

Encriptación de la Información

Tabla de Contenidos

6. Encriptación de la información. Claves simétricas y asimétricas.....	2
6.1 Historia de la Criptografía.....	2
6.2 Introducción a la Criptografía.....	5
Algunos términos importantes en criptografía.....	6
Criptografía simétrica y antisimétrica.....	6
6.3 ¿Qué es PGP?.....	7
Información adicional	17
Firma de otras claves públicas. Anillos de confianza	17



6. Encriptación de la información. Claves simétricas y asimétricas.

6.1 Historia De La Criptografía.

Las organizaciones de poder, a lo largo de la historia, han hecho del secreto de sus comunicaciones un principio fundamental de su actividad. Dicho secreto se intentó proteger mediante la encriptación, es decir, la codificación del lenguaje mediante una clave secreta sólo conocida por la organización emisora del mensaje y el destinatario del mensaje determinado por dicha organización. El anecdotario histórico abunda con ejemplos de batallas e, incluso, guerras supuestamente perdidas o ganadas mediante la interceptación y descryptación de mensajes decisivos entre los centros de poder. El origen de la informática contemporánea durante la Segunda Guerra Mundial parece estar relacionado con los esfuerzos de matemáticos extraordinarios, como el inglés Turing, para desarrollar algoritmos capaces de descifrar los códigos del enemigo.

Por tanto, en cierto modo, no es de extrañar en la era de la información, basada en la comunicación de todo tipo de mensajes, que el poder (y, por tanto, la libertad) tenga una relación cada vez más estrecha con la capacidad de encriptar y descifrar. Hete aquí que lo que era una arcaica tecnología matemática relegada a los dispositivos secretos de los servicios de inteligencia de los Estados se haya convertido, en el espacio de dos décadas, en la tecnología clave para el desarrollo del comercio electrónico, para la protección de la privacidad, para el ejercicio de la libertad en la red y, también, paradójicamente, para nuevas formas de control en la red. La encriptación es el principal campo de batalla tecnológico-social para la preservación de la libertad en Internet.

En Estados Unidos, la supersecreta National Security Agency (con poderes mucho más extensos que los del FBI o la CIA) fue y es la que dispone de la mayor capacidad tecnológica de encriptación/desciframiento del planeta. Tal importancia se le atribuyó a esta tecnología que se clasificó en el rubro de armamento que no se podía exportar fuera de Estados Unidos sin un permiso especial del Departamento de Defensa. De modo que enviar una fórmula matemática a un colega fuera de Estados Unidos se convirtió en un delito penado por la ley. Más aún, la NSA tuvo buen cuidado de cooptar, contratar o amenazar a aquellos matemáticos que se adentraron en ese complejo campo de investigación. Pero hubo quienes resistieron a la presión y se atrevieron a desarrollar fórmulas autónomas de encriptación. Tal fue el caso del legendario Whitfield Diffie, un matemático sin carrera académica, obsesionado por la encriptación desde joven, que, en colaboración con un profesor de Stanford, Marty Hellman, y con la ayuda de un estudiante de Berkeley, Ralph Merkel, descubrió, a mediados de los setenta, nuevas formas de encriptación y, pese a las presiones del gobierno, las publicó. Su genialidad consistió en el llamado principio de la doble clave o clave pública. Hasta entonces, toda clave se basaba en un algoritmo que permitía cifrar un mensaje de forma difícil de reconocer y, al mismo tiempo, reconstruirlo en su sentido original basándose en el conocimiento de dicho algoritmo. Este método

tradicional requería una centralización total del sistema de claves únicas y, por tanto, era vulnerable a quien penetrara en esa base de datos. Lo que se adaptaba al secreto militar de una organización separada de la sociedad no era practicable en una sociedad en que todo se basaba en comunicación electrónica y en que los individuos, las empresas y las propias instituciones necesitaban una protección cotidiana de sus mensajes para garantizar su privacidad y su autonomía. Esto requería una descentralización e individualización del sistema de encriptación. Mediante el principio de la doble clave, cada persona u organización tiene dos claves de encriptación (o sea, códigos informáticos que permiten transformar el texto de un mensaje en un sistema digital que altera el sentido lingüístico y lo puede volver a reconstruir).

Una de las claves es pública en el sentido de que es asignada al originario/destinatario de un mensaje y que se conoce, mediante un listado, qué clave corresponde a quién. Pero, sin el conocimiento de la clave privada, es muy difícil, si no imposible, descifrar el mensaje. Esa otra clave es específica a cada individuo u organización, sólo quien la detenta la puede utilizar, pero sólo sirve con relación a su clave pública en la que recibe el mensaje. Mediante este ingenioso sistema matemático, se garantiza a la vez la generalidad del cifrado y la individualidad de su desciframiento.

Como en otros temas de la historia de Internet, el poder de encriptación descentralizado recibió dos usos. Por un lado, fue comercializado. Por otro, sirvió como instrumento de construcción de autonomía de redes de comunicación. La comercialización, en su origen, corrió a cargo de tres matemáticos de MIT o asociados a MIT, Rivest, Shamir y Adleman, que perfeccionaron el sistema de encriptación Diffie-Hellman y, con ayuda de hombres de negocios más avezados que ellos, patentaron y desarrollaron la tecnología de encriptación RSA, que sirvió de base para buena parte de las tecnologías de protección de las comunicaciones electrónicas que se utilizan hoy en día.

En efecto, a partir del sistema de doble clave, no sólo se puede preservar el secreto del mensaje sino establecer la autenticidad de su originario. De modo que la encriptación es la base de las firmas digitales que permiten el desarrollo del comercio electrónico en condiciones de relativa seguridad. En efecto, si la gente pudiera encriptar sus mensajes en lugar de enviar un mensaje por correo electrónico con su número de tarjeta de crédito abierto a todo el mundo, no tendrían por qué temer su interceptación y mal uso. Esto es, en realidad, lo que hacen las grandes empresas con capacidad de encriptación para transferir fondos y comunicarse mensajes confidenciales. Pero la tecnología de autenticación y firma digital se está difundiendo bajo el control de las empresas e instituciones, sin transmitir la capacidad autónoma de encriptación a los usuarios. Ello es así, por un lado, porque la comercialización de la tecnología creó un sistema de patentes que la hacen costosa en su uso comercial.

Pero, más importante todavía, las administraciones de casi todos los países han puesto enormes cortapisas a la difusión de la tecnología de encriptación por lo que ello representa de posible autonomía para los individuos y organizaciones contestatarias con respecto a los gobiernos y a las grandes empresas. De ahí que se desarrollara una segunda tendencia, de matriz libertaria, para proporcionar a los ciudadanos la tecnología de encriptación. Un personaje fundamental en este sentido fue Phil Zimmerman, otro matemático rebelde que, en 1991, en respuesta a los intentos del Senado estadounidense de prohibir la encriptación en el marco de la legislación antiterrorista,

difundió en Internet su sistema PGP (Pretty Good Privacy). PGP está también basado en principios similares a los inventados por Diffie y Hellman, pero en lugar de crear un directorio de claves públicas se basa en una red autónoma de autenticación en la que cada persona autentifica con su firma digital a una persona que conoce y así sucesivamente, de modo que, con conocer bien a una persona de la cadena, dicho conocimiento es suficiente para saber que la identidad del detentor de una determinada clave pública es fidedigna.

Zimmerman pertenecía a una red informal de criptógrafos que se reunían anualmente en un movimiento contracultural (autodenominados cypherpunks) y que aumentaron su número e influencia con el advenimiento de Internet. Uno de los participantes más respetados en este movimiento tecnolibertario es John Gilmore, uno de los pioneros de Sun Microsystems, que, en 1990, creó, junto con Mitch Kapor y John Perry Barlow, la Electronic Frontier Foundation, una de las principales organizaciones de defensa de las libertades en el mundo digital. Es significativo el discurso que sobre la encriptación pronunció John Gilmore en 1991 en una reunión sobre "ordenadores, libertad y privacidad":

"¿Qué tal si creáramos una sociedad en la que la información nunca pudiera ser registrada? ¿En la que se pudiera pagar o alquilar un vídeo sin dejar un número de tarjeta de crédito o de cuenta bancaria? ¿En la que se pudiera certificar que tiene permiso de conducir sin dar su nombre? ¿En la que se pudiera enviar o recibir un mensaje sin revelar la localización física, como una casilla postal electrónica? Éste es el tipo de sociedad que quiero construir. Quiero garantizar, con física y matemáticas, no con leyes, cosas como la verdadera privacidad de las comunicaciones personales [...] la verdadera privacidad de los expedientes personales [...], la verdadera libertad de comercio [...], la verdadera privacidad financiera [...] y el verdadero control de la identificación" (citado por Levy, 2001; pág. 208).

Esta utopía de la libertad sin instituciones, mediante el poder de la tecnología en manos de los individuos, es la raíz de los proyectos libertarios en la sociedad de la información. Es una poderosa visión que informó proyectos empresariales y sociales a lo largo de la siguiente década. Por ejemplo, uno de los personajes más innovadores del mundo de la criptografía, David Chaum, desarrolló el dinero digital sin huella personal y fundó en Holanda una empresa, Digicash, para comercializar su invento. La empresa fracasó por falta de apoyos en el mundo empresarial, que siempre desconfió de su carácter visionario.

Pero, del mundo de los cypherpunks, como se autodenominaron los anarcocriptógrafos, salieron tecnologías de protección de la privacidad a través de los diseños de anonimato en la red mediante los remailers, es decir, programas que retransmiten automáticamente los mensajes a través de un circuito de servers hasta borrar los orígenes de procedencia de los mensajes (www.anonymizer.com). El más avanzado diseñador de estos remailers en los años noventa fue, en 1993, el informático finlandés Jufi Helsingius, que desarrolló sistemas de remail desde su casa de Helsinki para permitir la libre comunicación de alcohólicos en rehabilitación sin riesgo a ser identificados. Creó Penet, un sistema que opera en una máquina UNIX con un 386, y sin ningún tipo de publicidad empezó a recibir miles de mensajes de todo el mundo que, transitando por su sistema, borraban todo rastro. La ingenuidad de hacker de Helsingius acabó obligándolo a cerrar su servidor cuando una querrela criminal contra él, efectuada desde Los Ángeles, llevó a la policía finlandesa hasta su casa. Negándose a ejercer la censura y a denunciar los orígenes de las rutas que

llegaban a su servidor, prefirió cerrar Penet. Sin embargo, la idea de anonimizadores continuó desarrollándose y, en estos momentos, hay numerosas empresas (de las cuales la más conocida es la canadiense Zero Knowledge) que permiten a cualquiera utilizar Internet sin dejar huella (www.silentsurf.com).

Si tal posibilidad se generalizara, la libertad de las personas para comunicarse, expresarse y organizarse sería total. De ahí las diversas iniciativas en los gobiernos de todo el mundo para controlar la capacidad de encriptación y para limitar su uso.

Sin embargo, los términos del debate no son tan claros, porque la tecnología de encriptación sirve a la vez para proteger la privacidad (garantizando, por tanto, la libertad de comunicación) y para autenticar lo originario de un mensaje, permitiendo, por consiguiente, individualizar los mensajes (www.qsilver.queensu.ca/sociology). Más aún, en los movimientos contestatarios en torno a Internet, tales como la red Freenet, se produjo, en el año 2000, una evolución desde la defensa del derecho a encriptar (para proteger la privacidad del ciudadano) hacia el derecho a descifrar (para permitir el acceso de los ciudadanos a la información detenida por gobiernos y empresas). Ahora bien, en cualquier caso, la práctica de ambos derechos pasa por la capacidad autónoma de la gente para utilizar las tecnologías de encriptación. Esto significa, por un lado, el libre desarrollo de tecnologías de encriptación en comunicación horizontal del tipo PGP, a saber, con doble clave y autenticación mediante redes de confianza interpersonal. Por otro, requiere la capacidad de libre difusión de la información de tecnologías de encriptación en la red.

6.2 Introducción A La Criptografía.

Por "criptografía" se entiende un conjunto de técnicas que tratan sobre la protección de la información frente a observadores no autorizados.

La palabra criptografía proviene del griego *kryptos*, que significa esconder y *gráphein*, escribir, es decir, "escritura escondida". La criptografía ha sido usada a través de los años para mandar mensajes confidenciales cuyo propósito es que sólo las personas autorizadas puedan entenderlos.

Alguien que quiere mandar información confidencial aplica técnicas criptográficas para poder "esconder" el mensaje (lo llamaremos cifrar o encriptar), manda el mensaje por una línea de comunicación que se supone insegura y después solo el receptor autorizado pueda leer el mensaje "escondido" (lo llamamos descifrar o desencriptar).

Pero la "confidencialidad" no es lo único que permite la criptografía. También resuelve otros problemas de seguridad, como certificar la "autenticidad" (firmar mensajes) e "integridad" (comprobar que la información

transmitida no ha sido modificada) de la información.

PGP (del que luego daré más detalles) permite por ejemplo encriptar un mensaje para uno o varios destinatarios, y / o firmarlo, para que cualquiera pueda comprobar de quién es y que permanece tal y como fue emitido.

Algunos términos importantes en criptografía

- Texto claro: mensaje o información sin cifrar
- Ciphertext: mensaje cifrado
- Criptosistema: sistema completo formado por textos claros, ciphertexts, claves de cifrado, y algoritmos de cifrado - descifrado.
- Criptoanálisis: técnica que intenta comprometer la seguridad de un criptosistema, o bien descifrando un texto sin su clave, u obteniendo ésta a partir del estudio de pares texto claro - ciphertext.

Criptografía simétrica y asimétrica

Existen dos tipos fundamentales de criptosistemas:

- **Criptosistemas simétricos o de clave privada:** se utiliza la misma clave para cifrar y para descifrar, que ha de ser conocida por las partes autorizadas en la comunicación, y solo por éstas.
- **Criptosistemas asimétricos o de clave pública:** emplean una doble clave ($K_{pública}$, $K_{secreta}$) de forma que una cifra y la otra descifra, y en muchos casos son intercambiables.

La **criptografía simétrica** por lo tanto es a priori más sencilla... ¿quién no ha utilizado alguna vez un código con algún amiguete para decirse algo sin que nadie más lo entienda?

Sin embargo, aunque los algoritmos son más sencillos y generalmente rápidos, tiene varios problemas, como el hecho de que necesitamos un "canal seguro" para transmitir o acordar la clave.

La **criptografía asimétrica** en cambio, es más potente, y además de permitirnos la confidencialidad, nos permite un servicio de autenticidad y asegurar la integridad de los mensajes, sin necesidad de transmitir una clave secreta (solo ha de ser conocida la pública, que puede transmitirse por un canal inseguro pues no hay problema en que sea conocida).

Por supuesto, la elección de las claves y los algoritmos que las usan para cifrar y descifrar en criptografía asimétrica no es en absoluto trivial. Han de tener características muy concretas. La clave secreta y la pública han de estar profundamente relacionadas (lo que una encripta la otra lo desencripta), y sin embargo ha de ser "imposible" obtener una de la otra.

Partiendo de que un buen criptosistema asimétrico cumple con estas características, veamos con un ejemplo

cómo se hace uso de estas propiedades para conseguir los servicios mencionados:

Autenticación e integridad (firma digital):

¿Cómo sabemos que el mensaje enviado por HavoC lo ha escrito realmente HavoC?

Por las propiedades de las claves y los algoritmos, un mensaje cifrado por la clave secreta de HavoC, solo puede ser descifrado por su clave pública. Por tanto, HavoC envía el mensaje sin cifrar y además repite el mensaje cifrado con su clave secreta. Si la clave pública de HavoC descifra esa parte cifrada y coincide con el mensaje sin cifrar recibido, se puede asegurar que solo HavoC ha podido generarlo (pues es la única que conoce la clave secreta dual de la pública) y además el mensaje no ha sido modificado durante la comunicación (integridad).

Confidencialidad:

¿Cómo hacemos que un mensaje enviado a Hann solo pueda entenderlo Hann?

Un mensaje cifrado por la clave pública de Hann, solo puede ser descifrado utilizando la clave secreta dual de la misma. Por tanto, si ciframos un mensaje con la clave pública de Hann y se lo enviamos de esta forma, solo será "legible" por él, tras utilizar su clave secreta para descifrarlo.

6.3 ¿Qué Es PGP?

PGP (Pretty Good Privacy) se trata de un proyecto iniciado por Phill Zimmerman en 1993, cuando se carecía de herramientas sencillas pero a la vez potentes que permitiesen a los usuarios "comunes" hacer uso de una criptografía seria.

Con el tiempo PGP se ha convertido en uno de los mecanismos más populares para utilizar criptografía, tanto por usuarios particulares como grandes empresas. Se ha publicado su código fuente, y se permite su uso gratuitamente para fines no comerciales.

Se trata ya de un estándar internacional, RFC 2440, y dispone de numerosas aplicaciones (codificación de almacenamiento, codificación automática de tráfico TCP/IP, etc). Principalmente, intentaré explicar en este texto en qué consiste PGP, y sus dos funciones originales y más importantes: asegurar la confidencialidad de un texto, y la

autenticación de un emisor frente a su receptor (firma digital).

Funcionamiento De PGP

PGP funciona con criptografía asimétrica (aunque por cuestiones de eficiencia también hace uso de criptografía simétrica), y su punto fuerte radica en la facilidad que ofrece a los usuarios comunes para generar las claves (algo que como antes he mencionado no es en absoluto trivial) y gestionarlas.

PGP proporciona lo que se denomina "anillo de claves" (llavero), que es un único fichero donde el usuario puede guardar todas sus claves, con facilidad para realizar inserción y extracción de claves de manera sencilla.

Además proporciona un mecanismo de identificación y autenticación de claves (certificación de que una clave pública es realmente de quien dice que es) para evitar los "ataques de intermediario". Estos ataques consisten en que una persona que intervenga el canal de comunicación nos proporcione una clave pública falsa del destinatario al que deseamos enviar el mensaje. En ese caso, encriptaríamos con dicha clave, y el atacante podría desencriptar la información, encriptarla con la verdadera clave pública que ha intervenido, y enviársela al destinatario sin que nadie se percate de su presencia.

Para autenticar claves, PGP permite que los usuarios "firmen claves", por lo que podemos confiar en la autenticidad de una clave siempre que ésta venga firmada por una persona de confianza. Así la "autoridad de certificación" de otro tipo de sistemas (entidades que aseguran la autenticidad de las claves), en PGP son los propios usuarios.

Además, cada clave tiene una "huella digital" (fingerprint), que se trata de una secuencia lo suficientemente larga para que sea única, pero lo suficientemente corta para poder ser comunicada de viva voz o escrita en papel. Así, si queremos asegurarnos de la autenticidad de una clave, solo hemos de preguntar (por ejemplo, por teléfono o por IRC) a su autor la huella digital de su clave.

Como ejemplo, mi clave pública se puede obtener en el servidor de oficial de PGP (keyserver.pgp.com) y la huella digital es:

A119 1272 002F 37B4 62ED 7A9A 694B 0D34 312E DD52

Si la clave que alguno tiene en su anillo como mía no tuviese esta huella digital, es que no es verdadera (alguien

podría haberla subido a keyserver en mi lugar o a una web indicando que es mi clave).

Cuando una clave secreta queda comprometida, o se sustituye por una nueva (por ejemplo porque el valor de la información que deseamos proteger hace necesaria la utilización de un algoritmo más seguro o de clave más larga), puede ser revocada por su autor. Solo tiene que generar y distribuir un "certificado de revocación" que informará a los usuarios de PGP que esa clave ya no es válida. Por supuesto, para poder emitir dicho certificado es necesario tener la clave secreta.

Como cualquier herramienta, PGP proporciona un nivel de seguridad muy bueno y gran rendimiento si se utiliza correctamente. Sin embargo un uso inadecuado puede convertirlo en algo completamente inútil. Para que ésto no ocurra debemos cuidar algunos aspectos:

- **Escoger contraseñas adecuadas:** PGP para extraer del anillo una clave privada requiere al usuario una contraseña. Por supuesto, ésta ha de ser segura (memorable, larga, aleatoria, complicada, etc)
- **Proteger los ficheros sensibles:** hemos de proteger los anillos de claves (PUBRING.PKR y SECRING.SKR), tanto de intrusos como de su pérdida (conviene tener backup).
- **Firmar sólo las claves de cuya autenticidad estemos seguros:** hemos de ser cuidadosos para que las "redes de confianza" funcionen adecuadamente, o podemos certificar claves falsas (lo que nos engañaría a nosotros y a aquellos que confíen en nosotros como autoridad de certificación).

Instalación De PGP Y Generación De Claves

Para obtener la última versión de PGP solo tiene que visitar la página web de PGP internacional:

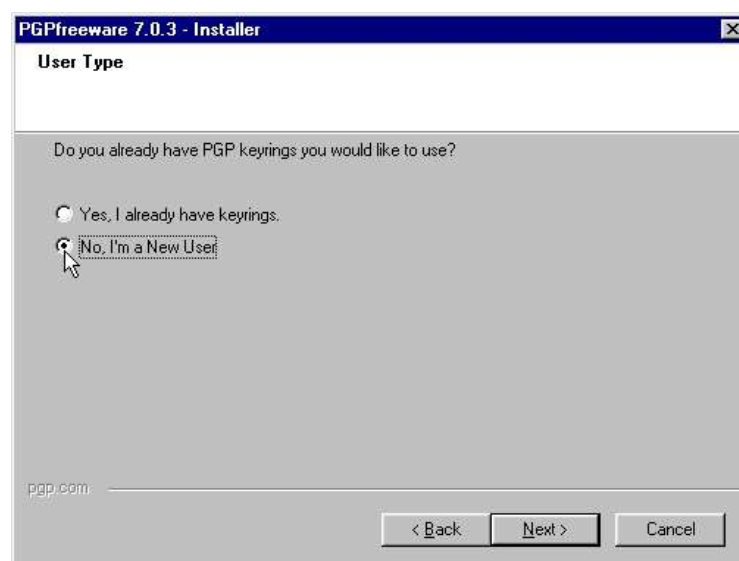
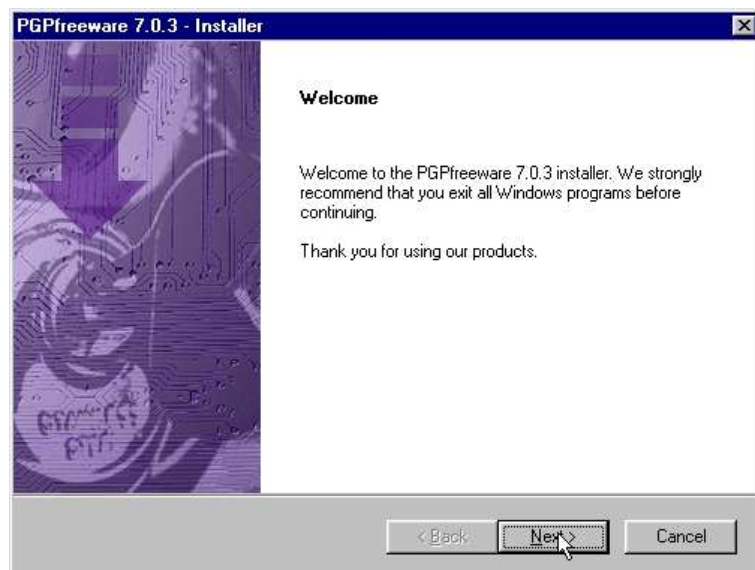
<http://www.pgpi.org/products/pgp/versions/freeware/>

Seleccione su sistema operativo y a continuación la versión más reciente del software. Todos los que encuentre en dicho link serán versiones gratuitas ;)

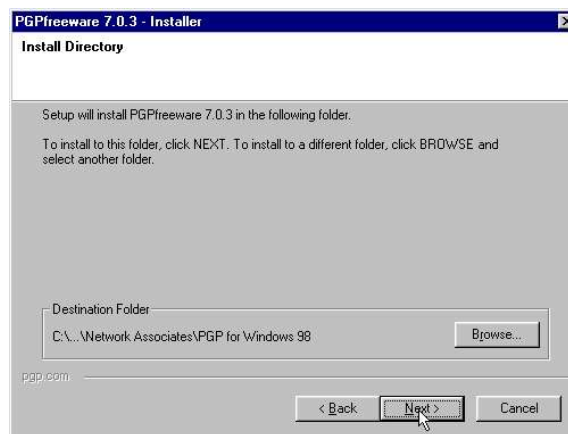
A continuación describiré en diez pasos el proceso para un usuario novato, es decir, instalación y generación de las claves. Este ejemplo es para una versión PGP FreeWare 7.0.3 sobre Windows 2000, aunque no varía en exceso para versiones posteriores.

1. Haga doble clic sobre el icono de instalación (en este caso PGPfreeware7.0.3.exe). El programa lanzará un

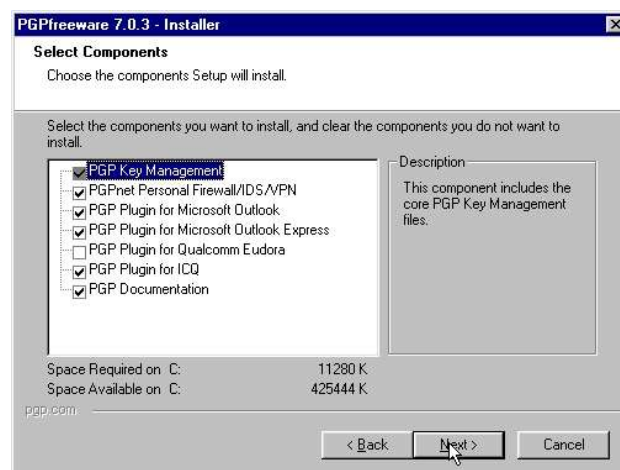
asistente que nos guiará durante el resto del proceso:



- Indique al programa la opción "No, I'm a New User". Si ya fuese usuario de PGP previamente y tuviese algún anillo de claves, escogería la otra opción.
- Mediante el botón "Browse..." puede escoger la carpeta en la que se grabarán los ficheros de PGP. Si únicamente pulsa "Next" los grabará en la carpeta por defecto, dentro de "Archivos de Programa" (recomendable).



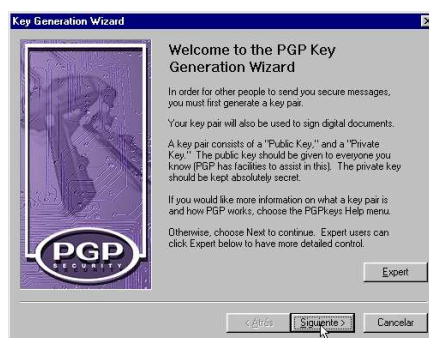
4. Seleccione los componentes que se instalarán. Necesariamente ha de seleccionar "PGP Key Management" (el núcleo o corazón de la aplicación). Si utiliza Outlook, Outlook Express, Eudora, o ICQ y desea utilizar PGP con estas aplicaciones, también ha de marcar sus casillas. Por último, la "PGP Documentation" es siempre recomendable.



5. El programa comienza a instalar los ficheros y aparecerán algunas pantallas de confirmación - publicidad. Paciencia y algún clic en "Next".

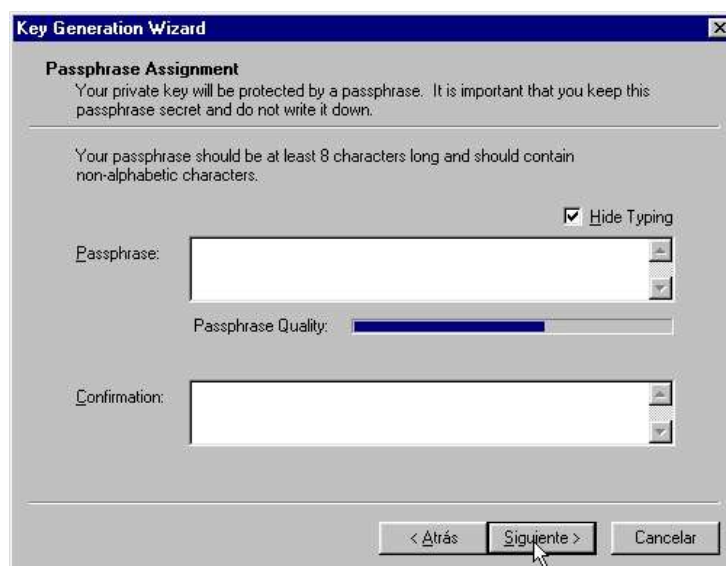


6. Si usted ha elegido la opción de nuevo usuario, el programa de instalación lanzará un nuevo asistente, en esta ocasión para generar sus anillos de claves (y proporcionarle su clave pública y privada).

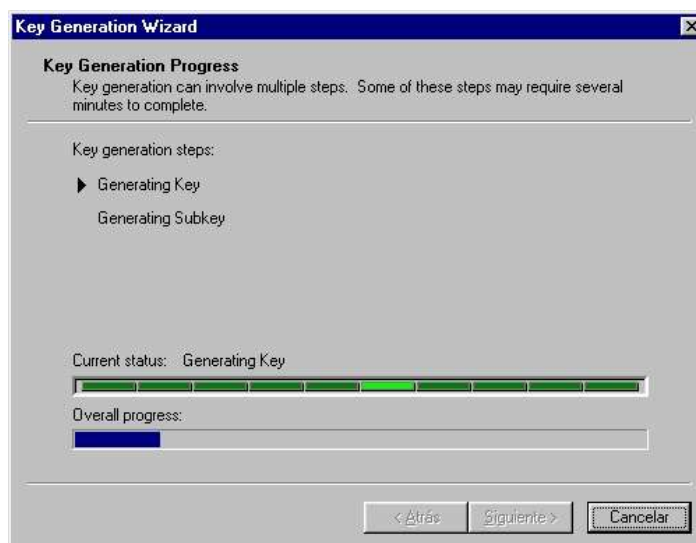


7. Para generar su clave pública, ha de proporcionar el nombre y dirección de correo electrónico que se asociará a dicha clave.
8. Para poder acceder a su clave secreta, tendrá que utilizar una "passphrase" o contraseña. En este paso es cuando tendrá que elegirla. Procure que tenga una calidad aceptable (según la escriba irá aumentando el marcador de "calidad" según la aleatoriedad, longitud, etc). Influyen las mayúsculas y minúsculas y se permiten espacios. Confirme la contraseña escogida, y pulse "Siguiente".



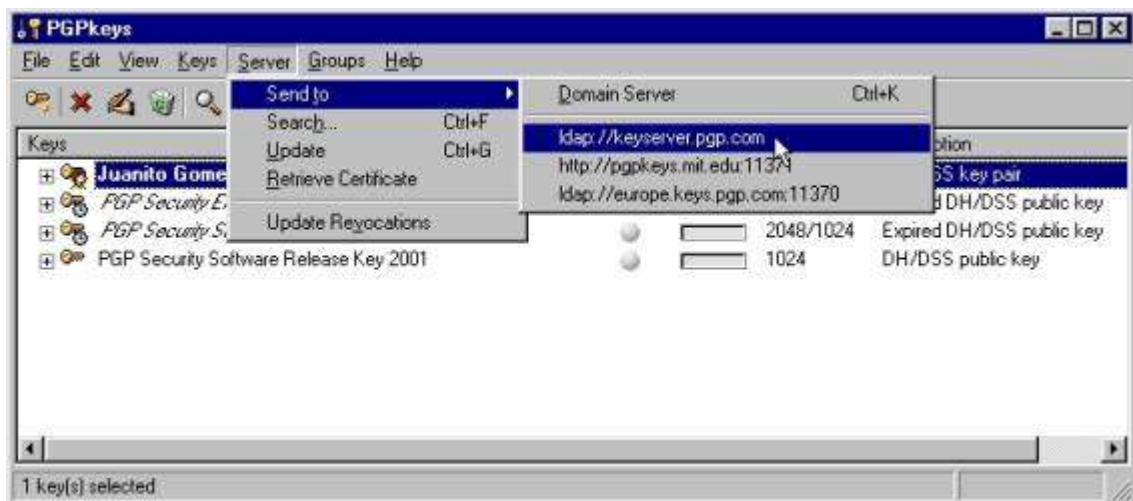


9. El asistente generará las claves. Como he explicado en anteriores apartados, la generación de un par de claves asimétricas no es trivial, por lo que en ordenadores lentos esto puede llevar unos minutos.



10. Finalmente aparecerá la pantalla de confirmación, y tras pulsar "Finalizar" nos pedirá reiniciar el equipo. Por supuesto, hemos de aceptar para que la aplicación se instale correctamente y podamos empezar a usarla.

Una vez creadas las claves, podremos acceder al anillo de claves públicas mediante la aplicación "PGP Keys", en el menú de inicio, o pulsando sobre el icono de PGP en el systray. Si queremos enviarlas al servidor de claves públicas de PGP para que todo el mundo tenga acceso, podemos hacerlo a través de esta aplicación, seleccionando nuestra clave y haciendo clic sobre Server -> Send to -> Idap://keyserver.pgp.com (por supuesto, con conexión a internet).



GNUPG , En Que Consiste.

La idea que existe detrás de GnuPG es la de proporcionar un sistema eficaz de confianza y privacidad (al igual que PGP, sólo que GnuPG es software libre y ofrece mayor tranquilidad a los usuarios). GnuPG es un reemplazo libre al sistema PGP (Pretty Good Privacy) que hace tiempo cerró al público su desarrollo y del que se descubrió hace no mucho una puerta trasera en una de sus últimas versiones que permitía romper cualquier clave. GnuPG es casi totalmente compatible con PGP.

Cada persona dispone de dos llaves (también llamadas claves) llamadas **secreta** (o privada) y **pública**. Estas dos llaves son, al fin y al cabo, dos ficheros de ordenador (que llamaremos secreta.key y publica.key). Podemos entender estas dos llaves de la forma siguiente: la **llave pública** es nuestro buzón de correo postal (el de toda la vida) y la **llave secreta** es la llavecita de ese buzón. Nos interesará que la mayor cantidad de gente disponga de nuestra dirección (buzón/llave pública) pero la llavecita (llave secreta) la guardaremos para nosotros. Para completar el símil, supongamos un mundo en el que sólo se envían postales. Entendemos que, en general, los empleados y carteros de Correos actúan de buena fe y no se dedican a leerlas o copiar las direcciones de remitentes y escribir más tarde suplantando identidades.

Pero todos sabemos que siempre habrá gente que se aproveche de la facilidad que ofrece este sistema y que intentará por todos los medios conocer la correspondencia de sus vecinos. Las razones para espiar de esta forma van desde motivos industriales/comerciales hasta el clásico intrusismo.

Este mundo imaginario representa Internet en el apartado de los correos electrónicos y la transmisión de la

información en general. En la mayoría de los casos, los datos circulan sin protección de ningún tipo y cualquier persona que tenga conocimientos y tiempo necesario puede dedicarse a espiar la correspondencia pública de los ciudadanos. Es más, por si eso fuera poco, es trivial suplantar la identidad de otra persona. Mi experiencia personal es bastante dura en este aspecto pues he sufrido ambos problemas.

Hoy en día es cada vez más sencillo interceptar las comunicaciones entre varias partes sin que éstas se den cuenta. Esto es debido a la reproducibilidad sin pérdida de los datos digitales ya que copiar una transmisión mientras ésta se está realizando puede resultar inadvertida para los implicados en la comunicación. Quizá en un futuro podamos emplear la criptografía cuántica basada en la rama homónima de la Física que defiende la imposibilidad de ver un sistema cuántico sin dejar marcas deladoras. De esta forma, el destinatario sabría si alguien ha intentado espiar la transmisión porque el estado cuántico de un sistema adjunto al mensaje revelaría esto mismo. Saber si le están espiando a uno es muy importante a la hora de escoger un canal seguro de comunicación.

Para evitar esta situación de desamparo existe desde hace tiempo un nuevo sistema de envío de mensajes, que en nuestro mundo imaginario podría tomar la forma de 'postal dentro de sobre', de manera que sólo el receptor tiene acceso al envío efectuado debido a que la única llave disponible del buzón la conserva él además de gozar de la intimidad que asegura el sobre que contiene a la postal (supongamos un sobre caja fuerte). Y para asegurarse de que realmente la carta la envía la persona que aparece en el remite, al final del texto hay siempre una suerte de frase escrita, en color verde y con letras góticas -por ejemplo-, y que sólo el remitente sería capaz de escribir.

Aunque hay personas que acusan a los que utilizan la criptografía de conspi-paranoicos lo cierto es que ya hay pruebas de sistemas de espionaje a escala mundial.

Nuestro consejo es escribir siempre esa *extraña frase verde* que nos identifica claramente (nadie hace los ribetes de la G gótica como nosotros, por poner un ejemplo) -esto es la firma- y meter la postal en un sobre sólo si se trata de información confidencial -esto es la encriptación.

Pasos a seguir para tener nuestro par de llaves secreta/pública.

1. Instale GnuPG. Prácticamente todas las distribuciones modernas de GNU/Linux lo incorporan. En caso contrario visite <http://www.gnupg.org> y descargue la versión apropiada para su sistema.
2. Ejecute desde su usuario normal `$ gpg -gen-key`
Nota: la primera vez que se ejecuta un comando con gpg se crea el directorio `/.gnupg` y no se hace nada más así que si es su caso tendrá que volver a ejecutar
`$ gpg -gen-key`
para confirmar la acción.
3. en la primera pregunta seleccione la opción 1) (Posibilidad de firmar y encriptar)



1. en la segunda pregunta seleccione 1024 bits (robustez de la encriptación)

Nota: cuanto mayor sea el nº de bits, más fuerte será la encriptación pero mayor será el tamaño de la clave pública y los productos derivados (la relación no es lineal)

2. en la tercera pregunta cada uno elegirá lo que le convenga. Si es la primera llave que fabrica, es mejor poner un año de límite, si planea hacerlo en serio, elija 0 (nunca caduca)

3. confirme que todo es correcto

4. Nombre y Apellidos: Felipe Pérez López

5. E-mail: felipeperezlopez@midominio.org

Comentario: opcional. La gente suele poner un pseudónimo o algo parecido. Yo puse la dirección de mi página web.

6. confirmación

7. la clave es lo más importante. Se recomienda una frase de una seis palabras o más. No es realmente necesario meter caracteres raros porque la dificultad de romper, utilizando la fuerza bruta, un código del que no sabemos su longitud y que puede llegar a varias frases es enorme no importa el tipo de caracteres.

8. empieza la construcción de las claves. Se recomienda generar 'entropía' mediante el uso del ratón o el teclado. Tras unos segundos se ha generado el par de llaves.

4. Generación de la llave pública en formato ASCII para su libre distribución:

1. Escriba `$ gpg -a --export dato > publica.key`

donde **dato** es el nombre de pila de usted, un apellido o su dirección de correo electrónico (recuerde lo que escribió mientras fabricaba las claves)

Nota: este fichero es lo que puede distribuir a los cuatro vientos. Póngala en su página web o un servidor de llaves públicas como <http://www.keyserver.net>.

Nota 2: el parámetro -a sirve para que la salida se realice en formato ASCII, si prefiere distribuir su llave pública en binario no añada este parámetro.

Mi llave pública puede encontrarse en <http://www.indetec.tk/chema.gpg>

2. Importar una llave pública de otra persona:

3. Consiga el fichero de la llave pública de esa persona y escriba:

4. `$ gpg --import otrapublica.key`



Información adicional

Siempre que se nos pida una contraseña (al firmar un correo saliente o leer un correo encriptado para nosotros), ésta será la famosa frase de cuando creamos el par de llaves. Es importante que no se nos olvide esta clave, de lo contrario tendremos que fabricarnos otro par de llaves y asegurarnos de que la gente actualiza nuestra llave pública en sus ordenadores (Aquí no hay nada para averiguar la frase del estilo 'dime el nombre de tu madre y te enviaremos la clave a tu correo'). Dependiendo del cliente de correo que utilicemos, podremos configurar más o menos detalladamente aspectos de la interacción de éste con GnuPG.

Firma de otras claves públicas. Anillos de confianza

Yo puedo generar un par de llaves secreta/pública haciéndome pasar por otra persona y ofrecer una seguridad ficticia a los conocidos de esa otra persona (recordemos que suplantar la dirección de correo es tan fácil como editar las preferencias de nuestro cliente de correo).

Por ello, es bueno 'premiar' aquellas llaves públicas que son claramente fidedignas. Este acto de premiar se conoce como 'firmar la llave pública con la llave privada/secreta de uno mismo' (no confundir con firmar un correo). Cuando firmamos un correo estamos diciendo 'este correo es mío'. Cuando firmamos una llave pública estamos diciendo 'yo de esta llave pública me fío'. Naturalmente, si yo recibo una clave pública (un fichero) firmada por gente desconocida para mí, seguirá estando marcada como 'UNTRUSTED'. No es digna de confianza ni la llave pública ni los correos firmados por la llave secreta asociada (aunque ya tenemos más que antes) porque yo no he dado ninguna confianza a esas otras personas y en este sentido la transitiva es vital. Pero si yo he firmado las llaves públicas de las personas que, a su vez, han firmado otra llave pública de un n-personaje, la llave pública de ese n-personaje tendrá cierta confianza por mi parte. Cuando firmamos una llave pública se nos ofrecen varias opciones.

- Podemos decir que 'creemos' que esa llave pública es de la persona correcta pero no hemos hecho ninguna comprobación.
- Podemos decir que 'seguramente' sea fiable porque hemos realizado alguna comprobación.
- podemos decir que 'sin lugar a dudas' ya que nos hemos asegurado totalmente.

Ahora bien, sólo en el caso de que nos hayamos visto personalmente y letra por letra me haya dictado el contenido de su llave pública, nunca deberemos otorgar nuestra plena confianza a una llave pública. Aquí radica toda la fuerza de este sistema; en la **confianza**. Si yo soy un incauto y voy firmando llaves públicas ajenas con mi llave secreta sin previa comprobación (aunque sea mínima) puedo actuar como un virus si otras personas confían en mí y aceptan como válidas y dignas de confianza las llaves públicas que yo he firmado sin ton ni son.

Existen organismos en internet (o empresas privadas) que se encargan de firmar llaves públicas de empresas, colectivos y particulares. El objetivo es proporcionar seguridad y confianza en las transacciones electrónicas. Una persona pensará 'si Verisign ha firmado esta llave pública, será que es fiable y por tanto, estoy mandando dinero a la

persona correcta'. Lo cierto es que todo depende de la confianza que tengas en una empresa privada.

Si desea firmar una llave pública con su llave privada ejecute:

```
$ gpg --sign-key dato
```

donde "dato" es el nombre de pila, un apellido, el comentario o la dirección de correo electrónico (lo más recomendable) de la llave pública. Tras ejecutar este comando, se le harán unas preguntas para concretar la confianza que desea otorgar a esa llave pública.

Si tiene dudas sobre los datos de las llaves públicas almacenadas, pruebe a ejecutar (prepárese para un volcado enorme de información con una tubería y un paginador):

```
$ gpg --list-public-keys
```

Una vez firmada con su llave secreta, esta llave pública, si es distribuida por Internet (puede generar el fichero correspondiente ejecutando `$ gpg -a -export dato > publica.key`), gozará de mejor imagen que la misma llave pública sin firmar. Por supuesto, una persona puede generar miles de pares de llaves pública/privada y firmar con todas ellas la firma que él quiere usar. Esta maniobra sólo funcionará si una persona que reciba esa llave pública sobada se cree que todas esas personas (en realidad ficticias) realmente firmaron esa llave. Como es probable que no reconozca dentro de su anillo de confianza a ninguna de ellas, su sistema GnuPG no le otorgará mayor confianza que una llave pública sin firmar.

Huella Dactilar O Key Fingerprint

La Huella dactilar o *Key fingerprint* es un resumen de la llave pública de uno mismo. Su utilidad es variada. Por ejemplo, sirve para identificar unívocamente una llave pública. Los programas PGP/GPG tienen un algoritmo que a partir de una serie de operaciones con la clave pública (la tuya o la de tus destinatarios) extrae una cadena de 40 caracteres que se denomina fingerprint. Una vez que una persona ha obtenido tu clave pública de un servidor de claves debe ponerse en contacto contigo por algún medio seguro (en persona o a través de teléfono, por ejemplo) y verificar que esa fingerprint coincide con la que él ha generado de su clave pública. Con este paso termina el proceso de autenticación de un usuario y se añade un nuevo elemento al anillo de confianza.

Es importante que sólo se añadan elementos al anillo de confianza en los cuales se confíe plenamente y se haya verificado la autenticidad de la clave pública, porque una cadena es tan frágil como el más frágil de sus elementos. Si se cumple estrictamente esta norma todo irá bien pero si, en cambio, añadimos elementos en los que la confianza no

es plena ese elemento podrá añadir otros elementos y podría terminar con el anillo.

Programas Útiles

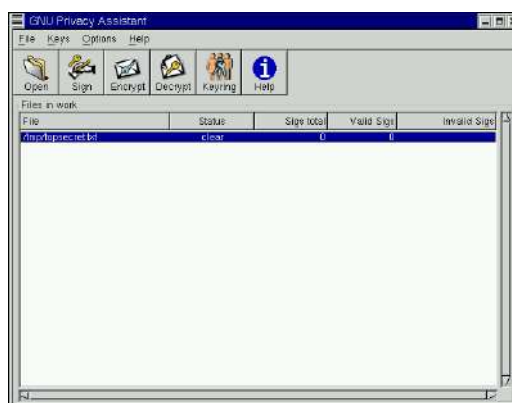
Recomiendo el uso de algún 'gestor de claves' que evita el tener que utilizar la línea de comandos y acceder a funciones un poco escondidas. En mi caso, me gusta mucho The GNU Privacy Assistant (gpa).

El *Asistente de Privacidad de GNU* (GPA - *GNU Privacy Assistant*) es una interfaz de usuario gráfica para el GNUPG (Guardián de Privacidad de GNU - *GNU Privacy Guard*).

GPA utiliza GTK (el GIMP Tool Kit - Conjunto de Herramientas de GIMP) y compila para varias plataformas. Puede echar un vistazo a algunas capturas de pantalla. Puede igualmente aprender más sobre los iconos de GPA.



Logo de GPA



ventana principal

ventana de dialogo de llaves públicas