# Atelier 1 : outils de chiffrement

## 1 - Mise en place des outils de chiffrement

Explications inspirées de : https://support.mozilla.org/fr/kb/signature-numerique-et-chiffrement-des-messages

Ce tutoriel ne comporte pas de copies d'écran avec de belles ellipses rouges pour indiquer où il faut cliquer parce que les écrans évoluent sans cesse et les copies d'écran ne sont jamais à jour. Et puis ce serait bien que, vous comme moi, arrêtions de cliquer où on nous dit de cliquer sans lire. Les boutons « J'accepte » sont assez suspects…

L'installation des outils de chiffrement est la phase la plus délicate, l'utilisation au quotidien est extrêmement simple.

Cette petite doc explique comment installer les outils nécessaires au chiffrement asymétrique des emails (voir autre doc pour savoir comment cela fonctionne). Le protocole utilisé pour chiffrer les courriels est appelée PGP (Pretty Good Privacy, en français : « assez bonne confidentialité »). Il s'agit de chiffrement asymétrique dans lequel un **message est chiffré avec la clé publique du destinataire.**

Il y a plusieurs solutions techniques possibles, celle présentée ici :

- nécessite l'utilisation de Thunderbird comme programme de messagerie
- utilise GnuPG et Enigmail pour le chiffrement

### Installation et paramétrage de Thunderbird

Thunderbird peut se traduire en français par oiseau tonnerre. Cet oiseau appartient à la mythologie amérindienne (https://fr.wikipedia.org/wiki/Oiseau-tonnerre).

Pour l'installation et le paramétrage de Thunderbird
- sur Linux : https://support.mozilla.org/fr/kb/installer-thunderbird-sur-linux,
- sur windows : https://support.mozilla.org/fr/kb/installer-thunderbird-sous-windows,
- sur Mac : https://support.mozilla.org/fr/kb/installation-thunderbird-mac.

On y trouve la dernière version, les bonnes explications, les bons écrans et tout.

### Installation de GnuPG2

GnuPG (GNU Privacy Guard) est une version libre du système PGP (Pretty Good Privacy).

### Liens de téléchargement de GnuPG2 et remarques

- Windows : https://www.gpg4win.org/download.html
  On vous propose de donner et un dialogue Paypal est présenté. Il est possible de donner à **0 $** : vous ne donnez pas les informations de votre CB à Paypal et on vous remercie ! Sur l'écran pour choisir les composants : décocher **Kleopatra**, on utilise Enigmail. Laisser les autres options comme elles sont.

- Debian ou Ubuntu :
  Installer depuis le paquet depuis la console :
  sudo apt-get install gnupg2

- Linux Mint :
  Aller dans le **Gestionnaire de logiciels** et chercher GnuPG2 dans la barre de recherche en haut à droite, cliquer sur le nom puis sur **Installer**

- MacOSX : https://gpgtools.org/
  Sur l'écran Custom Install on Macintosh HD : Décocher : **GPG mail** (L'outil de mail d'Apple est déconseillé pour le chiffrement). Enigmail est, ou pas, proposé. Le mieux est de l'installer par Thunderbird, comme expliqué plus loin. Laisser les autres options comme elles sont.

- Autre système, aller sur GnuPG binary releases : https://www.gnupg.org/download/index.en.html#binary

## Installation d' Enigmail

*NB : ajuster ces informations en fonction de la version de Thunderbird et de l'OS.*

Installation dans Thunderbird :

- Aller dans le menu **Outils** et sélectionner **Modules complémentaires** (en anglais : `Tools` > `Add-ons`)
- Utiliser la barre de recherche en haut à droite pour rechercher **Enigmail**.
- Sélectionner **Enigmail** dans les résultats de la recherche et suivre les instructions pour installer le module complémentaire.

Après cela :

→ un menu `Enigmail` est présent
- dans la barre de menu de Thunderbird, entre le menu `Messages` et le menu `Outils`
- ou dans le menu ≡ tout à droite de la ligne avec les items : Relever, Ecrire ...
Il vous permet d'accéder à l'**Assistant de configuration** et à la **Gestion des clés**, entre autres.

**IMPORTANT SOUS WINDOWS** :
Si l'item **Assistant de configuration** est absent, vous êtes en mode junior (p≡p) !!
Pour en sortir : Aller dans les **Préférences** d'Enigmail.
Dans l'onglet **Compatibilité**, cocher l'option **forcer l'utilisation de S/MIME et enigmail**.
Et vous aurez accès aux menus d'Enigmail.

→ dans la fenêtre de rédaction d'un courriel, sur la ligne Envoyer, Orthographe, Joindre,... deux nouveaux items sont présents : un crayon et un cadenas (voir plus loin).

## Création de votre jeu de clefs Gnu PG

**ATTENTION** : Ne passer à cette partie que si vous n"êtes plus en mode junior (p≡p), c'est à dire si vous avez accès à l'assistant de configuration

Le chiffrement asymétrique utilise 2 clés par utilisateur :

- une clé publique, mise à disposition de ses correspondants
- une clé privée qui ne doit être partagée avec personne

La première chose à faire est de créer votre jeu de clés ou biclé : la clé privée et la clé publique.
Pour cela :

- Dans le menu **Enigmail** de Thunderbird, choisir **Assistant de configuration**
- La fenêtre de configuration s'ouvre, sélectionner : **Je préfère la configuration normale (recommandée pour les débutants)**
- Puis cliquer sur **Suivant** pour continuer. La liste des clés connues de Enigmail sur cet ordinateur s'affiche. À l'installation cette liste est vide.
- Sélectionner : **Je veux créer une nouvelle biclé pour signer et chiffrer mes courriels**
- Dans la fenêtre suivante, il faut entrer un mot de passe dans la zone de texte « **Phrase secrète** » qui sera utilisé pour protéger votre clé privée. Cette phrase secrète protège vos clés, comme un mot de passe. Elle vous sera demander occasionnellement par Enigmail. Voir l'article politique des mots de passe sur Wikipédia pour plus d'informations sur la création de mots de passe robustes. Saisir ce mot de passe deux fois.
- Cliquer sur **Suivant**
- Cliquer sur **Créer un certificat de révocation**
- Puis cliquer sur **Suivant** et enfin sur **Terminer** pour fermer l'assistant.

Pour plus de détails, consulter le site d'Enigmail : https://enigmail.net.

## Révocation de votre jeu de clef

Si vous pensez que votre clef privée a été « compromise » (quelqu'un d'autre a eu accès au dossier qui contient votre clef privée), vous devrez révoquer votre jeu de clés actuelles dès que possible et en créer un nouveau.

Pour vous préparer à cela il faut disposer d'un certificat de révocation, dès la création de votre clé. Pour révoquer une clé :

- Dans le menu **Enigmail** de **Thunderbird**, choisir : **Gestion de clefs**
- Une 1° boîte de dialogue apparaît : cliquer-droit sur la clef que vous souhaitez révoquer et sélectionner **Révoquer la clef** (ou dans le menu **Édition** choisir **Révoquer la clef** )
- Une 2° boîte de dialogue apparaît, vous demandant si vous voulez vraiment révoquer la clef. Cliquer sur **Révoquer la clef** pour continuer.
- Une 3° boîte de dialogue apparaît, vous demandant d'entrer votre phrase secrète. Entrer la phrase secrète et cliquer sur **OK** pour révoquer la clef.

Si nécessaire envoyer le certificat de révocation à vos correspondants afin qu'ils sachent que votre clef

actuelle n'est plus valide. Cela garantit que si quelqu'un tente d'utiliser votre clef actuelle pour usurper votre identité, les bénéficiaires savent que votre clé publique n'est plus valide.

# 2 - Utilisation des outils

## Envoi d'un message : les fonctions d'Enigmail

Dans la barre d'outils "Envoyer Orthographe ..." de la fenêtre de rédaction :

- le **cadenas** permet de
  - chiffrer le courriel : cadenas jaune fermé
  - ne pas chiffrer le courriel : cadenas gris ouvert avec une croix rouge
- le **crayon** permet de signer (crayon jaune) ou de ne pas signer le couriel (crayon gris avec une croix rouge)

Dans le menu Enigmail, un item propose d'attacher sa clé publique (voir plus loin la gestion des clés).

Remarques :

- Si la clé publique du destinataire est connue de Enigmail, le message sera chiffré par défaut, c'est à dire au quotidien RIEN À FAIRE !!
- Par défaut le sujet du mail n'est pas chiffré.
  Modification :
  Menu **Enigmail** > **Préférences** > **Afficher les menus et paramètres pour experts**.
  Dans l'onglet **Avancé**, la 1° option propose de chiffrer l'objet des mails.
- Par défaut Enigmail chiffre les pièces jointes.
  Modification :
  Dans le menu Enigmail disponible à l'envoi du message, décocher **Protocole PGP/mime**.
- Le HTML est désactivé : le message chiffré perdra les effets de présentation liés à des balises HTML, mais les hyperliens sont conservés dans le message déchiffré
- S'il y a plusieurs destinataires, le courriel est chiffré si Enigmail a enregistré les clés publiques de chaque destinataire. Si Enigmail ne connaît pas la clé publique d'un destinataire, le courriel n'est chiffré pour personne.
- Enigmail est installé sur votre ordinateur, vos clés sont sur votre ordinateur : vous ne pouvez ni chiffrer, ni déchiffrer en utilisant un webmail.

## Réception d'un message signé numériquement et/ou chiffré

L'information sur le chiffrement et la signature numérique est indiquée sur la première ligne du message.

-> Si le message a été chiffré et signé, une barre verte affiche le texte :
**Enigmail Message déchiffré; Signature valide de xxx.xxx@xxx.xx**

Un cadenas gris est affiché à droite, à côté de la date. L'enveloppe juste à côté, permet d'accéder aux informations de chiffrement.

-> Si le message a été signé, mais pas chiffré une barre verte affiche :
**Enigmail Signature valide de xxx.xxx@xxx.xx**

Seul une enveloppe grise est affichée à droite, à côté de la date. Il permet d'accéder aux information de chiffrement.

-> Si le message a été chiffré, mais pas signé une barre bleue affiche :
**Enigmail Message déchiffré**

Seul un cadenas gris est affiché à droite, à côté de la date. Il permet d'accéder aux information de chiffrement.

-> Si le message n'est ni signé ni chiffré, la ligne Enigmail n'apparaît pas. Il n'y a ni enveloppe ni cadenas à droite.

**Remarque** : Lorsque vous recevez un message chiffré, Thunderbird vous demande de temps en temps d'entrer votre phrase secrète pour déchiffrer le message.

# Gestions des clés

## Sauvegarde des clés

Dans le menu **Enigmail** de Thunderbird, choisir l'item : **Gestion des clés**

- La liste des clés s'affichent dans une fenêtre
- Dans le menu **Fichier** de cette fenêtre, cliquer sur le 2° item :
- Exporter ces clés vers un fichier

Il vous permet de sauvegarder les clés, et surtout votre propre jeu de clés ailleurs.

La sauvegarde des clés peut générer 3 sortes de fichiers « .asc », le format de fichier des clés :

- pnom@mail.org (0x11111111) pub.asv → une clé publique
- pnom@mail.org (0x11111111) pub-priv.asc →une clé publique + une clé privée
- pnom@mail.org (0x11111111) rev.asv → un certificat de révocation

Il est prudent de sauvegarder pour vous même ailleurs :

- votre clé privée au cas où votre ordinateur se crash : ...pub-priv.asc
- votre certificat de révocation au cas où on vous vole votre ordinateur : ...rev.asc

## Récupération de sa propre clé publique

Dans le gestionnaire de clé d'Enigmail, votre clé est en fait une biclé, c'est à dire la clé publique **plus** la clé privée. Deux méthodes pour récupérer sa propre clé publique :

- Par le menu **Gestion des clés** d'Enigmail :
  Sélectionner votre clé, puis dans le menu **Fichiers** choisir : **Exporter des clés dans un fichier**. Un dialogue s'ouvre où il faut bien préciser : **Exporter les clés publiques seulement**.

- Par Thunderbird : S'envoyer un message à soi-même auquel on attache sa clé publique par le menu Enigmail : **Joindre ma clé publique**.

## L'envoi de votre clef publique à un correspondant

Pour recevoir des messages chiffrés en provenance d'autres personnes, il faut d'abord leur donner votre clé publique. Pour cela, plusieurs possibilités :

- On leur donne notre clef publique sur une clef USB
- On exporte notre clef publique sur un serveur de clef
- On envoie un message avec sa clef publique en pièce jointe :
    - Composer le message.
    - Choisir sur **Joindre ma clef publique** dans le menu Enigmail.
    - Envoyer le courriel comme d'habitude. Cette méthode est la moins sure, le correspondant ne peut pas être sur qu'il s'agit bien de votre clé. Dans ce cas, *toujours* confirmer par un moyen de communication sûr que la clef reçue est la bonne.
      Elle a pu être interceptée et échangée.

→ Votre phrase de passe phrase (secrète) est demandé régulièrement.

## Réception d'une clef publique par courriel

Pour envoyer des messages chiffrés à un destinataire, il faut d'abord recevoir et conserver sa clef publique.

- Ouvrir le message qui contient sa clef publique.
- Vérifier que l'identifiant (i.e. la signature) de la clef est bien celui que vous attendez (quelque chose comme 26B905641811F1D0)
- Au bas de la fenêtre, double-cliquer sur la pièce jointe qui se termine en « .asc » (ce fichier contient la clef publique).

### 1° cas : Thunderbird reconnaît qu'il s'agit d'une clé PGP

- Une boîte de dialogue apparaît, vous invitant à « Importer » ou « Voir » la clé. Cliquer sur **Importer** pour importer la clef.
- Une confirmation que la clef a été importée avec succès s'affiche. Cliquer sur **OK** pour terminer le processus.

### 2° cas : Thunderbird ne reconnaît pas qu'il s'agit d'une clé PGP

- Enregistrer le fichier .asc (la clé) avec vos autres clés
- Puis dans le menu **Enigmail** de Thunderbird, choisir **Gestion des clés**
- Dans la fenêtre qui s'ouvre, aller dans le menu **Fichier** et choisir : **Importer des clés depuis un fichier**
- Sélectionner ensuite le fichier .asc qui vient d'être sauvegardé
- Une confirmation que la clef a été importée avec succès s'affiche.
- Cliquer sur **OK** pour terminer.

---



*Dernière édition le jeudi 24 septembre 2020 à 15:47*