Des chiffres et des lettres

Protéger ses communications en ligne
et autres aspects de sa vie numérique

GnuPG et OpenPGP pour tous

Stéphane 22Decembre Guedon

version base 1 du 3 juillet 2015

Chapitre 1

Préambule

Ce document utilise les textes issus du tutoriel ou how-to GPG que j'ai écris. Il s'agit là de la version *de base*, soit les fonctions que j'estime les plus importantes de GnuPG et OpenPG.

Ce How-to peut être lu sur mon site internet [1] Je vous encourage vivement à le partager, le repartager, que ce soit pour la version en ligne (html) ou hors-ligne (le pdf que vous êtes en train de lire).

Bien entendu, les textes ont été légèrement modifiés pour correspondre à la forme qui lui est donné ici, à savoir un mini livre. Mais j'ai conservé les exercices.

Le but avoué de ce document est d'encourager les utilisateurs d'internet, soit en fait une grosse partie de la population occidentale, à protéger leurs communications telles que courriels et messagerie instantanée.

Au moment même de la rédaction de ce livre, une loi extrêmement dangereuse pour les libertés civiles est en cours d'adoption par le parlement et le gouvernement français. [2]

Le fichier support à ce document, à savoir le fichier pdf que vous lisez, est signé avec ma clé gpg ainsi que la clé gpg créée exprès pour les besoins de ce tutoriel et les deux clés ont été incluses en pièces jointes au fichier pdf.

Voici leurs empreintes :

$$30CF\ 1DA5\ 7E87\ 6BAA\ 730D\ E561\ 42E0\ A02E\ F1C9\ 35A4$$

$$F6B2\ DCE3\ B6F6\ A972\ FF3A\ 1C9B\ 2041\ 3A8E\ 7F36\ CE55$$

Le texte de ce document (soit en fait, mon travail) est placé sous licence Creative Commons BY. J'ai utilisé des illustrations provenant de sources externes :

- le logo de GnuPG, sous licence CC-BY-SA [3]
- la bande dessinée de XKCD relavite à la force des mots de passe, sous licence CC BY-NC 2.5 [4]
- L'ombre de la Justice, sous licence CC BY-NC-ND 2.0. [5]

Les sources au format LaTeXsont disponibles dans le dépot github https://github.com/tutogpgIn22D/book-fr. Cette version a été tagée "version base 1" et signée avec ma clé gpg personnelle.

1. version anglaise : http://www.22decembre.eu/category/howto-gpg.html. Cliquez sur les liens «fr» sous les titres pour lire les articles en français.
2. http://www.senat.fr/espace_presse/actualites/201505/un_projet_de_loi_pour_renforcer_les_services_de_renseignement.html
3. http://www.gnupg.org
4. https://xkcd.com/936/
5. https://www.flickr.com/photos/jmtimages/3286566742/

Table des matières

Chapitre 2

Introduction :Pourquoi vous devez utiliser GPG ?

Quand j'écris des courriels ou que je montre ma carte de visite, il y a des gens qui me demandent : c'est quoi GPG ? C'est quoi ce fichier en pièce joint de votre courriel ?

Figure 2.1 – *Des cartes de visites comportant une empreinte de clé GPG*

Je suis toujours aussi surpris qu'après les révélations d'Edward Snowden[1] sur la surveillance de masse des services secrets américains (NSA, CIA...), et les découvertes, chaque jour de l'étendue et des pouvoirs des services secrets occidentaux[2] - y compris français -, il y ait des gens (la *majorité* des gens en fait, aussi triste que ça puisse paraître !) qui ne connaissent pas GPG !

1. https://fr.wikipedia.org/wiki/Révélations_d'Edward_Snowden
2. http://www.lemonde.fr/pixels/article/2015/02/17/un-nouveau-logiciel-espion-de-la-nsa-mis-au-jour_4577707_4408996.html

Je me suis donc décidé à publier ce puis un tutoriel au long court qui j'espère, vous permettront d'apprendre à l'utiliser correctement.

2.1 La démarche

À l'opposé de la plupart des tutoriels que vous trouverez sur le net à propos de GPG, je vais m'efforcer de vous donner les points importants progressivement, de sorte que vous preniez le temps d'assimiler tout cela.

En effet, il est inutile, si ce n'est dangereux de vous montrer comment créer des clés de chiffrement, de vous mener par la main sur tout le chemin et de vous lâcher dans la nature au bout, à peine deux jours après vous avoir mis dans le bain.

Il vaut mieux être bien plus progressif. Vous faire réflechir et vous donner les liens pour comprendre et vous permettre d'approfondir votre apprentissage et votre compréhension.

2.2 C'est quoi GPG ?

2.2.1 Tout d'abord il y eu PGP

PGP est un sigle pour *Pretty Good Privacy*, *Plutôt Bonne Vie Privée* en français.

PGP est le logiciel originel, conçu par Philip Zimmermann [3], dans le but explicite de défendre la vie privée, les libertés individuelles et plus largement la démocratie [4]. C'est à la base un outil permettant de signer et chiffrer sa correspondance électronique. En français, son mail ou son courriel.

Ce mot, *chiffrement*, il est très important : il indique que l'on fait appel ici à des mathématiques de très haut niveau, avec des concepts et des algorithmes complexes.
Pas d'inquiétude toutefois ! C'est le logiciel lui-même qui fait ces opérations mathématiques.

2.2.2 Puis OpenPGP

Puis l'IETF, a normalisé PGP et ça a donné le format de chiffrement OpenPGP [5], qui garantit que les différents utilisateurs du format peuvent échanger grâce à ce même format d'échanges.

2.2.3 Finalement est venu GPG

Ceci a permis à des développeurs libristes de concevoir un logiciel, GnuPG [6], abrégé en GPG, implémentant le format OpenPGP. Autrement dit : grâce à OpenPGP, les utilisateurs de GnuPG et PGP peuvent correspondre ensemble sans problème.

2.3 Pourquoi l'utiliser ?

Vous êtes en couple ? Votre femme (ou votre homme ...) vous envoie des photos osées pour vous exciter, ou plus simplement vous échangez des propos classés X, que vous ne souhaiteriez surtout pas laisser à disposition du premier venu !

Vous avez une compétition de cuisine et voulez partager votre recette de la tarte au citron avec Bree Hodges, mais pas avec Katherine Mayfair ?

3. http://philzimmermann.com/FR/background/index.html
4. http://openpgp.vie-privee.org/pourquoi.htm
5. https://fr.wikipedia.org/wiki/OpenPGP
6. https://www.gnupg.org/

Vous voulez monter une entreprise, ou vous travaillez déjà, et souhaiter donc communiquer en toute sécurité avec vos associés ?

Vous êtes journaliste et voulez communiquer de manière sécurisée avec vos sources ? Ce cas est particulier, puisqu'idéalement, vos sources doivent pouvoir, dès le départ, sans même vous connaître, communiquer avec vous de manière confidentielle ! Il est à noter que ce fut le cas d'Edward Snowden : il a utilisé PGP et demandé à ses contacts de faire de même pour assurer des échanges sûrs.

Certaines de ces raisons semblent futiles. Mais ce que *Desperate Housewives*, et les gens autour de nous, nous ont bel et bien montré, c'est que, aussi futile que ce soit, quelqu'un peut néanmoins être assez motivé pour vouloir ouvrir votre courrier et dans ce cas, cette personne mettra aussi en œuvre les moyens les plus importants, et parfois de manière totalement disproportionnée.

Mais passons à autre chose... Ouuuuiiii...

Google [7], Yahoo [8] et Microsoft [9] lisent vos courriels pour faire du profilage ! Vous rappelez-vous de ce scandale, avec des photos de stars de cinéma volées [10] ?
Si vous estimez que la reaction de ces stars (indignation devant les violations de leur vie privée) est normale, saine, pourquoi n'accordez-vous pas la même valeur à votre vie privée aussi ?

Bonne nouvelle toutefois, GPG est toujours sûr apparament [11] !

D'ailleurs, pour vous donner une autre raison d'utiliser GPG : le mail, à la base, c'est du texte. Rien de plus simple à intercepter, lire, détourner. En fait, envoyer un mail, c'est envoyer une carte postale ! Ça va bien pour parler des photos du chat, mais très rapidement, ça devient critique... Non ?

2.4 C'est douloureux ?

Disons que l'utilisation du chiffrement n'est pas forcement hyper-simple. Toutefois, je ne vois aucun moyen, ni aucune raison sérieuse de s'en passer.

En mettant à disposition de tous un tutoriel perenne, en vous permettant, progressivement, de découvrir le fonctionnement d'OpenPGP, j'espère vous permettre et vous encourager à proteger votre vie privée et vos libertés individuelles, et celles des personnes qui vous sont chères. Vous verrez qu'après un peu d'entrainement, l'utilisation de cet outil devient très vite naturel.

7. http://www.linformaticien.com/actualites/id/32860/google-lit-vos-mails-et-assume.aspx
8. http://www.zdnet.fr/actualites/yahoo-lit-les-emails-de-ses-utilisateurs-quoi-de-neuf-doc-39791003.htm
9. http://www.numerama.com/magazine/33357-windows-10-microsoft-et-vos-donnees-privees-ce-que-vous-devez-savoir.html
10. http://www.huffingtonpost.fr/2014/09/02/jennifer-lawrence-nue-piratage-internet-kate-upton-photos-celebgate_n_5745970.html
11. http://www.ginjfo.com/actualites/politique-et-economie/espionnage-nsa-depose-les-armes-devant-certaines-solut

Chapitre 3

Existe t-il des alternatives sérieuses à l'utilisation de GPG ?

Notice

Ce chapitre est plutôt destiné aux personnes à compétences techniques dans le domaine de l'informatique, communément appelées **geeks** ou ***nerds***. Toutefois les novices peuvent y lire des choses intéressantes pour eux. Ils sont donc invités dans ce cas à faire des recherches et à avoir beaucoup de patience dans celles-ci.

On a donc OpenPGP et ses implémentations logicielles, PGP et GPG, des outils pour protéger son courriels des regards indiscrèts. Mais est-ce le meilleur moyen ?

3.1 Bitmessage

Il existe par exemple Bitmessage[1], qui est pour moi l'anti-exemple parfait, puisqu'il ne respecte pas le paradoxe de la moquette[2] : les adresses ressemblent furieusement à des chaînes de caractères aléatoires, il n'est donc pas aisé de donner son adresse à son interlocuteur.

Même donner son adresse sur papier présente le risque que votre interlocuteur se trompe en la recopiant.
Il n'est donc rien de plus facile que de se gourer et d'envoyer son message à quelqu'un d'autre.
Je pense que le moyen le plus efficace est encore de copier son adresse sur un site web (et encore faut-il être prudent !).

La base du fonctionnement du réseau Bitmessage lui-même est compréhensible. Mais dès qu'on essaye de comprendre davantage (essentiel, lorsqu'il s'agit de protocoles de sécurité et de chiffrement), on se met à se gratter la tête !

3.1.1 Un petit truc étrange, une réflexion, comme ça...

Il y a également un truc qui me chiffonne, outre l'aspect obscur, non-écologique, non-efficient au plan énergétique : le protocole Bitmessage est conçu pour noyer les communications chiffrées dans le flot des données P2P bit-torrent. Ainsi, soit disant, la NSA (qui est typiquement l'organisme auquel

1. http://www.bortzmeyer.org/bitmessage.html
2. http://www.22decembre.eu/2015/02/23/carpet-paradox-fr/

les concepteurs du protocole tentent d'échapper) ne verrait pas ce flot de données. Mais justement, la NSA a maintenant connaissance d'un protocole de communications sécurisé utilisé par des hackers de haut-niveau ! Enfin du moins, elle doit être au courant : elle lit des courriels, visite les sites web et les forums...

On *doit* assumer qu'elle est au courant ! Donc quelqu'un a conçu un protocole de communications dans le but d'échapper à la NSA, et ce protocole envoie en permanence *tous* les messages à *tout* le réseau. Quoi de plus facile pour la NSA (et pour tous les autres maintenant) de se créer une ou plusieurs adresses Bitmessage, moissoner le flux indistinctement, et tenter de casser le code de chiffrement, puisqu'apparemment, c'est ce qu'elle fait déjà[3] !

Le code de Bitmessage repose, en partie sur SSL/TLS, une technologie commune et répandue, sur laquelle tout le monde travaille. Pas le plus sûr comme je l'indique plus bas.

3.1.2 GPG ou Bitmessage ?

Notice

Je précise que ceci est mon opinion, mon utilisation de mes outils informatiques. Ce n'est pas un commandement sacré à respecter au pied de la lettre. Il peut y avoir débat. Si vous voulez troller, libre à vous, mais ce sera sans moi !

Je préfère donc utiliser GPG plutôt que Bitmessage. Le courriel est légitime, je n'ai pas de raison de le cacher - même si je comprends les arguments de ceux qui le veulent, entre autre cacher *à qui on écrit*.

Utiliser Bitmessage me marque automatiquement comme un *hacker* de haut vol, ce que je ne suis pas. Tout juste puis-je et souhaite prétendre au status de *petit* hacker ou de *padawan*. En utilisant Bitmessage, j'encourage des gens à surveiller mon courriel et à tenter de le lire. Au contraire, en écrivant des courriels signés et/ou chiffrés, j'assume ma correspondance, et en même temps je la protège, ce qui est on ne peut plus légitime. Et comme c'est toujours du courriel, ça incite mes contacts à utiliser GPG.

Et si quelqu'un s'amuse à décrypter mon courriel, il découvrira alors probablement mes échanges avec mon amie lesbienne ou mes propositions de projets dans le cadre de mon travail. Des choses hautement inutiles pour NSA & co !

Point bonus : à moi, ça me m'a demandé aucun effort, alors que mon amie la NSA a gâché X heures de temps de calcul dessus !

> *Et faire chier les gens qu'on n'aime pas dès le matin, c'est vraiment gratifiant !*
>
> *Extrait de l'interview de Coreight par Cyrille Borne*[4]

3.2 Les autres systèmes de chiffrement classiques

On peut chiffrer et authentifier son courrier avec SSL/TLS, par le biais du format S/Mime. Certaines entités fournissent des certificats personnels gratuitement. C'est le cas de DanID qui fournit le système d'authentification NemID, permettant d'accéder aux sites bancaires et gouvernementaux

3. http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html - lien en anglais
4. http://cyrille-borne.com/article47/du-berger-a-la-bergere-l-interview-de-coreight

danois. Les certificats fournis par NemID sont valides pour signer et chiffrer du courrier, et s'authentifier sur certains sites web, notamment DBA, le Bon Coin danois, mais pas pour sécuriser son site web - hélas. En apparence, ces certificats sont donc une bonne chose pour sécuriser son courrier (les certificats de NemID sont un premier pas en avant vers l'identité virtuelle des citoyens après tout). Mais SSL et TLS sont assez sujets à critiques dernièrement, et la NSA (et d'autres agences de renseignement certainement) a déjà cassé nombre de ses algorithmes apparemment.

J'ai tendance à me mefier de plus en plus de TLS, en plus de son manque d'ergonomie, parce qu'apparemment c'est aussi solide qu'une passoire en plastique et tout aussi troué.

Notice

Néamoins, je recommande toujours l'utilisation de TLS dans la navigation web ! Un bouclier en plastique, c'est mieux que pas de bouclier du tout !

SSL/TLS et GPG sont toutefois deux implémentations légerement différentes du même principe : chiffrement asymétrique, avec une clé publique et une clé privée. Dans les faits, ce n'est donc pas vraiment plus facile, et certainement pas plus sûr d'utiliser SSL/TLS.

Pour le courriel, je pense qu'il vaut mieux utiliser un outil conçu pour ça, à savoir GPG.

3.3 Retour à GPG

GPG lui s'efforce de respecter le paradoxe de la moquette : il s'appuie sur des protocoles connus, assez bien maîtrisés et facile à prendre en main (le courriel). Les clés peuvent être identifiées par l'adresse courriel et/ou l'empreinte. Ceci permet de les trouver facilement et rassure les utilisateurs.

Et il n'était pas cassé par la NSA au dernières nouvelles.

Chapitre 4

Installation des outils de base

4.1 Les logiciels nécessaires

Pour pouvoir utiliser GPG, il vous faut ...

1. GPG
2. Un gestionnaire de clés tel que :
   - Kgpg/Kleopatra
   - Enigmail
3. Un client courriel tel que :
   - Kmail
   - Thunderbird
   - Évolution

Très souvent, les gestionnaires de clés sont des logiciels additifs aux clients courriels, des extensions. Ils ont pour la plupart les mêmes options de base. Le choix de tel ou tel environnement s'avère donc trivial, une affaire de goût et d'esthétique plutôt que de fonctionnalités.

Kgpg est un élément de la suite KDE, qui s'utilise donc surtout avec Kmail et Kontact. De même Enigmail fonctionne avec Thunderbird.

Notice

Il est à noter que les tablettes et téléphones Samsung avec Android ont maintenant tous les outils GPG nécessaires. Le problème c'est que vous ne pouvez vraiment leur faire confiance.

C'est néanmoins un bon moyen pour faire votre initiation à GPG. Vous voudrez certainement recréer des clés après ça sur un vrai ordinateur.

Au passage, vous pouvez envisager, si vous êtes vraiment motivé, d'installer votre propre système de courriel. Ça devient accessible au non-informaticien, grâce à YunoHost[1] par exemple. Ou dans une autre philosophie, OpenBSD, très simple d'installation[2], mais un poil difficile à prendre en main. Toutefois, pas plus difficile, de base, qu'une Debian.

1. https://yunohost.org/
2. http://blog.chown.me/pourquoi-j-adore-openbsd.html

4.2 Recommandations

Notice

La plupart de ces recommandations sont d'ordre général. Il s'agit de ce qu'on pourrait appeler "des pratiques de base saines pour votre ordinateur".

4.2.1 Sécurité du courriel

En gros, il faut éviter le webmail, qui est une très mauvaise chose - déjà de base - puisque vous accédez à votre courriel via le web, donc on ne maîtrise pas la sécurité. Sans même parler d'utiliser GPG là dedans !

Le chiffrement et les signatures de vos courriels ne vous protégeront nullement contre les virus et autres saloperies qui traînent ! Ils vous garantiront que vos courriels sont bien authentiques et/ou n'ont pas été lus par une autre personne que le destinataire légitime.

4.2.2 Sécurité des logiciels

Il faut également éviter de récupérer des logiciels sur des sites tiers comme 01net et telecharger.com. Il est plutôt recommandé d'aller voir le site web du concepteur du logiciel - tout en restant prudent [3], ou un site officiel, comme le site web d'Apple pour le cas d'un logiciel pour Mac par exemple.

Lorsque vous pouvez utiliser un logiciel libre ou open-source plutôt qu'un logiciel propriétaire, faîtes le. C'est d'autant plus important dans le cadre de protocoles critiques (sécurité...). En effet, avec un code en libre accès, n'importe qui peut vérifier la qualité du code, garantir l'absence de portes dérobées, de pratiques douteuses. Un code source ouvert (*opensource*) signifie donc que vous pouvez lui faire confiance pour *vous protéger, vous et votre vie privée* ! Et si vraiment vous êtes paranoïaque (c'est votre droit) alors vous pouvez prendre des cours de code, puis faire vous même cette vérification !

Lors de l'installation d'un logiciel, ne faîtes pas «entrée» à tout va. Regardez les options. Il est fréquent qu'un installateur vous propose une barre d'outils ou autre, que vous n'avez pas demandé, et dont vous n'avez pas besoin. Ces micro-ajouts permanents sont source de ralentissements multiples, et contiennent parfois des logiciels espions.

Certains auteurs de logiciels signent leurs binaires (le fichier à télécharger) avec leur clé gpg ou indiquent les sommes de contrôle MD5 ou SHA. Je ne vous ai pas encore expliqué comment vérifier les signatures, mais si vous savez le faire, faîtes le !

4.2.3 autres liens et documentations utiles

SPF a écrit un guide pour la navigation internet plus sûre [4]. Genma (un fervent partisan de l'utilisation des outils de chiffrement) a son guide d'hygiène numérique [5] [6].

3. http://cyrille-borne.com/article398/le-site-de-confiance-c-est-termine
4. http://sanspseudofix.fr/kit-de-base-du-surf-tranquille-2/
5. http://genma.free.fr/?Petit-guide-d-hygiene-numerique
6. https://github.com/genma/Conference_Guide_d_hygiene_numerique/blob/master/Genma_Petit_Guide_d_hygiene_numerique.pdf?raw=true

4.3 GPG

Comme je l'ai écris dans l'introduction, *OpenPGP* est une norme décrivant le protocole, soit en fait l'ensemble de ce que doit faire le logiciel et ses composants (signatures, chiffrements, algorithmes, formats de messages...). *GPG* ou *GnuPG*, est un logiciel libre conçu suivant cette spécification.

Je peux parler indifférement de clé *GPG* ou *OpenPGP*, puisqu'en l'occurence, les clés créées par *GPG* doivent belles et bien correspondre au standard *OpenPGP*.

Sinon, quand j'utilise le terme *OpenPGP*, je fais réference au protocole, donc, pour ce qui vous concerne, à la manière d'utiliser vos clés. Quand j'utilise *GPG*, alors je parle du logiciel lui-même.

4.3.1 Linux and co

Gpg est dans les standards des distributions Linux. Si vous ne l'avez pas, c'est que votre distro est tellement particulière que je n'en connais pas le mode d'installation ou de gestion des paquets (*Slitaz* ?).

Sous Debian & co, si c'est pas déjà installé - ce qui serait bizarre puisque Debian utilise GPG pour signer et vérifier l'intégrité et l'authenticité des paquetages logiciels (!) , ça donne ça :

```
apt-get install gnupg gnupg2
```

J'indique les deux paquets. La version 2 est celle recommandée aujourd'hui.

De toute façon, il est dans les dépendances de tous les gestionnaires de clés qu'on verra plus loin.

Les utilisateurs d'autres distributions ou d'outils graphiques tels que Synaptic, Apper ou Muom feront simplement une recherche sur **gnupg**. Il y a de fortes chances que votre gestionnaire de paquets vous dise qu'il est déjà installé.

Il est aussi dans la base des Unix tel qu'OpenBSD.

4.3.2 Windows

Bon, là on s'attaque à un gros morceau !

Il vous faut en fait Gpg4win[7], qui contient d'ailleurs tout le nécessaire[8] : gestionnaire de clés, client courriel...

Une fois l'installateur téléchargé, lancez le. Il vous proposera d'installer d'autres logiciels en plus de GPG.

- GPA est un gestionnaire de clés
- Kleopatra est un autre gestionnaire de clés

Vous avez besoin d'un des deux. Kleopatra est le plus décrit sur le web, c'est donc celui que je conseille (et je l'ai sous la main, si vous me demandez de l'aide, je pourrais plus facilement vous aider).

- GpgOL, plugin pour Outlook
- GpgEX, plugin pour l'explorateur de fichier de Windows.

Installez les si vous avez besoin.

- Claws-Mail, logiciel de courrier léger

Les windowsiens, on vous facilite la vie décidément !

7. http://www.gpg4win.org/download.html - prenez la première version en haut, sauf si vous savez ce que vous faîtes
8. http://www.gpg4win.org/about.html

4.3.3 MacOS

Je n'ai pas de Mac sous la main. Mais Thunderbird est disponible sous Mac et vous pouvez donc l'utiliser. Apparemment le client courriel natif de Mac supporte également le chiffrement [9].

Vous avez besoin, des outils de chiffrements Gpg pour Mac. Téléchargez donc la suite gpg [10].

Vous pouvez (bon en fait vous *devriez*) vérifier l'intégrité du fichier dmg en allant dans votre dossier de téléchargement (je suppose ici qu'il s'appelle *downloads*) dans votre terminal :

```
cd downloads
openssl sha1 GPG_Suite
```

En tapant le nom du fichier, vous pouvez après faire auto-complétion : utilisez la touche de tabulation, le terminal complétera le nom du fichier.

La commande ssl va vous indiquer une suite de caractères qui doivent correspondre à celle indiquée sur le site de gpgtools en dessus du bouton de téléchargement.

Reste plus qu'à installer. Ouvrez le fichier dmg et cochez ou décochez les options qui vont bien. Il vous faut *MacGPG2*, *GPGPreferences*, *GPG Keychain Access*.

Si vous utilisez le logiciel natif **Mail**, il vous faut aussi **GPG for Mail**, mais si vous utilisez Thunderbird, il vous faut par contre **GPG Services**.

4.4 Un client couriel

Notice

Je ne décrirais pas la configuration de la messagerie, des adresses courriels. Si vous êtes venus jusqu'ici, ce dont je vous félicite, c'est que vous êtes motivés pour apprendre/chercher la solution par vous-même et/ou que vous savez déjà configurer une adresse courriel.
Toutefois, on peut toujours me contacter [a] pour demander de l'aide. Les tutoriels pour la configuration de la messagerie de Thunderbird (aisement transposable aux autres logiciels de courrier) sont légions sur le web. [b].

a. via l'adresse du tutoriel, ou aller sur http://http://www.22decembre.eu/fr/contact.html
b. http://www.astucesinternet.com/modules/news/article.php?storyid=180 par exemple

Bon, vous avez le logiciel de base installé, mais rien d'autre pour l'instant à priori. Prenez le client courriel de votre choix.

4.4.1 Thunderbird

Thunderbird est disponible en téléchargement et installation pour toutes les plates-formes majeures [11].

Vous pouvez donc l'installer avec apt [12] :

```
apt-get install icedove
```

9. http://www.gbronner.net/mail/GPGMacOSX.html
10. https://gpgtools.org/
11. lien vers la page de téléchargement universelle : https://www.mozilla.org/en-US/thunderbird/all.html. Vous l'avez ici en français, et pour votre systême : https://www.mozilla.org/fr/thunderbird/
12. Il est à noter que le logiciel est renommé Icedove sous Debian suite à la controverse entre Debian et Mozilla : http://fr.wikipedia.org/wiki/Renommage_des_applications_de_Mozilla_par_Debian

4.4.2 Claws-Mail

Si vous êtes sous Windows, vous avez le client **Claws-Mail** dans l'installateur de **Gpg4win**

4.4.3 Kmail et Évolution

Kmail est disponible comme partie de la distribution KDE, Évolution comme partie de Gnome, donc si vous êtes sous GNU/Linux, vous devriez utiliser votre gestionnaire de paquet favori.

```
apt-get install kmail

apt-get install evolution
```

Même remarque qu'auparavant pour ce qui est des installateurs graphiques : Synaptic et consorts installeront toutes les dépendances, y compris **gnupg** si ce n'est pas encore le cas.

4.4.4 Les autres

Il existe une version Windows de KDE[13], mais je n'ai jamais pris le temps de l'essayer.
Sylpheed, client courriel disponible sous distributions Linux, Windows, Mac et d'autres Unix.

4.5 Un gestionnaire de clés

Notice

Rappel : Vous n'avez besoin que d'un seul de ces logiciels. Et très souvent le choix de tel ou tel logiciel dépend de votre environnement !

4.5.1 GPG Keychain sous Mac OS

Le gestionnaire de clés s'appelle GPG Keychain sous Mac Os et vous l'avez normalement déjà installé lorsque vous avez installé GPG pour Mac.

4.5.2 Thunderbird : Enigmail

Si vous utilisez Thunderbird, vous avez besoin d'Énigmail, qui est en fait une extension, un plugin du logiciel utilisé par Thunderbird pour gérer son interaction avec GPG. Les utilisateurs de Thunderbird peuvent suivre le tutoriel du Hollandais Vollant[14], qui est complet et dont je m'inspire beaucoup. Toutefois je le trouve indigeste car très long.

Première solution : le site web

L'installation est ici la même que pour l'installation d'un module Firefox : xpi.[15] Au passage, signalons comme l'indique bien la page de traduction[16] qu'Énigmail est traduit dans de nombreuses

13. https://windows.kde.org/
14. http://lehollandaisvolant.net/tuto/gpg/#i2
15. Il vous faut télécharger le plugin sur https://www.enigmail.net/download/ et bien sûr prendre la version correspondant à votre OS.
16. http://beta.babelzilla.org/projects/p/Enigmail/

langues, y compris français (90%), mais pas danois, hélas.

L'extension xpi s'installe comme suit : il faut démarrer Thunderbird, sélectionner «Outils» dans la barre des menus en haut, puis «plugins», «extensions» ou «modules».
Ou alors (suivant votre version de Thunderbird) cliquer sur le gros bouton en haut à droite, et sélectionner «plugins», «extensions» ou «modules». Ici, vous pouvez indiquer à Thunderbird que vous souhaiter installer une extension en cliquant en bas à gauche sur «installer...». Thunderbird vous demandera dans quel dossier de votre ordinateur vous avez téléchargé le fichier xpi d'Énigmail.

Une fois cette opération réalisée, il faut redémarrer Thunderbird.

Deuxième solution : télécharger via Thunderbird lui-même

Vous pouvez demander à Thunderbird/Icedove de vous télécharger et installer l'extension par lui-même. Allez dans la fenêtre des modules, comme indiqué précédemment et faîtes une recherche sur Enigmail. Normalement vous devriez l'avoir en tête de liste avec un bouton d'installation.

Bonus Debian : installation via Apt

Si vous utilisez Icedove (sic !) sous Debian, sachez qu'Énigmail est dans les dépots Debian et que vous pouvez donc l'installer via apt. C'est une bonne solution si vous partagez votre ordinateur avec d'autres utilisateurs. Par contre, je pense que si on installe Énigmail par ce biais, il faut alors éviter à tout prix de l'installer après par un autre moyen si vous voulez mettre à jour. Si vous souhaitez une autre version que celle des dépots, il vous faut la désinstaller au préalable.

Attention !

Une seule version de ce logiciel par machine ! C'est, je pense, une mesure de sécurité.

```
apt-get install enigmail
```

Notice

NB : Il n'y a pas de raison, si Debian a inclus Énigmail dans ses dépots que d'autres distributions GNU/Linux ne l'ai pas fait...
Essayez donc de chercher Énigmail dans votre gestionnaire de paquets.

4.5.3 Kgpg/Kleopatra

Kgpg et Kleopatra sont deux logiciels de gestion des clés et certificats de chiffrement sous le bureau KDE. Pour ma part, je préfère me servir de Kgpg, mais il est quand même très utile d'avoir les deux installés.

Il y a de fortes chances, si vous êtes un fan de KDE comme moi que ces logiciels soient déjà installés. Mais sinon, comme précédemment, et suivant votre distribution :

```
apt-get install kgpg kleopatra
```

Rappelez-vous que Kleopatra est aussi distribué dans l'installateur Gpg4win sous Windows.

4.5.4 Les autres

Il y a Seahorse sous Gnome, mais je ne connais pas du tout. Mais je doute fortement qu'il soit très différent de Kgpg. Il est disponible sous Debian :

```
apt-get install seahorse
```

Chapitre 5

Un peu de théorie et de logique

5.1 OpenPGP, comment ça marche ?

OpenPGP repose sur le principe de la cryptographie - ou chiffrement en français - asymétrique.

Quand on parle de clés GPG, on parle en fait de couples de clés : une clé publique et une clé privée.

5.2 Pourquoi se compliquer la vie avec ça ?

Lorsque vous signez un message, vous voulez garantir que celui-ci vient bien de vous et qu'il n'a pas été altéré.
C'est le même principe que les sceaux au Moyen-Âge : le cachet de cire intact garantissait l'authenticité et l'inviolabilité du message.

Vous devez donc signer votre message avec quelque chose que vous seul avez en votre possession : votre clé ***privée*** !

Et comment vos interlocuteurs vérifient-ils que ce message est authentique ?
Avec un élément qui est connu de tous, qui est public : la vérification des signatures se fait avec votre clé ***publique*** !

Inversement, quand on chiffre un message à votre attention, on le rend illisible pour toute personne n'en ayant pas la clé. Vous seul devez pouvoir le lire avec quelque chose que vous seul avez en votre possession : votre clé ***privée*** !

Mais comme n'importe qui doit pouvoir vous envoyer des messages chiffrés, l'opération de chiffrement doit se faire avec une information connue de tous : votre clé ***publique*** !

5.3 Attention !

Faîtes attention ! Un message signé **peut être lu par n'importe qui sur le net**.

La signature garantit que vous êtes bien l'émetteur du message, et que celui-ci n'a pas été altéré. Un message signé a donc plus de valeur juridique qu'un message non signé.

5.4 Récapitulatif

On signe ses messages avec sa clé *privée*. On vérifie l'authenticité des messages d'autres personnes avec leur clé *publique*.

On chiffre les messages à destination d'autres personnes avec leur clé *publique*, qu'ils déchiffreront avec leur clé *privée*.

Observez que c'est presque toujours le même côté de la liaison qui utilise le même coté de la clé : vous utilisez presque toujours votre clé privée, et vos correspondants n'utilisent que votre clé publique.

Votre clé privée doit donc être jalousement gardée et protégée !

C'est elle qui vous permet de contrôler votre coté de la liaison, de prouver votre identité et de lire votre courrier !

Chapitre 6

Générez et exportez vos clés GPG

Let's go ! Vous allez faire votre première action concrète pour l'utilisation de GPG : générer votre première clé !
Ou plus exactement votre première paire de clés, puisque rappelez vous : chaque clé GPG a en fait une face privée et une face publique.

Ce chapitre peut sembler long ou ardu, mais il est important. Créer les clés prend juste quelques minutes et vous n'avez quasiment rien à faire. Donc s'il vous plait, prenez votre temps.

6.1 notice

S'il y a des gens inquiets : vous pouvez tout à fait utiliser une adresse bidon pour ce tutoriel. Après tout, c'est bien ce que je fais avec l'adresse du tuto. Après cela, vous vous refaîtes des clés gpg avec votre vraie adresse, en suivant à nouveau le tutoriel, mais vous ne les envoyez pas ici. Pas de soucis !

6.2 Génération de la clé

Ouvrez votre gestionnaire de clés : Kgpg, Kleopatra ou Énigmail (ou un autre encore...) et chercher l'option de création de clés.

Kleopatra : *Fichier > Nouveau certificat > Créer une paire de clés personnelles OpenPGP*

Kgpg : *Clés > Générer une paire de clés*

Énigmail (donc dans Thunderbird lui-même) : *OpenPGP > Gestion de clés.* Sélectionnez alors *Générer > Nouvelle paire de clés.*

6.2.1 L'adresse à indiquer

Le logiciel vous demandera quelle(s) adresse(s) vous voulez sécuriser avec votre clé. Vous pouvez en effet mettre plusieurs adresses. Pour le moment, c'est mieux de n'en mettre qu'une.

6.2.2 Algorithme

Il vous sera peut-être proposé plusieurs algorithmes : DSA & ElGamal, RSA & RSA ou RSA. Choisissez RSA & RSA (dans Enigmail, onglet *Avancé...*, il s'agit de l'option RSA). Il s'agit de la combinaison d'algorithmes la plus forte et permet de chiffrer et signer.

6.2.3 Longueur de clé

On vous demandera aussi la longueur de la clé à générer, avec ce choix : 1024, 2048 ou 4096 bits. Il y a peut-être d'autres choix, mais globalement c'est ça. Cette question indique en fait quelle sera la force de votre clé, sa solidité, mais aussi le temps necessaire à la génération de la clé. La longueur de clé choisie va demander au *générateur de hasard* de votre ordinateur une certaine quantité d'*entropie*, quantité exprimée avec ce nombre en *bits*.

Notice

Je dois ici avouer ne pas comprendre vraiment le fondement profond de la chose.
Dès que j'essaye de comprendre ces concepts d'entropie, de quantité d'entropie, je suis largué.
En revanche, ce que je comprends bien, c'est que plus il y a d'entropie, plus la clé est forte et le chiffrement difficile à casser.

Aujourd'hui, il est très recommandé de mettre 4096 bits. D'ailleurs je pense que les prochaines versions des logiciels OpenPGP verront apparaître des tailles de clés supérieures (puisque pour l'instant, 4096 est la limite) et/ou de nouveaux algorithmes.

La génération de la clé va prendre pas mal de temps. Il ne faut donc pas s'inquiéter ou arreter votre logiciel précipitement.

Vous pouvez réduire ce temps en utilisant votre ordinateur. En effet, plus vous utilisez votre ordinateur (particulièrement les accès disques), plus vous générez l'entropie pour le générateur de hasard.L'idéal, c'est donc d'en profiter pour mettre à jour sa distribution (haute utilisation du disque dur).

6.2.4 Durée de validité

On vous demandera normalement combien de temps la clé doit rester valide. Moi, ce que je fais, c'est que je donne une durée de validité d'un an, que je repousse juste avant (un mois avant) l'échéance. Il s'agit ici de ce qu'on appellerait un *dispositif de l'homme mort* : si vous veniez à perdre le contrôle de votre clé, celle-ci s'*éteindra* d'elle-même.

6.2.5 Passphrase

Il vous sera demandé une ***passphrase***. Une *passphrase* est un mot de passe très long. Donc par exemple quinze ou vingt caractères. Il existe plusieurs excellentes méthodes pour créer un bon mot de passe.

Bonus pour les profs de français ou les gens vivants en pays étranger : utilisez un mot compliqué, tel qu'un verbe particulièrement ardu de la langue française à un temps de conjugaison improbable, et hop, le mot de passe est presque impossible à trouver pour un humain puisque peu de monde comprend votre langue, du moins à ce niveau.

Moi, ce que je fais, c'est que je prends un ou des mots de mon environnement immédiat, ou un concept auquel je pense (en français, donc j'ai déjà l'avantage indiqué au dessus). Puis je le *tords*. Je remplace le A par un À ou un @. Le L par ! ou autre chose du même genre. J'ajoute des chiffres à un

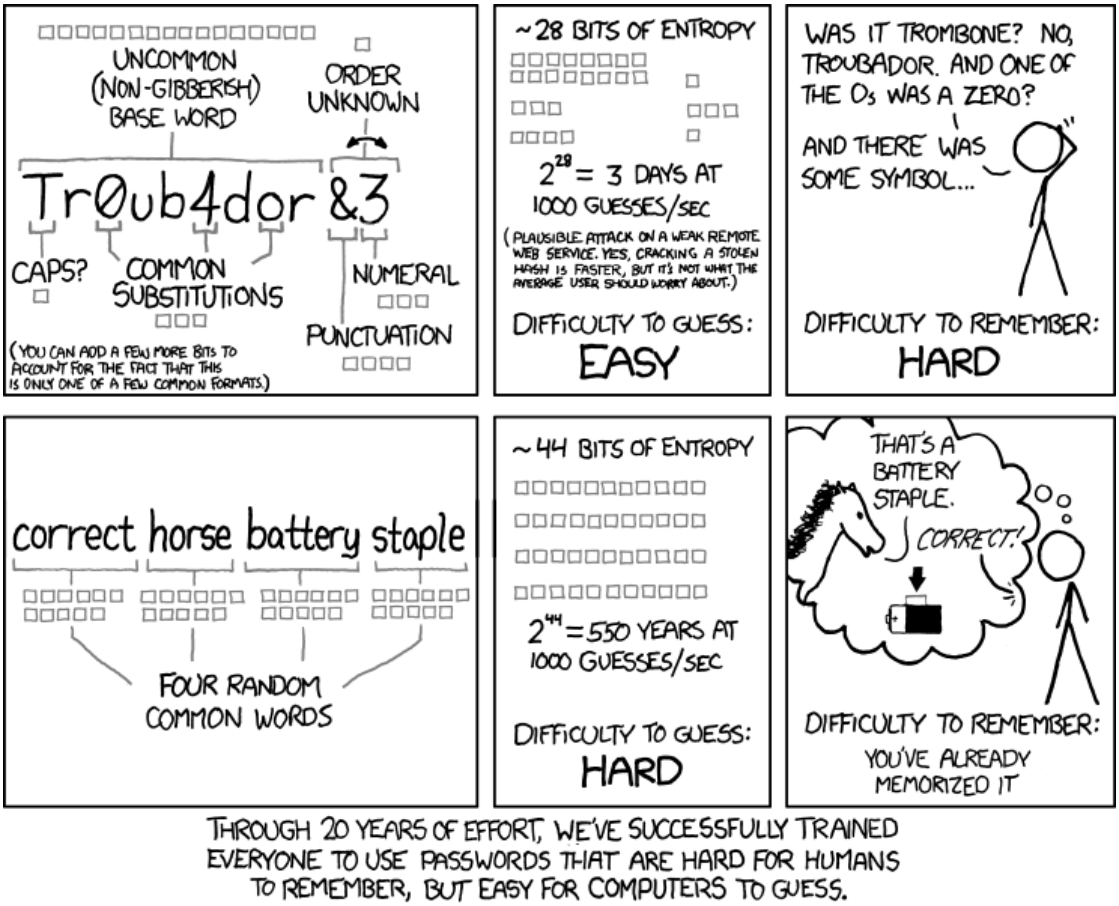

Figure 6.1

endroit choisi dans le mot. Deux ou trois changements de cet acabit et le mot est méconnaissable et donc difficile à deviner pour un humain, et un ordinateur (à cause de sa longueur).

6.2.6 De l'utilité de la passhprase

Vous pouvez choisir de ne pas mettre de passhprase. Je dois avouer ne pas l'avoir fait durant un long moment. Aujourd'hui je le fais et je le recommande.

Ça ajoute tout simplement une sécurité supplémentaire. Chaque fois que vous utiliserez votre clé, pour signer ou déchiffrer un message, ce mot de passe vous sera demandé. Si vous n'êtes pas le seul à utiliser votre ordinateur, ou si vous utilisez vos clés gpg sur votre tablette ou votre smartphone (qu'on laisse fréquemment accessible sans le verrouiller), alors vous avez intérêt à donner une passhprase.

6.2.7 Certificat de revocation

Il est très probable que le gestionnaire de clé vous propose de générer un certificat de révocation. C'est en effet une très bonne chose, donc faîtes le s'il vous plait. En cas de perte de la clé, de corruption, que quelqu'un entre en possession de votre clé privée, hop, on publie ce certificat de révocation sur

les serveurs de clés. Très rapidement, par le jeu des mises à jour mutuelles des serveurs, la clé est marquée comme invalide sur l'ensemble du monde internet. Ceci constitue donc une sécurité pour le cas où on vous volerait la clé privée.

Si le logiciel ne vous propose pas la création d'un certificat de révocation, ne vous en faîtes pas, je vous expliquerais la démarche en détail dans un chapitre futur.

Si vous voulez changer de clé proprement, ce n'est absolument pas la bonne méthode. Je vous en parlerais dans un autre chapitre.

6.3 Exercice

Comme j'ai pensé ce tutoriel comme pédagogique, je vais faire des petits exercices ici et dans les chapitres suivants. Pour les besoins de ces exercices, j'ai créée une adresse courriel sur mon serveur et des clés pour cette adresse.

Ces clés ne seront jamais utilisées pour une autre raison que ce tutoriel.

Je vais vous demander en l'occurence d'exporter votre clé publique fraichement générée, et de me l'envoyer en courriel, tout simplement. C'est ce que beaucoup de personnes font pour échanger leurs clés. Je vous renverrais alors un courriel où je vous dirais si votre clé a les bonnes caractéristiques. J'ai également besoin de votre clé pour l'exercice de l'exercice suivant.

6.3.1 Exporter sa clé

Pour m'envoyer votre clé, il vous faut l'*exporter*. Pour se faire, vous devez le demander à votre gestionnaire de clés. Faîtes bien attention, votre gestionnaire de clés pourra vous proposer d'exporter la paire de clés complète ou la clé privée.

Je parle bien, ici, de votre clé **publique** !

En effet, comme on l'a déjà signalé plus tot, et comme son nom l'indique bien, la clé publique est à la disposition de tous.

Le gestionnaire de clé va vous proposer l'exportation de votre clé sous forme d'un fichier d'extension gpg ou asc. Ce fichier est en fait un bête fichier texte, qui contient la clé publique, sous la forme d'une longue suite de caractères. Vous pouvez en effet ouvrir le fichier avec Notepad ou un autre éditeur de texte par exemple.

Et non, OpenOffice ou Word ne sont pas des éditeurs texte !

Attention !

Si vous ouvrez le fichier texte, ne le modifiez surtout pas !

Vous pouvez alors me l'envoyer en pièce jointe d'un courriel à *Tuto-gpg @ 22decembre.eu*. Ni plus, ni moins.

NB : Kmail (client courriel de KDE), propose également dans son menu **Joindre...*** de mettre sa clé publique en pièce jointe du courriel. Tout simple.

Chapitre 7

Signer son courriel

Vous avez suivi jusqu'ici et avez donc une clé gpg. Excellent ! On va maintenant faire en sorte que vous puissiez utiliser votre clé dans votre courriel.

7.1 Mais comment faire pour que vos divers contacts puissent utiliser votre clé ?

7.1.1 Config' du client courriel

Déjà, il faut leur signaler l'existence de gpg.
Un petit texte en bas de votre courriel suffira. Ce texte est généralement appelé *signature*. Il faut bien le différencier de la signature par GPG de vos messages.

Voici ma signature française par exemple :

> *Ce fichier* **signature.asc** *? C'est une signature GPG.*
> *Si vous voulez savoir pourquoi j'utilise GPG et pourquoi vous le devriez aussi,*
> *vous pouvez lire mon article :*
> *http ://www.22decembre.eu/2015/03/21/introduction-fr/*

Ce texte est à renseigner dans les options de votre client courriel. C'est également là que vous indiquez vos options pour vos signatures GPG.

Kmail

Dans Kmail, c'est ***Configuration*** > ***Configurer Kmail*** > ***Identités***.

Là, vous trouverez les options de chiffrement, où vous indiquez quelle clé ***privée*** vous utilisez pour signer vos messages. Vous indiquez aussi ici quelle clé ***publique*** est à utiliser pour chiffrer les messages à destination de vous-même (excellent moyen pour partager une info, un mot de passe entre plusieurs ordinateurs).

Sur la question du format, il vaut mieux utiliser le chiffrement *OpenPGP/Mime*, plutôt que *inline*[1].

1. Le chiffrement ou la signature via *OpenPGP/Mime* crée un fichier détaché contenant soit la signature, soit le message chiffré. *OpenPGP/inline* se contente lui de copier le résultat de la signature ou le message chiffré directement en clair dans le courriel. Vous avez donc un énorme bloc de texte sans aucun sens au milieu de votre courriel. La plupart des clients courriels n'affichent pas ce bloc de texte, mais c'est néanmoins moche. Je vous encourage à lire cet article sur cette question : http://blog.chown.me/choisir-pgp-mime-ou-pgp-inline.html

Il est également important d'indiquer vos préférences quand à la rédaction des messages dans ***Configuration > Configurer Kmail > Sécurité > Rédaction***. Moi, j'ai presque tout coché (signer par défaut, chiffrer quand c'est possible...) sauf *Toujours afficher les clés de chiffrement*.

Thunderbird

Dans ***Outils > Paramètres des comptes***, sélectionnez le menu *Sécurité OpenPGP* sous l'adresse qui vous plaît. Cochez l'option *Activer le support OpenPGP (Enigmail) pour cette identité* ainsi que l'option *Utiliser l'adresse électronique de cette identité* pour identifier la clef OpenPGP.

Vous pouvez ensuite choisir vos options par défaut : chiffrer, signer tous vos courriels ou non, et si vous voulez utiliser le format *PGP/Mime*, ce que je recommande.

Vous avez aussi des options à choisir dans ***Enigmail > Préférences***.

Évolution

Édition > Préférences

Dans la fenêtre dans l'onglet *Comptes de messagerie*, puis le compte en question et cliquer sur *modifier*.

Dans l'Editeur de comptes qui s'ouvre, aller dans l'onglet *Sécurité*.

Dans le champ *ID de la clé PGP/GPG* : entrer l'identifiant en 8 caractères tel que récupéré dans votre gestionnaire de clés.

Pensez aussi à mettre vos options par défaut.

Lors de la rédaction d'un nouveau message, dans le menu *Options*, cliquer sur *Chiffrer* ou *Signer*.

7.2 Faut-il signer et chiffrer tout son courriel ?

La question est plus ou moins de nature philosophique et constitue un choix personnel.
De toute façon le logiciel de courriel a très certainement de gros boutons qui n'attendent que d'être utilisés pour réaliser ces opérations.

Pour ma part, j'aime bien cette remarque de Philip Zimmermann :

> *Que se passerait-il si tout le monde estimait que les citoyens honnêtes devraient utiliser des cartes postales pour leur courrier ? Si un non-conformiste s'avisait alors d'imposer le respect de son intimité en utilisant une enveloppe, cela attirerait la suspicion. Peut-être que les autorités ouvriraient son courrier pour voir ce que cette personne cache. Heureusement, nous ne vivons pas dans ce genre de société car chacun protège la plupart de son courrier avec des enveloppes. Aussi personne n'attire la suspicion en protégeant son intimité avec une enveloppe. La sécurité vient du nombre. De la même manière, ce serait excellent si tout le monde utilisait la cryptographie de manière systématique pour tous ses e-mails, qu'ils soient innocents ou non, de telle sorte que personne n'attirerait la suspicion en protégeant l'intimité de ses e-mails par la cryptographie. Pensez à le faire comme une forme de solidarité.*

Dans tous les cas, vous pouvez signer tous vos courriers sans que cela pose de problème pour vos correspondants (normalement - il est possible qu'ils en aient s'ils utilisent un mauvais client de messagerie. Mais c'est extrêmement rare !).

Un courriel signé est authentique. Votre correspondant aura la certitude qu'il vient bien de vous et qu'il n'a pas été changé au cours de son acheminement. En revanche, il n'est pas encore possible de garantir que personne d'autre ne l'ait lû !

En revanche, vous ne pouvez chiffrer vos courriers que si vos correspondants utilisent eux aussi GPG ; puisque, rappelez-vous : vous avez besoin de leur clé publique pour chiffrer des messages à leur attention.

7.3 Exercice

Je vais vous demander de *signer* un courriel à mon intention. Tout simplement ! C'est pour cette raison que je vous ai demandé de m'envoyer la clé que vous avez généré lors de la lecture du précédent article : j'en ai besoin pour vérifier votre signature, donc pour vérifier que vous avez bien compris cette partie du tutoriel.

Donc, revenons à l'exercice. Pour envoyer un courriel signé, ouvrez votre logiciel de courriel, et écrivez un message à *Tuto-gpg @ 22decembre.eu*. Vous pouvez écrire ce que vous souhaitez, y compris une critique du tutoriel. Mais dans ce cas, j'aimerais qu'elle soit constructive, qu'elle me permette de l'améliorer.

Avant de l'envoyer, sélectionnez *Signer* dans les options ou utiliser le bouton adéquat. Si (comme moi) vous avez demandé à votre logiciel de courriel de signer tous vos messages, vous n'avez rien à faire en fait ! Sauf appuyer sur le bouton *Envoyer*...

Chapitre 8

Lire et écrire du courrier chiffré

Bon, j'ai dû vous envoyer un courriel chiffré. Donc lisible seulement par vous.

8.1 Ce que j'ai fais

Lorsque j'ai récupéré votre clé publique, je l'ai mise dans mon trousseau de clés.
Ceci m'a permis de l'analyser, et donc de vous indiquer que, oui, *votre clé est bien générée*.

8.2 Conséquences

Puisque j'ai votre clé publique, je peux désormais vous envoyer des messages chiffrés.

Avec un courriel chiffré, vous avez la certitude que vous seul avez pu lire ce message. En revanche vous ne pouvez être sûr de l'expéditeur.

Par contre, si je signe également mes messages, vous ne pouvez pas vérifier ma signature.
En effet, encore une fois, pour vérifier ma signature, vous avez besoin de ma clé publique, et je ne vous ai pas encore indiqué comment la récupérer.

La signature est une preuve d'authenticité du message, donc de l'expéditeur.

C'est pour cette raison que votre logiciel de courriel vous indique sûrement que le courriel que je vous ai envoyé est signé par gpg, mais qu'il ne peut en vérifier la signature.

8.3 Un petit accroc

Attention ! Seul le corps du message est chiffré ! Le sujet, l'en-tête du message, ainsi que les méta-données (d'où le message a été envoyé, à qui, et par où il est passé) sont en clair et lisibles de tous. Il est difficile de faire autrement : comment les serveurs de messagerie pourraient-ils savoir à qui remettre le message si la destination n'est pas lisible ?

Il est donc recommandé de mettre un sujet assez neutre et générique si vous voulez assurer une bonne confidentialité.

Quelque chose comme «Un bon plan» plutôt que «le plan de domination du monde», ou «les derniers chiffres de production» plutôt que «chiffres de prod' en hausse de 50 % : on a tout bon ! »

8.4 Comment récupérer la clé publique ?

8.4.1 Par courriel

J'aurais pu vous envoyer la clé publique du tutoriel, de la même façon que vous m'avez envoyé la votre.

Mais ce n'est en fait pas très sûr : qu'est-ce qui garanti qu'une personne malveillante n'a pas détourné votre courriel et remplacé votre clé par une autre ?

C'est le genre de réflexions que je souhaite vous voir développer. La sécurité sur internet est un processus, une manière de penser.

8.4.2 Sur une page web

Pour les personnes qui ont une page web, vous pouvez mettre votre clé à disposition dessus. Il est de bon ton d'indiquer aussi l'empreinte de la clé dans la page en question. Une empreinte de clé gpg est une suite de caractères alphanumériques propre à chaque clé. Une empreinte permet donc à la fois d'identifier de façon (relativement) sûre une clé et de garantir qu'elle est bien intègre, que personne ne l'a corrompue.

Il est intéressant de voir qu'on utilise un vocabulaire réservé d'habitude aux humains : *intégrité* et *corruption*. Il s'agit bien d'indiquer des notions de confiance, d'absence de doute, de probité.

Votre gestionnaire de clé vous donnera cette empreinte qui ressemblera à ceci :

$$30CF\ 1DA5\ 7E87\ 6BAA\ 730D\ E561\ 42E0\ A02E\ F1C9\ 35A4$$

Cette empreinte est celle de la clé publique de *Tuto-gpg @ 22decembre.eu*.
C'est le même principe que les sommes de contrôle MD5 [1] des fichiers téléchargés sur internet - typiquement une iso de distribution Linux.

Certaines personnes mettent aussi l'empreinte de leur clé gpg sur leur carte de visite, pour pouvoir les distribuer plus facilement.

8.4.3 Les serveurs de clés

En connaissant une empreinte de clé gpg, on peut demander à son gestionnaire de clés de trouver la clé sur internet ! En fait sur des serveurs que l'on appelle «serveurs de clés» ou «serveurs gpg».

Voici quelques adresses de serveurs :

- hkp ://keyserver.ubuntu.com/
- hkp ://pool.sks-servers.net/ [2].
- hkp ://pgp.mit.edu/
- hkp(s) ://keys.gnupg.net/

Vous pouvez indiquer à gpg d'utiliser en priorité le serveur que vous préférez grâce à la configuration de votre gestionnaire de clés. Le S indique que vous pouvez utiliser ce serveur avec une connexion sécurisée par TLS. L'avantage, si vous êtes parano, c'est que personne ne sait quelles clés vous recherchez. L'intérêt de ces serveurs c'est de vous permettre de publier votre clé, et de recevoir des clés et des messages signés et/ou chiffrés de la part de personnes que vous ne connaissez pas.

1. D'ailleurs les sommes de contrôle MD5 sont encore utilisées par OpenPGP, sauf que l'algorithme MD5 est aujourd'hui considéré comme obsolète. Le sujet sera évoqué dans la suite du tutoriel. Vous pouvez en apprendre davantage sur http://fr.wikipedia.org/wiki/MD5.
2. Ce serveur est en fait un pool de serveurs de clés distribué par round-robind DNS. C'est le *serveur* de clé le plus utilisé aujourd'hui.

8.5 Exercice

En guise d'exercice aujourd'hui, je vais vous demander de récupérer la clé publique du tutoriel, et de m'envoyer un courriel chiffré.

8.5.1 Récupérer la clé publique

Vous l'avez compris, il s'agit de vous faire comprendre le fonctionnement des serveurs de clés.

Pour se faire, vous devez ouvrir la boite de dialogue avec le serveur de clé de votre gestionnaire de clés. Le logiciel vous proposera de faire une recherche avec une chaîne de caractères. Autrement dit, une empreinte, ou une adresse courriel. Soit vous copiez-collez l'empreinte de la clé du tutoriel (indiquée juste au dessus) ou l'adresse courriel dans la boite de dialogue. Votre gestionnaire de clés va alors vous proposer une ou plusieurs clés à télécharger.

Si vous avez indiqué l'adresse courriel, vérifiez que l'empreinte est bien la bonne. Inversement, si vous avez indiqué l'empreinte, vérifiez qu'il s'agit bien de la bonne adresse ! En effet, grâce à ces empreintes, on peut vérifier que la clé que l'on a téléchargée est bien celle qu'on cherchait.

Justement, j'ai créée plusieurs jeux de clés, non pas pour vous piéger, mais pour vous faire réfléchir. Le but de ce tutoriel c'est de vous apprendre à utiliser GPG, donc il vous faut l'utiliser pour le comprendre.

Au passage, vous pouvez noter que ces personnes ont signé cette clé :

- alterlibriste
- le hollandais volant

Je me suis en effet inspiré de leurs textes, ou ils m'ont encouragé à écrire ce tutoriel. Je profite donc de ce moment pour les remercier, ainsi que :

- genma
- Maymay qui m'a entre autre aidé avec quelques uns des articles anglais.

Regarder maintenant le courriel que je vous ai envoyé : votre logiciel vous indique sûrement que la signature est valide, non ?

8.5.2 Envoyer un courriel chiffré

Il faut donc que vous m'écriviez un courriel chiffré. Vous pouvez aussi le signer, mais cela n'a pas d'incidence.

Juste avant de l'envoyer donc, cliquez sur le bouton *Chiffrer* ou selectionner l'option qui va bien. Voila !

Il est à noter que comme vous avez récupéré la clé publique du tutoriel, il est très probable que votre logiciel de courriel vous ait proposé de chiffrer le message lors de sa rédaction !

Chapitre 9

Signer des clés

Je souhaite que vous puissiez commencer à utiliser activement gpg, au moins avec des amis proches ou des membres de votre famille qui auraient lu ce tutoriel, et pour cela, il faut que vous puissiez signer des clés.

9.1 Signer des clés...

Oui, avec gpg, on peut signer des courriels, des fichiers, mais aussi des clés gpg !

Délicieusement récursif

Lorsque vous signez une clé, vous accordez un certain crédit à celle-ci, et vous l'indiquez également à tous ceux qui récupéreront votre signature. La signature d'une clé indique en fait que vous considérez que le propriétaire de cette clé est bien légitime. On va parler, là de *cercle de confiance immédiat* (CCI pour résumer) : ce sont toutes les personnes que vous avez rencontré, dont **vous** avez vérifié l'identité et signé la clé.

Retenez bien qu'il s'agit d'un concept que je définis ici, pour les besoins de l'article, pour vous permettre de comprendre toutes les notions ci dessous.

9.2 Un problème d'identité

On va prendre un exemple : quelqu'un se présente pour faire signer sa clé. Appelons le John. Vous devez d'abord vérifier que John est bien le propriétaire de cette clé, et pour se faire, vérifier avec lui l'empreinte de la clé.

Vous devez ensuite vérifier que John est bien qui il prétend être. Un coup d'oeil (soigneux) à ses papiers d'identité vous le confirmera, mais pas seulement ! Car l'identité, c'est bien plus qu'un simple bout de carton plastifié, fut-il protégé avec des encres spéciales. L'identité, c'est aussi les diverses fonctions qu'on occupe : trésorier d'une association, blogueur plus ou moins anonyme, présence sur des réseaux sociaux. Tout ce qui renforce la confiance dans l'identité qu'une personne nous indique peut être vérifié. Une fois ces divers points validés, vous êtes à peu près sûr qu'il s'agit bien de la bonne clé et de la bonne personne. Vous pouvez donc signer sa clé.

9.3 Confiance

En signant une clé, vous accordez également un certain niveau de confiance dans son propriétaire. Ce sont deux choses liées mais néanmoins distinctes, et il est important de le comprendre.

Il y a cinq niveaux de confiance différents :

- indéterminée/je ne sais pas (c'est le défaut)
- absence de confiance/nulle
- partielle
- totale
- absolue/c'est ma clé

Ce niveau de confiance traduit quelle confiance vous avez dans ce propriétaire pour, lui-même, vérifier les identités et donc assurer son cercle de confiance immédiat (CCI). Et ultimement, quelle confiance vous accordez à son jugement à lui sur ceux d'autres personnes !

Par exemple, vous pouvez avoir vérifié soigneusement la clé d'un membre de votre famille, un cousin mettons. Vous avez donc absolument confiance dans ***cette*** clé !

Mais par contre, vous pensez que votre cousin n'est pas encore bien rodé avec OpenPGP. Peut-être qu'il signe un peu n'importe qui, ou qu'il accorde une confiance excessive. Vous n'avez donc aucune confiance dans son CCI. Donc vous signez sa clé, mais avec une confiance nulle.

Et cette confiance nulle est quelque chose que vous pouvez (*devez* !) indiquer sans honte ni crainte. Pour ce faire, le niveau de confiance est codé, inscrit dans la signature, de telle façon qu'il soit et reste une information *privée*.

Vous êtes libre de votre jugement sur les gens dont vous signez la clé ! Il s'agit là d'un cas de liberté d'expression et d'opinion.

Plus vous respecterez ces diverses considérations, plus votre propre jugement sera respecté par d'autres, en particulier des gens que vous connaissez bien. Et donc plus votre CCI prendra, lui une valeur haute également.

Pour ma part, je pense qu'on devrait signer avec une confiance partielle par défaut, et réserver la confiance totale aux gens dont on connaît le sérieux.

Votre CCI est donc à la fois constitué des clés (et donc de leurs propriétaires) que vous avez signées, mais également du niveau de confiance qui leur est accordé !

9.4 Des exemples

Vous rencontrez quelques personnes dans un bar lors d'un rendez-vous de votre LUG.

9.4.1 Arthur

Arthur vous explique qu'il débute dans l'utilisation de GPG et souhaite donc se construire une toile de confiance. *Ok*. Vous vérifiez correctement son identité et il fait de même avec vous. Puis, chez vous, vous signez sa clé, puisque vous l'avez vérifiée.

En revanche vous lui accordez une confiance nulle, car vous estimez que sa pratique de Gpg est encore trop récente. Cette confiance nulle ne vous empêche pas, un mois plus tard, lors d'une autre rencontre, de lui demander comment il gère son trousseau de clé, de constater son sérieux et d'élever son niveau de confiance.

Cette confiance nulle n'empêche pas non plus cette personne de vous accorder un jugement haut ou bas également. Et les signatures d'autres personnes sur sa clé s'ajoute à la votre. Signatures peut-être plus positives !

Il ne faut pas que vous vous sentiez honteux ou irrespectueux d'indiquer une confiance basse à Arthur.

9.4.2 Miriam

Miriam vous explique qu'elle est développeuse Debian. Vous vérifiez son identité et sa clé. Chez vous, vous vérifiez également ses dires au sujet de Debian et vous constatez qu'elle a bien dit la vérité. Donc vous signez sa clé, et vous lui accordez une confiance totale car vous savez que les dev' Debian utilisent beaucoup GPG et doivent respecter un certain sérieux.

9.4.3 Greg

Greg vous indique qu'il utilise très régulièrement Gpg. Après avoir vérifié sa clé, vous la signez, avec une confiance partielle. Simplement parce que vous ne le connaissez pas, mais vous voyez Greg comme quelqu'un de sérieux. Sans plus.

9.4.4 Karolina

Karolina vous explique qu'elle a adopté un système de signature très précis décrit avec beaucoup de détails dans un document disponible sur son blog (on parle là de *politique de signatures*). Vous trouvez sa démarche très juste et décidez de lui accorder une confiance totale, précisément à cause de ce système de signatures dont vous estimez le fonctionnement très équilibré.

9.5 La Toile de confiance

C'est quoi la toile de confiance (les anglophones parlent de *Web of Trust*) ?

La toile de confiance, ce sont tous les CCI additionnés et mis bout à bout, constituant des chaînes :

Vous avez mis une confiance partielle en Greg. Donc son CCI se retrouve lui aussi avec une confiance partielle.

Vous avez mis une confiance complète en Miriam. C'est comme si vous aviez fait entrer tous ses contacts dans votre cercle de confiance à vous. Et c'est Miriam qui a défini si oui ou non vous pouvez faire confiance dans telle ou telle personne que vous n'avez jamais rencontré - puisque vous avez confiance dans le jugement de Miriam. Si, donc, elle a mis elle-même quelqu'un d'autre en confiance totale, alors cette troisième se retrouve à nouveau *de facto* dans votre cercle de confiance *étendu*. Seulement, et c'est bien important, il ne *faut pas que* ***vous*** *signiez* une des clés signées par Miriam sans avoir rencontré la/le propriétaire de cette clé. Miriam l'a fait. Donc la clé qu'elle a signée sera reconnue comme valide par votre gestionnaire de clés. D'ailleurs pourquoi signeriez vous une clé sans avoir rencontré la personne ?

Gpg va déterminer par un algorithme jusqu'à quel point vous pouvez faire confiance à telle clé, que vous n'avez pas signé, à travers le mécanisme de la toile de confiance. Par défaut, Gpg n'ira pas plus loin que cinq cercles de confiance. Et il faut trois signatures avec une confiance partielle, ou une signature avec une confiance complète pour qu'une clé soit valide.

9.5.1 Corollaires

Il faut se rendre compte également que la Toile de confiance doit être considérée avec sérieux.

Par exemple, les opinions politiques, religieuses, son origine, son sexe, sa couleur de peau ni même votre proximité sentimentale (ami, membre de la famille...) avec le propriétaire de la clé n'ont rien à voir ici. Seul compte le sérieux qu'il accorde à son CCI.

Si vous rencontrez quelqu'un qui vous explique qu'il signe des gens d'une manière très précise, avec une politique de signature détaillée, vous pouvez être admiratif de son sérieux et décider de lui accorder une confiance totale. Puis au cours de la discussion, vous vous rendez compte que c'est un pédophile néonazi pronnant l'eugénisme et mangeant des chatons au petit-déjeuner avec de la sauce soja, vous *devriez quand même* signer sa clé !

Bien sûr, vous le dénoncer à la police aussi sec, mais les deux actions sont compatibles.

9.5.2 Quelle est ma responsabilité dans tout ça ?

Il s'agit donc bien d'un système, d'un réseau de confiance *relative*.

Il n'y a pas d'autorité centrale de type étatique qui indique quelle identité est vraie ou fausse. C'est vous qui devez estimer quelle confiance vous accordez et à qui vous l'accordez. Ne soyez toutefois pas effrayé d'une telle responsabilité !

Le fonctionnement du réseau est démocratique : si vous attribuez un mauvais degré de confiance à un utilisateur, votre "vote" sera contrebalancé par ceux des autres.

Les *politiques de signature* documentées et accessibles en ligne renforcent cet aspect démocratique, parce qu'elles sont impartiales, comme décrit au dessus (cf le néonazi mangeur de chatons).

Figure 9.1 – *L'ombre de la Justice*

La responsabilité est donc individuelle et distribuée. C'est en fait du pair-à-pair ! C'est nous tous qui, collectivement, sommes l'autorité en laquelle nous faisons confiance pour valider les clés.

9.6 Tromperies ?

9.6.1 Que faire si quelqu'un tente de me tromper en me faisant signer une fausse clé ?

Déjà, il faut bien voir qu'en signant une clé, vous validez aussi une adresse courriel. Donc c'est aussi l'adresse courriel qu'il s'agit de vérifier. Et le plus simple dans ce cas est que la personne vous envoie un courriel signé depuis cette adresse. (Il peut le faire quelques heures plus tard, ce n'est pas un soucis). De cette façon, vous êtes sûr que vous signiez la clé associée à cette adresse courriel, et qu'elle appartient à la personne que vous avez rencontré.

C'est toutefois un poil lourd comme procédure. À vous de voir.

9.6.2 Il peut arriver qu'on veuille écrire à quelqu'un qu'on ne connaît pas ! Comment être sûr qu'on récupère la bonne clé ?

C'est le rôle de la toile de confiance, décrite au dessus. Si vous souhaitez écrire à Valentina, et que des gens mal-intentionnés ont crée une ou des fausse(s) clé(s) qu'ils ont envoyés sur les serveurs de clés, comment reconnaître la bonne ?

Il y a de fortes chances que la clé de Valentina soit celle qui comporte le plus de signatures. Et, très important, plus ces signatures viennent de personnes diverses (de nationalités, de fonctions diverses...), plus la clé sera sûre !

Il est par exemple très facile de créer des clés avec vingt signatures dessus. Il est par contre assez difficile de créer une clé avec une ou deux *fausses* signatures de dev' Debian. Or il est très facile d'obtenir la signature d'un dev' Debian ! Non pas que ce soient des gars ou des filles *faciles*. Mais ils sont nombreux et éparpillés un peu partout. Si vous habitez une grande ville occidentale, il est probable que vous ayez *un dev' Debian à portée de main* et qu'il signera votre clé (en suivant sa politique de signature) si vous l'invitez pour une bière dans un bar.

S'il est donc facile de créer des clés avec de fausses signatures, il est tout aussi facile de faire signer sa clé par une personne publique à l'identité vérifiable (dev' Debian ou dev' d'autres logiciels libres, blogueur, membre d'une association...).

Et c'est donc cette dernière clé que vous utiliserez en cas de doute !

9.7 Exercice

Bon, c'est bon, vous pigez le truc de la toile de confiance ? Je vais vous demander pour l'exercice du jour, de signer la clé du tutoriel, d'y mettre la confiance qui vous paraît correcte, puis de me l'envoyer par courriel.

Nous sommes bien d'accord qu'il ne faut pas faire cela normalement, puisque qu'on ne s'est pas rencontré. C'est la raison pour laquelle j'ai indiqué dans un des articles que la clé du tutoriel ne sera utilisée que pour les besoins du tutoriel.

9.7.1 Donc, comment qu'on fait ?

Dans votre gestionnaire de clés, vous devez sélectionner la clé en question, puis l'option ***Signer***. Le logiciel vous demandera quelle confiance vous souhaitez accorder à cette clé. Si vous avez plusieurs clés privées, il vous sera demandé avec laquelle vous souhaitez signer.

Vous pouvez également passer par l'édition des propriétés de la clé et changer simplement le niveau de confiance. La signature sera alors faîte automatiquement.

Vous exportez ensuite la clé dans un fichier, que vous envoyez en pièce jointe de courriel à *Tuto-gpg @ 22decembre.eu*. Lorsque je vais récuperer la clé, les signatures vont s'additionner les unes les autres. Je vais alors vous répondre et vous envoyer votre clé, signée avec la clé du tutoriel.

Summum de la feignantise, KGpg et d'autres logiciels vous proposent de faire le tout s'un seul coup : avec l'option ***Signer et envoyer par courrier electronique***, KGpg va effectivement signer suivant vos directives, puis préparer le courriel avec la clé dedans.

9.7.2 Précisions

Certains logiciels (notamment KGpg) mettent l'accent sur la vérification de l'identité du propriétaire de la clé pour vous indiquer le niveau de confiance que vous pouvez accordez.

Il s'agit là en fait d'une assertion selon laquelle, puisque l'identité et la clé ont bien été validées sérieusement, il est raisonnable de penser que le propriétaire de la clé accorde le même sérieux dans d'autres signatures.

Ceci ne change pas la signification de votre signature et ma description reste valable : la confiance accordée indique à quel point vous estimez le propriétaire de la clé capable d'entretenir son CCI. C'est donc ce niveau de confiance que vous devez indiquer.

Chapitre 10

Inspirations diverses

Conférence TED en anglais de Glenn Greenwald, un des deux journalistes ayant aidé Edward Snowden : https://www.ted.com/talks/glenn_greenwald_why_privacy_matters

Jujusete, une journaliste : http://seteici.ondule.fr/2013/05/emails-sortez-couverts/

Décidément, on en voit beaucoup des journalistes ici... Qu'est-ce qu'ils ont tous avec ça ?

> *Quand il y en a un ça va. C'est quand il y en a beaucoup qu'il y a des problèmes.*

Pourquoi j'utilise OpenPGP, par Jean-Marc Manach http://www.uzine.net/article128.html

Security in a Box : https://securityinabox.org/fr/thunderbird_utiliserenigmail

Le tutoriel du hollandais volant, qui m'a beaucoup inspiré : http://lehollandaisvolant.net/tuto/gpg/

Les bonnes pratiques de Gpg et OpenPGP : https://help.riseup.net/fr/security/message-security/openpgp/gpg-best-practices

Le blog de Miriam Ruiz, développeuse Debian, dont j'ai utilisé le nom dans l'article sur la signature des clés : http://www.miriamruiz.es/

Samizdat : http://matrix.samizdat.net/crypto/gpg_intro/gpg-intro-5.html

et l'Amula : http://www.amula.asso.fr/site/article.php?id_article=80

qui m'ont parmi de comprendre le concept de Toile de confiance.