Correo ¿seguro?

Guía para personas usuarias

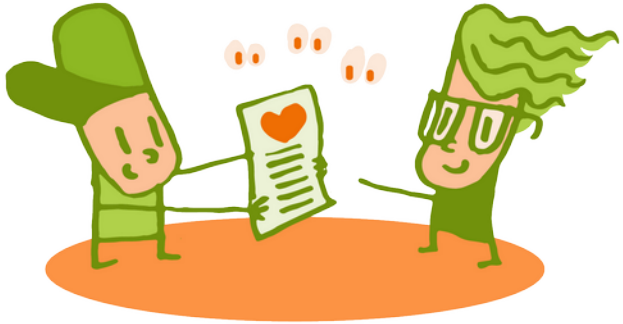
[ÍNDICE]

Contenidos

[ÍNDICE]

1 CORREO ¿SEGURO?

El correo, a diferencia de la web, viaja sin proteger por la internet. Podemos proteger nuestros mensajes de modificaciones que alteren nuestros mensajes (firmar) o protegerlos para que solo los pueda descifrar el destinatario de nuestro mensaje (cifrar o encriptar).



[ÍNDICE]

2 CONCEPTOS DE CIFRADO (CRIPTOGRAFÍA)

Clave (llave): un texto, que puede contener todo tipo de caracteres. Mediante un algoritmo criptográfico puede transformar otro texto (cifrar o descifrar). Quién conoce la clave determina quién puede cifrar o descifrar y quién no.

Algoritmo de cifrado (encriptación): el procedimiento que transforma la información de un formato legible, texto en claro, en un formato ilegible, texto cifrado. Las operaciones se llaman **cifrar** y **descifrar**.

Si el algoritmo es **simétrico**, compartir la clave permite que un mensaje cifrado con la clave pueda ser descifrado a partir de la misma clave. En la metáfora de llave, todas las copias de una llave pueden abrir y cerrar cajas (texto cifrado) que contienen el texto legible (sin cifrar).

Si el algoritmo es **asimétrico**, hacen falta dos **claves complementarias**: lo que cifra una lo puede descifrar la otra. Cuando se generan, si una se hace pública y la otra no, se llaman **clave pública y clave privada (secreta)**. En la metáfora de llaves, tenemos una **llave privada** y muchos **candados abiertos públicos**. Cualquiera puede cerrar una caja con un candado que contenga un texto legible para generar un texto cifrado. Solo puede abrir el candado (descifrar) quien tiene la llave privada, que no la debe compartir con nadie (secreta).

¿Qué es un algoritmo?

En matemáticas, lógica, ciencias de la computación y disciplinas relacionadas, un algoritmo es un conjunto de instrucciones o reglas definidas y no-ambiguas, ordenadas y finitas que permite, típicamente, solucionar un problema, realizar un cómputo, procesar datos y llevar a cabo otras tareas o actividades.

En la vida cotidiana, se emplean algoritmos frecuentemente para resolver problemas determinados. Algunos ejemplos son los manuales de usuario, que muestran algoritmos para usar un aparato, o las instrucciones que recibe un trabajador de su patrón. Algunos ejemplos en matemática son el algoritmo de multiplicación, para calcular el producto, el algoritmo de la división para calcular el cociente de dos números.

Wikipedia - https://es.wikipedia.org/wiki/Algoritmo

[ÍNDICE]

Por tanto, **nunca se ha de compartir con nadie nuestra clave privada**, por eso se llama también clave secreta, pues le damos la capacidad de usar esa clave por su cuenta. **Siempre hemos de compartir nuestra clave pública**, pues si no se hace pública nadie nos podrá enviar mensajes. Metafóricamente, hemos de regalar candados abiertos para que nuestra llave privada pueda abrirlos.

Función resumen: cualquier función que sirva para calcular a partir de datos de longitud arbitraria un resultado de tamaño fijo. Por ejemplo el resto de la división por 100 (módulo 100) genera siempre un resultado entre 0 y 99 para enteros con cualquier número de cifras: el módulo es una representación compacta de cualquier entero. Además una buena función resumen debería ser rápida de calcular y difícil de revertir (es decir, encontrar entradas correspondientes a partir de un resumen).

La **huella digital de la clave pública** es una breve secuencia de bytes que identifica una clave pública más larga. Es el resultado de una función resumen de la clave pública.

Por ejemplo:

La clave de leandro@pangea.org tiene 4096 bytes, y su huella (o resumen) es:

3987 0457 1F85 B6D9 6551 D827 260C 3E8C 8E9E CEC6

[ÍNDICE]

3 PROTECCIÓN DE MENSAJES

Firmar: facilitar que cualquiera pueda verificar la integridad de un mensaje (contenido) y su autenticidad (remitente), **añadiendo** al texto un valor que permite **verificar** que el conjunto no ha cambiado.

Cifrar: permitir que solo una persona pueda leerlo (extraer el mensaje legible de un mensaje cifrado), **sustituyendo** el texto legible por uno cifrado.

Por ejemplo, si Ana quiere enviar un mensaje a Blanca:

Firmar:

Ana puede preparar su mensaje: su dirección (identidad) y el texto a enviar. El mensaje pasa por una función resumen y el resultado lo cifra con su clave privada. Esta es la firma, que se añade al mensaje.

Por tanto, Blanca y cualquier otra persona podrá leer el texto y además podrá verificar su integridad: puede aplicarle la función resumen y descifrar la firma. Si ambos resúmenes coinciden, el mensaje no ha sido alterado.

[ÍNDICE]

Por tanto, **firmamos** nuestros mensajes con **nuestra clave privada** (no con la del receptor, ya que es nuestra firma).

Cifrar:

Ana quiere enviar un mensaje que solo Blanca pueda leer. Ana busca la clave pública de Blanca y cifra el mensaje, que sustituye al texto legible. Si nadie más que Blanca tiene su clave privada, solo Blanca lo puede descifrar.

Por tanto, **cifra**mos nuestros mensajes con la **clave pública del receptor**.

3.1 ¿Como publicar nuestra clave pública?

Podemos **publicarla** en un servidor de claves público (asociada a nuestra dirección de correo). Podemos también incluir nuestra clave pública en cualquier mensaje que enviamos, o incluir un enlace al servidor público donde esté o a nuestra página web personal.

Siempre podemos enviar un mensaje firmado a cualquiera: solo tenemos que decir algo y firmarlo con nuestra clave privada.

En cambio, para enviar un mensaje cifrado a alguien, hemos de conseguir su clave pública para cifrarlo con su clave. Así solo él lo podrá leer. Ni siquiera nosotros podremos.

[ÍNDICE]

4 ¿CORREO SEGURO?

A diferencia de la web, que en su mayoría ha pasado de HTTP a HTTPS (cifrado), el transporte de correo (SMTP) no se suele cifrar, no hay garantía. Si no se puede garantizar el transporte de correo, toca proteger los mensajes: asegurar integridad (contenido), asegurar autenticidad (remitente), asegurar confidencialidad (solo lo pueda leer el destinatario).

Para tener integridad y autenticidad hemos de firmar (un resumen) con nuestra propia clave y añadirlo al mensaje. Cualquiera podrá verificar la integridad y autenticidad de un mensaje firmado utilizando la clave pública del remitente.

Para conseguir confidencialidad hemos de cifrar nuestro mensaje con la clave pública de la persona receptora, que solo ella podrá descifrar (si ella y solo ella tiene su clave privada).

4.1 Métodos

- La pareja de claves nos las otorga una autoridad: nos da nuestra clave privada y publica la otra. Este es el caso de S/MIME.
- La pareja de claves nos las generamos nosotros: individual. Generamos la pareja de claves, guardando la privada y publicando la otra. Este es el caso de OpenPGP.

[ÍNDICE]

- Si no tenemos una autoridad que nos proporcione el servicio de gestión de claves (S/MIME), nos las hemos de generar nosotros (OpenPGP).

4.2 Herramientas recomendadas

Thunderbird para PC.

K-9 Mail y OpenKeychain para móvil (Android).

Flowcrypt y Mailvelope para clientes de correo web como Gmail en PC.

5 PUESTA EN PRÁCTICA

5.1 Instalación y configuración

Si tenemos una cuenta de correo configurada en Thunderbird en nuestro PC, solo hemos de generar nuestra pareja de claves[1]. Hemos de publicar la clave pública[2] y guardar con cuidado la privada en nuestro PC, protegida por una contraseña. Es recomendable usar un gestor de contraseñas como KeepassXC para evitar olvidar una contraseña más, pues no hay que reutilizarlas.

Si tenemos la misma cuenta de correo configurada en la aplicación “K-9 mail” de nuestro móvil y la aplicación OpenKeychain instalada (Android), solo tenemos que exportar nuestra pareja de claves a un archivo, transferirlo al móvil, importarlo en OpenKeychain y decirle a K-9 que queremos usar “cifrado extremo a extremo” para nuestra cuenta de correo, habilitar OpenPGP y elegir nuestra clave en OpenKeychain.

1 Herrramientas → Configuración de la cuenta → Cifrado extremo a extremo → Añadir Clave… → Crear una nueva clave OpenPGP

2 Herrramientas → Configuración de la cuenta → Cifrado extremo a extremo → [X] Añadir mi clave pública al añadir una firma digital OpenPGP

[ÍNDICE]

5.2 Pruebas

Si yo soy Ana@pangea.org, puedo generar un mensaje de correo para Blanca y en las opciones activar la firma[3]. Al enviarlo, nos puede pedir la contraseña que protege nuestra clave privada. Añadirá una firma y lo enviará.

Cuando lo reciba Blanca verá en su cliente de correo que el mensaje está firmado por Ana@pangea.org. También verá la clave pública de Ana o una parte de ella (la huella de la clave pública). Con eso podría usar o encontrar la clave pública de Ana y le podrá enviar un mensaje cifrado.

Si Ana no se ha comunicado nunca con Blanca, no tiene su clave pública. La puede encontrar en algún servidor de claves en Internet a partir de su dirección de correo (aunque no estaremos seguros si la ha publicado Ana), o si Ana tiene, en su página web personal. Si la conocemos, podemos pedirle directamente a Ana su huella. Así estaremos más seguros. También nos la puede pasar alguien que conoce a ambos (pero firmada para no perder confianza), o a través de intermediarios que se conocen entre sí (una red de confianza) y que las han intercambiado con cuidado. No debemos fiarnos de una firma que nos llega por correo electrónico hecha con una clave pública que desconocemos, pues la puede haber enviado otra persona para confundirnos y aparentar que viene de Blanca (el transporte de correo no comprueba mucho).

3 Thunderbird: En la ventana del nuevo mensaje: Seguridad → Firmar digitalmente este mensaje
K-9 Android: Clic en los en los tres puntos verticales arriba a la derecha y elige activar el modo de solo firma-PGP. Aparece un icono junto a mi dirección de remitente que indica firma, no cifrado

Esta explicación pretende que sepamos cómo hacer el correo electrónico más seguro: integridad del contenido, autenticidad del remitente y confidencialidad del contenido para el destinatario.

5.3 Programas

Thunderbird

https://www.thunderbird.net/[4]

K-9 Mail Android[5]

https://k9mail.app

OpenKeychain Android

https://www.openkeychain.org

Mailvelope

https://www.mailvelope.com/en/

Flowcrypt

https://flowcrypt.com

Keepassxc

https://keepassxc.org

4 Hemos completado en Pangea la traducción al castellano ES-ES del soporte para OpenPGP. Algunos mensajes todavía salen en inglés, pero esperamos que pronto, todos los mensajes salgan en castellano.

5 Recomendado en F-Droid, como el resto de aplicaciones libres para Android: https://f-droid.org

www.pangea.org
Plaça Eusebi Güell 6-7
Edifici Vertex, planta 0
08034 Barcelona
Tel: +34 934015664
Correu: suport@pangea.org

CON EL SOPORTE DE:

APC
ASSOCIATION FOR PROGRESSIVE COMMUNICATIONS

Pangea.org
< INTERNET
ÈTIC I SOLIDARI >

[ÍNDICE]