

PRACTICA 10. Encriptar mensajes de correo con PGP (Por HxC Mods-Adm)

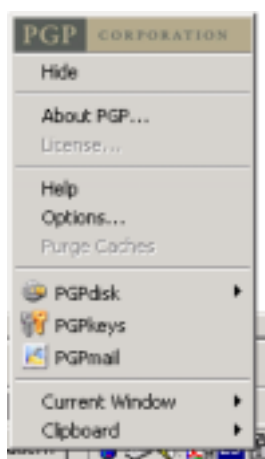
Ahora nos toca otra práctica de seguridad. “*Lo de la criptografía, ya te lo conté, las guerras, los alemanes, los egipcios,...*”

Lo primero: Instalar PGP, existe una versión comercial, más completa, pero esta que es gratuita nos servirá perfectamente....

Durante el proceso de instalación se puede configurar **PGP** mediante los asistentes, no configures nada que no sepas como hacerlo, límitate indicar el directorio de instalación y otras preguntas típicas. No configures tipos de claves ni nada que aún no te lo he explicado, para que **PGP** se instale correctamente, una vez terminado el proceso de instalación debes reiniciar el equipo, después de esto se habrá configurado *Outlook* y otros programas para utilizar **PGP**

Tras el reinicio del equipo, observarás un pequeño icono con forma de candado en *la bandeja del sistema*.

¿Cómo? ¿Qué no sabes dónde está la bandeja del Sistema? Creo que tienes que aprender Windows (el básico, en el que se aprende a cambiar los “*colorines*”, a manejar el ratón etc.), bueno siempre queda la opción de *Inicio-Programas-PGP-PGPKeys*, aunque espero que encuentres la Bandeja del Sistema



PGP se compone de varios módulos, puedes “*cifrar*” discos, correo, la ventana actual, el portapapeles, etc.

El programa **PGPKeys** es el encargado de crear las claves, administrarlas y distribuir las a terceros, a su vez, también puede importar las claves ajenas o buscar las claves públicas de otras personas.

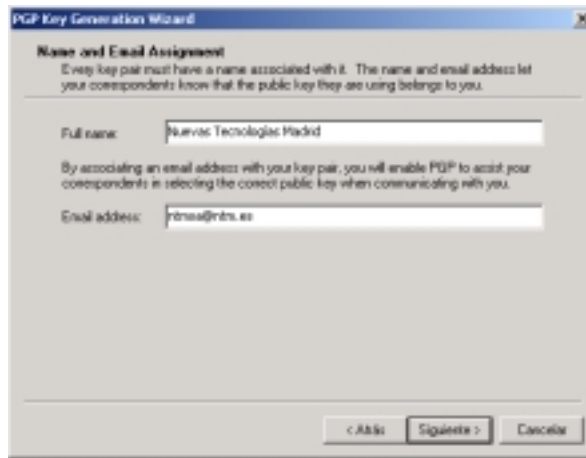
PGPMail es un módulo de correo, sólo será útil si usamos un programa de correo electrónico que no permita PGP, no es el caso de *Outlook*, por lo que no explicaré nada de ello, excepto la forma de encriptar archivos adjuntos.



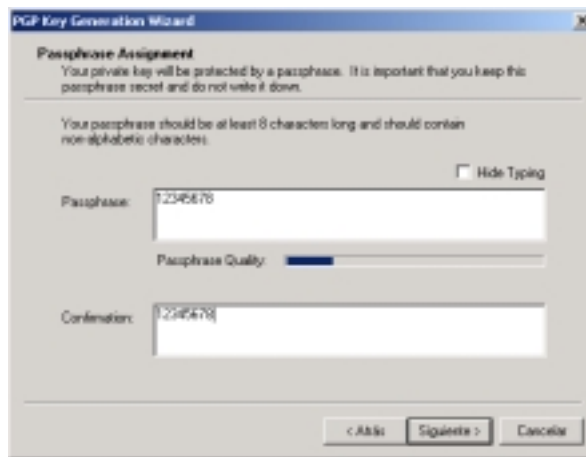
Para poder comunicarse utilizando la seguridad **PGP**, primero debemos generar al menos una pareja de claves, para ello utiliza el módulo **PGPKeys** y en el *Menú Keys* elige la opción **New Key...** se iniciará un asistente que te guiará paso a paso.

Crear una Clave

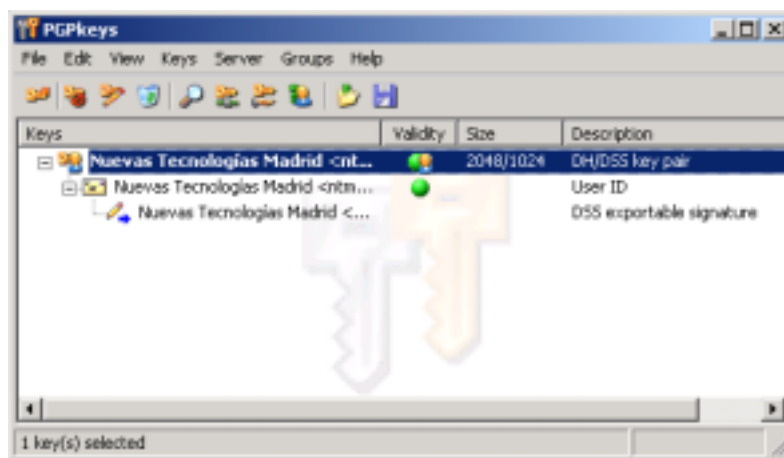
El primer paso es indicar el nombre y la dirección de correo, puedes introducir los que quieras, pero ten en cuenta que éstos se enviarán a tus compañeros de comunicación, por lo que debes utilizar denominaciones que te identifiquen claramente.



El segundo paso es proporcionar una contraseña para proteger la clave, se recomienda que tenga al menos 8 caracteres (es sólo una recomendación), la casilla **Hide Typing** permite o no mostrar lo que escribes:



Una vez introducida la contraseña, pulsa **Siguiente** y **finaliza** la instalación, aparecerá:



La pantalla anterior muestra por cada columna:

Keys: Nombre de la clave

Validity: Grado de confianza dependiendo de quién proporciona la clave. Los círculos verdes indican confianza total, los grises confianza restringida.

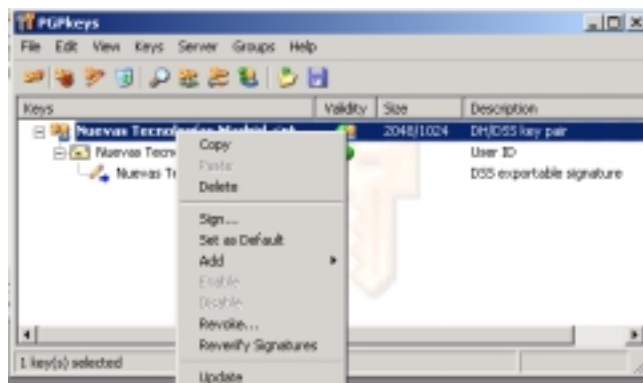
Size: Tamaño de la codificación. 1024/2048 bits es más que suficiente.

Description: Breve descripción de la clave y algoritmo de codificación RSA ó DH/DSS

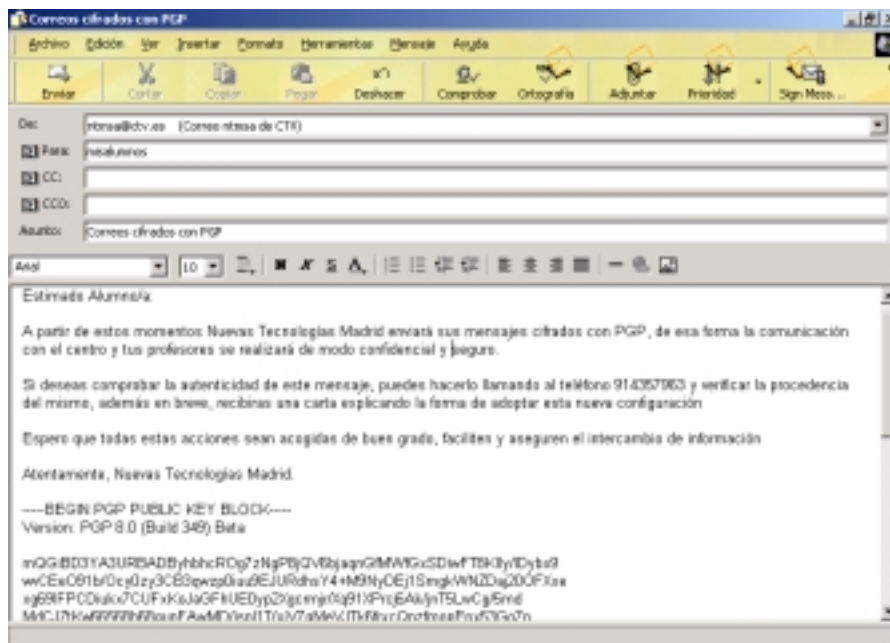
Distribuir la Clave Pública.

Para poder intercambiar la información codificada, los destinatarios deben conocer la **clave pública** generada, para ello enviaremos un correo electrónico al/los destinatarios explicando de qué se trata y pegaremos clave pública en el mismo, esto es:

Selecciona la clave, haz clic en el **botón derecho del ratón** y selecciona **Copy** (esto pasará la clave pública al portapapeles)



Escribe un correo mediante **Outlook** e incluye algún dato para que se reconozca la procedencia real del mismo, no está demás que incluyas teléfonos, etc. Después **Botón derecho y pegar**.



Foro de HackXcrack

Como verás se incluye la *clave pública*, después de la línea ---- **BEGIN PGP PUBLIC KEY BLOCK** ---

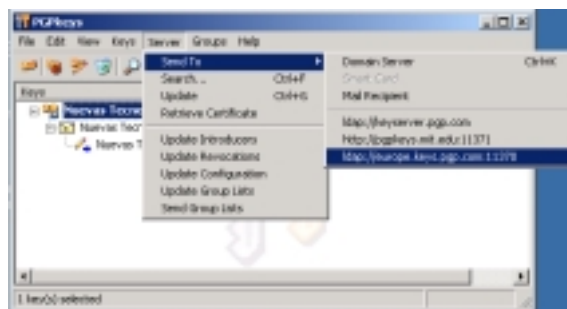
Envía el correo como de costumbre, más tarde los destinatarios podrán incluir la clave e instalarla en su Libreta de **PGPKeys**

Publicar claves en un Servidor de Claves.

Para que otras personas puedan enviarte correos confidenciales sin haberse puesto en contacto antes contigo existen **Servidores de Claves Públicas** que ponen a disposición archivos con *claves públicas PGP* en todo el mundo.

Para que nuestra clave figure en esos Servidores, debemos transmitir la nuestra.

Selecciona la clave en PGPKeys y en el **Menú Server/Send to** elige alguno de los Servidores que existan



Puedes publicar tus claves en varios servidores, repite la misma operación para cada uno de ellos.

Si la clave ha podido ser publicada correctamente en el servidor, aparecerá algo así como:

Key(s) successfully uploaded to Server

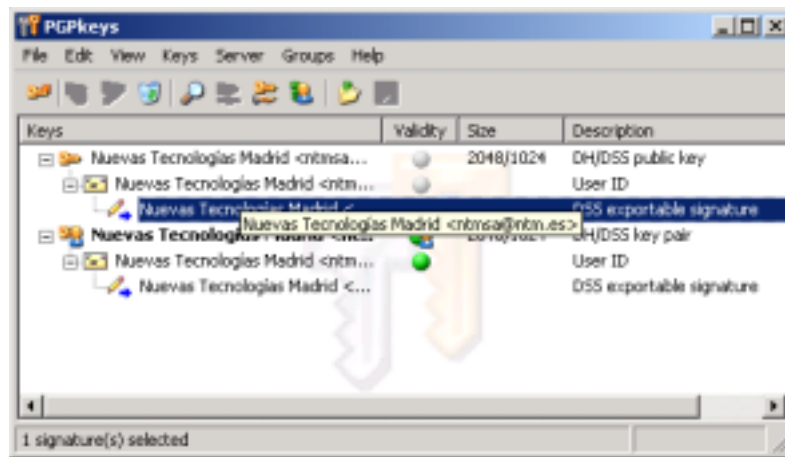
Desde este momento la nueva clave estará disponible en ese servidor, entonces los usuarios deberían buscar dicha clave pública e incluirla en la Libreta de Claves para poder usarla.

Incluir Claves Públicas en PGPKeys

Desde **Outlook**, abre el mensaje que contenga la clave pública enviada, no desde la vista previa, sino en una ventana propia.



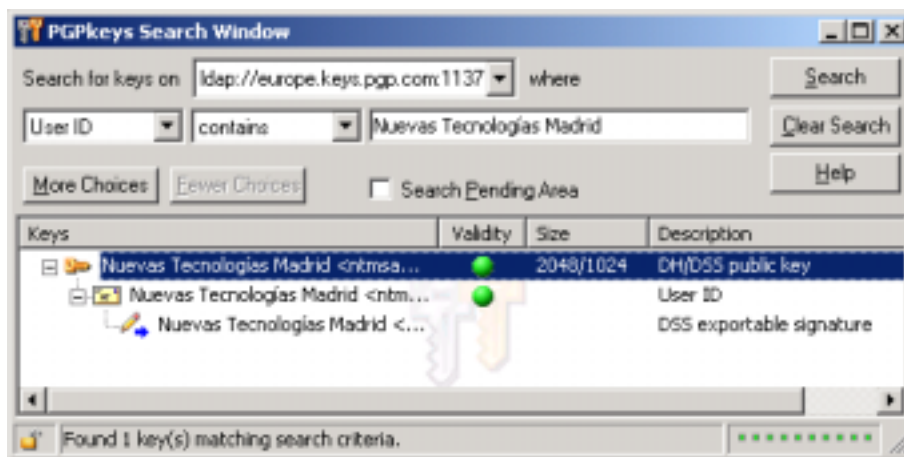
Haz **click en el icono Decrypt PGP...** de la barra de herramientas de **Outlook** y se mostrará la clave pública recibida por mail, pulsa en el **botón Import** y la clave se incluirá en **PGPKeys**



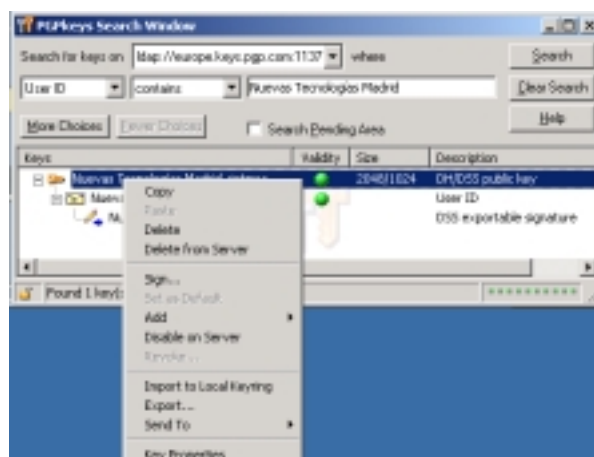
Observa que la clave pública importada tiene **Confianza Restringida (Validity en gris)**

Si lo que queremos es buscar una clave pública en un Servidor de Claves, debemos hacer lo siguiente:

Desde **PGPkeys** en el **Menú Server**, selecciona **Search**:



Selecciona el Servidor de claves donde deseas buscar y escribe el nombre de la clave deseada.



Una vez se haya encontrado, Impórtala, *botón derecho sobre la clave*, y elige *Import to Local Keying*

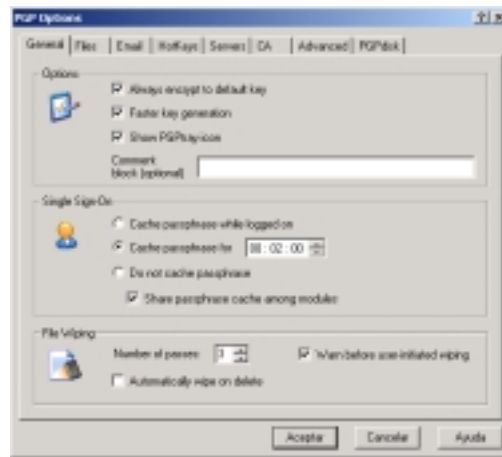
Encriptar y Des-encriptar mensajes.

Obviamente, nada de lo expuesto anteriormente tendría significado, si luego no ciframos los mensajes con las claves generadas o importadas, la creación de un mensaje encriptado no es diferente a uno que no lo sea, sólo tenemos que indicar que se codifique antes de enviarlo.

Supongamos que deseamos enviar un mail encriptado con **PGP** a otra persona, para ello utilizamos Outlook como siempre, pero *antes de pulsar sobre enviar haremos clic en el botón de la barra de herramientas que dice Encrypt PGP ó Encrypt Message PGP* y luego pulsa Enviar.

IMPORTANTE

Cuando se envía un correo encriptado con la clave pública de un destinatario sólo podrá ser leído con la clave privada del propio destinatario, es decir, si te envías un correo de este modo a ti mismo NO PODRAS leerlo, ni tan siquiera aparecerá legible en la bandeja de elementos enviados, para evitar que esto suceda desde el *Menú Edit de PGPKeys selecciona Options y activa la casilla Always encrypt to default key*, de este modo, además de cifrarse el mensaje con la clave pública del destinatario se hará con la propia clave privada y podrás ver los e-e-mail enviados cuando quieras.



Al recibir un mensaje cifrado (lo reconocerás porque siempre comienzan por **BEGIN PGP MESSAGE**, pulsa en el *botón Decrypt PGP* para poder ver su contenido, claro si se dispone de la clave pública suministrada.

El envío y recepción de correos encriptados con **PGP** son algo más lentos que lo normales, antes del envío al servidor SMTP que dispongamos, se realiza una conexión con el Servidor de Claves públicas escogido.

Firmar los mensajes

Todavía nos queda un punto débil. EL hecho de cifrar y descifrar un mensaje no garantiza la autenticidad del mismo, cualquiera que posea la clave pública puede encriptarlo y el receptor del mismo no podrá comprobar si el autor del mensaje ha dado su nombre verdadero o lo ha falsificado. Es el mismo caso que enviar un mensaje normal usando alguno de los programas de las prácticas anteriores, sólo que además encriptado con **PGP**.

La solución a este problema es muy sencilla, **Firma** los mensajes (*Sign Messages PGP*) cuando los envíes de ese modo, como sólo el destinatario conoce su clave privada podrá comprobar la autenticidad del correo. Como verás cuando se firma un correo, una vez se pulsa enviar, se pide a *contraseña o frase de paso para el uso de la clave privada* (en nuestro ejemplo 12345678)

La firma no encripta el mensaje sólo sirve para comprobar la autenticidad. Puedes usar mensajes firmados, encriptados o ambas cosas, ahora eso depende de ti.

¿Qué pasa si no utilizo Outlook?

Bien, **PGP** dispone de *plug-ins* para otros programas de correo, si el que usas no dispone del mismo, puedes escribir el mensaje como lo harías normalmente y luego copiarlo al portapapeles, una vez hecho esto usa la **función Clipboard de PGP** (botón derecho sobre el icono del candado en la bandeja del sistema) y **Encriptalo**, fírmalo o ambas cosas, después lo pegas de nuevo en tu programa de correo y lo envías como de costumbre.

El procedimiento para leer el correo encriptado es el mismo, una vez recibido el mensaje codificado:

lo copias al portapapeles-desencriptar mediante PGP-pegar en el programa de correo.

¿Se pueden encriptar los ficheros adjuntos?

Por supuesto. Podemos utilizar alguna utilidad extra como proteger mediante contraseña un archivo ZIP, ídem si el archivo es de Office, etc. Esta técnica desanimará a alguien que no conozca herramientas para reventar o crackear las contraseñas utilizadas con estos programas, realmente es un juego de niños “sacar” las claves de documentos Office o de archivos ZIP protegidos con contraseñas,

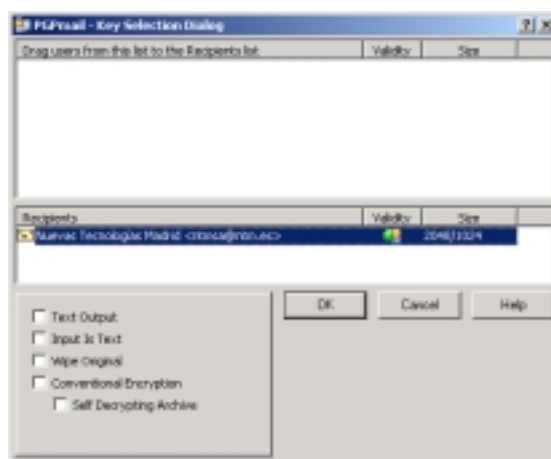
Sin embargo, si los ficheros adjuntos los codificamos como si se trataran de un correo encriptado, sólo el destinatario que conozca la clave pública usada podrá descifrarlos con su clave privada.

Para poder encriptar un archivo adjunto:

Abre **PGPMail** desde el icono de la *bandeja del sistema*



Haz clic en el botón **Encrypt**, luego **selecciona el archivo a encriptar** y pulsa **Abrir**, se mostrará la pantalla con las claves disponibles para la encriptación, **selecciona dicha clave y pulsa OK**



Se creará otro archivo de igual nombre pero con la extensión **.pgp** que podrás enviar como de costumbre con el programa de correo electrónico que uses.

Cuando el destinatario reciba el correo, se abrirá una ventana que le solicitará la contraseña o frase de acceso PGP de su clave privada, sólo así podrá abrirlo.

Como alternativa a **PGP** existe **S/MIME**, programas como *Outlook*, *NetScape* y otros utilizan esta técnica si necesidad de *plug-ins* ni aplicaciones añadidas como es **PGP**. El funcionamiento es muy parecido a **PGP** y la seguridad equiparable totalmente, si bien a mi modo de ver presenta algunas desventajas:

Con **PGP** los usuarios crean y publican sus propias claves, en estos otros los certificados son concedidos por entidades emisoras centralizadas, es decir, el usuario no controla quién o quienes disponen de su clave pública.

Esas organizaciones cobran por la expedición y generación de claves, con **PGP** todo es **GRATIS**

Casi todas están en EEUU, en este país la criptografía está considerada como tecnología militar y las versiones internacionales emplean claves con ciertos límites, son más vulnerables que las generadas con **PGP**

Aunque se conocen algunos ataques contra **PGP**, casi siempre se realizan contra el software propiamente dicho, no contra los correos cifrados. Utilizar un tamaño de clave de 1024 ó 2048 bits puede ser una tarea ilimitada en el tiempo para *destripar* el mensaje, es posible que la CIA, FBI u otros organismos similares dispongan de las máquinas y recursos para intentarlo, lo mas probable es que, primero se intente conseguir la clave privada antes de proceder a un ataque por fuerza bruta del correo codificado, como ejemplo que te sirva lo siguiente:

Un **ordenador que procesa 1 millón de instrucciones por segundo** (ya es de los muy buenos) **tardaría unos trescientos mil millones de años** (300.000.000.000) en des-criptar un mensaje cifrado con PGP, en el que se usó un tamaño de clave de 1024 bits., si se hiciera con 2048 bits tardaría:

300.000.000.000.000.000 años, pronuncia tu la cantidad...

Tristemente existe un troyano "*circulando por ahí*" cuya misión consiste en averiguar la contraseña o frase de acceso de la clave privada, se enmascara como un sonido WAV de soporte para *Sound Blaster*, etc. y recupera la contraseña utilizada para generar la clave privada y la envía junto con el mail o la coloca en servidores FTP. Bueno, si ponemos las medidas necesarias para evitar el acceso a los troyanos, evitaremos el problema.

También nos pueden "*poner*" un **keylogger** para registrar las pulsaciones del teclado, un **sniffer**, etc. Son técnicas siempre contra el almacenamiento de la clave, nunca contra el correo en sí mismo, si proteges tu equipo contra ese tipo de actividades es imposible que se descifren tus correos, aunque si ese tipo de ataques ya se han producido, o bien has caído en la trampa, no te preocupes de tu correo y corre a "*desenchufarte*" de la red (interna o Internet) porque sino, te vendrán males mayores.