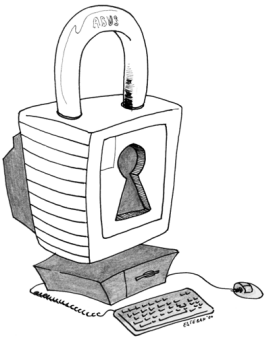


CRYPTER SES MAILS

DES CARTES POSTALES SANS ENVELOPPE

Le cryptage (ou chiffrement) est une opération mathématique qui permet de coder le contenu d'un message afin de garantir que seulE votre correspondantE pourra le déchiffrer (ou le décrypter).

Une mauvaise connaissance de l'Internet laisse souvent croire à beaucoup que la confidentialité des courriers est plus ou moins assurée ou respectée. Cependant, envoyer un mail non crypté revient strictement à poster une carte postale sans enveloppe !

Lors de son acheminement, un email est relayé par un certain nombre de serveurs où il se retrouve donc copié. Et derrière ces serveurs, ce sont autant d'entreprises commerciales ou d'administrateurices curieuSEx qui peuvent, bien que la loi défende les correspondances privées, fouiner dans vos courriers. Les mails peuvent également être interceptés lors de leurs transferts.

Il est de plus extrêmement facile de falsifier une identité par courrier électronique. La cryptographie permet de signer les messages afin de prouver qu'on en est bien l'auteurE.

Cette brochure propose une petite introduction aux mécanismes, aux outils et aux usages de la cryptographie à double clé. Nous allons utiliser pour cela trois logiciels libres disponibles aussi bien sous GNU/Linux, Windows que MacOS X :

- GPG (GNU Privacy Guard, un outil de cryptographie)
- Thunderbird (un logiciel pour écrire et recevoir des mails)
- Enigmail (une extension de Thunderbird qui permet d'utiliser GPG pour crypter ses mails)

COMMENT ÇA MARCHE ?

La cryptographie à double clé fait intervenir, comme son nom l'indique, deux clés lors d'un échange. Chaque participantE possède deux clés qui sont associées à son adresse email : une clé privée et une clé publique.

➔ sa clé privée est gardée secrète et lui servira à :
- décrypter les messages qui lui sont adressés
- signer les messages qu'ille envoie

➔ sa clé publique peut être communiquée librement et permettra à ses correspondantEs :
- de lui envoyer des messages qu'ille sera seulE à pouvoir décrypter
- de vérifier qu'ille est bien l'auteurE des messages

Revoyons ça en image. Alice veut envoyer un message à Bob :

cas du cryptage d'un mail

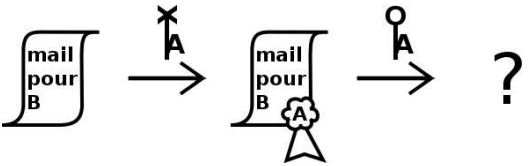
Alice utilise
la clé publique de Bob
pour lui crypter un message

Bob utilise
sa propre clé privée
pour déchiffrer le message

cas de la signature d'un mail

Alice utilise
sa propre clé privée
pour signer un message

Bob utilise
la clé publique d'Alice
pour vérifier qu'Alice est l'auteure



remarques

➔ Signer un mail rajoute juste quelques lignes spéciales à la fin du mail, son contenu reste « en clair ».

➔ Crypter un message encode le texte du message mais ne protège ni les adresses ni le sujet ni les autres entêtes.

➔ On peut combiner les deux techniques, cryptage et signature, afin d'avoir à la fois la confidentialité et l'authenticité.

LES OUTILS NÉCESSAIRES

Des tutoriaux plus complets sont disponibles sur Internet :

- ⇨ *http://www.geckozone.org/articles/2004/07/14/29-chiffrer-son-courriel-avec-mozilla-thunderbird-et-enigmail*
- ⇨ *http://www.fabianrodriguez.com/files/tb-enigmail.pdf*

thunderbird

Thunderbird est un client mail : un logiciel qui sert à écrire et à envoyer des mails. Il est très bien conçu et très utile, même hors du cadre de la cryptographie. Plus d'infos sur :

- ⇨ *http://www.mozilla-europe.org/fr/products/thunderbird*

gpg

Il en existe des versions pour GNU/Linux, Windows ou MacOS X :

- ⇨ *http://www.gnupg.org/(fr)/download/index.html#auto-ref-1*

enigmail

Enigmail est une extension de Thunderbird qui utilise GPG pour crypter et signer des mails. Elle permet également d'accéder simplement aux fonctionnalités de gestion de clés de GPG. Récupérez les fichiers .xpi d'Enigmail et de sa traduction française sur :

- ⇨ *http://enigmail.mozdev.org*
- ⇨ *http://enigmail.mozdev.org/langpack.html*

Installez ces extensions via le menu [Outils / Extensions / Installer] de Thunderbird. Redémarrez Thunderbird.

configuration d'enigmail

Indiquez l'emplacement de l'exécutable GPG dans [Enigmail / Préférences] (sous GNU/Linux `/usr/bin/gpg`, sous Windows ce peut être `C:\Program Files\GNU\GnuPG\gpg.exe`).

Dans [Outils / Paramètres des comptes ... / Sécurité OpenPGP] choisissez « Activer le support OpenPGP pour cette identité ».

création d'une clé

Il vous faut maintenant vous créer une paire de clés. Ouvrez le gestionnaire de clés ([Enigmail / Gestion de clefs OpenPGP]) puis [Générer / Nouvelle paire de clefs]. Pour une bonne phrase de passe, mélangez les minuscules, les majuscules et les chiffres.

importer des clés

Pour envoyer un message crypté à quelqu'unE il vous faudra auparavant lui demander sa clé publique sous forme de fichier (généralement .asc) puis l'importer. Utilisez le menu [Fichier / Importer des clefs depuis un fichier] du gestionnaire de clés. Vous pouvez également rechercher des clés sur un serveur de clés via [Serveur de clefs / Chercher des clefs].

exporter votre clé

Pour que vos correspondantEs puissent vous envoyer des mails cryptés ou vérifier vos signatures vous devez leur communiquer votre clé publique. Pour l'exporter, sélectionnez votre double clé dans le gestionnaire de clés et utilisez [Fichier / Exporter des clés vers un fichier] ou [Serveur de clefs / Envoyer les clefs publiques].

envoi d'un message crypté

Lors de la rédaction d'un mail cochez [Enigmail / Signer le message – Chiffrer le message]. La clé correspondant à l'adresse de destination du mail sera sélectionnée automatiquement. Vous pouvez modifier les options de cryptage et de signature par défaut dans [Outils / Paramètres des comptes ... / Sécurité OpenPGP] pour les rendre systématiques. GPG permet de crypter un message pour plusieurs destinataires à la fois.

SÉCURITÉ ET USAGE

La cryptographie proposée par GPG est aussi dite cryptographie « forte ». Il faudrait mobiliser plusieurs dizaines ou centaines d'ordinateurs pendant plusieurs dizaines d'années pour casser un seul mail. La sécurité proposée reste donc très confortable.

Il serait néanmoins maladroit de crypter uniquement les mails « sensibles » (qui seraient alors identifiables comme sensibles !). Une bonne habitude est donc de crypter régulièrement des mails même non sensibles.

Une autre bonne habitude à prendre est de signer systématiquement ses mails : les mails restent lisibles même si votre correspondantEs n'utilise pas la cryptographie mais cela montre que vous l'utilisez et, comme pour toute signature, plus vous vous en servez plus elle gagne en crédibilité.