Cifrado de correo con software libre

04/12/2024 13:43:18

FAQ Article Print

Category:	Correo electrónico	**Last update:**	08:55:28 - 07/07/2020
State:	public (all)		

Keywords

Cifrado, Correo, software libre

Solucion (public)

El cifrado de correo funciona empleando el sistema asimétrico de encriptación PGP (Pretty Good Privacy) que consiste en generar un par de claves que se utilizan para la encriptación de los mensajes y su descifrado. La primera de estas claves, utilizada para el cifrado, es de acceso público: todo el que la posea puede utilizarla para encriptar mensajes que sólo pueden ser descifrados con la otra clave. Por supuesto, la segunda clave es privada, y únicamente la posee (protegida por una contraseña), el usuario que ha creado el par de claves.

Los mensajes encriptados utilizando la clave pública únicamente pueden ser descifrados utilizando la clave privada. De este modo, sólo el destinatario del correo cifrado (poseedor de la clave privada correspondiente) puede leer el contenido del mensaje. Existen, sin embargo, muchas formas de utilizar PGP, todas ellas compatibles entre sí; utilizando de servicios de correo que lo integran automáticamente, como Betamail, por medio de programas específicos de gestión de claves como Kleopatra, a través de extensiones de cliente como Enigmail, o recurriendo a extensiones de navegador como Mailvelope. A continuación detallaremos el ejemplo de Betamail e incluiremos enlaces a explicaciones concienzudas de otros métodos de utilización de PGP.

Antes de empezar, sin embargo, es importante recalcar que es imprescindible mantener las claves públicas y privadas de forma segura.

====Betamail====

Betamail es una interfaz alternativa de correo al que se puede acceder con cualquier correo de la Universidad de Zaragoza ([1]https://betamail.unizar.es/) y que soporta nativamente el cifrado GPG. Para cifrar nuestro correo en Betamail solo hay que acceder al servicio y seguir los siguientes pasos que se explican a continuación.

Paso 1: creación de claves

Una vez iniciamos sesión en Betamail, debemos entral al menú de configuración que aparece indicado con el símbolo del engranaje en la parte inferior del menú:

Desde aquí, hacemos click en la opción de Open PGP, y acto seguido, en Generar llaves OpenPGP. Alternativamente podemos importar un par de claves, si ya disponemos de uno, haciendo click en la opción de "Importar llave OpenPGP" y pegando en la ventana emergente el texto correspondiente (para más información, consulta el final del paso 1):

Esto nos presentará una ventana en la que debemos introducir la dirección del correo para el que queremos generar las claves (el mismo que estamos utilizando), el nombre que deseamos asociar a dichas claves, la contraseña que asociaremos a nuestra clave privada (y sin la cual no podremos utilizarla, por lo que debemos ser capaces de recordarla y mantenerla a salvo) y la longitud de la clave de cifrado (una clave más larga es más segura matemáticamente, pero puede tardar más en descifrar los mensajes):

Una vez generado el par de claves, podremos verlas en la sección de OpenPGP del menú:

Las claves se guardan entre los datos del navegador, por lo que es recomendable exportarlas para garantizar que no se pierdan. Para ello sólo hay que hacer click en el icono del ojo correspondiente a cada clave y copiar el contenido de la ventana emergente en un archivo de texto que procederemos a guardar a buen recaudo. Además, puedes enviar por correo la clave pública a quienes quieras que sean capaces de escribirte mensajes privados. Así, ellos solo tienen que importar la información (como se indica al inicio de este mismo paso) para poder disfrutar de un canal de comunicación seguro contigo.

Paso 2: cifrado de mensajes

Ahora que disponemos de nuestras claves, podemos empezar a enviar mensajes cifrados. Para ello, debemos primero redactar el mensaje en texto plano, haciendo click en el icono que aparece en la parte izquierda del menú de formato de texto:

Una vez redactado el contenido, hacemos click en el menú de opciones de arriba a la derecha y seleccionamos la opción de "Open PGP (solo texto plano)":

Esto nos abrirá una ventana en la que se nos ofrecerá las opciones de firmar y cifrar el correo, debiendo seleccionar la clave pública asociada con la dirección de correo a la que queremos hacer llegar el mensaje. La firma se realiza utilizando la clave privada, por lo que requiere la utilización de la contraseña, pero garantiza a un receptor en posesión de nuestra clave pública que realmente hemos sido nosotros quienes enviamos el mensaje (pues la clave

pública únicamente puede descifrar la firma de la clave privada correspondiente). Tras seleccionar las opciones que nos interesen (firmar y cifrar, sólo firmar o sólo cifrar) volveremos a la ventana del correo, donde el mensaje será reemplazado por su versión cifrada:

Ahora podemos enviar el mensaje con normalidad, y este sólo podrá ser descifrado por quien disponga de la clave privada asociada con la clave pública que hemos utilizado para cifrar el texto.

Paso 3: descifrar mensajes

Una vez hemos recibido un mensaje cifrado usando nuestra clave pública, podemos utilizar nuestra clave privada correspondiente para descifrarlo. Para ello sólo tenemos que abrir el mensaje y hacer click en el icono del candado que aparece sobre el texto cifrado:

Esto nos abrirá una nueva ventana en la que deberemos seleccionar la clave privada correspondiente e introducir la contraseña asociada, tras lo cual haremos click en el botón de "Descifrar":

Finalmente podremos ver el mensaje descifrado, accediendo así a su contenido original:

====Kleopatra y Enigmail====

Kleopatra es un programa libre de gestión de claves que puede utilizarse para localizar y difundir claves públicas de correo a través de diversos servidores. Por su parte, Enigmail es una extensión libre de cifrado de correo para Thunderbird. El funcionamiento de ambos puede encontrarse en la guía del incibe, donde también disponemos de información al respecto del cliente de correo de Outlook:

[2]https://www.incibe-cert.es/sites/default/files/contenidos/guias/doc/incibe_cert_guia_para_el_uso_de_pgp_en_clientes_de_correo_electronico.pdf

====Mailvelope====

Mailvelope es una extensión código abierto de navegador que podemos utilizar en Firefox y Google Chrome para cifrar nuestros correos sin necesidad de utilizar otro programa. Las instrucciones de su uso las podemos encontrar en la propia página de Mailvelope:

[3]https://www.mailvelope.com/es/help

[1] https://betamail.unizar.es/
[2] https://www.incibe-cert.es/sites/default/files/contenidos/guias/doc/incibe_cert_guia_para_el_uso_de_pgp_en_clientes_de_correo_electronico.pdf
[3] https://www.mailvelope.com/es/help