

Sobre PGP

PGP son las siglas de Pretty Good Privacy (intimidad bastante buena), que es un sistema que cifra datos de cualquier tipo, escrito por Philip Zimmermann. Éste permite el intercambio de información digital con intimidad, autenticación y comodidad. Por *intimidad* entendamos que la información solo puede ser leído a quien va dirigido este. *Autenticación* quiere decir que la información que parece ser de una persona únicamente pueden venir de tal persona; y por *Comodidad* la forma sencilla y sin complicaciones de realizar estos dos últimos.

PGP es un programa de cifrado híbrido, es decir combina de cifrado simétrico en bloque (cifrando bloques de bits) con cifrado asimétrico.

En los algoritmos simétricos cifrados en bloque se requiere el mismo algoritmo tanto para el emisor como para el receptor, y es esta su principal desventaja, ya que debe de existir una comunicación segura entre el emisor y el receptor. Pero ¿cuál es el sentido de hacer uso de un canal de comunicación seguro? Si no hay posibilidad de fisgar, no hay necesidad de cifrar. Los problemas de intercambio y gestión de claves, de esta forma de cifrado, se resuelven con los sistemas de clave asimétrica o de clave pública.

En el algoritmo de cifrado asimétrico o de clave pública se hace uso de dos claves distintas, una para el cifrado (clave pública) y otra para el descifrado (clave privada), evitando de esta forma los peligros de intercambio de claves por un medio inseguro. En teoría es posible obtener la clave privada a partir de la clave pública, pero es prácticamente imposible. Los algoritmos de cifrado asimétrico adolecen de eficiencia comparado con los algoritmos simétricos. El cifrado de un mensaje por el algoritmo de cifrado simétrico es del orden de mil veces más rápido que el de cifrado asimétrico. Y el tamaño como resultado después de cifrar, para el cifrado simétrico es muchísimo menor.

ARTÍCULO

PGP para correo electrónico cifrado

¿Porqué cifrar nuestros mensajes?

Aunque el riesgo para la interceptación de mensajes es bajo, es fácil interceptar y romper la conversación que fisgona en el propio e-mail. Cifrar nuestros mensajes significa que nadie a quien no se haya enviado el mensaje pueda leerlo, para esto ampliamente el uso de PGP ayuda a impedir que otros fisgoneen en nuestros mensajes electrónicos. PGP nos permite realizar 'firmas digitales' permitiendo probar que uno y sólo uno es el autor de un mensaje. Cifrar nuestros mensajes afirma nuestro derecho fundamental a la privacidad en línea.

PGP es efectivo si el emisor y el receptor tienen instalado el software PGP, pero no es efectivo si los mensajes son distribuidos a lista de e-mails.

En el cifrado híbrido, la clave pública se usa para cifrar sólo la clave simétrica con que va cifrado el mensaje que se desea enviar. Esta clave de cifrado es la misma para el descifrado. Eso quiere decir que para cada mensaje cifrado se puede elegir diferentes claves, lo que mejora la seguridad. Aquí, los ataques no son factibles en la práctica, ya que la complejidad para criptoanalizar el sistema es igual al espacio de claves, pudiendo realizarlo únicamente por fuerza bruta.

PGP esta disponible para múltiples plataformas, que permite el cifrado de datos, archivos y mensajes. PGP usa dos formas diferentes de clave pública: RSA (con función hash MD5) y Diffie-Hellman (con función hash SHA-1), con longitud de clave de hasta 2048 (RSA) o 4096 (DH) bits. Los algoritmos de clave simétrica que puede utilizar son: CAST, IDEA y TripleDES.

¿Cómo lo hacemos?

Para usar PGP, tanto el usuario emisor como el receptor debe de tener el software PGP. Si alguien no tiene el software y no ha generado y distribuido su clave pública no se puede enviar mensajes cifrados a esa persona.

Se recomienda:

- Bajar e instalar el software PGP desde el web site de distribución de PGP del MIT en [http://www.onenw.org/bin/page.cfm?pageid=37#PGP Freeware download site](http://www.onenw.org/bin/page.cfm?pageid=37#PGP%20Freeware%20download%20site)
- Actualizar la versión actual de algún programa de envío de emails que soporte PGP plugins.
- Generar una clave pública y publicarla en un servidor de claves públicas, el cual otros usuarios pueden encontrarlo usando simplemente el email del destinatario. Se puede encontrar mayor información sobre la distribución de la clave pública en la documentación de PGP.
- Y, hacer uso de éste.

Cifrar nuestros mensajes es probablemente no necesario para muchas personas en comunicaciones digitales, pero mientras la interceptación de mensajes sea técnicamente posible, aunque no trivial, es recomendable hacer uso de ésta.

Para mayor información

- PGP Freeware download site
<http://web.mit.edu/network/pgp.html>
- Tom McCune's "PGP Questions and Answers"
<http://www.pgp.com/privacy/intro-priv.cgi>

Referencias

- PGP Internacional
<http://www.pgpi.com/>
- Kriptopolis
<http://www.kriptopolis.com/>
- Todo sobre el PGP
<http://www.geocities.com/SiliconValley/Pines/2332/>

Por:

- Jesús Mena Chalco.

e-mail: j.mena@usp.edu.pe

Universidad de San Pablo-Arequipa