Correu segur?

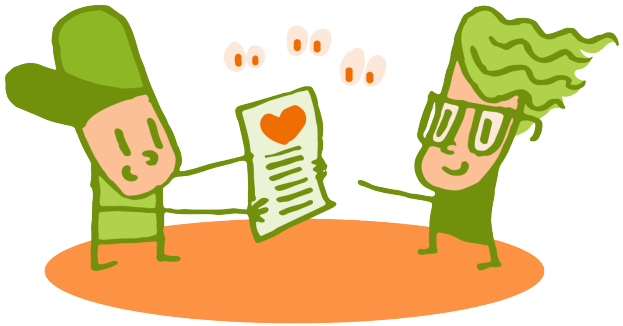
Guia per a persones usuàries

[ÍNDEX]

Continguts

1 CORREU SEGUR?

El correu, a diferència de la web, viatja sense protegir per internet. Podem protegir els nostres missatges de modificacions que alterin els nostres missatges (signar) o protegir-los perquè només els pugui desxifrar el destinatari del nostre missatge (xifrar o encriptar).



[ÍNDEX]

2 CONCEPTES DE XIFRAT (CRIPTOGRAFIA)

Clau (clau): un text, que pot contenir tota mena de caràcters. Mitjançant un algoritme criptogràfic pot transformar un altre text (xifrar o desxifrar). Qui coneix la clau determina qui pot xifrar o desxifrar i qui no.

Algorisme de xifrat (encriptació): el procediment que transforma la informació d'un format llegible, text en clar, en un format il·legible, text xifrat. Les operacions s'anomenen **xifrar** i **desxifrar**.

Si l'algoritme és **simètric**, compartir la clau permet que un missatge xifrat amb la clau pugui ser desxifrat a partir de la mateixa clau. A la metàfora de clau, totes les còpies d'una clau poden obrir i tancar caixes (text xifrat) que contenen el text llegible (sense xifrar).

Si l'algoritme és **asimètric**, calen dues **claus complementàries**: el que xifra una ho pot desxifrar l'altra. Quan es generen, si una es fa pública i l'altra no, s'anomenen **clau pública i clau privada (secreta)**. A la metàfora de claus, tenim una **clau privada** i molts **cadenats oberts públics**. Qualsevol pot tancar una caixa amb un cadenat que contingui un text llegible per generar un text xifrat. Només pot obrir el cadenat (desxifrar) qui té la clau privada, que no l'ha de compartir amb ningú (secreta).

Per tant, **mai no s'ha de compartir amb ningú la nostra clau privada**, per això s'anomena també clau secreta, doncs li donem la capacitat d'usar aquesta clau pel seu compte. **Sempre hem de compartir la nostra clau pública**, ja que si no es fa pública ningú ens podrà

Què és un algorisme?

En matemàtiques, lògica, ciències de la computació i disciplines relacionades, un algorisme és un conjunt d'instruccions o regles definides i no ambigües, ordenades i finites que permet, típicament, solucionar un problema, realitzar un còmput, processar dades i dur a terme altres tasques o activitats.

A la vida quotidiana, s'utilitzen algorismes freqüentment per resoldre problemes determinats. Alguns exemples són els manuals d'usuari, que mostren algorismes per utilitzar un aparell, o les instruccions que rep un treballador del patró. Alguns exemples en matemàtica són l'algorisme de multiplicació, per calcular el producte, l'algorisme de la divisió per calcular el quocient de dos números.

enviar missatges. Metafòricament, hem de regalar cadenats oberts perquè la nostra clau privada els pugui obrir.

Funció resum: qualsevol funció que serveixi per calcular a partir de dades de longitud arbitrària un resultat de mida fixa. Per exemple, la resta de la divisió per 100 (mòdul 100) genera sempre un resultat entre 0 i 99 per a enters amb qualsevol nombre de xifres: el mòdul és una representació compacta de qualsevol sencer. A més, una bona funció resum hauria de ser ràpida de calcular i difícil de revertir (és a dir, trobar entrades corresponents a partir d'un resum).

La **petjada digital de la clau pública** és una breu seqüència de bytes que identifica una clau pública més llarga. És el resultat d'una funció resum de la clau pública.

Per exemple:

La clau de leandro@pangea.org té 4096 bytes, i la seva petjada (o resum) és:

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

3

PROTECCIÓ DE MISSATGES

Signar: facilitar que qualsevol pugui verificar la integritat d'un missatge (contingut) i la seva autenticitat (remitent), **afegint** al text un valor que permet **verificar** que el conjunt no ha canviat.

Xifrar: permet que només una persona pugui llegir-lo (extreure el missatge llegible d'un missatge xifrat), **substituint** el text llegible per un xifrat.

Per exemple, si l'Anna vol enviar un missatge a la Blanca:

Signar:

Anna pot preparar el missatge: la seva adreça (identitat) i el text a enviar. El missatge passa per una funció resum i el resultat el xifra amb la clau privada. Aquesta és la signatura que s'afegeix al missatge.

Per tant, Blanca i qualsevol altra persona podrà llegir el text ia més podrà verificar-ne la integritat: pot aplicar-li la funció resum i desxifrar la signatura. Si tots dos resums coincideixen, el missatge no ha estat alterat.

Per tant, **signem** els nostres missatges amb **la nostra clau privada** (no amb la del receptor, ja que és la nostra signatura).

[ÍNDEX]

Xifrar:

L'Anna vol enviar un missatge que només la Blanca pugui llegir. Anna busca la clau pública de Blanca i xifra el missatge, que substitueix el text llegible. Si ningú més que la Blanca té la seva clau privada, només la Blanca ho pot desxifrar.

Per tant, **xifrem** els nostres missatges amb la **clau pública del receptor**.

3.1 Com publicar la nostra clau pública?

Podem **publicar-la** a un servidor de claus públic (associada a la nostra adreça de correu). Podem també incloure la nostra clau pública en qualsevol missatge que enviem, o incloure un enllaç al servidor públic on sigui oa la nostra pàgina web personal.

Sempre podem enviar un missatge signat a qualsevol: només hem de dir alguna cosa i signar-ho amb la nostra clau privada.

En canvi, per enviar un missatge xifrat a algú, hem d'aconseguir la vostra clau pública per xifrar-lo amb la vostra clau. Així només ell ho podrà llegir. Ni tan sols nosaltres podrem.

4 CORREU SEGUR?

A diferència de la web, que la majoria ha passat de HTTP a HTTPS (xifrat), el transport de correu (SMTP) no se sol xifrar, no hi ha garantia. Si no es pot garantir el transport de correu, toca protegir els missatges: assegurar integritat (contingut), assegurar autenticitat (remitent), assegurar confidencialitat (només ho pot llegir el destinatari).

Per tenir integritat i autenticitat hem de signar (un resum) amb la nostra pròpia clau i afegir-ho al missatge. Qualsevol podrà verificar la integritat i l'autenticitat d'un missatge signat utilitzant la clau pública del remitent.

Per aconseguir confidencialitat hem de xifrar el nostre missatge amb la clau pública de la persona receptora, que només ella podrà desxifrar (si ella i només ella en té la clau privada).

4.1 Mètodes

- La parella de claus ens les atorga una autoritat: ens dóna la nostra clau privada i en publica l'altra. Aquest és el cas de S/MIME.
- La parella de claus ens les generem nosaltres: individual. Generem la parella de claus, desant la privada i publicant l'altra. Aquest és el cas de l'OpenPGP.

[ÍNDEX]

- Si no tenim una autoritat que ens proporcioni el servei de gestió de claus (S/MIME), ens les hem de generar nosaltres (OpenPGP).

4.2 Eines recomanades

Thunderbird per a PC.

K-9 Mail i OpenKeychain per a mòbil (Android).

Flowcrypt i Mailvelope per a clients de correu web com Gmail a PC.

5 POSADA EN PRÀCTICA

5.1 Instal·lació i configuració

Si tenim un compte de correu configurat a Thunderbird al nostre PC, només hem de generar la nostra parella de claus[1]. Hem de publicar la clau pública[2] i desar amb cura la privada al nostre PC, protegida per una contrasenya. És recomanable utilitzar un gestor de contrasenyes com KeepassXC per evitar oblidar una contrasenya més, ja que no cal reutilitzar-les.

Si tenim el mateix compte de correu configurat a l'aplicació “K-9 mail” del nostre mòbil i l'aplicació OpenKeychain instal·lada (Android), només hem d'exportar la nostra parella de claus a un fitxer, transferir-lo al mòbil, importar-lo a OpenKeychain i dir-li a K-9 que volem utilitzar “xifrat extrem a extrem” per al nostre compte de correu, habilitar OpenPGP i triar la nostra clau a OpenKeychain.

1 Eines → Configuració del compte → Xifratge extrem a extrem → Afegir Clau… → Crear una nova clau OpenPGP
2 Eines → Configuració del compte → Xifrat extrem a extrem → [X] Afegir la meva clau pública en afegir una signatura digital OpenPGP

[ÍNDEX]

5.2 Proves

Si jo sóc ana@pangea.org, puc generar un missatge de correu per a Blanca i a les opcions activar la signatura[3]. En enviar-lo, ens podeu demanar la contrasenya que protegeix la nostra clau privada. Afegirà una signatura i ho enviarà.

Quan el rebi Blanca veurà al seu client de correu que el missatge està signat per ana@pangea.org. També veureu la clau pública d'Anna o una part d'ella (l'empremta de la clau pública). Amb això podeu utilitzar o trobar la clau pública d'Anna i us podrà enviar un missatge xifrat.

Si l'Anna no s'ha comunicat mai amb la Blanca, no té clau pública. La podeu trobar en algun servidor de claus a Internet a partir de la vostra adreça de correu (tot i que no estarem segurs si l'ha publicada Ana), o si Ana en té, a la seva pàgina web personal. Si la coneixem, podem demanar directament a l'Anna la seva empremta. Així estarem més segurs. També ens la pot passar algú que coneix a tots dos (però signada per no perdre confiança), o mitjançant intermediaris que es coneixen entre si (una xarxa de confiança) i que les han intercanviat amb cura. No ens hem de fiar d'una firma que ens arriba per correu electrònic feta amb una clau pública que desconeixem, ja que la pot haver enviat una altra persona per confondre'ns i aparentar que ve de Blanca (el transport de correu no comprova gaire).

Aquesta explicació pretén que sapiguem com fer el correu electrònic més segur: integritat del contingut, autenticitat del remitent i confidencialitat del contingut per al destinatari.

3 Thunderbird: A la finestra del nou missatge: Seguretat → Signar digitalment aquest missatge
K-9 Android: Clic als en els tres punts verticals a dalt a la dreta i tria activar el mode de només signatura-PGP . Apareixerà una icona al costat de la meva adreça de remitent que indica signatura, no xifrada

5.3 Programes

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 Hem completat a Pangea la traducció al castellà ES-ES del suport per a OpenPGP. Alguns missatges encara surten en anglès, però esperem que aviat tots els missatges surtin en castellà. (aviat en Català)

5 F -Droid, com la resta d'aplicacions lliures per a 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

AMB EL SUPORT DE:

Pangea.org

< INTERNET
ÈTIC I SOLIDARI >

[ÍNDEX]