PGP

autodefensa digital

PGP (Pretty Good Privacy, "privacidad bastante buena"), "encriptación de clave pública para las masas", es un pequeño programa de ordenador que sirve para cifrar y descifrar textos y archivos de datos y para hacer firmas digitales mediante sistemas de criptografía. A nosotr@s nos va a servir fundamentalmente para proteger los mensajes que enviamos a través del correo electrónico. Es llamativo cómo nos relajamos con el uso del mail, escribiendo cosas que nunca contaríamos por teléfono o por carta, como si fuese más seguro el ordenador que, por ejemplo, el teléfono. Y resulta que es justo al contrario: pinchar el teléfono o abrir la correspondencia de modo masivo no es nada sencillo (requiere alguien que escuche o que lea uno por uno) y, sin embargo, es tremendamente fácil pinchar algún servidor a través de los que pasa el correo electrónico y leer un mensaje o, peor aún, establecer un filtro automático de modo que se almacenen selectivamente aquellos mensajes que cumplan una cierta condición (el remitente, cierta palabra, etc.). Lo hace la máquina, no requiere intervención humana más que para visualizar el resultado del pinchazo.

Breve reseña histórica

La criptografía es un arte muy antiguo –aparece ya en los jeroglíficos egipcios y en textos cuneiformes; los judíos la usaron desde Jeremías y también Julio César nos dejó su nombre encriptado– usado para proteger el secreto de la correspondencia mediante escritura convencional. El procedimiento más sencillo (el de Julio César por ejemplo) consiste en desplazar un número constante cada letra del alfabeto –a por ejemplo se convierte en D,b en E, c en F, etc.– con lo que resulta un texto ilegible para quien desconoce el método. Este método evidentemente es muy fácil de descubrir, pero los antiguos usaron ya algoritmos de trasposición y sustitución de letras bastante más complejos. Modernamente han sido los militares y los servicios secretos de los Estados quienes más lo han desarrollado, inventando máquinas cifradoras (manuales o mecánicas) que permitían utilizar con rapidez los métodos de sustitución o sistemas de códigos cifrados (los famosos diccionarios de claves de las películas de espías). Los bancos también han estado últimamente muy interesados en la criptografía como forma de evitar cualquier otra operación fraudulenta que no sea las que ellos mismos realizan.

Con la introducción de los ordenadores y su formidable capacidad para el cálculo intensivo, se han podido desarrollar y llevar a la práctica algoritmos extraordinariamente complejos, hasta el punto de que se piensa que sólo el ensayo sucesivo de todas y cada una de las posibilidades (a esto se le llama "ataque de fuerza bruta") podría llegar a "romper" (descrifrar) estos códigos. Eso ha hecho que los antiguos métodos manuales hayan quedado muy desfasados y se consideren solamente formas de camuflaje de textos y no verdaderos métodos de encriptación.

Desde sus orígenes, los sistemas informáticos de encriptación han estado en manos del poder (gobiernos, ejército, bancos, corporaciones privadas), que iba ensayando algoritmos cada vez más sofisticados aunque casi siempre se encontraban con un problema insoluble derivado de usar el método de "clave secreta", con el que las partes que se quieren comunicar debían conocer previamente la clave. En 1991 un programador que trabajaba para la NASA –Phil Zimmermann– ante la perspectiva inminente de que se ilegalizara en Estados Unidos el uso libre –no controlado por el Gobierno– de la criptografía decide hacer público el código fuente del PGP y ponerlo a disposición de todo el mundo en Internet. Se armó un tremendo escándalo que le condujo a la cárcel en 1993 acusado de exportar armas militares. Semejante estatus se le daba a un programa informático: arma militar. El fiscal pedía varios años de cárcel y una multa elevadísima. Finalmente, y gracias a una extraordinaria campaña a favor de su libertad realizada a nivel mundial a través de Internet y de movilizaciones en la calle en Estados Unidos, Zimmermann salió libre de cargos y hoy día cualquiera puede obtener versiones mejoradas de PGP en numerosos servidores de FTP de Internet, aunque la legislación estadounidense mantiene un control penal para la importación y exportación de PGP.

¿Qué es el PGP?

No voy a entrar en detalles técnicos, pero creo que sí es interesante estar familiarizad@ con el modo de funcionamiento de PGP y su diferencia con otros sistemas de encriptación. El PGP usa un

sistema de clave pública. Como he mencionado más arriba, anteriormente los sistema de encriptación más empleados –de clave secreta– precisaban que el/la remitente y el/la destinatari@ se comunicaran de algún modo dicha clave. La clave secreta servía para encriptar y para desencriptar. Eso obligaba a que el intercambio de la clave debía realizarse por un "canal seguro" (pues de otro modo puede caer en manos de quien no debe :-) y de nada iba a servir encriptar). Pero resulta que si se dispone de un canal seguro no hace falta encriptar nada. Para solucionar este problema y poder transferir la clave por canales no seguros o sin necesidad de hacerlo personalmente, se ideó un sistema llamado de "clave pública", que básicamente consiste en crear dos claves diferentes generadas a la vez, una para encriptar y otra desencriptar. Se consiguió crear un algoritmo en que a partir de la clave de descifrado era imposible deducir la clave de cifrado con lo cual se podía hacer pública esta última a cuanta más gente mejor (la "clave pública"). Eso permitió masificar el uso de la encriptación al poderse usar canales no seguros para transferir la clave sin miedo a que alguien la intercepte. El mensaje se encripta usando simultáneamente la clave secreta del/la remitente y la clave pública del/la destinatari@. Para desencriptar se hará al revés: el/la destinatari@ usará la clave pública del/la remitente y su clave secreta (la del/la destinatari@). Se consigue así que cada mensaje únicamente pueda ser desencriptado por la persona a quien se lo dirigimos hasta el punto de que, una vez encriptado, ni siquiera quien lo ha encriptado puede volver a desencriptarlo: sólo a quien ha sido enviado puede hacerlo mediante su clave privada (más la clave pública del remitente). Es como el anillo de Schazan, hacen falta las dos mitades de la llave, y esa llave es siempre distinta porque es generada aleatoriamente mediante una frase secreta (passphrase) que sólo necesita conocer el remitente. Eso convierte a un mensaje encriptado con PGP en irrompible a no ser que se conozca la passphrase.

Otro uso muy importante del PGP –aunque creo que no para nosotr@s, sino más bien para cuestiones legales y para transacciones comerciales– es la posibilidad de firmar digitalmente un documento. Por ejemplo, puede interesar enviar un mensaje claro para que lo pueda leer cualquiera pero queremos que llegue intacto, que nadie lo manipule y que sepamos con total seguridad que lo ha escrito quien dice haberlo hecho. Es decir, la firma digital impide técnicamente falsificar un mensaje o suplantar la personalidad de otr@ para enviar un mensaje. Si se ha manipulado en algún momento, PGP avisa de ello.

Pero ¿por qué es tan importante el PGP?

Que un fiscal lo considerara un arma militar no fue una ida de olla. La dimensión política de PGP es extraordinaria, se trata de una máquina insólita en nuestro tiempo. Asegura a cualquier persona que sepa usar un ordenador la total privacidad de sus comunicaciones escritas a través de la red. Total privacidad significa que nadie que no sea el destinatario del mensaje podrá de ningún modo leer su contenido. Nadie significa nadie: ni la policía, ni todos los servicios de seguridad de todos los Estados trabajando juntos. Nadie. Porque nadie ha conseguido romper PGP ni es previsible que lo logre en un número muy significativo de años. Hasta hace poco, sistemas de blindaje tan poderosos sólo estaban al alcance de los Estados. En cualquier parte del mundo, el Estado –a través de los jueces o de la policía directamente– se reserva la posibilidad de intervenir la correspondencia o pinchar el teléfono o registrar a la fuerza el domicilio de quien sea. Con PGP no se puede hacer. Es insólito que una tecnología de inteligencia militar esté al alcance de cualquiera y es insólito que en la era del Estado-control haya una parcela tan importante como la de la comunicación privada cuyo control escape al Estado de modo tan sencillo y eficaz. Probablemente, se trata de la primera vez en que la gente tiene semejante capacidad de defensa frente al poder estatal: la posibilidad real de proteger sus comunicaciones de un modo seguro y de defenderse de la injerencia de la policía o de los jueces. Por eso en varios países usar PGP es ilegal (Francia, Rusia, Irán, Irak, China...) e incluso se paga con la cárcel o con el pelotón de fusilamiento. En el Estado español, por suerte, todavía no hay legislación al respecto y se puede encriptar tranquilamente. Pero hay que tener cuidado de no enviar un mensaje encriptado con PGP a países donde podríamos comprometer gravemente al/la destinatari@ (hay información específica en Internet sobre la situación de las legislaciones en cada país sobre criptografía).

PGP además es free software bajo licencia copyleft registrada por su autor Phil Zimmermann. Es

decir, no tiene copyright, pertenece a la comunidad de usuari@s y nadie se lo puede apropiar. Puede ser copiado y distribuido libremente, puede ser estudiado para mejorarlo y para comprobar que no tiene errores ni "puertas traseras". Al ser público el código fuente de PGP, hay miles de usuari@s que durante años lo están poniendo a prueba y revisando sus algoritmos para garantizar que no contiene "puertas traseras" (trucos que un programador puede implementar en el código interno del PGP para "romperlo" sin necesidad de conocer la clave secreta y sin que nadie lo advierta). Además PGP funciona en casi todas las plataformas, no sólo en la de las ventanitas.

En Estados Unidos –que sirve como avancilla y ejemplo a otros países a la hora de establecer políticas restrictivas– el contraataque del Gobierno ha consistido en implementar el chip Clipper. El chip Clipper es un sistema de encriptación que avala el gobierno para que lo vayan incluyendo los fabricantes de dispositivos digitales de comunicaciones (modems, fax, teléfonos, etc.). Lo vende como un sistema que va a garantizar la privacidad de l@s ciudadan@s en sus comunicaciones, pero, eso sí, el gobierno, a través de los jueces, guarda en depósito la llave de cada clave secreta que se genere con el chip Clipper. Es decir, que en caso de necesidad (como con la correspondencia convencional, el domicilio, etc.) puede violar la comunicación privada de cualquiera que use ese chip. De momento, usar el chip Clipper es voluntario, pero el paso siguiente es muy fácil preverlo: ilegalizar cualquier sistema de encriptación que no sea Clipper y obligar a implementarlo en exclusiva. El algoritmo que usa Clipper es secreto, lo cual no asegura su eficacia (sólo poniéndolo a prueba masivamente, como ocurre con PGP, se puede asegurar con un sistema es seguro) y, sobre todo, no garantiza en absoluto que no tenga "puertas traseras" que permitan a la policía leer las comunicaciones sin necesidad de pasar por una orden judicial.

Modo de usarlo

Para instalar y configurar PGP, hay un manual en castellano en http://linux.nodo50.org/seguridad y el propio programa trae una ayuda en línea en castellano. Aquí sólo me voy a referir a cómo usarlo desde el ordenador del Laboratorio.

1. Se pide la passphrase a alguien del Área Telemática.
2. Escribimos el mensaje en formato texto (con el word o con la propia ventana de correo, salvándolo como fichero de texto *.txt y copiándolo en el directorio c:\pgp)
2. Abrimos una ventana del DOS y nos vamos al directorio pgp.
tecleamos cd c:\pgp
3. Tecleamos el siguiente comando para enviárselo, por ejemplo a Marta
pgp -e mifichero.txt marta
o bien si quiero enviarlo a varias personas:
pgp -e mifichero.txt marta david alicia
Esto genera un fichero encriptado que ya podemos enviar pegándolo a un mensaje de correo.
(Se supone que a quien le enviamos el mensaje está en nuestro anillo de claves públicas. Si no, la persona a quien queremos mandarle el mensaje encriptado debe enviarnos antes su clave pública (o decirnos de qué servidor pillarla) e incluirla en nuestro anillo. Hay servidores de claves públicas que se las intercambian entre sí. En http://linux.nodo50.org/seguridad están las claves públicas del Nodo50 y de Ipanex.)

Para incluir la clave pública de alguien en nuestro anillo tecleamos:
pgp -ka marta.asc

Para desencriptar un fichero:
pgp nombre_de_fichero_cifrado

A modo de conclusión

A parte de PGP, hay otras técnicas interesantes para proteger la confidencialidad del correo como son los remailer anónimos, servidores que permiten reenviar un mensaje de modo que quien lo recibe no tenga modo de saber quién se lo ha enviado. Estos servidores no está claro que vayan a garantizar el anonimato en toda circunstancia, por lo que hay que ser precavid@. Pero la cuestión de los remailer anónimos constituye un tema en sí mismo que podremos tratar en otra ocasión.

El PGP, como la red Internet y con los propios ordenadores personales, tienen su origen en una

extraña y anómala confluencia de intereses militares y/o comerciales, junto a prácticas antagonistas y de resistencia antiautoritaria. Podemos oír hablar de PGP a responsables de seguridad de empresas, o como forma de proteger copyrights y, al tiempo, constituye una herramienta única y alcance de tod@s para protegernos de esos mismos que tratan de desarrollar formas de control y dominio cada vez más sofisticados.