Facultad de Ciencias Sociales y de la Comiunicación

Diplomatura en Gestión y Administración Pública

Redes de datos

Correo electrónico: conceptos

Departamento de Lenguajes y Sistemas Informáticos.
Profesor: Manuel Fernández Barcell.

Índice General

Correo electrónico

1 Correo electrónico

La idea del correo electrónico es fácil de entender porque es análoga al correo postal tradicional. Para enviar una carta a otra persona, tenemos que redactar la carta, escribir la dirección del destinatario, y depositarlo en un buzón de correos.

El correo electrónico es similar. Tenemos que redactar el mensaje, pero en vez de con lápiz y papel, utilizamos un ordenador, y un programa de correo electrónico. Para enviar la carta utilizamos las redes mundiales de ordenadores en vez del servicio de correos.

El correo electrónico es una utilidad que nos permite el intercambio de mensajes entre usuarios de ordenadores (local o remoto) aunque los usuarios no estén conectados en ese momento.

El sistema de correo electrónico lo almacena hasta que el receptor del mensaje decide leerlo.

Su principal virtud es que nos permite enviar mensajes a cualquier parte del mundo. Para ello basta con que el usuario de destino tenga cuenta en una máquina que esté en Internet. Normalmente al usuario se le avisa que le ha llegado correo al entrar en la computadora en la cual tiene definido su buzón. Suele ser una máquina multiusuario con la que se conecta, y que le informa de los mensajes que le llegaron. Metodologías más modernas, permiten incluso que el correo sea tratado directamente desde un ordenador personal en su despacho. Tener un buzón en el que recibir el correo, no es ni más ni menos que ser propietario de una cuenta en una máquina de Internet (normalmente una máquina **Unix**). Si usted dispone de una de estas cuentas, entonces posiblemente puede enviar y recibir correo a cualquier parte del mundo. Difiere del correo tradicional en varias cosas:

- No es necesario pagar por cada mensaje que enviamos.
- Es bastante más rápido.
- El documento que se envía es electrónico y no en papel.
- Los medios de transmisión son electrónicos, normalmente a través de los medios que componen Internet.
- Una misma copia del mensaje es fácil de distribuir a varios receptores simultáneos.
- El emisor y el receptor no deben ponerse de acuerdo en un instante, para que el emisor pueda enviar su mensaje y el receptor recibirlo. Si no que se entiende que el emisor manda su mensaje y que cuando llegue, en algún instante el receptor entra en su máquina y ésta le avisa que le ha llegado un mensaje de tal persona. En ocasiones esto supone una ventaja en cuanto a que en comunicaciones a larga distancia puede haber diferencias horarias que dificulten bastante que el emisor y el receptor estén trabajando o incluso despiertos a la misma hora.

El correo electrónico, no es una aplicación única de Internet, o de los protocolos TCP/IP, sino que existe en muchas otras redes, algunas veces utilizando la misma infraestructura de comunicaciones. Así, en ocasiones, es necesario enviar correo electrónico a un usuario que no esté en Internet, para ello existen unas máquinas específicas llamadas pasarelas o *gateways* de correo que permiten enviar correo entre distintos sistemas. Existen pasarelas conocidas, para redes Bitnet, Compuserve, Fidonet, UUCP, etc

1.1 Protocolos y direcciones

Como ya hemos comentado hay diversas redes de ordenadores que usan distintos protocolos de correo. Cada protocolo usa su propio sistema de dirección.

Existen pasarelas que interconectan redes y traducen direcciones de formatos heterogéneos.

INTERNET usa el protocolo **SMTP** (*Simple Mail Transfer Protocol* - Protocolo de transferencia simple de correos). Describe el formato de los mensajes de correo electrónico y cómo deben de manipularse para realizar su entrega. El formato de dirección se llama **RFC-822**.

nombre@dominio

1.2 Esquema del sistema de correo

El sistema de correo electrónico tiene varias capas o agentes, encargándose cada uno de ellos de ciertas misiones para asegurar el correcto funcionamiento del sistema. Los tres "agentes" que hay son los siguientes:

AGENTE DE USUARIO (A.U)
AGENTE DE TRANSPORTE (A.T.)
AGENTE DE DISTRIBUCIÓN Y ENTREGA (A.D.)

Ejemplos de cada uno de estos agentes son los siguientes:

<table>
<tr><td>/bin/mail</td><td>Mail</td><td>MH</td><td>Elm</td><td>RMAIL</td><td>Mush</td><td>Zmail</td><td>mailtool</td><td>A.U.</td></tr>
<tr><td colspan="6">/usr/lib/sendmail</td><td colspan="2"></td><td>A.T.</td></tr>
<tr><td colspan="2">sedmail
SMTP (Internet)</td><td colspan="2">/bin/mail
local</td><td colspan="2">/mail11dv
DECnet</td><td colspan="2">/usr/lib/uucp/uux
UUCP</td><td>A.D..</td></tr>
</table>

Vamos a ver las funciones de cada uno de los agentes mencionados.

Agente usuario

Es la aplicación que utiliza el usuario para el manejo del correo electrónico. Interactua directamente con el usuario y con el sistema de correo de Internet. Permite mandar mensajes nuevos, leerlos, borrarlos, recibir el correo, manejar sus buzones o carpetas y muchas cosas más.

Existen varios agentes de usuario, cada uno con sus características. En un mismo sistema pueden coexistir varios. Cada uno tendrá que decidir cual quiere que sea su agente de usuario favorito y aprender su uso. No es necesario ni útil aprenderse todos. La relación siguiente comenta alguno de los más populares.

Comparación entre distintos agentes usuarios de correo:

- **/bin/mail** Muy simple y pobre; antiguo.
- **Mail, mailx** Está en todos los sistemas. Rápido. Interfase de línea.
- **elm** Menú de pantalla, con ayudas. Muy fácil. Más lento que **Mail**.
- **MH** Muchos mandatos independientes para cada función. Bueno si se tiene buena memoria y se recibe mucho correo.
- **Rmail** Para amigos de **GNU Emacs**.
- **pine** Utiliza menús, muy sencillo de usar.
- Eudora, Pegasus, MS mail Cliente para Windows

No vamos a dar un curso de cada uno de estos programas. Sí vamos a comentar cuales son las operaciones habituales a realizar cuando trabajamos con el correo electrónico poniendo algún ejemplo con **Ximian Evolution**.

Da igual el agente que elijamos, el procedimiento es el mismo en todos. Lo primero y más importante de conocer es como obtener la "ayuda". Una vez conseguida, simplemente léela.

Aprender a usar el correo es prácticamente aprender a manejar nuestro agente de correo preferido. Vamos a ver las operaciones más frecuentes con el correo electrónico.

1.3 Enviar un mensaje a alguien

Antes de mandar un mensaje, vamos a ver algunos conceptos necesarios. Lo primero que necesitamos saber de la persona a la que quiere mandar un mensaje electrónico es su **dirección electrónica**. Si no lo hemos hecho, ahora te indicaremos cual es la tuya. Las direcciones electrónicas tienen el formato de dominios.

Lo segundo que tenemos que hacer es construir el mensaje electrónico que queremos enviar. Vamos a ver la estructura de un mensaje.

1.4 Estructura de un mensaje

Un mensaje electrónico tiene las siguientes partes:

- Una cabecera.
- El texto.
- La firma.

La cabecera

La cabecera consta de una serie de campos. No todos los campos que vamos a comentar tienen que estar presentes. Los más frecuente son los siguientes:

- **From** dirección real del remitente.
- **Received:** caminos por los que ha venido el mensaje.
- **Date:** fecha y hora de envío.
- **From:** Dirección a la que se puede replicar.
- **Subject:** asunto, breve resumen del mensaje.
- **To:** destinatario del mensaje.
- **Cc:** ***C****arbon* ***c****opy*; una copia del mensaje será enviada a todos los destinatarios que figuren en este apartado.
- **Bcc:** ***B****lind* ***c****arbon* ***c****opy*; se mandan copias pero el receptor, en el mensaje, no aparece este campo. Por lo tanto el destinatario original del mensaje (to:) no sabrá que se ha mandado una copia del mensaje a otras personas
- **Attachements:** Indicamos los nombres de los ficheros que queremos incluir en el mensaje.
- **Message-id:** N1de identificación del mensaje.
- **Status:** **N**ew, **U**nread, **O**ld, **R**ead.
- **X-cualquier_cosa:** específico del sistema de correo.

Texto

Es el mensaje en sí. Algunos clientes de correo sólo admiten el juego de caracteres del **ASCII** de 7 bits (no acentos, no caracteres especiales, etc). El motivo es que el protocolo **SMTP** originariamente sólo aceptaba estos caracteres.

La mayoría de los clientes de correo actuales admiten un protocolo llamado MIME (*Multipurpose Internet Mail Extension*) que si permite meter el juego de caracteres completo. También admiten tipos de letras etc.

Diferencia entre texto y dato binario

Para poder transmitir ficheros que contienen caracteres que no son **ASCII** (7 bits), es decir, ficheros binarios (ejecutables, archivos comprimidos, ficheros WP, imágenes,

sonidos, etc), previamente hay que "codificarlos" a ASCII de 7 bits. Esta operación aumenta el tamaño del fichero entre un 20% y un 30%.
Codificadores usuales

- **uuencode / uudecode** (codificador a binario/ decodificador a texto)
- **btoa / atob** (Binario TO Ascii/ Ascii TO Binario)
- tarmail / untarmail
- - Archivadores usuales:
- **tar shar** (UNIX)
- PKZIP LHARC ARJ (DOS)

Firma
La firma es opcional. Si se pone, DEBE SER CORTA (unas 4 líneas), que contenga datos tales como: Cargo, dirección, localización, teléfono, etc.
Se puede configurar el agente de usuario para que incluya automáticamente la firma.

1.5 Buzones y carpetas

Un **buzón** (*mailbox*) es un fichero donde se almacenan mensajes. Una **carpeta** (*folder*) contiene buzones y carpetas. Podemos crear una estructura parecidas a las de directorios y subdirectorios. Cada usuario tiene al menos tres buzones:
Buzón primario de correo nuevo (*incoming mailbox o system mailbox*).
Es donde se depositan los mensajes nuevos en el servidor.. Dependiendo del sistema el buzón será:
BSD /usr/spool/mail/identificación
SV.4 /var/mail/identificación
Buzón secundario
Es el sitio donde se guardan los mensajes en el cliente. Dependiendo del sistema puede cambiar. En Evolution es el Bandeja de entrada. Los mensajes nuevos están en negrita
Buzones o carpetas adicionales (*Mailbox, folder*).
Es el sito donde guardo mis cartas una vez leídas y sacadas del buzón de entrada. Puedo crearme los que quiera para tener ordenado mi correo. Si el fichero en el que quiero guardar un mensaje ya existe, el mensaje se añadirá al final.

1.6 Otras características

Búsquedas de mensajes

- www.yahoo.com buscar la opción *people search*
- www.altavista.magallanes.net
- www.lycos.com
- www.infoseek.com
- www.ozu.com
- www.ole.es seleccionar la opción infomail

Listines de correo electrónico

- www.infoespace.com
- www.four11.com
- www.bigfoot.com
- www.swithboard.com
- www.whowhere.com
- www.iaf.net
- www.listin.com en español

RFC (*Request For Comment*) sobre correo electrónico se pueden obtener en *Internet Mail Consortium* www.imc.org

2 MIME (1) y los caracteres especiales (acentos y eñes)

En principio el correo electrónico se diseñó como un sistema para transmitir pequeños mensajes de texto. Se habilitó un juego de 128 caracteres (del 0 al 127) que resultaba común a casi todas las máquinas y sistemas operativos implicados (se trataba del código ASCII (2) básico, de 7 bits). Renunciar al octavo bit aumentaba la compatibilidad entre sistemas, pero dejaba en fuera de juego a los caracteres habituales de otros idiomas, como las eñes y las vocales acentuadas; estos caracteres especiales utilizan códigos extendidos que se ubican en las posiciones superiores al carácter 127 y no resultan compatibles entre los diferentes sistemas operativos.

Los angloparlantes no sintieron que ese problema fuese un asunto urgente, pero enseguida se dieron cuenta de que sería muy útil habilitar algún mecanismo que permitiese incluir en los mensajes de correo información más compleja. Querían transmitir imágenes, programas, ficheros de cualquier clase. Esos datos sí que utilizaban el octavo bit. El problema es que querían mantener el sistema de correo con 7 bits y añadir el transporte de ficheros constituidos por conjuntos de 8 bits. ¿Cómo lograrlo? La solución podía ser un sistema "traductor" que convirtiese los ficheros a textos, bajo apariencia de caracteres (de 7 bits). La transformación fue denominada UUENCODE (3) y con ello se conseguía transmitir esos ficheros por el correo. Los ficheros eran incluidos como texto (incomprensible), con una cabecera y un final que delimitaban el texto correspondiente al contenido del fichero. El receptor del mensaje debía utilizar un programa decodificador que utiliza procedimientos inversos, UUDECODE (3), para generar nuevamente el fichero original. Al principio las transformaciones resultaban un poco engorrosas, pero pronto aparecieron programas automáticos que facilitaban la tarea.

Incluso surgieron programas de correo que evitaban la visualización del texto incomprensible que correspondía al fichero: más transparencia y simplificación para el usuario.

El sistema UUENCODE/UUDECODE aún se emplea con frecuencia en los grupos de noticias; y todavía existen programas independientes que realizan esta conversión. Con esto ya se había superado el asunto de la transmisión de ficheros. Pero todavía había problemas, el sistema aún tenía defectos de planteamiento que resultaban difíciles de superar. Por otro lado, los usuarios de otros idiomas empezaban a presionar para que las transmisiones de correo incluyesen los caracteres extendidos (las eñes, vocales acentuadas y otros similares).

Se reunieron los *gurus* de las altas esferas y llegaron a una conclusión: se necesitaba un nuevo estándar más capaz y que también admitiera los caracteres especiales. El nuevo sistema fue bautizado como MIME (1), teniendo la ventaja de que también resultaba compatible con los sistemas precedentes. MIME permite transmitir caracteres especiales, sin que ello ocasione trastornos. Aunque el emisor y el receptor utilicen sistemas operativos distintos, MIME facilita la conversión de esos caracteres, de forma que siempre resulten correctamente transmitidos.

En verdad, decir "SIEMPRE" es demasiado optimista; al final hay otras variables que pueden causar complicaciones, pero MIME es un avance importante en las transmisiones de correo.

Los problemas que todavía existen se deben a varias razones. La primera es que MIME puede funcionar de varias formas distintas. Por un lado existe la posibilidad de

usar MIME con transmisión de 8 bits por carácter, aunque lo habitual es emplear la otra alternativa, denominada "*Quoted Printable*" (algo así como "código imprimible"). El sistema *Quoted Printable* sigue manejando 7 bits, usando caracteres adicionales para representar los signos especiales; así, el carácter "é" (letra e acentuada) se transmite como una secuencia de tres caracteres "=E9", que luego debiera ser correctamente interpretado por el sistema MIME receptor. Si la configuración de tu programa permite activar la posibilidad "*Quoted Printable*", hazlo; es la opción adoptada mayoritariamente. También es más segura, puesto que el mensaje tendrá que pasar por muchas máquinas intermedias, algunas de las cuales manejan inadecuadamente los caracteres de 8 bits.

Por otro lado, MIME puede utilizar diferentes conjuntos de caracteres para la transmisión. Habitualmente se usa el juego denominado "ISO 8859-1", también llamado "Latin-1" (4). Aunque algunos programas permiten elegir otros juegos de caracteres alternativos, siempre es preferible utilizar el que se ha indicado, por ser el más utilizado.

Aún puede haber otro tipo de problemas, derivados de las características concretas de los programas de correo, puesto que algunos no implementan el estándar MIME de una forma totalmente correcta o completa. Hay dos aspectos que presentan dificultades con cierta frecuencia y que vamos a comentar: MIME transmite el texto del mensaje sin insertar artificiosos cambios de línea. Algunos programas insertan un cambio de línea de tipo "técnico" entre cada dos líneas del mismo párrafo. Con MIME, eso no debiera suceder; el cambio de línea se contempla igual que en los procesadores de texto, cuando el usuario haya marcado deliberadamente el final de un párrafo pulsado la tecla *Return* (también conocida como tecla *Intro*, *Enter* o tecla de cambio de línea). Así, el texto de un párrafo largo se transmite todo seguido, como una línea extremadamente larga. Se supone que el programa receptor siempre debe ser capaz de recomponer la presentación, adaptando el texto a la ventana visual que se use en cada momento. Este asunto concreto se aborda de forma específica en otra página dedicada al Tamaño de las líneas en los mensajes de correo electrónico.

La otra peculiaridad que presentan algunos programas consiste en la inadecuada manipulación de ciertos datos. Todos los programas que usan MIME hacen un tratamiento bastante correcto de los caracteres incluidos en el cuerpo del mensaje. Pero algunos no hacen lo mismo respecto a los textos de la cabecera del mensaje. Estos datos son los siguientes:

- Nombre y dirección del remitente.
- Nombre y dirección del destinatario (o destinatarios).
- Título (asunto, tema o "subjet").

Puesto que algunos programas todavía no implementan el adecuado procesamiento MIME para estos datos concretos, conviene ser muy prudente (o reprimirse) a la hora de introducir acentos y eñes en estas casillas.

MIME también añade avances importantes en las transmisiones de ficheros. Por ejemplo, es más eficaz para controlar los nombres y las características de los ficheros enviados. Pero estos detalles resulta de menor transcendencia para el internauta de a pie, que siempre encuentra muy molesto el problema de los caracteres especiales.

Conclusiones:

El éxito de una transmisión de correo depende de la coordinada configuración de ambos sistemas: emisor y receptor del mensaje. La transmisión de acentos y eñes solo

será posible si ambos utilizan MIME; con esto ya es muy probable que se puedan evitar todos los conflictos, aunque no es seguro. En algunos programas, la opción MIME debe ser configurada frente a otras alternativas (UUENCODE o, sencillamente, no-MIME); en otros casos, MIME viene preconfigurado y no es posible desactivarlo.

Para garantizar absolutamente la correcta transferencia de caracteres especiales habrá que verificar que ambos programas usan métodos idénticos; es muy conveniente verificar que el programa se halla configurado con las opciones "*Quoted Printable*" y con el juego de caracteres "ISO 8859-1" (ó "Latin-1"). En algunos programas es posible variar estos parámetros; otros no permiten su manipulación, pero los traen configurados por defecto.

Si tu programa de correo no tiene posibilidades de utilizar MIME, seguramente tendrás muchos problemas con estos caracteres; puesto que la mayoría de internautas ya emplean este sistema, será muy conveniente que vayas pensando en cambiar tu programa de correo para conseguir otro más actualizado que incorpore MIME. Todos los buenos programas que se distribuyen en la actualidad incorporan esta posibilidad, incluyendo algunos programas gratuitos y otros que son de tipo *shareware*.

Se puede encontrar información más detallada en la dirección siguiente, de la que se ha obtenido buena parte de la información aquí detallada.

http://idg.es/iworld/especial/correo.html.

También puede obtenerse otra información adicional en la página Acentos y eñes en la lista, que aborda un problema peculiar de la **lista Grumetes** y algunas otras listas de distribución.

2.1 MIME

Acrónimo de *Multipurpose Internet Mail Extensions* (Extensiones de Correo de Internet Multifunción). Estándar para adjuntar archivos a mensajes de correo de Internet. Archivos que no son de texto incluyen gráficos, documentos de procesadores de texto formateados, archivos de sonido, etc. Un programa de correo electrónico se dice que si puede recibir y enviar archivos usando un estándar MIME. Cuando se envían archivos de no texto, usando el estándar MIME se convierten (codifican) a texto, aunque, en realidad, el texto resultante no se puede leer (no es legible). El estándar MIME es una manera de especificar tanto el tipo de archivo que se envía como el método que se debería usar para devolverle su formato original.

Además de software de correo electrónico, el estándar MIME se usa para identificar los archivos que se envían a clientes Web, nuevos formatos de ficheros se pueden acomodar simplemente actualizando la lista de *browsers* de pares de tipos MIME y el *software* apropiado para manejar cada tipo. (Información consultada en el Glosario de Términos de Internet de la Universidad de Alcalá) (2) ASCII Acrónimo del código estándar americano para el intercambio de información (*American Standard Code for Information Interchange*). Es el código estándar de conjunto de caracteres que cualquier ordenador puede entender, usado para representar las letras latinas, en mayúsculas, minúsculas, números, puntuación, etc. Hay 128 códigos estándar ASCII, cada uno de los cuales puede representarse por un número binario de 7 dígitos. Sin embargo, otros conjuntos de caracteres como Latin-1 están comenzando a usarse. Los documentos HTML no se limitan a ASCII. (Información consultada en el Glosario de Términos de Internet de la Universidad de Alcalá)

2.2 UUENCODE/UUDECODE

Las letras UU hacen referencia a "*Unix to Unix*", comunicaciones entre sistemas Unix ()igual que en el más conocido UUCP, que significa "*Unix to Unix Copy Protocol*", protocolo de copia entre sistemas Unix). ENCODE significa "encriptación", "cifrado" o "codificación". Opuestamente, DECODE hace referencia a "des-encriptación", "descifrado" o "descodificación" (por cierto, "decodificación" no es correcto). Frecuentemente se usa el término UUENCODE para hacer referencia al sistema conjunto que implica las dos operaciones, UUENCODE y UUDECODE. El sistema UUENCODE/UUDECODE también se reconoce como BinHex (Binario Hexadecimal), aunque esta denominación es menos precisa y se suele aplicar a otras cuestiones no relacionadas con el correo electrónico.

(4) ISO 8859-1, también llamado Latin-1

Se trata de un juego de caracteres concreto, que incluye 256 caracteres (los 128 del ASCII básico y otros 128 adicionales) y que está pensado para representar los signos utilizados por el idioma español y otras lenguas europeas. Es el resultado de un acuerdo entre organismos y fabricantes de software. En el mundo de los PC, IBM adoptó esta norma y la denominó tabla de códigos 850; MicroSoft la llamó ANSI o ANSI-code en Windows. Otros, como Macintosh, todavía no tienen implementada esta normativa. Por cierto, "Latin-1" se escribe sin acento.

3 Smailer

:-)	Sonriente	<:-O	4Oye tú!
:-1	Sonrisa forzada	:-*	Silencio (boca tapada con mano)
:-y	Bastante sonriente	:-o	Sorprendido
:-D	Muy sonriente	:-O	Gritando
X-D	Tronchado de risa	:-{	Conde Drácula
:-):-)	Carcajadas	:-j	Ahí va un secreto
8-D	Sonriente con gafas	=|:-)=	Tío Sam
:-p	Sonriente y burlón (sacando la lengua)	:~i	Fumando
{:-)	Sonriente con tupé	:~j	Fumando y sonriente
:-{)	Sonriente con bigote (1)	:/i	No fumar
:<)	Sonriente con bigote (2)	o=	Cerilla encendida
:<)=	Sonriente con bigote y barba	-=	Cerilla apagada
%-)	Mareado pero sonriente	:-C	4Oh! Eso es increíble
:^{	Bigotudo	:-B	Con los labios mordidos
:-|	Serio (1)	<:>==	Un pavo
:-T	Serio (2)	:*)	Borracho
:/)	Eso no es divertido	:-8	Hablar sin parar
:-9	Relamiéndose	(:-)	Rumor
:-(	Triste, deprimido o decepcionado	@=	Guerra nuclear
:-c	Muy triste	<:-)	Tontorrón
(:(	Super triste	:-x	Besos
:-/	Mosqueado o escéptico	:->	Sarcástico
:-<	Desamparado	(:^(	Triste por tener rota la nariz
}:-)	Irónico / Picarón	:_)	Me he partido la nariz ...
O:-)	Santo / Inocente	B-)	Batman
'-)	Guiñar un ojo	B-|	Batman impasible
;-)	Guiñar un ojo con complicidad, ligón	#:-)	Peinado yuppy
8"-)	Llorar de felicidad	#:-o	Yuppy sorprendido

8-(	Apesadumbrado
:-I	Indiferente
P-)	Pirata simpático
:-X	Soy/eres una tumba
=:-)	Punk cachondo
=:-(	Punk tristón
(@@)	Me estás tomando el pelo
:-"	Fruncir los labios
:-v	Hablando (de lado)
:-V	Gritando (de lado)
:-w	Hablando con lengua viperina (de lado)
:-W	Gritando con lengua viperina (de lado)
:-f	Burlón (sacando la lengua) (1)
:-r	Burlón (sacando la lengua) (2)
{O-)	Cíclope
||*(	Se ofrece un apretón de manos
||*)	Se acepta el apretón de manos
(-_-)	Sonrisa secreta
<:-)<<|	Mensaje enviado desde un cohete espacial
<<(:-)	Vendedor sonriente con sombrero
(:>-<	4Arriba las manos!
{'	Alfred Hitchkock (presenta ...)
[:-)	Llevo walkman
.-)	Perdí un ojo ...
>:->	Satánico
>;->	Satánico lujurioso
(-:	Zurdo (inclinándose al revés)
8-)	Guapo con gafas
B:-)	Gafas en el pelo
8:-)	Jovencita
:-)-8	Chicarrona
:-{}	Lápiz de labios
}:-(	Tupé serio
:-[	Vampiro
:-S	Incoherente
<|-)	Chino
<|-(	Chino cabreado
:-D	Burlándose 4de ti!
#:-O	Yuppy cabreado
|-(	Dormidísimo
:^)	4Vaya narizota!
(:-$	Enfermo
(:-&	Muy cabreado
:-?	Pensativo y/o fumando en pipa
OO	Mensaje importante
(:<)	Chismoso
:-(=)	Dientes largos
&:-)	Pelo de diseño o rizado
@:-)	Pelo de diseño u ondulado
?-(	Puñetazo en el ojo
:	Mensaje sobre cosas vagas
+<:-|	Monja impasible
(:-|K-	Mensaje formal
c=:-)	Jefe de cocina
><><	Calcetines a cuadros
<{:-)}	Mensaje en una botella
(:-...	Mensaje descorazonador
(O-<	Mensaje dudoso
:-#	Censurado
@>--->--	Una rosa
(:I	Cara huevo
X-(	Fallecido
:-~)	Resfriado
:'-(	Llorando
:'-)	Llorando de alegría
:-@	Gritando
--:)	Punk amable
--:(	Punk normal
+-:-)	Religioso
':-)	Ceja cortada
|-I	Profundamente dormido
|-O	Bostezando
:-Q	Fumador
:-X	Secreto (labios sellados)
O :-)	Santo, Ángel

4 PGP

4.1 Introducción

El PGP (*Pretty Good Privacy* o Intimidad Bastante Buena), por ser el sistema de codificación más extendido para correo electrónico y uno de los primeros en aparecer (escrito en su primera versión por Philip R. Zimmermann en el año 1991)

PGP es el estándar de facto para correo electrónico y ha alcanzado gran popularidad gracias a que fue puesto a disposición de todo el mundo, junto con su código fuente, por su creador. Como ocurre con todos los sistemas de encriptación basados en clave pública, PGP permite el intercambio seguro de mensajes sin necesidad de que se haya producido antes un intercambio seguro de claves, como tiene que suceder, por ejemplo, si se emplease el DES.

El principio de funcionamiento de PGP es sencillo y se basa en una clave doble: para cada usuario existe una clave pública que se puede divulgar sin problemas, y también existe una clave privada que es realmente secreta y que nunca es enviada a otros. Cuando se desea enviar un mensaje confidencial, se codifica con la clave pública del destinatario, que es conocida; así, el mensaje se transmite encriptado y solo es posible leerlo si previamente se descodifica con la clave privada del receptor. Si bien, PGP permite que las claves públicas varíen desde 384 hasta 1.024 bits, en el momento del cifrado solamente se utilizan 128 bits, operando en bloques de 64 bits, sea cual sea la clave pública especificada, lo que establece una cierta limitación; no obstante, es mucho más seguro que DES, que utiliza una clave de 64 bits, pero que de ellos nada más que 56 son útiles como clave para cifrar la información. El PGP se encuentra compilado para casi todas las plataformas y sistemas operativos existentes: para MS-DOS (no las ultimas versiones), Windows 95 y 98, Windows NT, Sistemas MAC, Amiga, Atari, y para las plataformas UNIX se encuentra el código fuente.

- Con PGP los mensajes electrónicos son completamente privadas y también sirve para la identificación digital (realiza una firma digital) de un usuario asegurando que el mensaje procede de el y además asegura que no se ha realizado la mas mínima modificación en el texto del mensaje, pero esto plantea el problema se saber con certeza que la clave publica de X que se tiene es valida. Para poder asegurar que la clave publica de una persona es valida tenemos dos opciones. Que se conozca a la persona en cuestión y nos la haya proporcionado ella misma. Que conozcamos a una persona que conozca personalmente a la primera y nos confirme la clave publica de la primera.

En otros sistemas de seguridad, como SET, existen las entidades certificadoras de claves, pero aquí no hay nadie en concreto que autentique aunque existen Servidores de Claves, una red de ordenadores interconectados en la que se encuentran almacenadas las claves publicas, que en España se accede vía WWW en la dirección http://www.rediris.es/cert/keyserver. Por estos servidores podemos acceder a una base de datos en la que se encuentran miles de claves publicas y si lo deseamos incluso podemos enviar la nuestra que en pocas horas será conocida por el resto de servidores distribuidos por el mundo. Para utilizar PGP en sus últimas versiones no es necesario introducir opciones por la línea de teclado, basta simplemente con instalar el programa (se puede obtener gratuitamente en la dirección http://www.pgpi.com o la versión comercial en http://www.pgpinternational.com) y utilizar los menús, eso si lo primero

que hay que hacer es generar el par de claves (pública y privada) y guardar la clave privada en un lugar seguro.

Cuando hablamos de seguridad en Internet surgen infinidad de preguntas y términos como: integridad, autentificación, encriptación, autoridad de certificación, redes de confianza, claves, certificados, firma digital, SSL, PGP, SET, SEC, ... y un sinfín de acrónimos. Este es el primero de una serie de artículos que intentará aclarar los conceptos de seguridad desde un punto de vista del usuario, sin profundizar en algoritmos de encriptación o procesos matemáticos. No sólo nos centraremos en la seguridad personal sino también en la relacionada con el comercio electrónico y las tiendas en línea (*on-line*). Tras leer estos artículos podremos decir que Internet es segura siempre y cuando se tomen ciertas precauciones básicas.

4.2 Correo electrónico seguro y PGP

Unos conceptos básicos que son comunes a todos los aspectos de seguridad en Internet.

Muchas veces hemos oído hablar de encriptación, posiblemente a muchos nos suena a algo tétrico, cifrar es otro termino que se utiliza para la misma función. Encriptar consiste en aplicar un proceso matemático o algoritmo a un texto legible para convertirlo en algo totalmente ininteligible. Este proceso matemático (algoritmo) necesita de una clave de tal forma que al aplicar el mismo algoritmo a un texto con claves diferentes, el resultado es diferente y único para cada clave. Al considerar el proceso de desencriptación surgen dos tipos de sistemas: sistemas simétricos (o de clave única) y sistemas asimétricos (o de clave pública). En los sistemas simétricos la clave utilizada para descifrar es la misma que la que se utilizó para cifrar (o es una variación directa de ella). De esta forma, si usted quiere encriptar un mensaje debe poseer el algoritmo de encriptación (programa) y su clave personal, y esa clave personal debe distribuirla a todas aquellas personas a las que usted pretende enviar mensajes encriptados, ya que ellos deben utilizar su clave para desencriptar. Si algún indeseable consigue su clave, podrá leer todos sus mensajes, lo que se considera un gran agujero en la seguridad. Debido a ello aparecieron los sistemas asimétricos, en estos sistemas cada usuario dispone de dos claves, una privada y otra pública, de tal forma que lo que una cifra la otra descifra y viceversa. Lo importante en este proceso es que la clave privada sólo la conoce el usuario propietario de ella, y es la pública la que distribuye para que el resto del mundo la utilice para enviarnos mensajes, si alguien capta el mensaje no podrá descifrarlo ya que sólo se descifra con la clave privada y está en nuestra posesión. De esta forma la clave pública se utiliza para encriptar y la privada para desencriptar. Existe un sistema asimétrico que utiliza internamente un cifrado simétrico, de tal forma que el cifrado es doble, este sistema de encriptación lo veremos en profundidad al considerar SSL. Otra utilidad de la clave privada es la de firmar digitalmente un mensaje para asegurar la identidad del autor del mensaje (autentificación) y que no ha existido ninguna manipulación posterior de los datos (integridad), de esta forma si yo quiero enviarles un mensaje puedo encriptarlo con mi clave privada de tal forma que sólo se podrá desencriptar con mi clave pública, si alguien capta el mensaje por el camino, la desencripta y lo modifica, no puede volver a encriptarlo (ya que la clave privada está en mi posesión) por lo que al recibirlo usted verá que no se desencripta con mi clave pública y por lo tanto que el mensaje no lo he enviado yo o ha sido modificado. Lógicamente la encriptación y la firma digital no son excluyentes, pero recuerde que cada una tiene su misión: la encriptación impide que otros vean su mensaje, la firma digital asegura que lo que ha enviado lo ha hecho usted y no otra persona, asegurando además la integridad del mensaje. Los algoritmos de encriptación

suelen ser públicos ya que su robustez reside en que la probabilidad de descubrir las claves es prácticamente nula.

4.3 Firmas digitales

Una firma digital es un bloque de caracteres que acompaña a un documento, acreditando quién es su autor ("autentificación") y que no ha existido manipulación posterior de los datos ("integridad").

El proceso de la firma digital lo realiza un *software* (por ejemplo PGP, Eudora, Outlook,...) que aplica un algoritmo *Hash* (MD5 o SHA-1) sobre el texto a firmar, obteniendo un extracto (número) de longitud fija, y único para ese mensaje. Este extracto cuya longitud oscila entre 128 y 160 bits se somete a continuación al cifrado (RSA o DSS) mediante la clave secreta del autor, previa petición de contraseña.

Al recibir el mensaje se necesita disponer de la clave pública del firmante para desencriptar el extracto y comprobar la integridad del documento, esto lo hace aplicando *Hash* al texto y comparando el extracto resultante con el recibido.

Este sistema tiene un punto débil y es que nadie nos asegura que la clave pertenece a quién dice poseerla. Imagine que suplanto la identidad de una persona y que envío mi clave pública bajo su identidad. Mediante este sistema sólo la confianza entre las partes evita este problema. Para solucionar este gran agujero de seguridad aparece la figura de la Autoridad de Certificación como entidad en la que confían todas las partes y que certifican las claves de tal forma que para obtener una clave hay que dirigirse a una autoridad, presentar todos los datos personales y previa una comprobación de los mimos nos otorgan una clave privada y otra pública. De esta forma no hay forma de suplantar la identidad de otra persona, ya que la clave está registrada.

Existen sistemas como PGP que no utilizan autoridades de certificación externas, sino que delegan en el propio usuario la responsabilidad de certificar claves conforme a su criterio, estableciendo lo que se denomina una red de confianza (*Web of Trust*) totalmente descentralizada, pero con el apoyo de una red de servidores de claves.

4.4 PGP

PGP es el acrónimo de *Pretty Good Privacy*, o 'privacidad bastante buena', y sin duda es el programa más extendido, aunque no utilizado, para asegurar la privacidad del correo electrónico. Con PGP conseguimos dotar a nuestro correo de varios atributos: confidencialidad, integridad y autentificación. Es un sistema asimétrico y por lo tanto utiliza dos claves, una pública y otra privada. Es importante hacer notar que PGP es un programa autónomo que, aunque se integra con algunos gestores de correo como Outlook, funciona de forma independiente y que obliga a que todas las partes implicadas en el envío/recepción de correo seguro tengan instalado PGP.

4.4.1 Instalación y funcionamiento de PGP

PGP es un programa gratuito que podemos descargar de Internet (ver tabla al final del texto). Lógicamente para poder utilizar PGP todos los interlocutores deben tener instalado PGP en su ordenador, sino no podrán leer los *mails* cifrados.

El proceso de instalación utiliza un asistente que le guía en todos los pasos, que son:

1) Introducir su nombre y dirección e-mail.

2) Elegir tipo de clave que utilizará DSS o RSA. En la actualidad se recomienda Diffie-Hellman/DSS (más conocida como simplemente DSS) por su mayor grado de seguridad.
3) Nº de bits de la clave. Por defecto se utilizan 2048 bits, que es totalmente suficiente (a mayor nº de bits más seguridad y más lentitud en proceso de encriptación).
4) Fecha de expiración. Puede elegir entre nunca o una fecha concreta.
5) Introducción del *Password*. Este *password* será imprescindible para encriptar los mensajes, debe ser mayor a 8 caracteres.
6) Generación interna de números aleatorios. Se nos pedirá que movamos el ratón, utilizándose como semilla para esa generación aleatoria.
7) Generación automática de claves.
8) Posibilidad de publicar nuestra clave en un servidor de claves por defecto. Para ser coherentes con el resto del texto diremos que no las publique en el servidor por defecto.

Para poder utilizar el sistema de encriptación deberá distribuir su clave pública a todos los interlocutores para que puedan enviarle mensajes y comprobar sus firmas, por supuesto ¡nunca distribuya su clave privada!. Puede distribuir su clave pública adjuntándola a un mensaje que envía a esas personas aunque es mejor utilizar los servidores de claves que existen en Internet, éstos recopilan las claves de infinidad de usuarios de PGP en todo Internet, usted también puede introducir su clave pública en el servidor mediante un formulario. Como hemos visto en el proceso de instalación se nos pregunta si queremos utilizar servidores de claves, si respondemos que sí el mismo programa nos dará de alta en su servidor por defecto, también podemos darnos de alta a posteriori en el programa de configuración de PGP llamado *PGPKeys*. En la opción *Keys/Send Key to Server* aparecen una serie de servidores de claves, uno de los servidores oficiales es *www.keys.pgp.ne*t, puede elegir cualquiera de los servidores que aparecen en la lista. Si desea añadir algún servidor vaya a la opción *Edit/Preferences/Server* y añada el servidor deseado. Al elegir un servidor su clave pública estará en todos los servidores de claves del mundo ya que se replicarán de forma transparente al usuario. Para poder descifrar mensajes deberá conocer las claves públicas del interlocutor, esto lo puede hacer automáticamente el programa PGP en *Keys/Search* introduciendo cualquiera de los criterios indicados, como por ejemplo, la dirección de correo electrónico.

Llegados a este punto ya estamos preparados para utilizar PGP en nuestros mensajes. PGP no envía mensajes de correo, simplemente cifra un mensaje generado con un programa de correo electrónico. PGP incluye *plug-ins* para Eudora y Outlook 97/98, esto facilita mucho el trabajo ya que en estos gestores de correo aparecerán unas nuevas opciones PGP en el resto de gestores de correo electrónico el proceso será un poco diferente. Para Outlook Express existe un plug-in pero no va incluido con PGP, debe descargarse por separado (vea al final el lugar de descarga).

En *Outlook* (y todos aquellos para los que exista *plug-in*) PGP se añade como un menú más. Al crear un mail verá que aparecen unas opciones nuevas en la barra de herramientas, que le permiten encriptar, firmar y abrir el programa *PGKeys*. Cuando acabe de escribir el texto puede realizar cualquiera de esas funciones o ambas.
Encriptar el mensaje. Para encriptar un mensaje deberá conocer la clave pública del receptor. Búsquela mediante el programa *PGKeys*.
Firmar un mensaje. Para firmar un mensaje utilizará su clave privada y deberá distribuir su clave pública, esta puede incluirla en el mismo mail como un archivo adjunto. Para adjuntarlo deberá primero ir al programa *PGKeys* elegir su clave y con el menú

emergente (botón derecho del ratón) elija exportar y guárdelo en un directorio. Luego adjúntelo al mail.
Ejemplo. Imagínese que usted quiere enviarme un mensaje cifrado y firmado, una sugerencia de los pasos a seguir serían los siguientes (lógicamente usted ya ha instalado PGP y está conectado a internet):
1) Abra *Outlook* y vaya al nuevo menú llamado PGP y pulse *PGPKeys*.
2) Vaya al menú *Keys/Search* para buscar mi clave pública. Introduzca mi nombre: FRANCISCO GARCÍA LÓPEZ y pulse para buscar. Le aparecerá mi nombre, mi dirección de correo electrónico y mi clave pública. Púlsela para introducirla en su base de datos local.
3) Vuelva a Outlook y abra un mensaje nuevo, introduzca mi dirección de correo electrónico frangar@jet.es y el cuerpo del mensaje.
4) Si quiere puede incluir su clave pública en el mensaje como antes se ha descrito. Este paso no es imprescindible ya que puedo buscar su clave igual que usted a buscado la mía.
5) Pulse los botones de encriptar el mensaje y de firmar digitalmente en la barra de herramientas. Envíelo.
6) Introduzca la contraseña para firmar el mensaje.
Por favor, realicen este ejemplo sin vacilar, estaré encantado de recibir sus pruebas. Para desencriptarlo o verificar la firma utilice los botones de la barra de herramientas.

Si no existe *plug-in* para su gestor de correo el proceso es diferente. Utilizaremos el programa *PGPtray*, aparecerá en el menú de PGP y en la barra de tareas de Windows en la parte derecha. Pulse sobre el y aparecerá un menú que permite aplicar todas las funciones PGP al contenido del portapapeles (*clipboard*). Para cifrar un mensaje, creelo de la forma habitual, cuando haya acabado copie el texto en el portapapeles, pulse *PGPtray* y seleccione encriptar portapapeles (*encrypt clipboard*), le pedirá que seleccione la clave pública del destinatario, haga click sobre ella, el mensaje ahora estará cifrado en el portapeles. Vuelva al mensaje y sustituya el texto original por el contenido del portapapeles. Envíe el mensaje.

Para firmarlo realice lo mismo y elija *en PGPtray* cifrar portapapeles (*sign clipboard*), se le pedirá su contraseña. Envíelo.

Para encriptar y cifrar utilice la opción *Encrypt & Sign clipboard*. Para descifrar/desencriptar un mensaje copie el cuerpo del mismo en el portapeles y elija la opción *decrypt/verify clipboard*. Introduzca su contraseña y vea el resultado seleccionando *Edit Clipboard Text,* también puede pegarlo desde el portapapeles.

También puede encriptar o firmar ficheros que envía por correo electrónico. PGP se integra con el explorador de Windows, elija el archivo y abra el menú emergente con el botón derecho del ratón, verá que aparece la opción PGP y que podrá realizar cualquier operación.

Otros recursos:

Puede encontrar infinidad de recursos en internet que hablan sobre PGP, aquí se adjunta una pequeña lista:
Descarga de PGP (2,3MB):
ftp://ftp.ifi.uio.no/pub/pgp/5.5/win95nt/

Plug-ins para Outlook Express:
ftp://ftp.ifi.uio.no/pub/pgp/5.5/win95nt/PGPOEPlugin.zip

Kriptopolis:
www.kriptopolis.com/pgp.html

Red Iris:
www.rediris.es/pgp

PGP internacional:
www.pgpi.com

4.5 PGP 5.5i FAQ EN ESPAÑOL Ver. 1.1 (Julio 98)

- FAQ básica sobre el programa de encriptación PGP 5.5i para Windows95/98/NT.
- Esta FAQ incluye nociones básicas, instalación y utilización.
- Este documento puede copiarse cuantas veces se quiera sin modificaciones y para fines no comerciales.
- FAQ realizada por Antonio Montesinos (a.monte@jet.es) Para adiciones o sugerencias utilizar la dirección e-mail.

- ¿Qué es PGP?
- ¿Qué utilidad tiene PGP?
- ¿Es fiable PGP?
- ¿Cuánto cuesta el programa?
- ¿Dónde se puede conseguir?
- ¿Cómo funciona?
- ¿Qué peligro existe de que alguien intercepte mi clave pública?
- ¿Qué ocurre si alguien intercepta el mensaje PGP que me envía otra persona?
- ¿Qué ocurre si alguien intercepta el mensaje PGP que yo envío a otra persona?
- ¿Qué necesito para mandar un mensaje cifrado a otra persona?
- ¿Cómo se instala el programa?
- ¿Una vez instalado, qué?
- ¿Con qué programas de correo electrónico se puede utilizar?
- ¿Cómo enviar un mensaje encriptado?
- ¿Cómo desencriptar un mensaje que me han enviado?
- ¿Qué otros archivos se pueden codificar aparte de archivos de texto?
- ¿Puedo mandar un archivo codificado como adjunto en un mensaje de e-mail?
- ¿Cómo?
- ¿Cómo desencriptar un archivo adjunto que nos llegue por e-mail?
- ¿Qué son las firmas digitales?

¿QUÉ ES PGP?
PGP *(Pretty Good Privacy*) es un programa que encripta la información digital (textos o cualquier otro tipo de archivo) y luego permite desencriptarla. Por ejemplo, un texto que diga "Hola, soy yo" quedaría convertido en algo parecido a "DXCfg%/yfggER$%"
¿QUÉ UTILIDAD TIENE PGP?
La principal es esconder información a ojos de otras personas que quieran tener acceso a ella. Su uso más común es con el correo electrónico. Cuando se envía un mensaje de correo electrónico, ese mensaje pasa por muchos ordenadores antes de llegar a su destinatario. Cualquier persona con acceso a esos ordenadores y con malas intenciones podría tener acceso a los mensajes. Usando PGP los mensajes no viajan tal como se escribieron, sino que van codificados, decodificándose únicamente en su destino.
¿ES FIABLE PGP?

Actualmente es el sistema de encriptación más utilizado. Miles de usuarios lo usan día a día para sus comunicaciones. Con respecto a su seguridad aún no hay noticias fiables de que se haya conseguido romper una clave PGP. De hecho, se han realizado experimentos por parte de conocidos criptógrafos para intentarlo con resultados negativos. De todas formas, cualquiera que lo consiga obtendrá una fama bastante sonada y la noticia correrá como la pólvora entre los miles de usuarios que continuamente están al día de todo lo relacionado con PGP y la criptografía.

¿CUANTO CUESTA EL PROGRAMA?

PGP es gratuito para usos no comerciales.

¿DÓNDE SE PUEDE CONSEGUIR?

Hay montones de sitios en Internet para descargar PGP. En español existe una de las mejores páginas sobre criptografía desde donde se enlaza con las páginas internacionales de descarga, aparte de contener gran cantidad de información.

http://www.kriptopolis.com

¿CÓMO FUNCIONA PGP?

PGP funciona a través de claves. Cada usuario tiene una clave propia y única que genera el propio programa. Esta clave está partida en dos, una pública y otra privada. La clave pública, como su propio nombre indica, se puede hacer pública y hay que entregarla A AQUELLOS QUE NOS VAYAN A ENVIAR MENSAJES CIFRADOS. La clave privada hay que mantenerla en secreto y conviene sacarle copias de seguridad. Cuando alguien nos vaya a enviar un mensaje cifrado con PGP tendrá que encriptarlo CON NUESTRA CLAVE PÚBLICA que le habremos proporcionado previamente por correo electrónico o de otra forma.

¿QUÉ PELIGRO EXISTE DE QUE ALGUIEN INTERCEPTE MI CLAVE PÚBLICA?

Ninguno, ya que la clave pública no es nada sin la privada a efectos de desencriptar los mensajes.

¿QUÉ OCURRE SI ALGUIEN INTERCEPTA EL MENSAJE PGP QUE ME ENVÍA OTRA PERSONA?

Nada. Lo único que obtendrá es un conjunto de caracteres extraños sin pies ni cabeza que no podrá desencriptar, ya que no posee la clave privada que es la pieza necesaria para poder convertir el mensaje a su forma original. Sólo cuando el mensaje llegue a su destino final podrá ser desencriptado.

¿QUÉ OCURRE SI ALGUIEN INTERCEPTA EL MENSAJE PGP QUE YO ENVÍO OTRA PERSONA?

Absolutamente lo mismo.

¿QUÉ NECESITO PARA MANDAR UN MENSAJE CIFRADO A OTRA PERSONA?

El programa PGP y la clave pública de esa persona.

¿CÓMO SE INSTALA?

Una vez el archivo de instalación en nuestra máquina hay que ejecutarlo. Siguiendo las instrucciones que aparecen en pantalla, el programa genera nuestras claves pública y privada durante el proceso de instalación.

Cuando se generan las claves, PGP nos pide un password, de al menos 8 caracteres, para poder utilizarlas. Es conveniente recordar este password para poder luego desencriptar información.

¿UNA VEZ INSTALADO, QUÉ?

Estaremos dispuestos para utilizar PGP. Lo primero es crear una copia de nuestras claves pública y privada. Estas claves están ubicadas en la carpeta del programa, que por defecto es:
c:\Program Files\PGP\PGP55i
Clave pública: pubring.pkr
Clave privada: secring.skr

De todas formas, al cerrar el programa PGP se nos invita a crear una copia de seguridad de las claves.

Seguidamente exportaremos nuestra clave pública para poder entregarla adecuadamente a aquellos que nos vayan a enviar mensajes codificados. Para ello hay que abrir el programa PGP Keys, que está en INICIO/PROGRAMS/PGP/PGP Keys. Este programa es el que contiene las claves de las personas a las que enviamos normalmente correo cifrado, lo que ocurre es que PGP incluye una serie de claves de ejemplo de unos señores que no conocemos de nada y que se pueden borrar. Dentro de esa relación aparecerá la nuestra. Se selecciona nuestra clave y se pulsa en KEYS/EXPORT, en ese momento aparece un cuadro de diálogo pidiéndonos donde guardar la clave. Ese archivo es el que deberemos enviar como nuestra clave pública.

¿CON QUÉ PROGRAMAS DE CORREO ELECTRÓNICO SE PUEDE UTILIZAR?
PGP incorpora plug-ins para ser utilizado con Eudora, Exchange y Outlook, pero utilizando la opción "encriptar portapapeles" se puede utilizar con cualquier programa de correo.

¿CÓMO ENVIAR UN MENSAJE ENCRIPTADO?
Lo primero que hay que hacer es obtener la clave pública de la persona a quién vamos a enviar el mensaje. Para ello se la podemos pedir directamente por e-mail o la podemos extraer de su página WEB si la tiene allí publicada. Una vez con su archivo de clave pública en nuestro ordenador hay que importarlo a PGP Keys. Para ello:

- - Colocaremos el archivo en una carpeta (por ejemplo la del PGP), - Abrimos PGP Keys (INICIO/PROGRAMS/PGP/PGP Keys)
- - Pulsamos KEYS/IMPORT
- - En la ventana de diálogo se selecciona el tipo de archivo de la clave (.txt/asc/pkr/skr...) y se importa.

Este proceso no tendremos que repetirlo más veces y su clave pública quedará incorporada a nuestra relación de claves.
Estamos listos para enviar correo encriptado. Vamos a utilizar un programa que no esté soportado por PGP y lo haremos a través del portapapeles, que es la forma más estándar y compatible de hacerlo y vale para todos los programas.
- Lo primero es abrir el programa de correo (supongamos que es Netscape Messenger). Compondremos el mensaje normalmente, poniendo la dirección electrónica y el asunto en su sitio y el texto en el cuerpo del mensaje. - Una vez el texto acabado se selecciona y con las teclas CONTROL+X se corta al portapapeles. - Seguidamente pulsaremos en el icono que está junto al reloj de Windows, en la barra de tareas (un icono con un sobre blanco en el centro). Si no tenemos ese icono, lo podemos activar pulsando en INICIO/PROGRAMS/PGP/PGPtray. - Del menú emergente habremos de pulsar en "Encrypt Clipboard".
- En ese momento se nos pregunta con qué clave habremos de encriptar el texto. Selecionaremos la clave de la persona a la que vamos a enviar el mensaje haciendo

doble click sobre ella. Seguidamente se pulsa en OK. En ese momento el contenido del portapapeles queda encriptado.
- Pulsamos de nuevo en el cuerpo del mensaje, que estará en blanco, y con las teclas CONTROL+V pegaremos el contenido del portapapeles al cuerpo del mensaje. Observaremos que el mensaje ahora es una serie de caracteres sin ningún sentido.
- Procederemos entonces a enviar el mensaje normalmente via e-mail.

¿CÓMO DESENCRIPTAR UN MENSAJE QUE ME HAN ENVIADO?
Una vez abrimos el correo y vemos que tiene un mensaje encriptado procedemos a copiarlo íntegro al portapapeles:

```
-----BEGIN PGP MESSAGE-----
Version: PGPfreeware 5.5.3i for non-commercial use <http://www.pgpi.com>

qANQR1DBwU4DhZrHKiEmOtwQCACKcH+Cw1r2zcCaN6PAH5sK1ZjX5J4C1GjU
8Q9G
ajMEhvbHEB9tpbjfBD3UO5oZ8QFBvCaWIgZtg9cF317OfA5UaIhArInzPMRxgmPD
cHpciZS+83EMkZGcMjFAZfqMgCQgb0+Is1Ng6rCtRqdRAZlpmr7ABCIe1QeEG+6P
P79vzE3yf0JihVjSWz6dfAQ9nmyHDkRSA9p8VCdBKOXK9xPZMufjnHTSBRdxHC
Hz
Y55iZVrwEy4uRDHto3vHLet0fDWDDfqQ2CFL3xLW+EB9N2UVmquOhBjcSQu/po
uA
NR308f+ra0xGa0xLpXY4gaibx9TEQittfP1qgbHGQJOgZF+tCADzVFI8N4S6p04E
rIC/dmNaxBES8jnWyAcuqlmjV1vZdg0Nhv7ZeraPewG4Dsdzj0kqnBBhxYGOzboX
xTgicgZZIq30O23w910zvjyNuYXolUY/mwQIbrEzFDF42+M+CSd9C4dnb+GHmYU
8
sbhazvlFfhSAweWSbpDsd0sNHz8VFQnzj8exWN7UDF0tUPhkl2ceL7aLRDaPW4Ea
jRcoMORlZpoUYQcpHhtRskFDL3qT+SsTpy3K72BRGX32CD8DtSEeah1hbJaj2HMj
EyRGmYIM1HrmFc+ZXQDBJy84X0VwnPazIlLjaJnpHd9OExvGIcer5LHE66Gu2W
TP
UAnMw08QySNLgg6n2Uph+lKroCFvuG/W2toIWbGG+1TtbCxaA10IO7o7SQ==
=xtLd
-----END PGP MESSAGE-----
```

Incluyendo las líneas:

```
-----BEGIN PGP MESSAGE-----
.
.
.
-----END PGP MESSAGE-----
```

Seguidamente pulsamos en el icono PGPtray y seleccionamos la opción "Decrypt/Verify Clipboard". En ese momento se nos solicita el password para poder utilizar nuestra clave. Al introducirlo veremos en pantalla el texto original.

¿QUÉ OTROS ARCHIVOS SE PUEDEN CODIFICAR APARTE DE ARCHIVOS DE TEXTO?
Cualquier tipo de archivos.

¿PUEDO MANDAR UN ARCHIVO CODIFICADO COMO ADJUNTO EN UN MENSAJE DE E-MAIL?
Se puede y se recomienda si es información importante.

¿CÓMO?

Lo primero es codificar el archivo y después enviarlo normalmente como adjunto en un e-mail. Para ello PGP ha incluido su función de codificación en el menú emergente al utilizar el botón derecho del ratón.
- Localizar el archivo en la carpeta donde se encuentre.
- Pulsar sobre él con el botón derecho del ratón.
- Seleccionar "PGP"
- Seleccionar "Encrypt"
- Seleccionar la clave de la persona a la que se lo vamos a enviar haciendo doble click sobre ella.
- Pulsar OK
- En ese momento se creará un archivo nuevo ya encriptado con la extensión PGP. Por ejemplo, si el archivo original se llamaba informe.xls, el nuevo archivo resultante quedará como informe.xls.pgp. Ese es el archivo que deberemos enviar como adjunto.

¿CÓMO DESENCRIPTAR UN ARCHIVO QUE NOS LLEGUE POR E-MAIL?
Una vez el archivo en el disco duro hay que hacer doble click sobre él y aparecerá el cuadro de diálogo para introducir nuestro *password* para usar la clave privada. Al hacerlo el archivo quedará desencriptado.
¿QUÉ SON LAS FIRMAS DIGITALES?
Otra función de PGP que permite autentificar los documetos para garantizar que realmente proceden de la persona que lo envía y no un falsificador que pueda haberlos modificado. La firma digital se activa igual que la encriptación pero usando la opción "*Sign*". Incluso se pueden usar simultáneamente son "*Encrypt & Sign*".
--EOF--