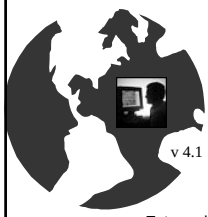
Capítulo 18
Aplicaciones de Correo Seguro

Seguridad Informática y Criptografía



Material Docente de
Libre Distribución

Ultima actualización del archivo: 01/03/06
Este archivo tiene: 97 diapositivas

Dr. Jorge Ramió Aguirre
Universidad Politécnica de Madrid

El correo electrónico seguro

En sistemas abiertos como en el caso de Internet, el correo seguro se logra a través de la plataforma S/MIME acrónimo de Secure Multipurpose Internet Mail Extensions.

A comienzos de los años 90 hacen su aparición dos sistemas o aplicaciones de correo electrónico seguro:

- ✉ PEM: Private Enhanced Mail
- ✉ PGP: Pretty Good Privacy

De los dos, ha sido PGP quien se ha convertido en un estándar de hecho en clientes de e-mail seguro en entornos cerrados.

Por lo tanto veremos sólo algunos aspectos genéricos de PEM y analizaremos más en profundidad PGP.

Private Enhanced Mail PEM

- Es una propuesta de la IETF Internet Engineering Task Force en 1985. El documento técnico se publica en 1993.
- Las especificaciones técnicas están en las RFCs Request For Comments números 1421, 1422, 1423 y 1424.
- Se usa conjuntamente con el protocolo SMTP Simple Mail Internet Protocol.
- Cifrado de la información: DES modo CBC.
- Generación y gestión de claves: RSA de 508 a 1024 bits. Estructura de certificados según la norma X.509.
- Clave de sesión: DES modo ECB, TripleDES-EDE.
- Firma digital: RSA, MD2, MD5.

http://www.ietf.org/rfc/rfc1421.txt

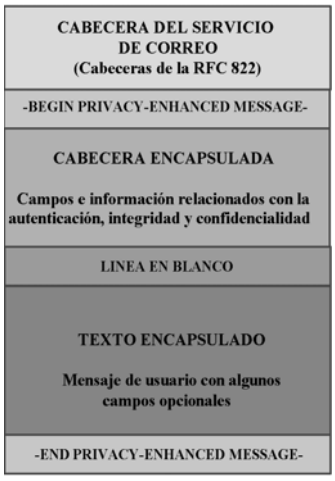
Implementación de PEM

- Es compatible con otros modelos de mensajería como, por ejemplo, X.400.
- PEM se implementa en el nivel de aplicación:
  - es independiente de los protocolos de los niveles OSI o TCP/IP inferiores.
  - es independiente de los sistemas operativos o del ordenador.
- Se puede implementar como un módulo independiente que trabaje con el cliente de correo habitual para el usuario.

Servicios de seguridad en PEM

- Servicios de seguridad contemplados:
  - Autenticación del origen.
  - Confidencialidad.
  - Integridad del mensaje.
  - No repudio del origen cuando se utiliza gestión de clave con algoritmo de clave asimétrica.
- Servicios de seguridad no contemplados:
  - Control de acceso.
  - Confidencialidad del tráfico de mensajes.
  - No repudio del mensaje por parte del receptor.

Formato e implementación de PEM



TIS/PEM
Plataformas UNIX. Trusted Information System. Código fuente disponible para los ciudadanos o empresas de Estados Unidos y Canadá. Usa una jerarquía de certificación múltiple.

RIPEM
Implementa parte de los protocolos PEM sin certificados para autenticación de claves. Gratuito para aplicaciones no comerciales. Exportación prohibida fuera de Estados Unidos. Existen versiones utilizadas en todo el mundo.

Pretty Good Privacy PGP

- Philip Zimmermann publica la versión 1.0 de PGP en 1991 con mínimos requisitos de hardware y software.
- En 1992 aparece la versión 2.0 en la que ya participan programadores de todo el mundo. Su código se escribe fuera de USA para evitar las leyes restrictivas respecto al software criptográfico y sus problemas legales.
- En 1993 aparece la versión 2.3a muy popular en sitios FTP y válida para varias plataformas de sistemas operativos.
- En 1994 participa en el proyecto el Massachusetts Institute of Technology MIT y aparecen las versiones 2.4, 2.5 y 2.6.
- La versión 2.6.3i se populariza a nivel mundial.

http://www.philzimmermann.com/ES/background/index.html

Nota aclaratoria sobre versiones de PGP

Aunque hay más de una oferta de software para correo seguro que el programa PGP, éste se ha convertido en un estándar de hecho. Si bien las últimas versiones del programa orientadas a entornos Windows presentan altas prestaciones, las operaciones básicas siguen siendo las mismas que en la conocida versión 2.6.3i.

Las nuevas versiones de PGP en entorno Windows cambian muy rápidamente por lo que resulta muy difícil tener unos apuntes permanentemente actualizados. Por ello, se usará la versión 2.6.3i como versión simple para la explicación de las operaciones de cifra y firma con PGP y, posteriormente, haremos un repaso de las características de la versiones 6.5.1 y 8.0, una de las últimas.

La filosofía de las nuevas versiones es exactamente la misma...

Tutorial de PGP 2.6.3i

Si no conoce PGP o no ha trabajado nunca con este entorno, le recomiendo que descargue desde la página Web de la Red Temática CriptoRed el archivo del Tutorial de PGP 2.6.3i en formato html que se indica.

http://www.criptored.upm.es/software/sw_m001g.htm

Esta aplicación le servirá para aprender rápidamente los comandos y prestaciones de esta versión de PGP, muy similar a las actuales. PGP 2.6.3i ocupa menos que un disquete de 1,4 MB, aunque todas sus operaciones son en modo comando.

http://www.criptored.upm.es/software.htm#freeware

Características de PGP 2.6.3i

- PGP, en su versión 2.6.3i (internacional) se convirtió a mediados de la década de los 90 en un estándar de hecho. De hecho, muchos usuarios “siguen fieles” a esta versión.
- Cifra todo tipo de datos en entornos MS-DOS y UNIX. Su orientación principal es el cifrado de los datos y la firma digital en correo electrónico.
- Los algoritmos básicos que usa son:
  - IDEA para cifrar con sistema de clave secreta.
  - RSA para intercambio de claves y firma digital.
  - MD5 para obtener la función hash de la firma digital y para recuperar clave privada asimétricas y cifrado local.

Algoritmos usados en PGP 2.6.3i

- Operación -	- Algoritmo -	- Descripción de su función -
Compresión	**ZIP**	• Se comprime el mensaje en claro y la firma para almacenarlo o transmitirlo.
Generación de claves	**RSA, MD5**	• Genera una clave pública y otra privada, encontrando dos números primos muy grandes. El valor privado se guarda cifrado con IDEA usando como clave un resumen MD5 de la frase de paso secreta.
Cifrado Convencional	**IDEA**	• Cifra el mensaje con una clave de sesión de 128 bits (única) generada en el emisor de forma aleatoria.
Intercambio de claves	**IDEA, RSA**	• Cifra la clave de sesión IDEA con la clave pública del destinatario con RSA y la añade en el criptograma.
Firma Digital	**MD5, RSA**	• La función hash MD5 genera un resumen de 128 bits, que representa al mensaje en claro completo, y que se cifra en RSA con la clave privada del emisor. Se añade al mensaje enviado.
Compatibilidad e-mail	**Base-64**	• Permite transmitir el mensaje a todo tipo de aplicaciones e-mail. Convierte los octetos en caracteres imprimibles.
Segmentación		• Divide el criptograma final en bloques de menos de 50.000 bytes para su correcta transmisión en Internet y su recuperación.

Características del cifrado local

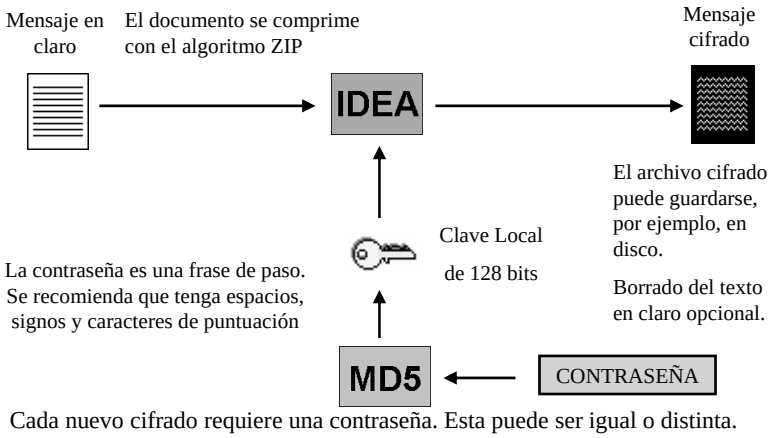
- Esta operación sirve para mantener los archivos protegidos, por ejemplo en el disco duro.
- El acceso al texto en claro sólo será posible si se conoce una clave o contraseña que es la frase de paso usada al cifrar.
- Recuerde que si después de cifrar el archivo borra físicamente el texto en claro -operación que realiza una grabación de unos y ceros aleatorios en la zona de almacenamiento del disco- le será imposible recuperarlo si olvida la contraseña.

Pasos del cifrado local con IDEA

Pasos:

1. PGP solicita una frase de paso: ésta debe ser lo suficientemente larga como para evitar ataques por combinaciones.
2. Se aplica el algoritmo de resumen MD5 a esa contraseña, generando así una clave de 128 bits.
3. Con esa clave, PGP cifra el documento con el algoritmo IDEA y le pone como extensión .pgp.
4. Como una opción, permite luego hacer un borrado físico del archivo en claro.

Esquema de cifrado local con IDEA



Cada nuevo cifrado requiere una contraseña. Esta puede ser igual o distinta. Recuerde que a igual contraseña (frase de paso), tendremos igual hash.

Operaciones con claves asimétricas

- Las operaciones de PGP para cifrar, descifrar, firmar y la comprobación posterior de la firma digital, usan los algoritmos de funciones hash, de clave pública y de clave secreta ya vistos en capítulos anteriores de este curso.
- Para poder enviar y recibir correo seguro, es necesario contar al menos con las siguientes claves:

  Clave pública del destinatario.

  Par de claves asimétricas del emisor.

  Generación de claves con RSA

Generación de claves asimétricas tipo RSA

- Una vez instalado PGP, se procede a la generación de claves asimétricas del usuario propietario.
- Se elige el tamaño del módulo n, por ejemplo 1.024 bits.
- PGP generará un par de números primos e (clave pública) y d (clave privada) de forma que $e*d \bmod \phi(n) = 1$.
- Para una mayor facilidad en el descifrado en destino, el valor de la clave pública e será pequeño. Un valor típico es el número primo $65.537 = 2^{16}+1$, en hexadecimal 10001.
- PGP pedirá una contraseña o *passphrase* y con ella y MD5 generará una clave de 128 bits con la que cifrará la clave privada antes de almacenarla en el disco.

Anillos de claves asimétricas

- Con las claves pública y privada generadas y otras claves públicas que el usuario podrá importar de otros usuarios, se crean dos anillos de claves:
  - Anillo de claves públicas: archivo pubring.pgp en el que se guardan las claves públicas del usuario propietario (puede tener más de una identidad) y las claves públicas importadas.
  - Anillo de claves privadas: archivo secring.pgp en el que se guarda la o las claves privadas del usuario propietario (más de una identidad).
  - Nota: estos anillos cambiarán su extensión en las nuevas versiones por pkr.

Estructura del anillo de claves privadas

Sellado de tiempo	Clave ID*	Clave pública	Clave privada cifrada	ID usuario
T_1	$e_1 \bmod 2^{64}$	Clave púb. 1	Clave priv. 1	Usuario 1
---	---	---	---	---
T_i	$e_i \bmod 2^{64}$	e_i	$E_{H(FPi)}(d_i)$	Usuario i
---	---	---	---	---
T_n	$e_n \bmod 2^{64}$	Clave púb. n	Clave priv. n	Usuario n

Descripción de los campos

(*) Se usa este campo para la indexación de la tabla en ambos anillos

Campos de los anillos de claves

Sellado de tiempo:

Fecha y hora de la generación del par de claves.

Clave ID:

Identificador de clave (últimos 64 bits de la clave pública e).

Clave pública:

Número primo e, inverso del primo d en el cuerpo $\phi(n)$.

Clave privada cifrada:

Cifra $E_{H(FPi)}$ de la clave privada d con IDEA y la función hash de la frase de paso del propietario como clave secreta.

ID usuario:

Identificación del usuario, normalmente dirección de email.

Estructura del anillo de claves públicas (1)

Sellado de tiempo	Clave ID*	Clave pública	Confianza propietario	ID usuario	
T_1	$e_1 \bmod 2^{64}$	Clave púb. 1	flag_confianza 1	Usuario 1	…
---	---	---	---	---	…
T_i	$e_i \bmod 2^{64}$	e_i	flag_confianza i	Usuario i	…
---	---	---	---	---	…
T_n	$e_n \bmod 2^{64}$	Clave púb. n	Clave priv. n	Usuario n	…

continúa en próxima diapositiva

(*) Se usa este campo para la indexación de la tabla en ambos anillos

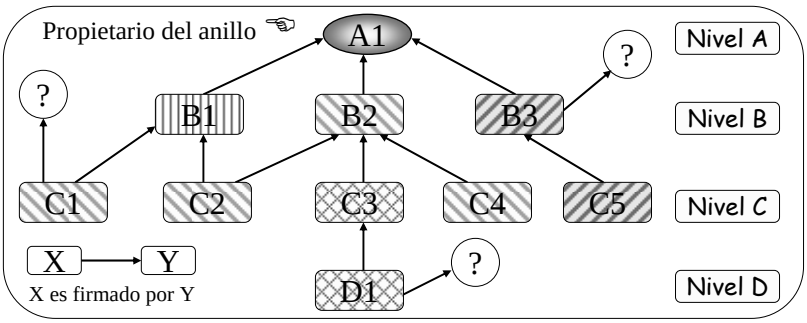
Estructura del anillo de claves públicas (2)

	Legitimación de clave	Firma(s)	Confianza de Firmas
...	flag_confianza 1	...	...
...	---	---	---
...	flag_confianza i	...	...
...	---	---	---
...	flag_confianza n	...	...

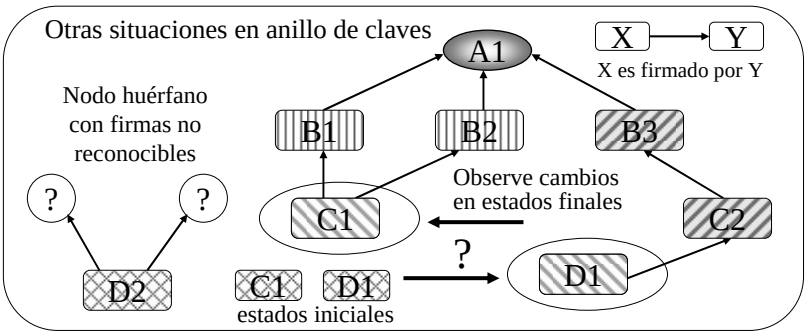
viene de la diapositiva anterior

Con la clave pública del destinatario ya podremos enviar correo cifrado y/o firmado. Pero ... ¿cómo se gestionan las claves en PGP?

Gestión del anillo de claves públicas



Otros escenarios de confianza en PGP



A1 cree en el propietario de la clave para firmar otra clave

A1 cree parcialmente en el propietario de la clave para firmar otra clave

PGP hace que A1 crea en la legitimidad de las claves pues tienen al menos dos firmas parciales (B1-B2)o una completa (C2) pero no da confianza para firmar

A1 no cree que la clave sea legítima

Problema en estos escenarios de confianza

La gestión de claves en PGP se basa en la confianza mutua y es adecuada solamente para entornos privados o intranet.

¿Los amigos de tus amigos serán mis amigos?

- ✓ En un sistema abierto como es Internet y aplicaciones como el comercio electrónico, esta situación y otras más que pueden darse en este sistema de gestión de claves por confianza mutua, resulta inaceptable.
- ✓ La solución, que PGP ya contempla en sus últimas versiones, es la aceptación de las Autoridades de Certificación como certificadores de claves públicas.

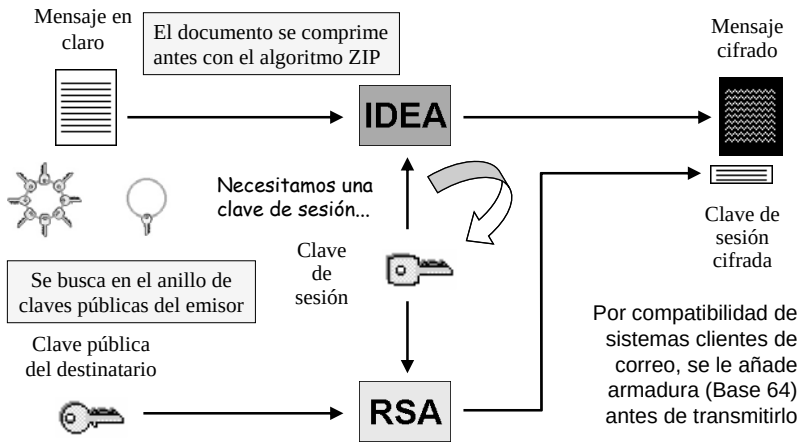
Pasos cifrado con clave pública de destino

Pasos:

1. PGP genera un número aleatorio de 128 bits que será la clave de sesión.
2. Se cifra el mensaje con dicha clave usando IDEA.
3. Se cifra la clave de sesión con la clave pública RSA del destinatario y se añade al criptograma.
4. Se añade el identificador ID de la clave pública del destinatario a la clave de sesión cifrada en el paso 3 como indicativo de la identidad del receptor.

Recuerde que el correo electrónico no es en general una comunicación en tiempo real por lo que, aunque se envía una clave para descifrar el criptograma en recepción, no se trata de una clave de sesión en los mismos términos que se usa, por ejemplo, en una comunicación SSL.

Cifrado con clave pública de destino

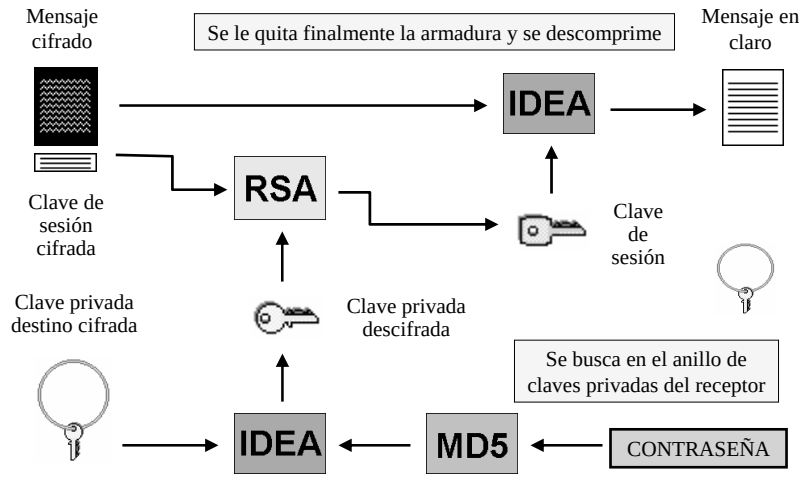


Pasos descifrado con clave privada destino

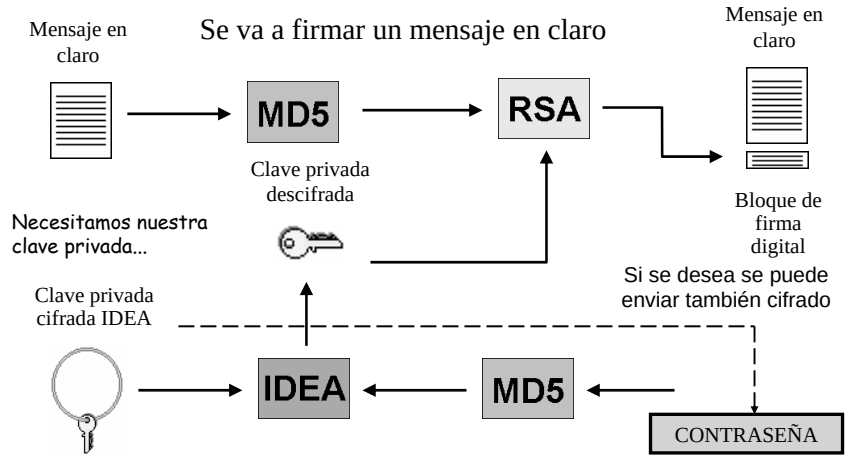
Pasos:

1. PGP busca en la cabecera del criptograma el identificador de usuario ID (receptor) que se ha añadido en la clave de sesión cifrada.
2. Se busca la clave privada del identificador ID en el anillo de claves privadas del receptor.
3. Se accede a la clave privada en claro, descifrándola con IDEA al introducir el propietario ID su frase de paso y el hash MD5 entregue la clave de descifrado.
4. Con la clave privada se descifra la clave de sesión.
5. Con la clave de sesión se descifra el criptograma.

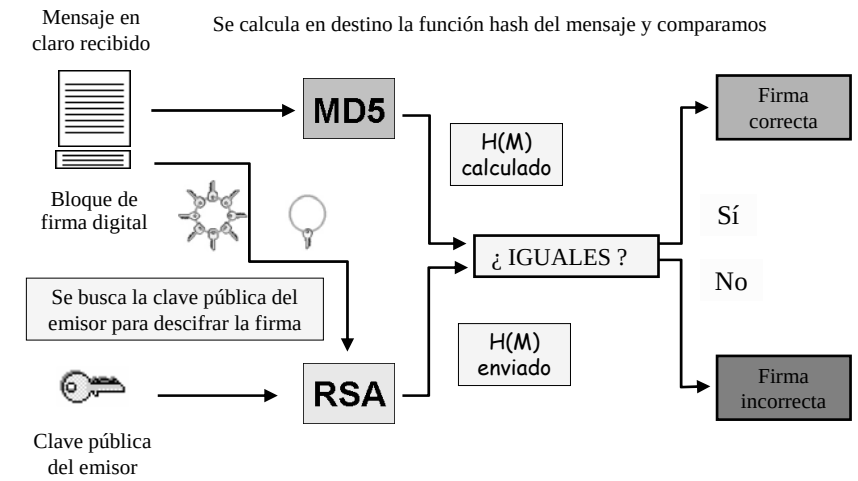
Descifrado con la clave privada de destino



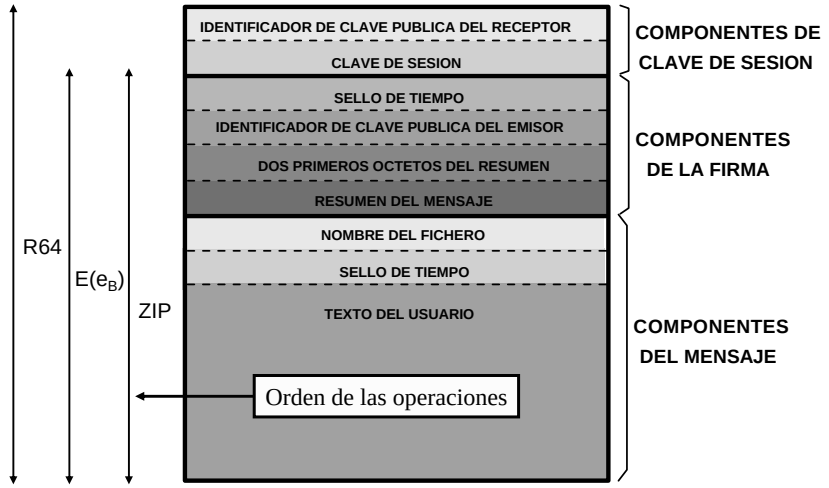
Firma digital RSA



Comprobación de la firma digital RSA



Formato de un mensaje PGP dirigido a B



Los tiempos cambian, pero ...

La mítica versión de PGP 2.6.3 del MIT se convierte rápidamente en el software de libre distribución freeware más popular en el mundo de los PCs y especialmente en entornos de correo electrónico: usa cifra y firma con criptografía calificada como fuerte.

Las versiones en entorno Windows a través de Network Associates presentan opciones avanzadas, servicios de red para seguimiento de paquetes y autenticación mediante Autoridades de Certificación.

Existe una versión freeware para usos no comerciales ☺.

Las versiones 5 y 6 tuvieron su código fuente abierto, en la 7 el código deja de ser público ☹ y a partir de la versión 8.0 (diciembre 2002) con PGP Corporation se ha liberado otra vez el código.

¿Ha vuelto otra vez la cordura? Aquí puede haber varias opiniones....

Algoritmos en nuevas versiones de PGP

- Generación de claves
  - RSA: 1.024 - 4.096 bits
  - Diffie y Hellman: 1.024 - 4.096 bits
- Firma digital
  - DSS Digital Signature Standard: 1.024 bits
- Cifrado
  - AES, CAST, IDEA, TripleDES, Twofish
- Resumen
  - SHA-1 (160 bits) y MD5 (128 bits)

Algunas versiones de PGP en Windows

Desde la versión 5.0 hasta las actuales (versiones 8.0 y siguientes) los esquemas de cifrado local, cifra asimétrica y firma digital han cambiado muy poco aunque presentan mayores prestaciones. No obstante, recuerde que algunas prestaciones sólo estarán activadas en versiones comerciales.

PGP 6.5.1

PGP 7.0.3

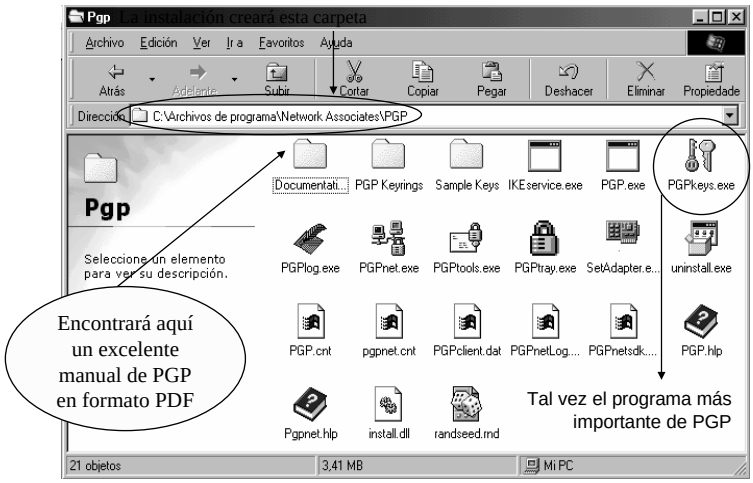
PGP 8.0

Veremos algunas operaciones de estas tres versiones con mayor detalle. Recuerde, eso sí, que la versión 7.0.3 no tiene su código fuente abierto.

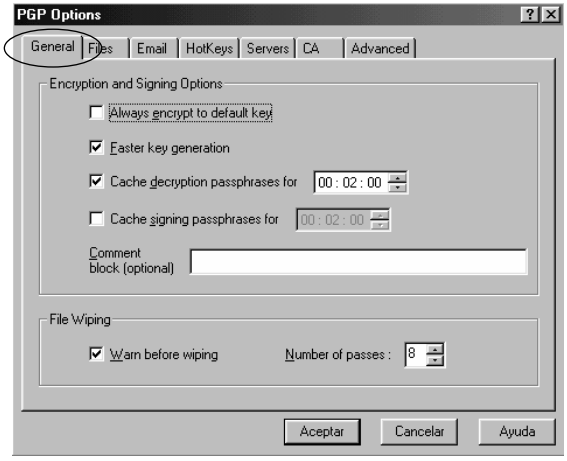
Instalación de la versión PGP 6.5.1

PGP 6.5.1 internacional aparece en el año 1999. Puede considerarse como una de las versiones seguras mejor optimizadas desde la primera en entorno Windows.

Carpetas y programas de PGP 6.5.1

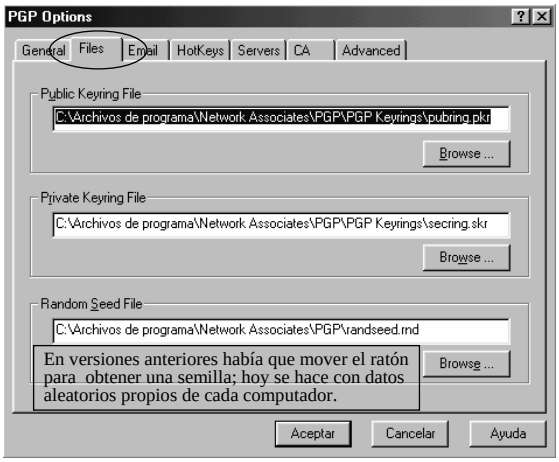


Opciones generales de PGP 6.5.1



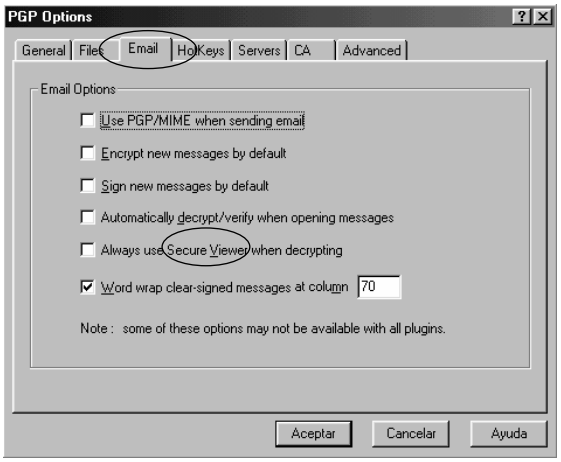
- ✓ La generación rápida de claves sólo puede hacerse para valores DH de una longitud predeterminada.
- ✓ Se puede limitar el tiempo de descifrado de la frase de paso en memoria caché.
- ✓ El borrado físico de datos y ficheros se hace escribiendo 1s y 0s aleatorios en los cluster, desde 8 hasta 32 veces.

Opciones de ficheros de PGP 6.5.1



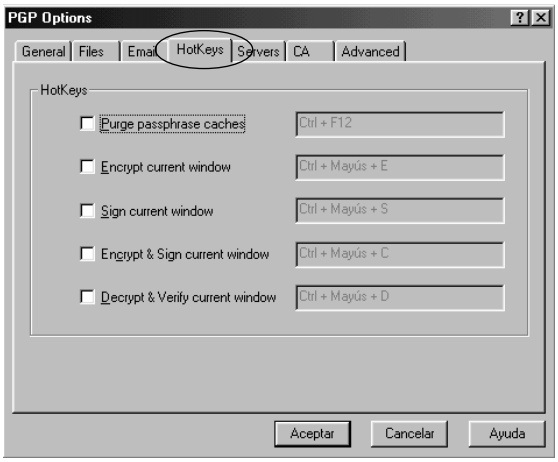
- ✓ Los archivos donde guarda las claves públicas y claves privadas siguen llamándose pubring y secring pero ahora, a diferencia de versiones anteriores, usa como extensiones pkr.
- ✓ El archivo de semilla permite generar números aleatorios para crear claves.

Opciones de e-mail de PGP 6.5.1



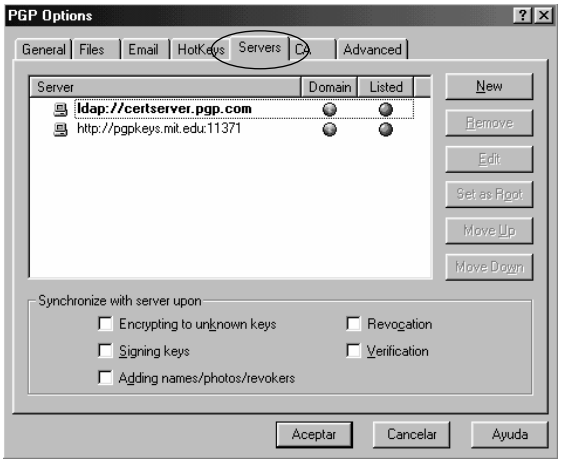
- ✓ El PGP/MIME sólo funciona con plugins.
- ✓ Se puede pedir que cifre, firme o descifre y compruebe firma por defecto al enviar o abrir mensajes.
- ✓ Si usa Secure Viewer, al descifrar un archivo éste sólo se muestra en la pantalla usando para ello una técnica de enmascarado que evita los ataques por captura de radiofrecuencias del teclado, TEMPEST.

Opciones de atajos de PGP 6.5.1



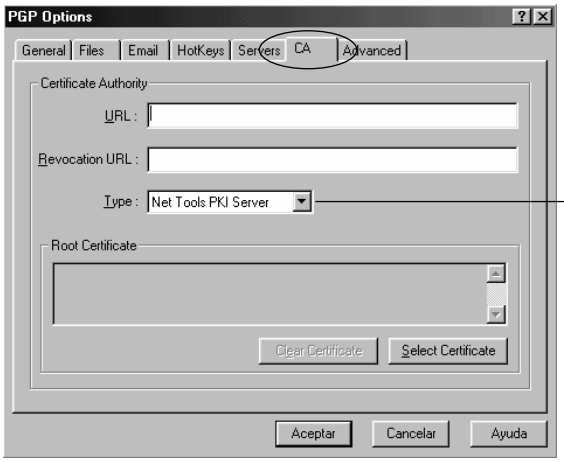
- ✓ La opción de usar teclas para atajos es poco interesante pero puede activarse si se desea.
- ✓ Tal vez se podría haber ahorrado esta ventana.

Opciones de servidores de PGP 6.5.1



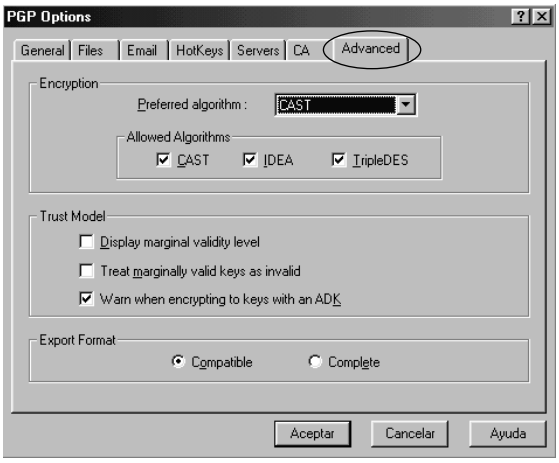
- ✓ A estos servidores se puede enviar nuestra clave pública para que los usuarios accedan más fácilmente a ella.
- ✓ Es interesante estar sincronizado con el servidor por el tema de las claves revocadas.

Opciones de ACs de PGP 6.5.1



También VeriSign OnSite y Entrust

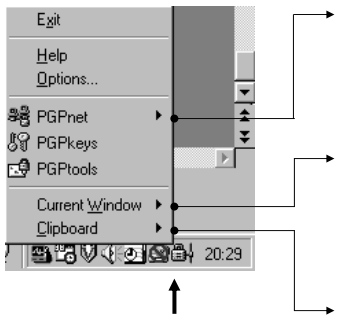
Opciones avanzadas de PGP 6.5.1



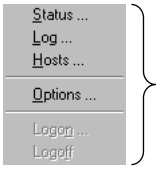
- ✓ IDEA era en versiones anteriores el algoritmo de cifra por defecto.
- ✓ El aviso sobre uso de Additional Decryption Key (ADK) significa que el administrador del sistema puede usar una clave extra que le permite descifrar lo cifrado, en caso de necesidad o por un requerimiento judicial.
- ✓ El formato compatible es el código base 64.

El programa PGPtray de acceso directo

☹ Lamentablemente PGPnet no se incluye en nuevas versiones freeware



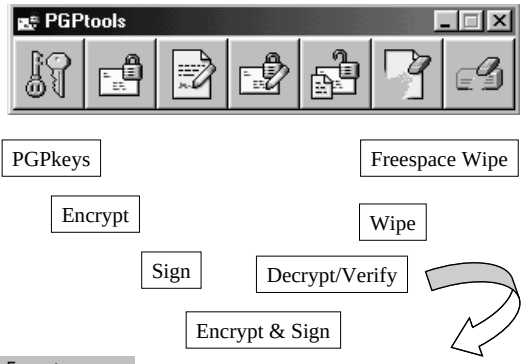
Barra de tareas del PC



Si PGPnet está instalado, en la barra de tareas, al lado del candado de PGPtray, nos aparecerá un icono vertical como se ve en la figura.

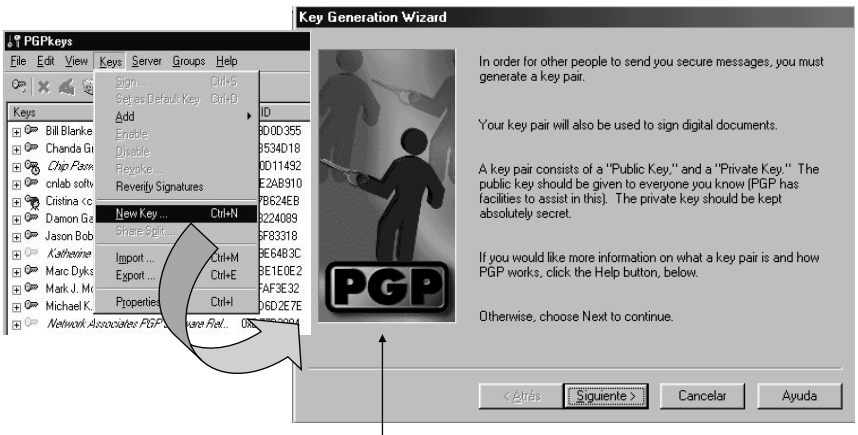
- ✓ La ventana actual cifra texto y no documentos con formato.
- ✓ El uso de portapapeles es la solución si no tenemos el plugin para correo electrónico.

Barra flotante de PGPtools



No es muy cómodo y resulta mejor usar el menú contextual con el botón derecho del ratón. En este caso sobre el archivo Kerberos_borrador.doc

Generación de claves con PGPkeys 6.5.1



Esta es la primera pantalla que aparece una vez instalado PGP.

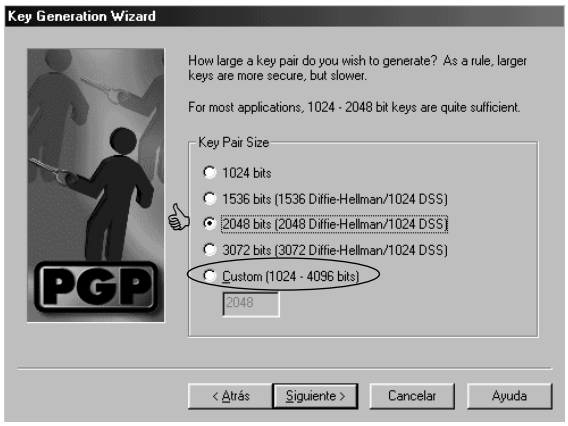
Nombre del usuario y su correo

- ✓ No es necesario que la dirección de correo sea la real.
- ✓ No obstante, sirve para los que se quieran comunicar con nosotros sepan que esa clave es real y pertenece a esa dirección de email.

Elección del tipo de clave asimétrica

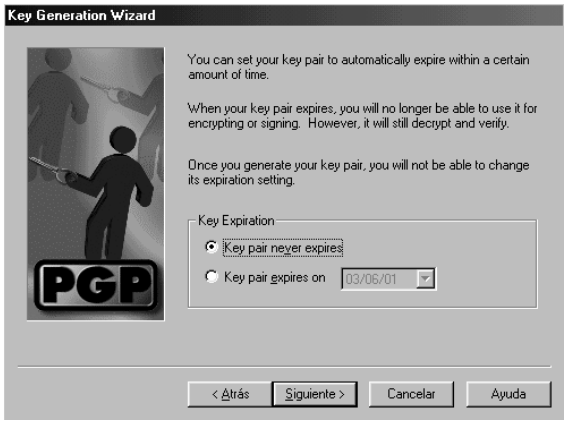
- ✓ El estándar para la generación de las claves asimétricas es en la actualidad Diffie y Hellman junto con la Digital Signature Standard, y se representará como DH/DSS.
- ✓ También puede usar claves RSA que son compatibles con las versiones anteriores de PGP.

Elección de la longitud de la clave



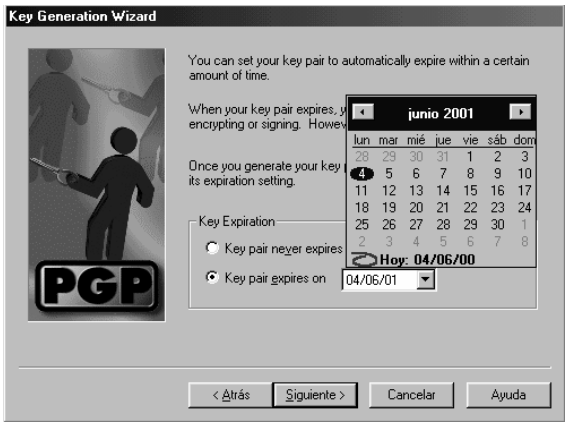
- ✓ Si genera claves de longitud distinta a los valores que se proponen, puede tardar bastante tiempo generarlas. Algo similar sucede si no usa la opción generación rápida de claves.
- ✓ Es recomendable que use una clave de 2.048 bits. Esta se generará sólo en esta fase.

Clave sin caducidad



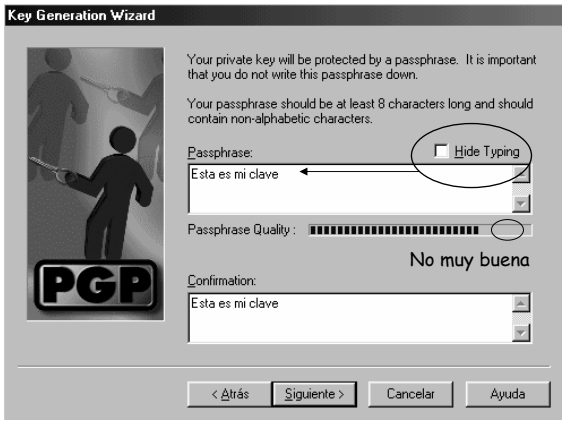
- ✓ Puede optar porque su clave no caduque nunca eligiendo esa opción que aparece por defecto, o bien...

Clave con caducidad



- ✓ Puede optar que la clave caduque de acuerdo con un calendario que nos muestra PGP.
- ✓ En el ejemplo la clave tiene validez desde el 4 de junio de 2000 al 4 de junio de 2001.

Frase de paso para cifrar la clave privada



- ✓ La frase de paso debe tener varias palabras para que sea difícil un ataque por diccionario.
- ✓ Si quita la opción Hide Typing, podrá ver lo que escribe.
- ✓ Por seguridad, no está permitido usar el portapapeles para copiar la frase de arriba en la ventana de confirmación.

Generación de los números primos

- ✓ PGP genera dos primos tanto para las claves RSA (los valores p y q) como para DH/DSS, en este caso el primo p para el intercambio de clave y el primo q para la firma DSS.
- ✓ Normalmente tarda pocos segundos si se eligen los valores estándar que nos propone PGP.

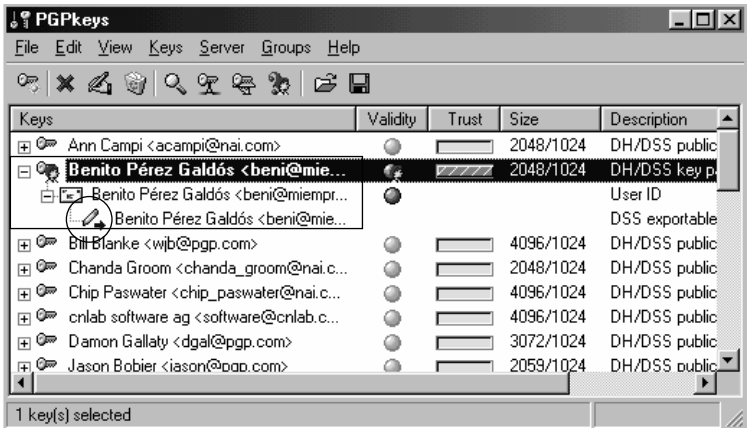
Envío de la clave al servidor de claves

- ✓ Si se desea y la clave es una clave real y de trabajo, ésta se puede enviar a un servidor.

Generación de clave concluida

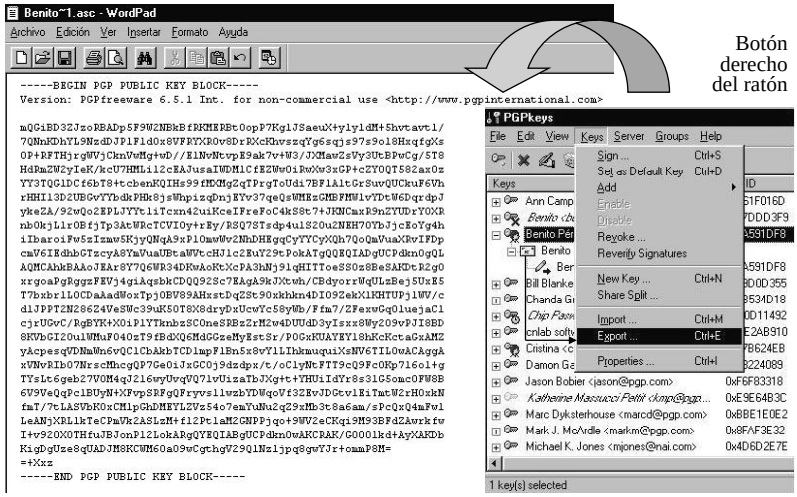
- ✓ Se ha concluido satisfactoriamente la generación del par de claves pública y privada que se guardarán en los anillos pubring.pkr y secring.pkr.
- ✓ La clave privada se guarda cifrada con una clave de sesión que se genera al aplicar una función hash a la frase de paso del propietario.

Visualización de la clave de Benito

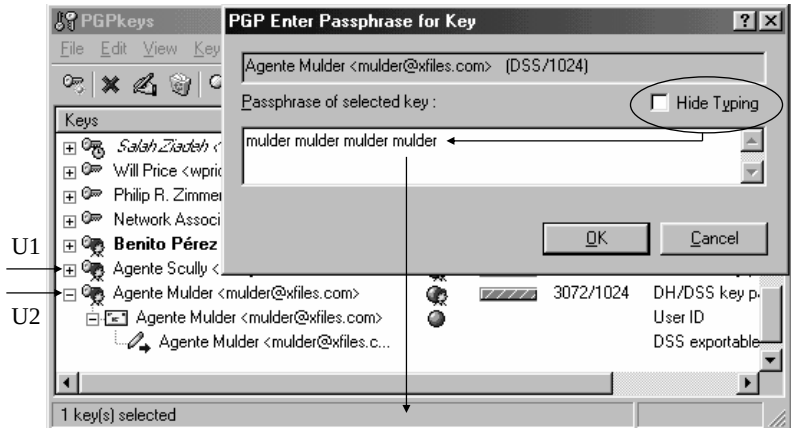


Por defecto, el propietario se firma la clave pública con su clave privada.

Exportación de la clave pública de Benito



Claves de dos usuarios para un ejemplo

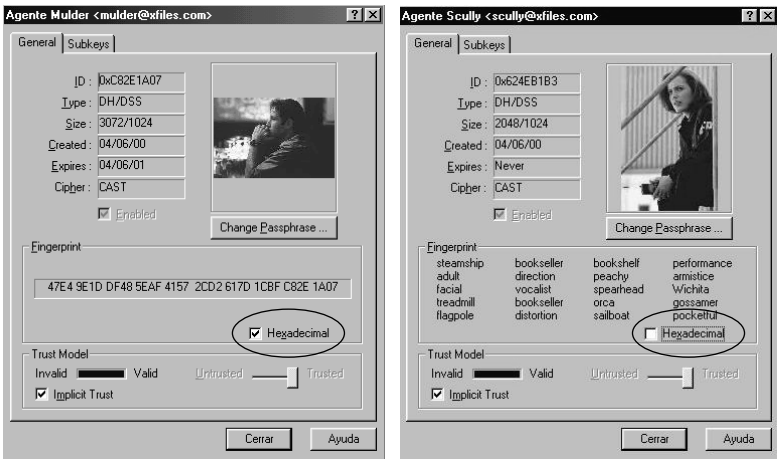


Frase de paso (muy mala) para descifrar la clave privada de este usuario

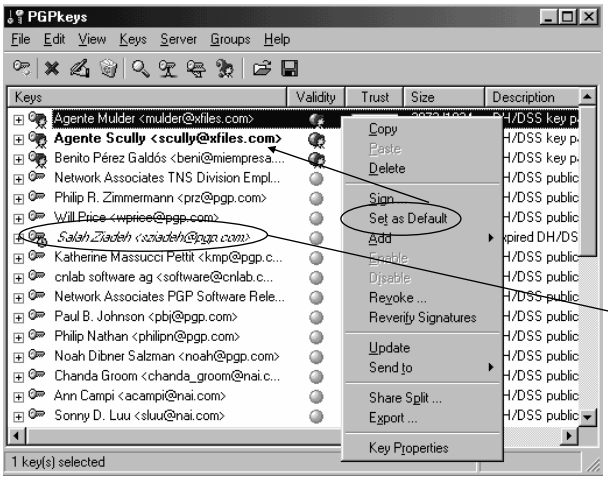
Inclusión de fotografía en clave pública

En negrita aparece el usuario por defecto (Benito).
No es necesario que lo sea para esta operación.

Las claves públicas los amigos de Xfiles



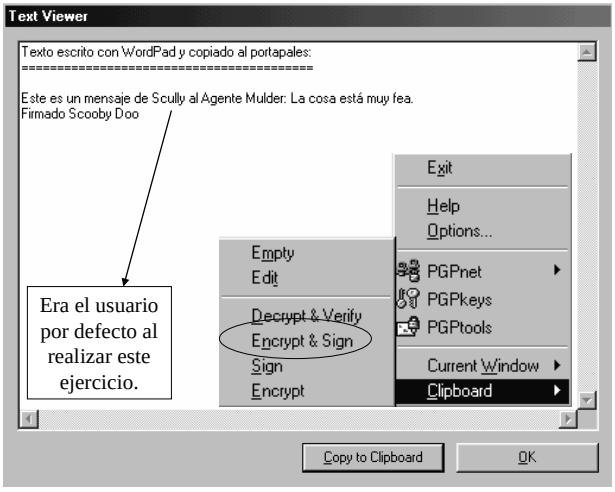
Usuario por defecto y clave revocada



El usuario en negrita es aquel que se ha definido por defecto. Todas las cifras, firmas y descifrados serán suyos si no se cambia el status.

En cursiva: usuario cuya clave ha sido revocada o bien ha caducado su validez.

Ejemplo de cifra y firma con portapapeles

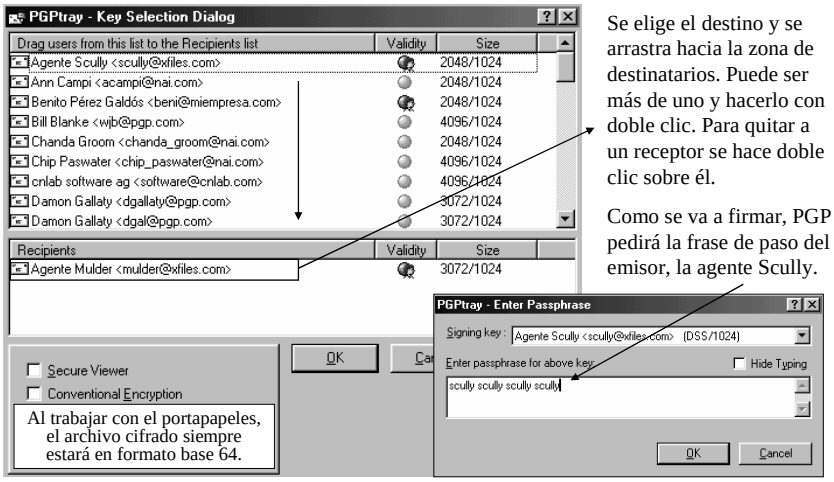


El texto se escribe con WordPad o con el Bloc de Notas y luego se copia al portapapeles.

Si lo desea también puede crear el texto con la opción Edit y copiarlo luego al portapapeles.

Las operaciones (sólo sobre textos) se realizarán en el portapapeles por lo que en este entorno no creará archivos.

Destinatario y frase de paso para la firma



Al trabajar con el portapapeles, el archivo cifrado siempre estará en formato base 64.

Se elige el destino y se arrastra hacia la zona de destinatarios. Puede ser más de uno y hacerlo con doble clic. Para quitar a un receptor se hace doble clic sobre él.

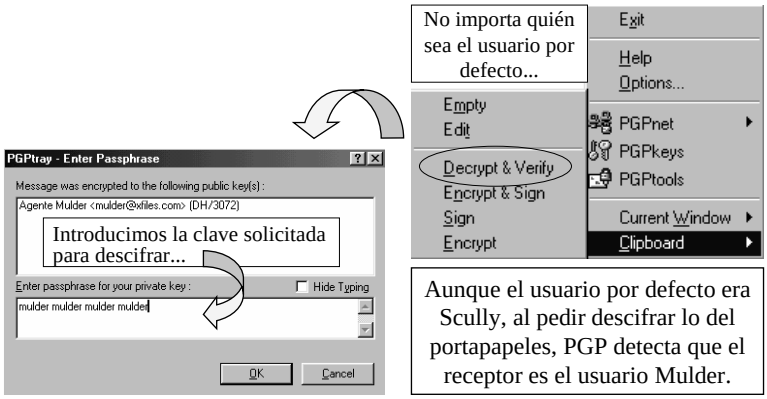
Como se va a firmar, PGP pedirá la frase de paso del emisor, la agente Scully.

Documento portapapeles formato base 64

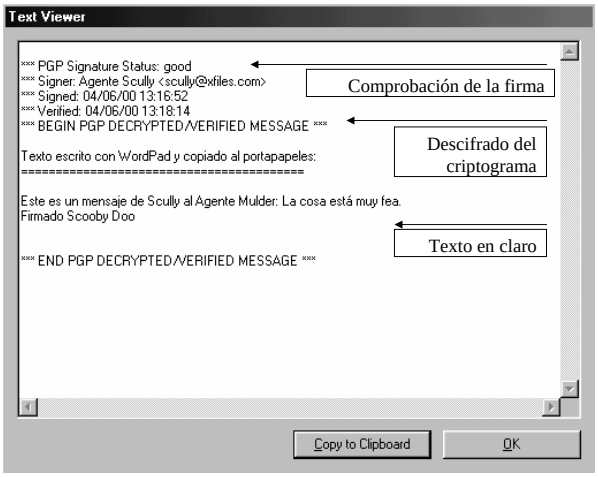
Todo el texto que hay en el portapapeles, incluido BEGIN PGP y END PGP, puede ahora copiarse en el cuerpo del cliente de correo electrónico.

Si desea enviar por el cliente de correo un archivo adjunto cifrado y/o firmado, deberá crear primero ese documento con cualquier programa como Word, Excel, etc. y aplicar sobre el archivo el menú contextual del botón derecho del ratón.

Descifrado del criptograma por destinatario



Mensaje en claro y firma comprobada



Otras operaciones con PGP

PGP permite hacer otras operaciones interesantes:

- Dividir (split) una clave privada en varias subclaves, de forma que para deshacer una operación de cifra o firmar un documento se requiere un umbral de estas subclaves dadas por diseño. Está basado en el esquema de Blakely-Shamir.
- Firmar las claves públicas de otros usuarios con distintos niveles de confianza.
- Revocar una clave, habilitar o deshabilitar una clave.
- Enviar, buscar y actualizar claves desde servidores.
- Cifrar con la opción sólo para tus ojos, crear grupos, etc.

Le recomiendo que éstas y otras operaciones las realice a modo de ejercicio, instalando PGP en su computador.

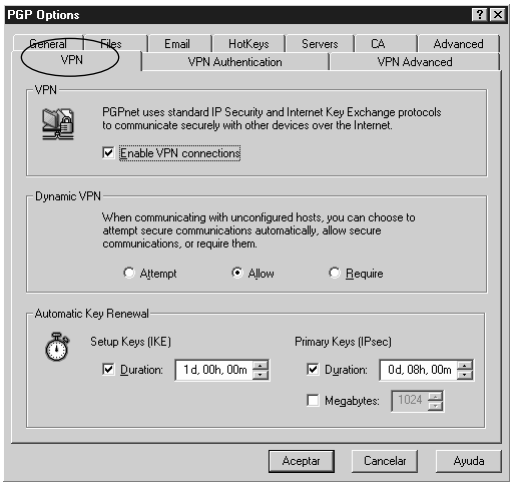
PGP versión 7.0.3

Es básicamente el mismo programa de la versión 6.5.1 pero con ligeras diferencias:

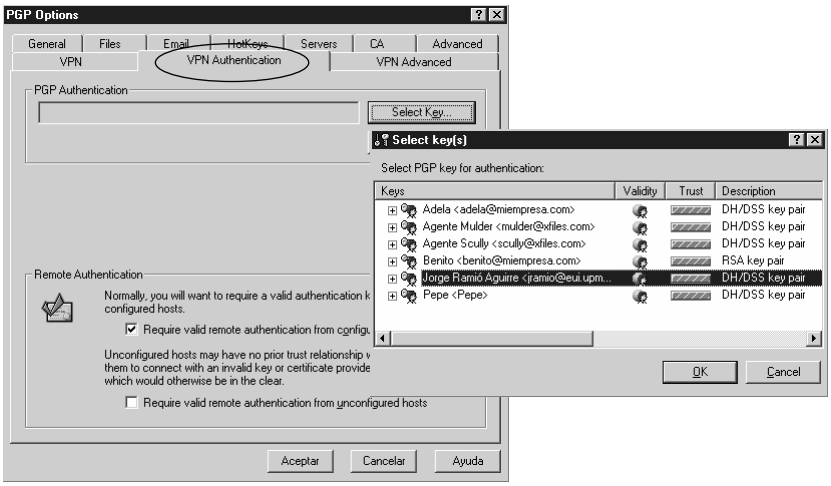
- Los mayores cambios se observan en menú PGP Options. Incluye opción de descifrado automático muy interesante.
- Incluye dos nuevos algoritmos: AES y Twofish
- La creación de claves es de forma automática DH/DSS con 1.024 bits. Si queremos crear claves RSA, debemos entrar obligatoriamente en la opción experto.
- Añade opciones de configuración de VPNs.

El peor inconveniente es que su código no es público por lo que nadie puede asegurar que el programa haga exactamente lo que dice que hace, por ejemplo la fortaleza de la cifra, protección ante ataques tempest, etc.

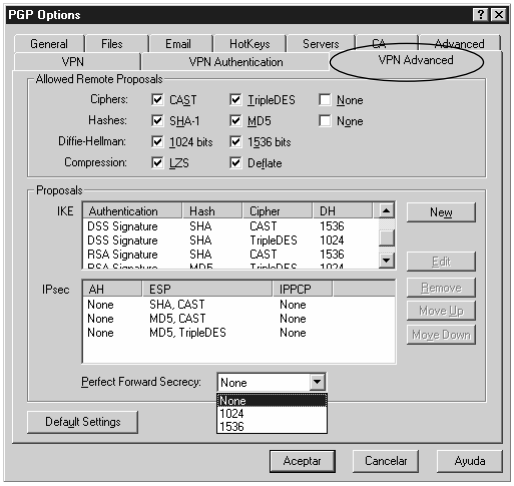
Opciones de VPN en PGP 7.0.3



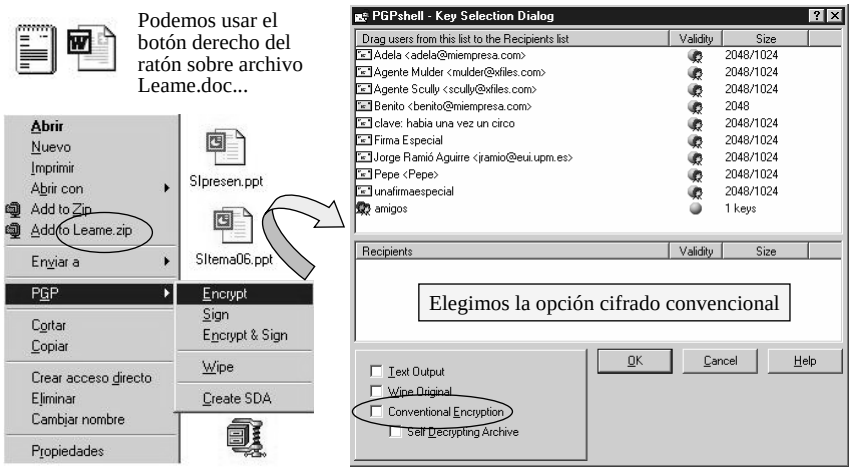
Autenticación VPN en PGP 7.0.3



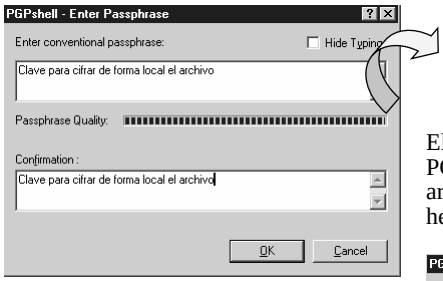
Opciones VPN avanzadas en PGP 7.0.3

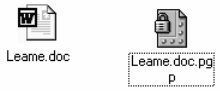


Cifrado local de ficheros con PGP 7.0.3



Descifrado de ficheros con PGP 7.0.3



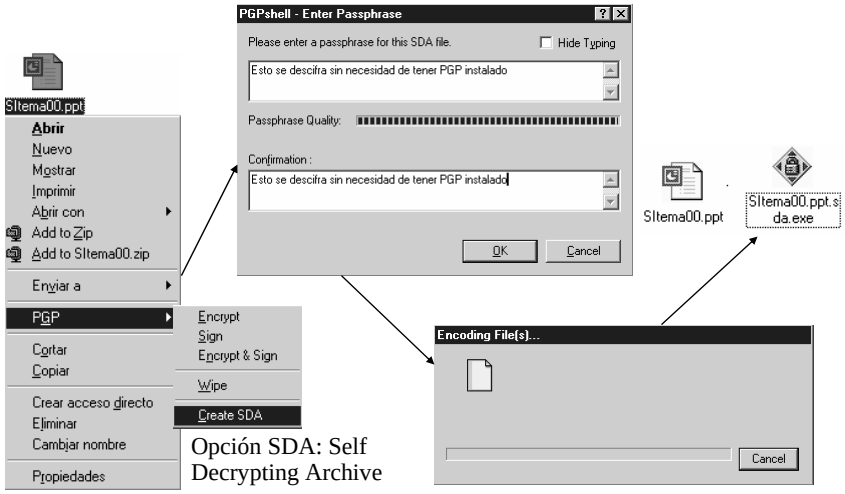


El archivo queda cifrado, con icono de PGP y extensión pgp. Observe que el archivo original permanece porque no hemos activado la opción wipe original.

Pinchando dos veces sobre el icono...

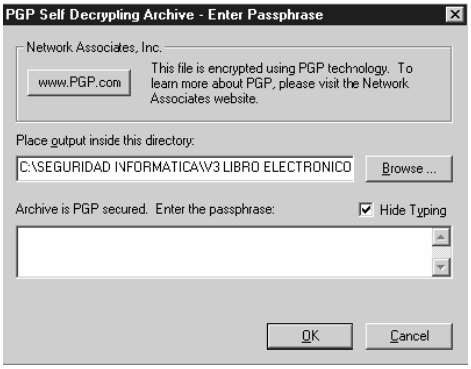
¡Si olvidamos la clave y usamos wipe, nunca podremos recuperar el archivo!

Cifrado en modo SDA con PGP 7.0.3



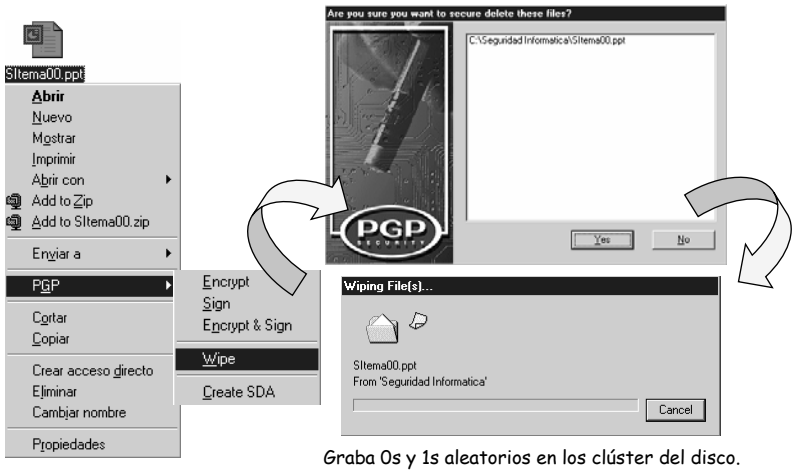
Opción SDA: Self Decrypting Archive

Descifrado SDA con PGP 7.0.3



Este es un archivo ejecutable y se descifra de forma automática haciendo doble clic sobre él, sin necesidad de que el usuario de destina deba tener PGP instalado en su PC... ☺

Borrado físico de archivos con PGP 7.0.3



Graba 0s y 1s aleatorios en los clúster del disco.

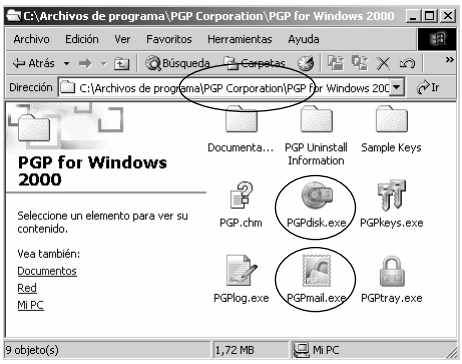
PGP versión 8.0

Las operaciones sobre archivos para cifra y firma digital siguen siendo muy similares a las versiones anteriores. La oferta de producto, además de la versión freeware contempla:

- PGP Desktop
- PGP Desktop Upgrade to Enterprise
- PGP Enterprise
- PGP Mobile
- PGP Personal

Además de las carpetas de instalación, veremos algunas de las opciones de configuración con diferencias notables respecto a las versiones anteriores.

Carpeta e iconos de PGP versión 8.0

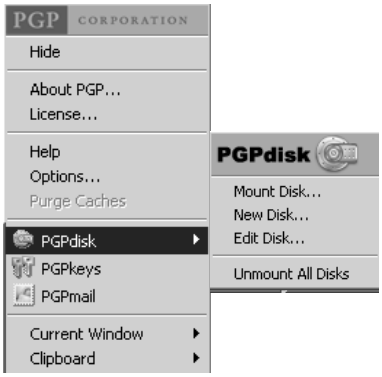


La versión 8.0 se instala en la carpeta PGP Corporation que cuelga de la carpeta de C:/Archivos de Programa.

Incluye un nuevo programa: PGPdisk

El programa PGPmail es el antiguo PGPtools

Programa PGPdisk

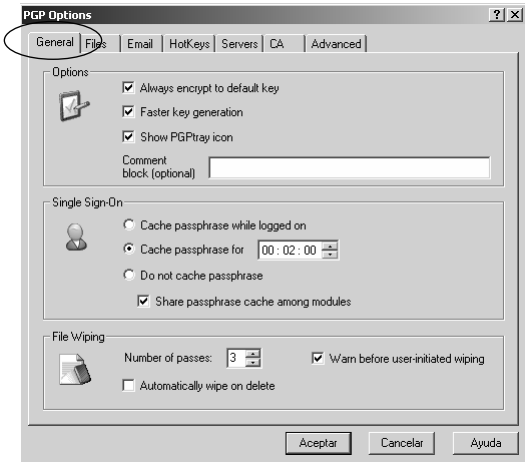


El programa PGPdisk permite montar una sección del disco como si se tratase de una unidad más en su PC.

De esta forma toda la información que allí se almacene estará protegida por una clave.

Desgraciadamente esta opción no viene incluida en la edición freeware.

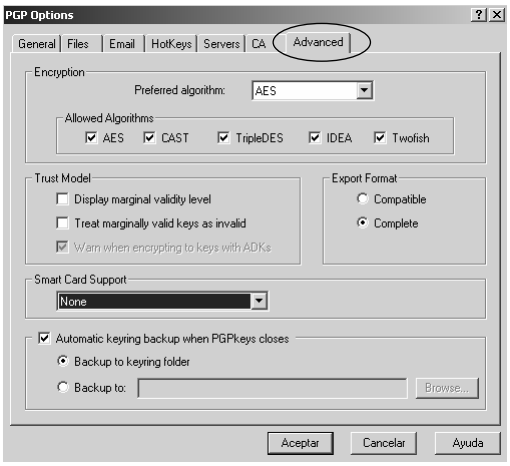
Opciones generales de PGP 8.0



Incluye al igual que en la versión 7.03 la opción de Single Sign On. Consiste en permitir la cifra/firma digital de documentos durante un tiempo dado, sin tener que introducir en cada uno de ellos la frase de paso para acceder a clave privada.

Las demás opciones son las mismas, con ligeras modificaciones.

Opciones avanzadas de PGP 8.0



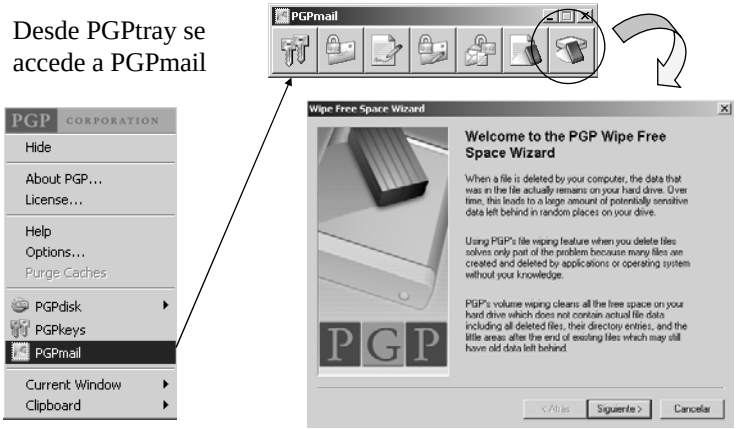
El algoritmo por defecto es el nuevo estándar AES (Rijndael) y cambia Blowfish por Twofish.

Incluye la opción de usar tarjetas inteligentes para almacenar y gestionar claves.

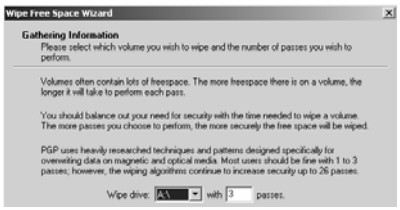
Se puede configurar un backup automático del anillo de claves al cerrar el programa.

Acceso a Wipe Free Space desde PGPmail

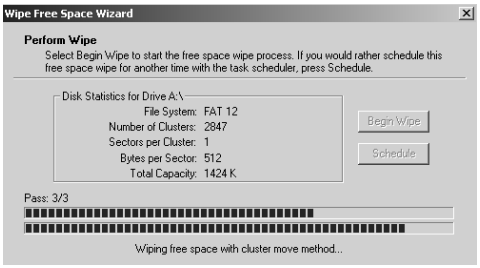
Desde PGPtray se accede a PGPmail



Free Space Wipe con PGP 8.0



Seleccionamos la unidad en la que vamos a borrar archivos temporales y el espacio libre al final del cluster de cada archivo del disco.



Se elige el número de pasos que hará el programa de borrado.

Nota: es una acción que toma bastante tiempo. En este caso de unidad A:\ y con sólo dos archivos, tres pasadas han significado más de 7 minutos.

Recomendaciones con las claves de PGP

- Observe que si crea nuevas claves y cierra el programa, PGP le avisará que es recomendable hacer una copia de seguridad de sus nuevos pares de claves asimétricas.
- Esto es así porque cualquier persona que conozca algo de PGP y entre en su computador, puede abrir el programa PGPkeys y borrar las claves. Aunque pueda parecerle poco lógico, no se pide ninguna clave para esta operación.
- Por lo tanto, si trabaja con PGP de forma frecuente, haga de vez en cuando un volcado de sus claves asimétricas y de las claves públicas externas como copia de seguridad.

GnuPG: Gnu Privacy Guard

- GnuPG es un reemplazo completo y libre para PGP. Debido a que no utiliza el algoritmo patentado IDEA, puede ser utilizado sin restricciones. GnuPG es una aplicación que cumple el RFC 2440 (OpenPGP).
- La versión 1.0.0 fue publicada el 7 de septiembre de 1999. La versión actual a comienzos de 2005 es la 1.4.0.
- GnuPG es Software Libre. Puede ser utilizado, modificado y distribuido libremente bajo los términos de la Licencia Pública General de GNU.
  - Texto sacado de la web de GnuPG http://www.gnupg.org/

Correo seguro a través de S/MIME

- S/MIME: Secure Multipurpose Internet Mail Extensions
  - A diferencia del PGP estándar, que se basa en la confianza entre los usuarios, S/MIME usa certificados digitales X.509 entregados por una Autoridad de Certificación que los clientes de correo deben reconocer como tal.
  - Añadirá servicios de cifrado y firma en los clientes de correo (Outlook Express, Netscape Messenger, ...) en formato MIME.
  - Crea una especie de sobre en el que se envuelven los datos cifrados y/o firmados.
  - Usa plataformas de estándares PKCS, Public-Key Cryptography Standards.

http://www.imc.org/smime-pgpmime.html

Fin del capítulo

Cuestiones y ejercicios (1 de 4)

1. Usando la tabla correspondiente represente en base 64 los siguientes mensajes ASCII: M_1 = AMIGOS, M_2 = ¿Qué pasa?
2. Instale una versión de PGP, vaya a la carpeta del programa y luego imprima el documento que verá en la carpeta documentation.
3. Con cualquier versión de PGP cifre de forma local y con armadura (base 64) un archivo que haya creado con el bloc de notas y observe los rellenos que introduce en el criptograma y al final de él. Añada una letra al texto en claro y vuelva a comparar los textos ASC.
4. Cifre el documento TXT anterior y observe la salida ASC. Vuelva a cifrarlo y observe la salida. ¿Coinciden? ¿Qué ha pasado?
5. ¿Es posible que PGP cifre un documento y éste salga en claro?
6. ¿Por qué siempre se comprime el mensaje antes de cifrar?
7. ¿Qué puede decir de la gestión de claves públicas que ofrece PGP?

Cuestiones y ejercicios (2 de 4)

8. ¿Qué tipo de esquema de cifra es el que utiliza PGP?
9. Después de instalar PGP en nuestro computador, ¿qué es lo primero que nos sugiere?
10. ¿Qué diferencia hay entre elegir una clave DH/DSS y RSA?
11. Si creamos un nuevo par de claves asimétricas, ¿queda el nuevo usuario como usuario por defecto?
12. Cree tres nuevos usuarios Hugo, Paco y Luis con diferentes tipos y longitudes de clave. Haga que entre ellos se firmen sus claves.
13. Incluya en cada uno una fotografía en sus propiedades. Puede ser cualquier archivo con formato de imagen.
14. ¿Qué sucede si creamos que un nuevo usuario Ana con una clave tipo DH/DSS con una longitud exacta de 4.000 bits? ¿Podemos crear una clave RSA de 4.000 bits?

Cuestiones y ejercicios (3 de 4)

15. Revoque una clave y observe sus propiedades. ¿Se puede recuperar esa clave? ¿Puede deshabilitar una clave? ¿Qué significa esto?
16. Cree el grupo Sobrinos con los usuarios Hugo, Paco y Luis. Envíe un mensaje a ese grupo eligiendo desde PGPkeys Show Groups.
17. Cree el usuario FirmaEspecial con frase de paso UnaFirmaEspecial en la que intervengan 4 usuarios, cada uno con una porción igual de la clave y umbral 3. Cifre y firme un documento con dicha clave. ¿Podría alguien tener más de una participación de la clave?
18. Mediante el botón derecho del ratón cifre de forma local un archivo por ejemplo de Word, en modo formato compatible. Vuelva a cifrar el archivo original con otro nombre pero ahora sin formato base 64. ¿Cómo son ambos criptogramas? ¿Cómo son sus tamaños en bytes?
19. Si se cifra un archivo txt con la opción Secure Viewer, ¿se guarda el archivo descifrado? ¿Es seguro? ¿Puede hacerse con archivo Word?

Cuestiones y ejercicios (4 de 4)

20. Cree el nuevo usuario Pepillo y exporte su clave a un archivo. Borre ahora este usuario y desde PGPkey importe ese archivo de clave pública. ¿Se añade el usuario al anillo de claves públicas?
21. ¿Qué pasa en un cifrado local de un archivo con self decrypting? Compruébelo con un archivo cualquiera. ¿Podríamos usar esta opción si además de cifrar vamos a firmar ese documento?
22. ¿Qué significa actualizar una clave desde PGPkeys?
23. Añada un nuevo nombre a una clave. ¿Para qué puede servir esto?
24. ¿Qué son el KeyID y el Fingerprint? ¿Qué utilidad puede tener que la huella dactilar también esté dada como un conjunto de palabras?
25. Si una clave está revocada, ¿puede recibir archivos cifrados con su clave pública? ¿Puede firmar nuevos documentos? ¿Puede descifrar y/o comprobar documentos anteriores a la fecha de revocación?

Use el portapapeles Prácticas del tema 18 (1/7)

Software PGP 8.0: http://www.criptored.upm.es/software.htm#freeware

1. Si no tiene instalado PGP, descárguelo e instálelo. Acepte por defecto todas las opciones, reiniciando su computador y observe que en este caso le fuerza a crear un par de claves asimétricas: cree una cualquiera. Si tiene instalada una versión anterior a la ésta, instálela indicando que tiene claves y que desea conservarlas en esta nueva versión.
2. Pinche en el icono PGPtray (candado) que aparece en la barra de tareas y observe en PGPkeys que están sus claves y la nueva, si la ha creado.
3. Abra la carpeta Archivos de programa\PGP Corporation\ y observe los documentos pdf en la carpeta Documentation. Si puede, imprímalos.
4. Desde PGPkey - Keys - New Key cree la siguientes clave:
   Nombre: Juan Pérez email: juanito@empresa.com
   Passphrase: Esta es la clave de Juanito
5. Observe la clave generada en PGPkeys.

Use el portapapeles Prácticas del tema 18 (2/7)

6. Repita el ejercicio anterior entrando ahora en modo Expert, generado una clave DH/DSS de 1024 bits y duración un año para el usuario José Ramos; y una clave RSA de 1024 y duración seis meses para el usuario Ana Vélez. Observe las nuevas claves y sus características: Key Properties.
7. Abra la opción View de PGPkeys, active todas las casillas y obsérvelas.
8. Active como usuario por defecto a José Ramos: botón derecho del ratón y Set by Default. Hecho esto, sobre las claves de Juan Pérez y Ana Vélez pulse el botón derecho y firme esas claves: sign. Observe las propiedades de esas claves después de esta firma.
9. Con la opción PGPkeys - Keys - Add - Photo, incluya una fotografía a cada una de estas tres claves. Observe que le pide la clave privada de cada uno, sin necesidad que sea el usuario por defecto. Vea las propiedades.
10. Con PGPkeys - Keys - Export, exporte la clave pública de José Ramos. Observe el fichero creado. Repita el ejercicio exportando ahora además la clave privada y observe el fichero creado.

Use el portapapeles Prácticas del tema 18 (3/7)

11. Copie al portapapeles todo el bloque siguiente y dentro de PGPkeys pegue su contenido (Crtl V) para importar la clave pública que supuestamente le ha llegado en un correo electrónico o se la ha entregado en mano Patricia:


```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: PGP 8.0 - not licensed for commercial use: www.pgp.com

mQGiBEF+iZsRBADV5uEp8xSuM/9s8Yo35ajTivI0sFoGr0X7o0iCGIL3MXMqbLUQ
t/4gFH2joQQT7FxzCUuLwItFGVbWN6sE/1Pl0WJ24ltTBoS9jkvPJ4GTZSrAZqzj
dWgv16VAyKvEMZ/8vjetd/YRcx5KORdbMkZFsn+YEBt+amGEG7bPl+UA3QCg//h/
PSn1CgNxfP/MdTHb0lhmspcD/j7G7pA/GAJ1aZi4Xsp4QH2dJhSBBDxdaoRDVuQe
CADER2DFgC1KcPHkh1QnNWRNyAL3JLriy884mCSMTC0nF7MBq7bQCng6P6WdfZAP
lYAwrmNTlJTJLOISnxPuI++vM+Awqv/zPNkvYog5F12j//0Cm51sQ8rBB5MMppDK
wc8jA/0WD31Pt3wT0CPBdlzsywB+S1eXvYriMcK5yezKQElasaXyBtMPOTcfagXC
J/bwYQ/JFZGuAtXcR9YVoUKKPZToibV1Forj4O8g7kOCgFM7hKe+PuwRSFTkrcXK
usm0tci+O0c8WkmkdhtmC4BigRALPk7wfObtjmWhzrTXQWDxl7QcUGF0cmljaWEg
PHBhdHR5QGVtcHJlc2EuY29tPokAWAQQEQIAGAUCQX6JmwgLCQgHAwIBCgIZAQUb
AwAAAAKCRBTdLP9mT9CeipHAJ0dBgLluHQ5R2MzZ2K26sEdZ0NcaQCgmPr6GKTU
5vSeNunxGUZJXDMWeUO5AQ0EQX6JnhAEAOcINMith6D/dqoqLPyE7Dm9U8wV5I5R
jQ8vX+5kRr5nenKs0DZHZD88Q/ciGy/6IZapSrUU8Ob72wVJtsitLjr/9IrZFfaY
1M/ry4n57dKbSlUtIuoAMUduyaC2LXIHjA8aHcjkf1HzI5ZyN2VX47kBEvPCFK0X
90C6wlCsUMmzAAICBAC0+F5Iqf1Wcuix0tkzpxb85cRHqVkjKoV7vtOvx1wW7NLu
nAytWolWkmpmGknrxTM2XdHUJBDvi4KYwxOwMJCuxkAzpNWiOaGzjfiSZWcXK0T4
oiBs8OL2y9gdpFGvdIzZdc2m09iYJs7hGU5uGOFTyp7YJUsI35zUn0fO/o7vdlkA
TAQYEQIADAUCQX6JngUbDAAAAAAKCRBTdLP9mT9Ces1tAKDhyokWrHR4DmyWxaJS
9cMs9AssfACdEfDYQ/hJa5PVfUPQfk6yDjDg0IY=
=d8QC
-----END PGP PUBLIC KEY BLOCK-----
```


Use el portapapeles Prácticas del tema 18 (4/7)

12. Observe las propiedades de la clave importada. ¿Se puede definir a Patricia como usuario por defecto?
13. Vamos a crear una clave cualquiera para un usuario de nombre Alicia. Una vez creada, exporte la clave pública y privada. Hecho esto borre la clave de Alicia en PGPkeys con tecla suprimir o bien Edit - Delete.
14. Con PGPkeys - Keys - Import, importe la clave de Alicia desde el archivo creado en el paso anterior, observe el mensaje y compruébelo desde las propiedades de la misma. Modifique la confianza en dicha clave.
15. Con el usuario Ana Vélez por defecto, firme las claves de los otros usuarios creados con distintos noveles de confianza. Observe luego las propiedades de las claves firmadas por Ana Vélez.
16. Revoque la clave de uno de los usuarios creados y observe las propiedades.
17. Con el botón derecho del ratón sobre documento de este libro electrónico CriptoClasica.doc, cifre de forma convencional o cifrado local con la clave K = Clave de cifra convencional. Abra el archivo con WordPad.

Use el portapapeles Prácticas del tema 18 (5/7)

18. Observe el tamaño del fichero cifrado y compárelo con el original.
19. Vuelva a cifrar de forma convencional el documento CriptoClasica.doc con la misma clave, pero añada ahora la opción Text Output. Abra el archivo con WordPad y vuelva a comprara el tamaño de los ficheros.
20. Cree un documento cualquiera con Word, Excel, etc. sencillo y cífrelo de forma local con la clave K = Borrado de verdad, con las opciones Text Output y Wipe. El archivo original ha sido destruido.
21. Recupere el archivo cifrado haciendo doble clic en él.
22. Para saber con qué algoritmo hemos cifrado, con qué profundidad se ha realizado el borrado físico y otras propiedades de PGP, desde el icono del candado abra la pestaña Options y observe todas estas opciones.
23. Cifre nuevamente el documento CriptoClasica.doc de forma convencional con la opción Self Decrypting Archive. Observe el icono y el tamaño del fichero. Si puede hacerlo, descífrelo en un computador que no tenga instalada ninguna versión de PGP.

Use el portapapeles Prácticas del tema 18 (6/7)

24. Ponga por defecto al usuario José Ramos y desde el icono PGPtray abra el portapapeles (Clipboard Edit), escriba un texto de algunas líneas y cópielo al portapapeles (Copy to Clipboard). Luego cífrelo (Clipboard Encrypt) para Ana Vélez, arrastrando su nombre a la ventana. Abra el portapapeles (Clipboard Edit) y observe que el contenido está en Base 64. Si no sabe qué significa esto, vaya al anexo de estos apuntes.
25. Descifre su contenido (Clipboard Decrypt & Verify). Observe que puede copiar ese texto en claro y guardarlo en un achivo.
26. Repita la cifra anterior activando ahora en la cifra el modo Secure Viewer. ¿Puede guardar ahora el texto en claro?
27. Repita el ejercicio anterior pero ahora José Ramos sólo firmará el texto. Hecho esto, abra el portapapeles y observe su contenido. Compruebe que la firma es válida con la opción (Clipboard Decrypt & Verify).
28. Repita el ejercicio anterior activando ahora la opción de cifrar y firmar (Clipboard Encrypt & Sign) . Descifre el criptograma.

Use el portapapeles

Prácticas del tema 18 (7/7)

29. Si tiene un cliente de correo que tenga los plugins de PGP, envíe y reciba correo cifrado y firmado, bien a sí mismo o con otro usuario.
30. Cree cinco claves de cualquier tipo con nombres Gerente, Consejero1, Consejero2, Consejero3 y Consejero4. Cree ahora una clave de nombre Empresa. Hecho esto, divida esta última clave (Share Split), defina como umbral para recuperar la clave 5 y arrastre a la ventana a los cinco usuarios antes creados, entregando a Gerente 3 partes y a cada Consejero 1 parte. Observe que en este escenario siempre deberá firmar Gerente.
31. Con Empresa como usuario por defecto, firme CriptoClasica.doc y observe cómo se van solicitando las partes de la clave. Compruebe luego la firma.
32. Si tiene acceso a Internet, compruebe cómo funcionan los servidores de clave, las listas de revocación de certificados, etc.
33. Para terminar, en modo Expert cree algunas claves de tamaños “extraños” como 1893 bits, 2871 bits, 4017 bits, ... y observe los tiempos que tarda PGP en crearlas. ¿Qué opina de la seguridad de esas claves RSA?