Sécurité Informatique

Comment crypter ses messages ?

Sur PC / laptop

* Sur GNU/Linux:

- Debian: Installez les paquets `icedove` et `enigmail`
- Ubuntu: Installez les paquets `thunderbird` et `enigmail`
- **Attention**: ne téléchargez pas directement des sites externes, l'installation par paquets du système permet de gérer automatiquement les mises-à-jour et l'intégrité de l'installation
- Assurez-vous que votre compte de courriel est bien configuré
- Configurez Enigmail pour générer un paire de clés et l'assigner à votre compte

* Sur Windows 7 / 10 et sur MAC OS:

- Téléchargez et installez Thunderbird
- Assurez-vous que votre compte de courriel est bien confiugré
- Téléchargez et installez l'extension Enigmail
- Configurez Enigmail pour générer un paire de clés et l'assigner à votre compte

Sur Mobile / tablette

Notes

- Utilisez un PIN / code de vérrouillage pour votre appareil
- Il est suggéré d'utiliser des clés séparées pour une installation mobile vs. bureau
- Tenez compte des risques élevés lors de la perte plus probable d'un appareil mobile

* Installez le logiciel F-Droid permettant de gérer l'installation, l'intégrité et la mise-à-jour de logiciels libres sur Android

- Si vous ne pouvez absolument pas installer F-Droid, utilisez Google Play - tenez compte des problèmes liés aux suivis et traçage d'applications de cet environnement

* Installez OpenKeyChain via F-Droid # Procédez à la configuration du compte via OpenKeyChain.

Sur web

En dernier recours, si vous utilisez uniquement un service de courriel web, il est quand même possible de crypter et signer vos courriels. **Tenez compte des risques élevés de compromettre vos clés et/ou votre mot de passe dans ce contexte**.

L'extension / application MailVelope est suggérée pour ce genre d'utilisation.

Pourquoi crypter ses messages ?

Le courriel demeure un moyen efficace de communiquer avec ses amis, ses collègues, ou encore sa famille, mais:

- il ne permet pas d'authentifier l'identité de l'expéditeur,
- il ne permet pas de s'assurer qu'il n'est déchiffrable que par le destinataire.

Malgré la possibilité de chiffrer et signer les courriels par des méthodes cryptographiques, **gardons à l'espirt que les métadonnées peuvent être modifiées en transit** (expéditeur, objet, date et heure). La date et heure sont les seule métadonnées pouvant être vérifiés dans la signature électronique (voir ci-bas).

> *Le cryptage de messages permet d'encoder un courrier électronique, ce qui le rend lisible uniquement par la personne possédant la clé permettant de le déchiffrer.*

OpenPGP: Le chiffrement asymétrique

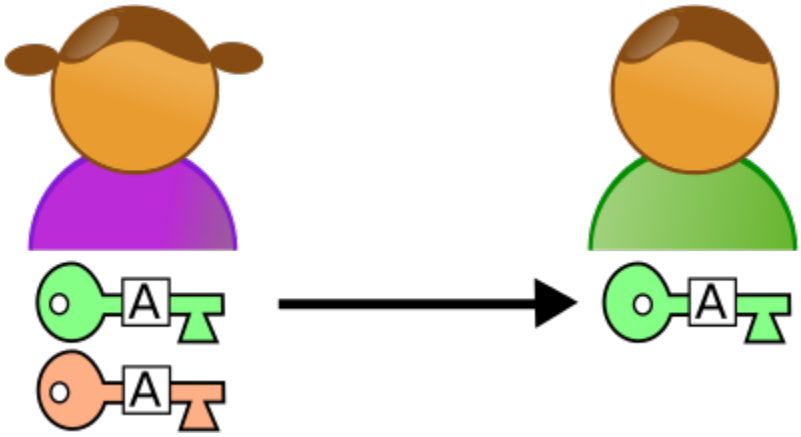
Pour pallier au problème d'échange de clés lors de l'établissement de communications sécuritaires, des logiciels utilisant *le chiffrement asymétrique* ont été conçus.

Une des normes basées sur ce concept est la norme **OpenPGP**. Ce type de chiffrement utilise deux clés liées mathématiquement :

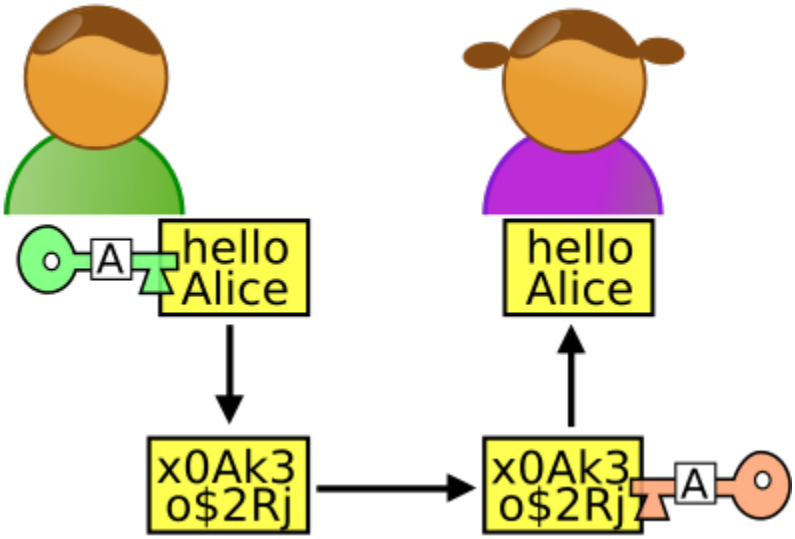
- Une clé privée : Elle est utilisée pour déchiffrer un message que vous avez reçu. La vôtre ne devra jamais être révélée, même si elle est elle-même chiffrée par un mot de passe que vous détenez.
- Une clé publique : n'importe qui peut utiliser votre clé publique pour chiffrer un message avant de vous l'envoyer. Elle peut être communiquée à n'importe qui.

Voici un exemple:

Bob et Alice veulent s'échanger des messages chiffrés. Si Bob veut envoyer un message crypté à Alice, il doit connaître la clé publique de cette dernière. On présume qu'Alice a installé un logiciel qui lui a permis de créer sa paire de clés: une clé privée (clé "A" rouge) et une clé publique (clé "A" verte):



Étant donné qu'elle est autorisée à communiquer sa clé publique (Clé "A" verte) à d'autres personnes, Alice l'envoie par courriel à Bob. Ce dernier peut maintenant l'utiliser pour crypter son message avant de l'envoyer à Alice.



Bob crypte le message avec la clef publique d'Alice et envoie le texte crypté. Alice déchiffre le message grâce à sa clé privée.

Maintenant, imaginons qu'une troisième personne, Robert, veuille intercepter et lire les messages de Bob et d'Alice. Bob a donc crypté son courriel avec la clé publique d'Alice:

- Robert ouvre le logiciel de messagerie d'Alice alors qu'elle n'est pas à son ordinateur, et découvre que Bob lui a envoyé un message crypté.
- En regardant dans le répertoire « Courriels envoyés » d'Alice Robert voit que celle-ci avait transmis à Bob sa clé publique.

Il ne pourra pas déchiffrer le message de Bob car **seule la clé privée d'Alice combinée au mot de passe qui y est associé permettent de déchiffrer le message** que Bob a envoyé.

Notes: *On peut augmenter le niveau de protection des clés en utilisant un stockage amovible (clé USB) pour entreposer la clé privée, et en s'assurant d'utiliser une phrase de passe complexe. Si Robert a accès physique à l'ordinateur, il pourrait installer un* ***keylogger*** *permettant d'enregistrer le mot de passe.*

La signature numérique

Qu’est-ce que « signer » un message ?

C’est le fait d’utiliser la clé privée pour assurer l'intégrite de son contenu et métadonnées de date/heure de création: * l'authenticité du message * l'origine * la date de création de contenus.

Si vous signez vos courriels, votre destinataire saura que c’est obligatoirement le possesseur de la paire de clés qui a signé ce message.

Des fonctionnalités plus avancées de OpenPGP permettent de signer la clé publique de vos interlocuteurs afin de signaler une vérification d'identité à un degré plus ou moins élevé de confiance. Ce processus ressemble au travail des notaires et constitue, dans son ensemble, ce qu'on appelle la « Web of Trust » (toile de confiance).

Ainsi, il est suggéré de faire signer sa clé publique par autant de vos interlocuteurs qu'il sera possible, afin que son authenticité soit plus facile à déterminer.

Une signature dite *de révocation* permet de créer un fichier qui servira à annuler la validité une paire de clés OpenPGP si on voudrait le faire (suite à une perte, ou intrusion).

Liens utiles

- Guide d'autodéfense courriel de la FSF
- Introduction à la cryptographie à clé publique - guide de la EFF

Références

- Security in a box, outils et tactiques de sécurité numérique
- Guide Thunderbird et Enigmail, Fabian Rodriguez