensión correcta en el PC a menos que esa extensión sea añadida manualmente por el usuario que envía. Usando el modo Inteligente, el archivo resultante podría no ser el mismo que el original cuando se envía a otro Macintosh, porque podría perder sus códigos creador y de tipo. Este modo permanece en el producto principalmente debido al hecho que estaba en PGP versión 5.0 y algunos usuarios podrían tener necesidad de enviar solamente los tipos de archivos mencionados anteriormente. Esta opción no es recomendada para la mayoría de los casos.

Resumiendo, si está enviando solamente a versiones 5.5 o posteriores, seleccione siempre 'MacBinary: Sí' (predeterminada). Así no se complica si su entorno está usando exclusivamente

PGP versión 5.5. Cuando envíe a usuarios con versiones anteriores, debe seleccionar 'MacBinary: No' para archivos de tipo multiplataforma y 'MacBinary: Sí' para archivos que de cualquier modo no serían legibles para los usuarios de PC (como una aplicación MacOS).

Nota sobre PGP versión 5.0: PGP versión 5.0 no tenía una opción 'MacBinary: No'. Para enviar archivos del tipo sin MacBinary, y que no están incluidos en la lista 'MacBinary: Inteligente' a un PC que use la versión 5.0, antes de ser enviado el archivo debe configurarse manualmente con alguno de los códigos creador y de tipo de la lista 'MacBinary: Inteligente'.

## **Recepción de archivos Windows en MacOS**

Cuando descifra, PGP versión 5.5 intenta traducir automáticamente las extensiones de los archivos que no son MacBinary en información de creador y tipo de MacOS. Por ejemplo, si recibe un archivo de Windows con una extensión .doc, el archivo será guardado como documento Microsoft Word. La misma lista de aplicaciones usada para añadir extensiones al recibir un archivo MacBinary en Windows es usado para traducir las extensiones al equivalente MacOS cuando son recibidos en un equipo Macintosh. En casi todos los casos, esto resulta en archivos que son inmediatamente legibles y manipulables con 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 Microsoft Word. En el caso de Microsoft Word, después de determinar la aplicación creadora, simplemente se usa el diálogo Abrir para abrir el archivo seleccionando "Todos los Archivos" desde el menú emergente. Muchas otras aplicaciones también tienen esta característica, pero no todas. Si el documento no puede ser abierto desde la aplicación, el usuario debe averiguar cuáles son los códigos creador y de tipo apropiados para ese archivo, y configurarlos manualmente con una utilidad de terceros. Hay muchas utilidades gratuitas que sirven para hacer esto. En este caso, la opción más sencilla probablemente sea actualizar a la versión 5.5, ya que elimina este problema.

## **Aplicaciones soportadas**

La siguiente lista de aplicaciones conocidas produce documentos que son traducidos automáticamente por PGP 5.5 cuando son enviados desde Windows a MacOS y viceversa. Estas conversiones pueden ser añadidas manualmente y cambiadas editando el archivo "PGPMacBinaryMappings.txt" en el directorio de su sistema..

\* 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 (text,RTF, plantillas)
- \* PGP
- \* Microsoft PowerPoint
- \* StuffIt
- \* QuickTime
- \* Corel WordPerfect
- \* Microsoft Excel (muchos tipos diferentes de archivos)
- \* Quark XPress

También son convertidas las siguientes extensiones:

.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

**Archivo de claves [keyring]:**

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 [private keyring]:**

Conjunto de una o más claves privadas, todas ellas pertenecientes al propietario del archivo.

**Archivo de claves públicas [Public keyring]:**

Conjunto de claves públicas. Su archivo de claves públicas contiene además su propia clave pública (o claves).

**Autenticación [authentication]:**

Determinación del origen de la información cifrada mediante la verificación de la firma digital o de la clave pública de una persona comprobando su huella única.

**Autoridad certificadora [certifying authority]:**

Uno o más individuos de confianza a quienes se les asigna la responsabilidad de certificar el origen de las claves y añadirlas a una base de datos común.

**Certificar [certify]:**

Firmar la clave pública de otra persona.

**Cifrado [encryption]:**

Método de modificar la información para hacerla ilegible para todos menos para el destinatario deseado, quien debe descifrarla para poder leerla.

**Cifrado convencional [conventional encryption]:**

Cifrado que se basa en una contraseña común, en vez de criptografía de clave pública. El archivo se cifra usando una clave de sesión, que a su vez es cifrada usando una contraseña que se le pedirá elija.

**Clave [key]:**

Código digital usado para cifrar y firmar, y descifrar y verificar mensajes de correo electrónico y archivos. Las claves se encuentran como pares de claves y se almacenan en archivos de claves.

**Clave privada [private key]:**

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

**Clave pública [public key]:**

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 sin cuidado a colegas y extraños. Conocer la clave pública de una persona no ayuda a nadie a descubrir la clave privada correspondiente.

**Condensado de mensaje [message digest]:**

Extracto compacto de su mensaje, o control de integridad de su archivo. Representa a su mensaje, de modo que si el mensaje fuese modificado de alguna manera, se obtendría un condensado de mensaje diferente.

**Confiable [trusted]:**

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

**Contraseña [passphrase]:**

Introducción por teclado de una serie de caracteres que le dan acceso a su clave privada, la que usted usa para firmar y descifrar mensajes de correo electrónico y archivos adjuntos.

**Criptografía de clave pública [public-key cryptography]:**

Criptografía en la que se utiliza un par de claves, compuesto por una clave pública y una clave privada, y que no necesita seguridad en el canal de comunicación en sí.

**Depósito de claves [key escrow]:**

Práctica donde un usuario de un sistema de cifrado por clave pública debe entregar su clave privada a terceros permitiéndoles de este modo controlar sus comunicaciones cifradas.

**Descifrado [decryption]:**

Método de recomposición de la información cifrada para volverla legible de nuevo. Para descifrar se usa la clave privada privada del destinatario.

**Firma [signature]:**

Código digital creado con una clave privada. Las firmas permiten la autenticación de la información mediante el proceso de verificación de firma. Cuando usted firma un mensaje o archivo, el programa PGP usa su clave privada para crear un código digital que es único tanto para los contenidos del mensaje como para su clave privada. Cualquiera puede utilizar su clave pública para verificar su firma.

**Firma digital [digital signature]:**

Ver firma

**Firmar [sign]:**

Poner una firma.

**Huella [fingerprint]:**

Cadena identificatoria única de números y caracteres usada para autenticar claves públicas. Esta es la manera principal de comprobar la autenticidad de una clave.

**Huella de clave [key fingerprint]:**

Cadena identificatoria única de números y caracteres usada para autenticar claves públicas. Por ejemplo, usted puede llamar por teléfono al propietario de una clave pública y pedirle que le lea la huella asociada a esa clave de modo que usted pueda compararla con la huella de su copia de esa clave pública para ver si coinciden. Si la huella no coincide, entonces usted sabrá que tiene una clave falsa.

**Identificador [ID] de clave [key ID]:**

Código legible que identifica de manera única a un par de claves. Dos pares de claves pueden tener el mismo ID de Usuario, pero tendrán diferentes IDs de clave.

**Identificador [ID] de usuario [user ID]:**

Texto de una frase 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 (propietario y colegas) a identificar al propietario del par de claves.

**Par de claves [key pair]:**

Clave pública y su clave privada complementaria. En sistemas de criptografía de clave pública como el programa PGP, cada usuario tiene como mínimo un par de claves.

**Presentador [introducer]:**

Persona u organización a la que se le permite garantizar la autenticidad de la clave pública de alguien. Usted designa a un presentador firmando la clave pública del mismo.

**Presentador fiable [trusted introducer]:**

Alguien en quien usted confía para proveerle a usted con claves que son válidas. Cuando un introductor confiable firma las claves de otra persona, usted confía que esas claves son válidas, y no necesita verificarlas antes de utilizarlas.

**Red de confianza [web of trust]:**

Modelo de confiabilidad distribuida utilizado por PGP para validar al propietario de una clave pública en el que el grado de confianza es acumulativo y se basa en el conocimiento de los presentadores por parte del individuo.

**Texto [text]:**

Texto normal imprimible ASCII de 7-bits.

**Texto con armadura ASCII [ASCII-Armoured Text]:**

Información binaria que ha sido codificada utilizando un juego de caracteres normales e imprimibles ASCII de 7-bits, por su conveniencia para transportar la información a través de sistemas de comunicaciones. En el programa PGP, la extensión predeterminada que se da a los archivos de texto armado ASCII es .asc, y son codificados y decodificados en el formato ASCII base-64 [radix-64].

**Texto llano [plaintext]:**

Texto normal, legible, no cifrado, no firmado.

**Verificación [verification]:**

Acto de comparar una firma creada con una clave privada usando la clave pública complementaria. La verificación demuestra que la información fue enviada realmente por el firmante, y que posteriormente el mensaje no ha sido alterado por nadie más.

# Índice

## A

- Actualización
  - de una versión previa de PGP 18
  - de ViaCrypt 18
- Adjuntos de archivo 51
- Administración de claves 54
- Administración de grupos 45
- Algoritmo de cifrado preferido 58
- Almacenamiento de archivos 108
- Almacenamiento de claves 33-34
- Alteración, protección contra 90
- Análisis de tráfico 107
- Archivos
  - configurar ubicación de archivos de claves 68
  - exportar claves a 64
  - exportar claves públicas a 36
  - importar claves desde 64
  - importar claves públicas desde 39
- Archivos de claves
  - cambiar atributos 54-59
  - descripción 54
  - establecer ubicación 68
  - guardar en otro lugar 54
  - repaso rápido 13
  - ubicación 54
  - ver atributos 54-59
  - ver propiedades 58
- Atacantes, protección contra 90
- Atajos 25
- Atributos de archivo de claves
  - cambiar 54-59
  - ver 54-59
- Autoridad de Certificación 91

## B

- Barra de tareas, uso de PGP desde 22
- Búsquedas de clave 72

## C

- Caducidad
  - de clave 30
  - propiedad 57
- Cambiar contraseña 63
- Certificación de claves públicas 14, 91
- Certificado de clave comprometida 96
- Cifrado
  - algoritmos de 58
  - cómo funciona 28
  - establecer preferencias 66
- Cifrar
  - correo electrónico 15, 41
    - repaso 13
  - desde el Explorador de Windows 49-51
  - desde el portapapeles 22
  - usando Eudora 41, 43
- Clave de Descifrado Adicional 17
- Claves
  - administración 54
  - colores de 32
  - comprobación de huella 60
  - copia de seguridad 33-34
  - distribución 42
  - eliminación 63
  - establecer tamaño de 30
  - establecer ubicación de 68
  - examinar 23,58

- exportación a archivos 64
- firmar 60
- guardar 33-34
- generación 28
- inhabilitación 62
- importación desde archivos 64
- otorgar confianza para validaciones 62
- propiedades de visualización 58
- protección 33-34, 90
- repaso 28
- revocación 65
- verificar autenticidad 39
- Claves privadas
  - almacenamiento 33-34
  - comprometidas 101
  - creación 14
  - creación con el Asistente de Claves PGP 23
  - establecer ubicación de 68
  - protección 33-34
  - repaso 13
  - ubicación 54
  - ver 23
- Claves públicas
  - certificar 14, 91
  - copiar desde un mensaje de correo electrónico 39
  - crear 14
  - crear con el Asistente de Claves PGP 23
  - dar a otros usuarios 14
  - distribuir 34
  - enviar a servidor de claves 32, 34-35
  - establecer ubicación 68
  - exportar a archivos 36
  - firmar 60, 91
  - importar desde archivos 39
  - intercambiar 14
  - obtener de otros 36-39
  - obtener de un servidor de claves 37
  - proteger 33-34
  - proteger contra alteración 90
  - repaso 13
  - ubicación 54
  - validar 14
  - ventajas de enviar a un servidor de claves 34
  - ver 23
- Comparar huellas 40
- Compatibilidad
  - norma PGP/MIME 18
  - versiones de PGP 16
- Comprobar
  - autenticidad de una clave 39
  - huella 60
- Complementos [plug-ins] 13, 41
- Condensado del mensaje, descripción 87
- Confianza
  - modelo de 57
  - para validaciones de clave 62
  - presentador de 40, 91, 95
- Contraseña
  - cambiar 59, 63
  - comprometida 101
  - establecer 30
  - establecer preferencias 66
  - olvidar 65
  - sugerencias ix, 31
- Correo electrónico
  - añadir un nuevo nombre de usuario 59
  - cifrar
    - desde el Explorador de Windows 49, 51
    - desde el portapapeles 47
    - con Eudora 41, 43
  - comprobar una firma 13
  - copiar claves públicas de un mensaje de 39
  - descifrar 15, 43, 44
    - con Eudora 41, 43
    - desde el Explorador de Windows 51
  - firmar
    - desde el Explorador de Windows 49, 50
    - desde el portapapeles 47
    - con Eudora 41, 43
  - privado

- enviar 14, 41
- recibir 14, 41
- verificar 15, 43
  - desde el Explorador de Windows 51
  - con Eudora 44

Crear

- grupos 45
- par de claves 28

Criptografía, repaso 13  
Criptografía de clave pública, repaso 13

## D

Descifrado

- cómo funciona 29
- establecer preferencias 59

Descifrar

- archivos adjuntos 44
- correo electrónico 15
  - de otros 43
  - repaso 13
- desde el Explorador de Windows 51
- desde el portapapeles 22

Destinatarios 25

Dirección de correo electrónico, añadir 59

Disco, requerimientos de sistema 16

Distribuir su clave pública 34

## E

Eliminar

- claves 63
- firmas digitales 63

Envío de correo electrónico privado 41

Establecer

- contraseña de clave 30
- preferencias 66

Explorador de Windows

- cifrar desde 49-51
- descifrar desde 51
- firmar desde 49-51
- verificar desde 51

Exportar

- claves a archivos 64
- claves públicas a archivos 36

Exposición, protección de clave privada contra 95

## F

Firma de claves 60, 91

Firma digital

- borrado 63
- correo electrónico 15, 41
  - comprobación de firma 15
  - desde el explorador de Windows 49-51
  - por medio del portapapeles 47
- descripción 87
- repaso 13
- usando Eudora 41, 43
- verificación 14

Función hash, descripción 87

Frase de contraseña

- ver Contraseña

Fuga en la seguridad 105

## G

Generación

- clave, establecer preferencias 66
- par de claves 28

Grupos de destinatarios 45

Guardar claves 33-34

Gusano como atacante 103

## H

Habilitar claves 62

Huellas

- comparación 40
- comprobación 60
- descripción 92
- propiedad 58

## I

Identificador de clave 58

Identificador de usuario, comprobación 92

Importar

claves desde archivos 64

claves públicas desde archivos 39

Inhabilitación de claves 62

Instalación

de PGP 21

desde la Web 22

desde un CD ROM 21

## L

Línea de asunto para mensaje de correo electrónico 41

## M

MacBinary 108

MacOS 108

Memoria, requerimientos de sistema 16

Memoria virtual 53

MIME, norma

para cifrar correo 41, 43

para descifrar correo 43

## N

Nombre de usuario, añadir 59

Nueva dirección de correo electrónico, añadir 59

Números aleatorios como claves de sesión 86

## O

Obtención de claves públicas de otros 36-39

Obtención de claves públicas de un servidor 37

Otorgar confianza para validación de claves 62

## P

Par de claves

creación 14, 28

creación con el Asistente de Clave

PGP 23

descripción 28

especificar propiedades 59

establecimiento de caducidad 30

examinar 23

generación 28

ver 32

PGP

actualizaciones

de PGP, Inc. 18

de ViaCrypt 18

de una versión previa 18

asistente de claves 23, 28

atajos 25

compatibilidad 16

complementos [plug-ins] 13, 41

formas de usar 22

función de tachado seguro 53

funciones desde el explorador de

Windows 52

historia 16

instalación 21

repaso 22

uso desde el portapapeles 22

uso desde la barra de tareas 22

PGP for Business Security

Clave de Descifrado Adicional 17

Clave Corporativa de Firma 17

PGPkeys

abrir 23

descripción 55

examinar propiedades de clave

caduca 58

cambiar contraseña 59

creada 58

habilitada 58

huella 58

ID de clave 58

modelo de confianza 59

tipo de clave 58

etiqueta de Confianza 57

etiqueta de Creación 57

etiqueta de Tamaño 57

etiqueta de Validez 56



- iconos 26
- usos
- ventana
  - creación de pares de claves 28
  - ventana de búsqueda 72
  - visualización 55
- PGPlog 44
- PGP/MIME
  - compatibilidad 18
  - para cifrar correo 41, 43
  - para descifrar correo 44
- PGPtools 13
  - plataformas soportadas 13
- Plug-ins
  - ver Complementos
- Portapapeles
  - cifrar mediante el 47
  - usar PGP desde el 22
- Preferencias
  - archivos de clave 68
  - caché 66
  - cifrado 66
  - establecer 66
  - generación de claves 67
  - general 66
  - servidor de claves 70
- Presentador
  - de confianza 91, 93
  - descripción 91
  - y firma digital 91, 105
- Private Enhanced Mail, institución 58
- Propiedad Creada 58
- Propiedad Habilitada 58
- Propiedades de grupo 45
- Protección de claves 33-34
- pubring.pkr 54

## R

- Recepción de correo electrónico privado 41
- Requerimientos de sistema 16
- Repasos
  - archivos de clave 13
  - cifrado de correo electrónico 15

- claves privadas 13
- claves públicas 13
- comprobación de firma digital 15
- conceptos clave 13
- criptografía 13
- criptografía de clave pública 13
- descifrado de correo electrónico 13
- firma de correo electrónico 13
- firma digital 13
- verificación de firma digital 13

- Revocación de claves 65

## S

- secring.srk 54
- Seleccionar columnas para mostrar 55
- Seleccionar destinatarios 25
- Servidor de claves
  - diseminación de claves revocadas 65
  - enviar su clave pública a 32, 34-35
  - establecer preferencias 70
  - obtener una clave pública de 37
- Sobreescritura permanente de archivos 53

## T

- Tachado seguro [wipe]
  - función 53
  - memoria virtual 53
- Tamaño de clave
  - establecer 29
  - ventajas e inconvenientes 29
- Tipo de clave 58
- Transferencia de archivos
  - al MacOS 108
  - aplicaciones soportadas 111
  - entre sistemas operativos 108
  - extensiones de nombre de archivos 112
  - mediante FTP 108
  - sistemas operativos 108

## U

- Uso de PGP
  - desde el portapapeles 22

desde la barra de tareas 22

## V

Validación de claves

confianza para 62

claves públicas 14

Validez de clave, comprobación 39

Ventana PGPkeys, apertura 23

Ver

atributos de archivos de clave 55-59

atributos de clave 23

pares de claves 23

Verificar

autenticidad de una clave 39

correo electrónico 15

de otros 43

desde el explorador de

Windows 51

Versiones de PGP

actualización 18

compatibles 16

ViaCrypt, actualización de 18

Virus como atacantes 103

## W

Windows

extensiones de nombre de archivo  
109

requerimientos de sistema 16

Wipe

ver Tachado Seguro