Comment chiffrer ses mails

- Infos - Informatique -

Date de mise en ligne : samedi 18 avril 2009

Description :

Présentation et mise en place du chiffrement des mails, communément appelé cryptage.

Rebellyon.info

La cryptographie tout le monde en a déjà entendu parler mais rares sont ceux qui la pratiquent. Il s'agit de se protéger de la récupération policière de ces mails auxquels la majorité des personnes ne font, finalement, pas trop attention.

Avec la loi Hadopi et la criminalisation de l'échange sur le net se pose la question de la protection de la vie privé. Plus encore la question de nos libertés numériques deviens fondamental quand le gouvernement veut construire une autorité spécialisé dans la récolte d'adresse IP sur les réseau pair à pair (P2P)..
Mais il n'y a pas que cela, on sait que pour l'enquête de Tarnac les militants en question ont vue leurs mails interceptés. Quand est-il de la prudence des militants dans le contenu de nos courriels ? Bien souvent nous ne faisons vraiment pas attention et c'est dommageable. L'activité policière allant surement dans un élargissement vers le contrôle de cet outil dans les années à venir, nous vous proposons une introduction au chiffrement [1] des mails. Nous vous assurons qu'à l'usage cette solution de protection est vraiment devenu facile à mettre en oeuvre.
Chiffrer un e-mail c'est non seulement protéger la confidentialité de l'information, mais c'est aussi une garantie pour l'expéditeur que seul le destinataire pourras le lire, et une garantie pour le destinataire qu'il a bien été envoyé par le Â« bon Â» expéditeur (il est très facile d'envoyer un mail avec l'adresse de quelqu'un d'autre).
Il n'est pas anodin de protéger le contenus de vos mails. Et il est encore plus judicieux de le faire pour tout les mails, sinon cela met en évidence le caractère confidentiel du mail crypté, et surtout les noms de leur destinataire.

Le chiffrement de ses mails, comment ça marche ?

Cela fonctionne avec d'une part une clé publique pour chiffrer son mail donc c'est une clé que vous pouvez envoyé à vos amis. Pour l'utiliser pas besoin de code tout est transparent.
Pour déchiffrer par contre vous avez besoin d'une clé privée **à ne surtout pas donner**. Ce système de double clé est donc une méthode de chiffrement asymétrique.. En fait pour que le système marche correctement il faut que chacun des correspondants donne sa clé publique à l'autre et déchiffre de son coté avec sa clé privée.

[Chiffrement asymétrique]

Mise en place du chiffrement

Avant de vous lancer dans le chiffrement de votre mail vous devez créer votre paire de clés (privé/public).

Pour les windoziens il existe WinPT qui est une interface graphique à GnuPrivacyGuard (GPG). Ces programmes sont téléchargeable dans un seul installateur appelé Gpg4win. Pour générer votre clé sous WinPT c'est assez simple il vous suffit de suivre ce tutoriel.

Pour les linuxiens GPG est en principe installé par défaut (sinon il faut installer le paquet *gnupg* : `apt-get install gnupg`), et il vous suffit de taper dans votre console préférée la ligne suivante en tant que simple utilisateur :

gpg -gen-key

Laissez vous guider par les menus en choisissant les réponses suivantes :

- type de clé : DSA et ElGamal
- taille de clé : 2048 bits
- durée de validité de la clé : n'expire jamais
- renseigner les différentes entrées (mail, etc..) Pour le mot de passe il faut mettre un truc bien long avec de la ponctuation !

Un fois la paire de clés générée, il est conseillé de générer un certificat de révocation :

gpg -outpout certif-revoc.asc -gen-revoke votreadresse@mail

A noter que toutes ces commandes sont également valables sous windows dans une console DOS à partir du moment où GPG est installé.

Une fois vos clés créer garder les en sécurité par exemple sur une clé usb.

Concernant le mot de passe, n'hésiter pas à faire long et complexe (quitte à l'écrire sur un papier au début, que vous brûlerez par la suite !) car il constitue l'ultime protection de la clé privée. Pour utiliser la clé privée, il faut obligatoirement le mot de passe.

Une fois la paire de clé générée, vous pouvez l'utiliser pour chiffrer vos mails !

Le chiffrement des mails

Si vous utilisez un client mail tel que thunderbird ou outlook, il existe des plugins à installer qui vous permettront de chiffrer/déchiffrer très facilement :

- Plugin pour thunderbird : Enigmail
- Plugin pour outlook : G-Data

Dans le cas de thunderbird, le plugin ajoute un menu qui donne accès à différentes options : générer une paire de clés, signer un mail, chiffrer un mail, importer des clés, etc... Un tutoriel se trouve en pièce jointe de cet article.

!Attention ces plugins ne fonctionnent que si GPG est installé sur votre ordinateur !

Dans le cas où votre client mail ne supporte pas gpg...*mauvais logiciel, changer de logiciel !*

Si vous utiliser le navigateur web Firefox, il existe une extension Firefox appelé FireGpg qui vous permet de gérer votre trousseau de clé. Vous l'installer dans Firefox et il ne vous reste plus qu'à sélectionner dans vos courriel le texte et de lui demander de chiffrer. Pour déchiffrer sélectionner le texte et demander déchiffrer après avoir taper votre phrase secrète.

Différents liens pour mieux comprendre :

- Chiffrement
- Chiffrement asymétrique.
- Manuel d'utilisation de GnuPG

Post-scriptum :

Il est joint à cet article un petit tuto maison pour FireGpg, et deux autres pour GnuPG et enigmail (le plugin de thunderbird)

---

[1] Lorsque l'on crypte un message on parle de chiffrement. Le terme cryptage, bien que souvent employé n'est pas correcte. Il est tiré du terme anglais « encryption ».