La cryptographie avec GnuPG
Sous Linux

Campus Numérique Francophone de Tripoli

Yemen.sayour@auf.org

GnuPG

- Présentation
- Fonctionnement
- Exemple d'utilisation

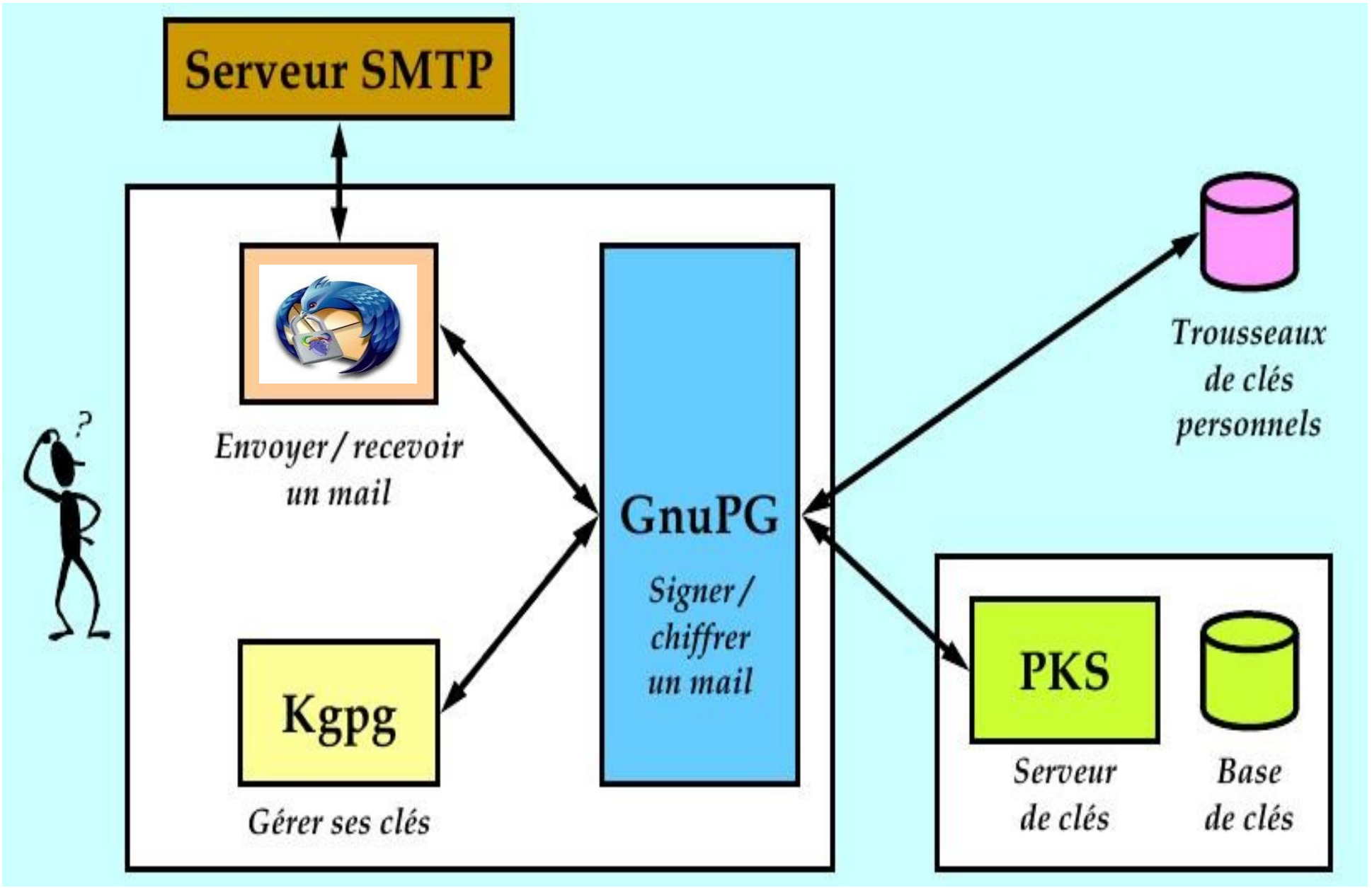
Présentation

- GnuPG est la version GNU de PGP permet de transmettre des messages signés et/ou chiffrés.

- il existe deux types de chiffrement : à clés asymétriques et à clés symétriques, GPG permet de chiffrer des communications par le biais d'un algorithme de chiffrement à clés asymétriques en assurant la confidentialité

- La signature numérique est un mécanisme permettant de garantir l'intégrité d'un document électronique et d'en authentifier l'auteur

Fonctionnement



Installation Gnugp

L'installation de GnuPG passe par les étapes suivants :

► Installation de programme GnuPG.

$ sudo aptitude install gnupg

► Génération des clefs

- Décider votre passphrase
- Générez votre propre paire de clés
- Générer la paire de clés
- Confirmer la paire de clés
- Une sauvegarde de votre porte-clés

Serveurs des clés

Les types par defaut sont :

* HKP pour les serveurs de type Horowitz ou compatible.
* LDAP pour les serveurs de type NAI LDAP.
*MAILTO pour les serveurs de clés par mail de type Horowitz.

$ gpg --send-keys maclé --keyserver ldap://serveurdeclef
permet d'exporter la clé maclé vers un serveur de clés.

Créer un certificat de révocation

La clé de révocation permet d'annuler la validité d'une clé.

```
$ gpg --gen-revoke maclé --output certificat
```

Exporter la clé publique

```
$ gpg --armor --export Nom d'utilisateur --output cle_utilisateur
```

Importer une clé publique

```
$ gpg --import blake.gpg
```

Chiffrer le courriel avec Mozilla Thunderbird et Enigmail

Thunderbird grâce à l'extension Enigmail permet de lire et d'envoyer des courriels chiffrés.

* Thunderbird, le client de messagerie

* GnuPG, le programme de chiffrement

* Enigmail, l'extension nécessaire au chiffrement de courriels

Enigmail

1- Installation du paquet **enigmail** depuis le *gestionnaire de paquets synaptic*

2- **Configuration deTthunderbird**

- **vérification de la liaison entre enigmail et gpg.**

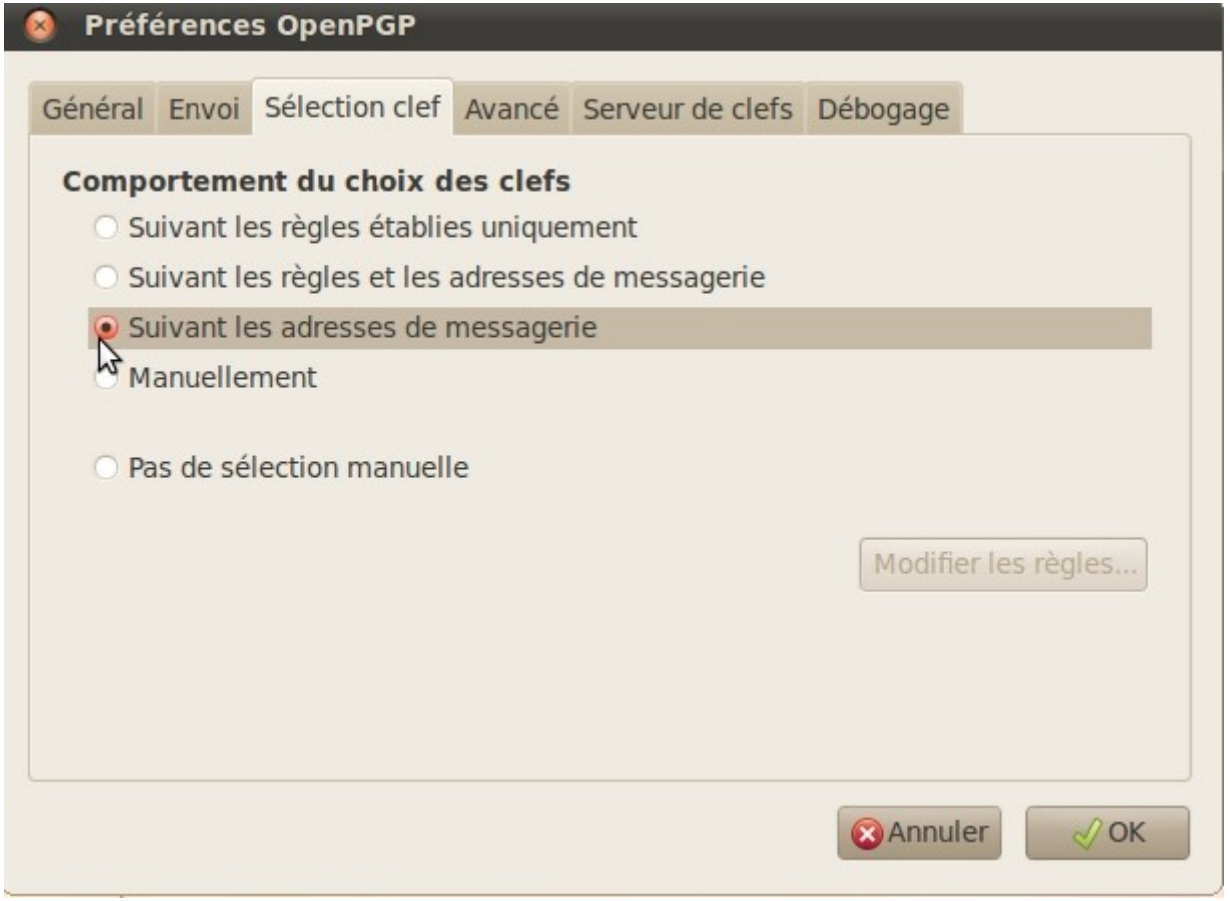
Dans Thunderbird, Ouvrez le menu OpenPGP → Préférences.Dans l'onglet Général, assurez-vous d'avoir un message comme GnuPG trouvé dans /usr/bin/gpg.

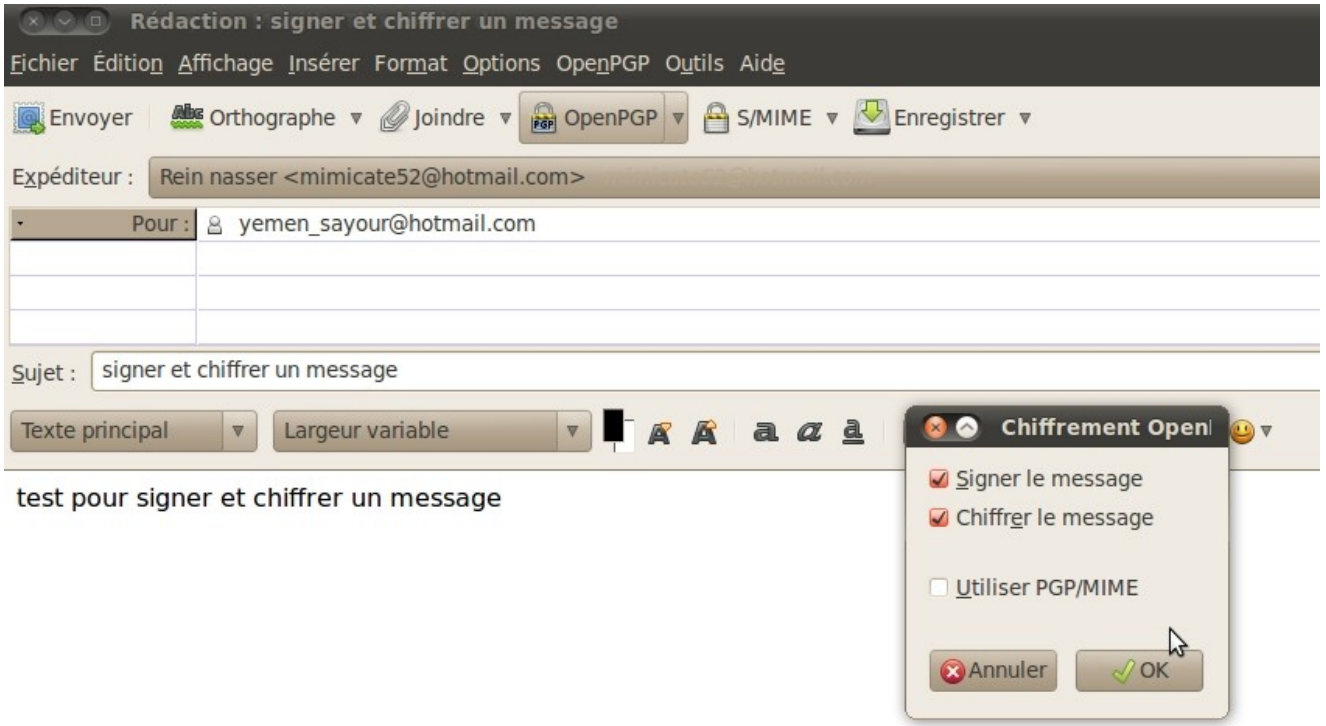
- **Activer Enigmail pour un compte**

Allez dans la sous-catégorie Sécurité OpenPGP et choisissez Activer le support OpenPGP (Enigmail) pour ce compte.

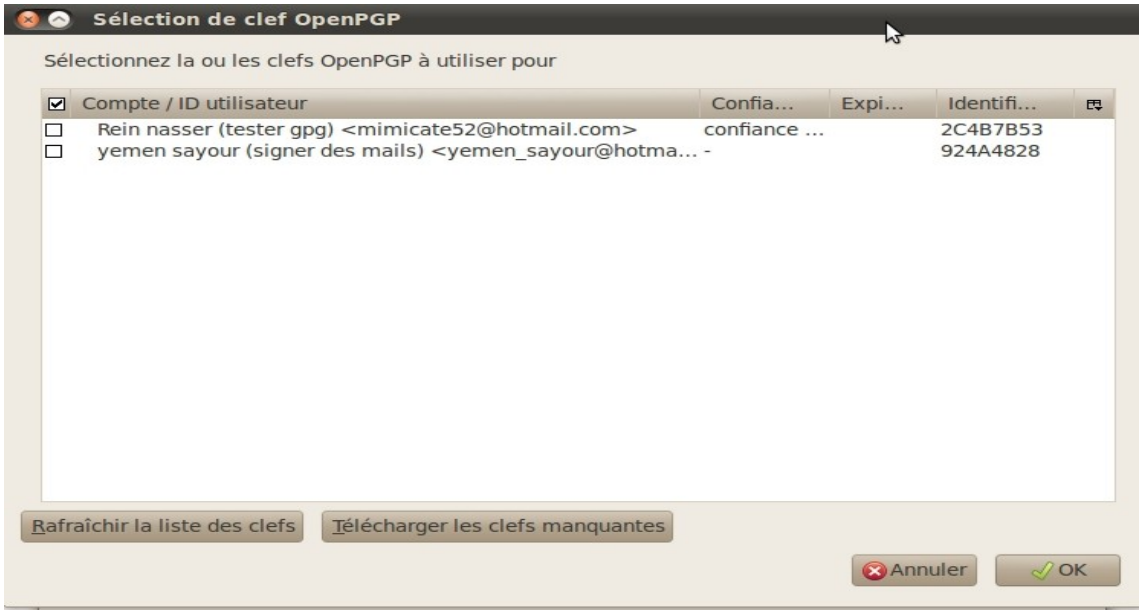
Configuration Enigmail

Sélection des clés des destinataires

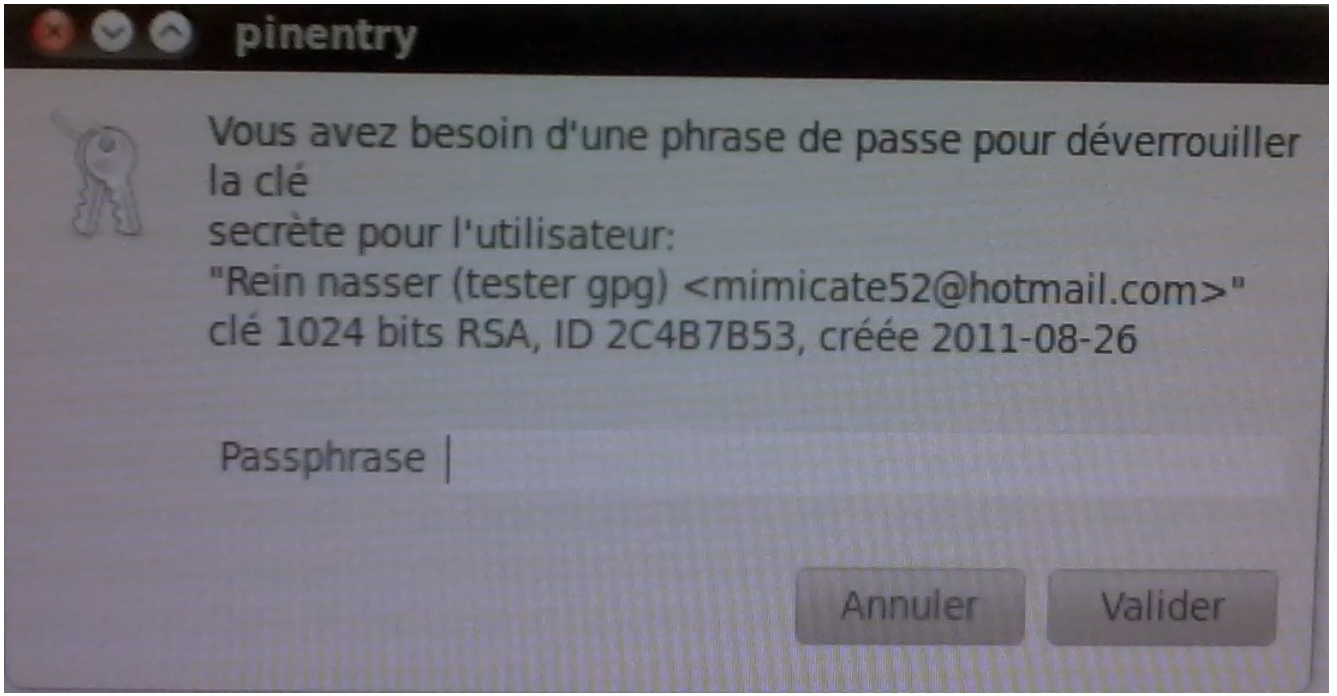




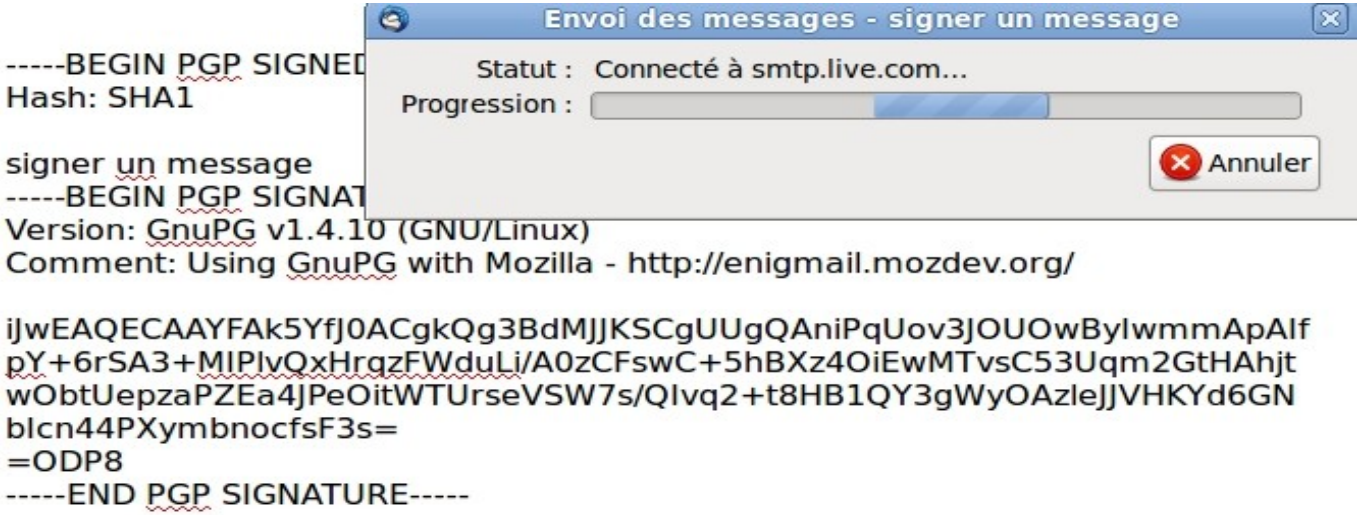
Chiffrer et signer le message
Envoyé en même temps



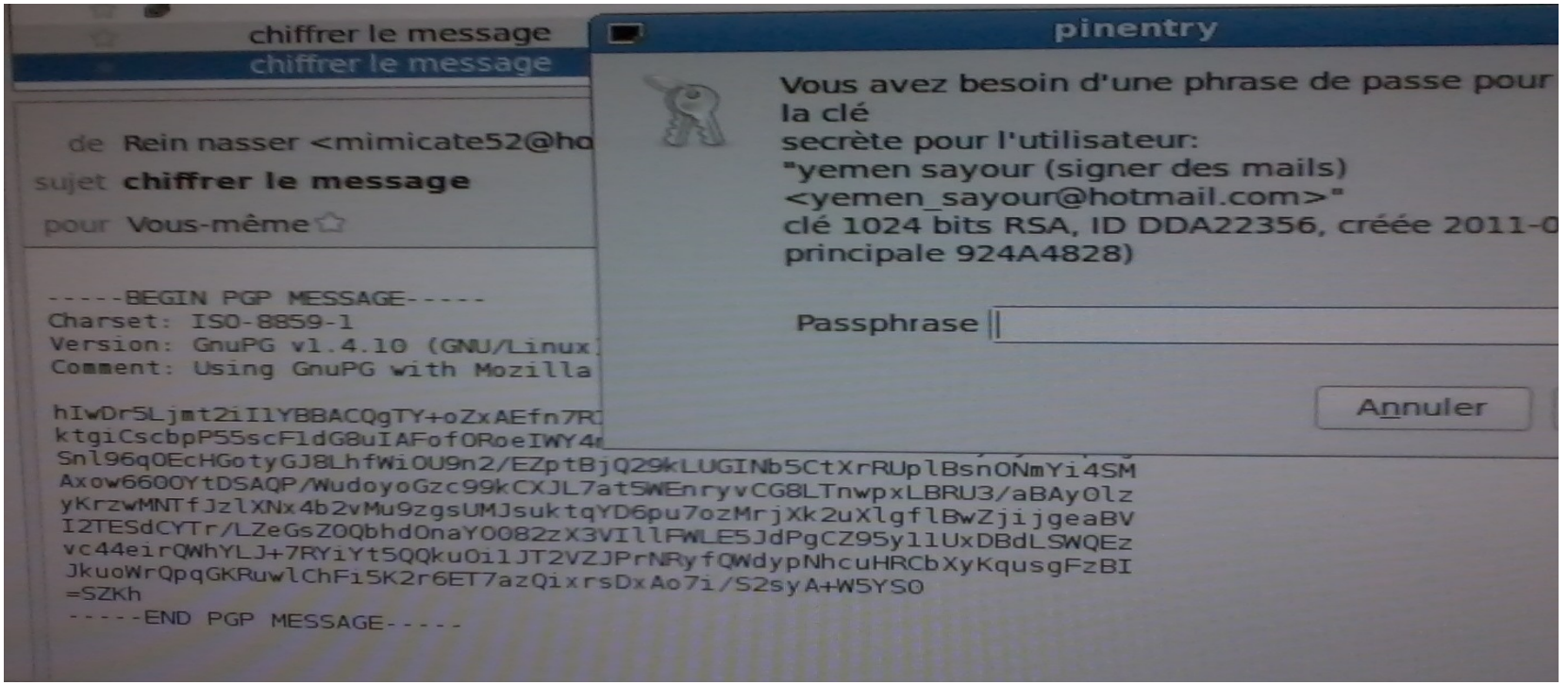
Sélection du clé qui va chiffrer le message



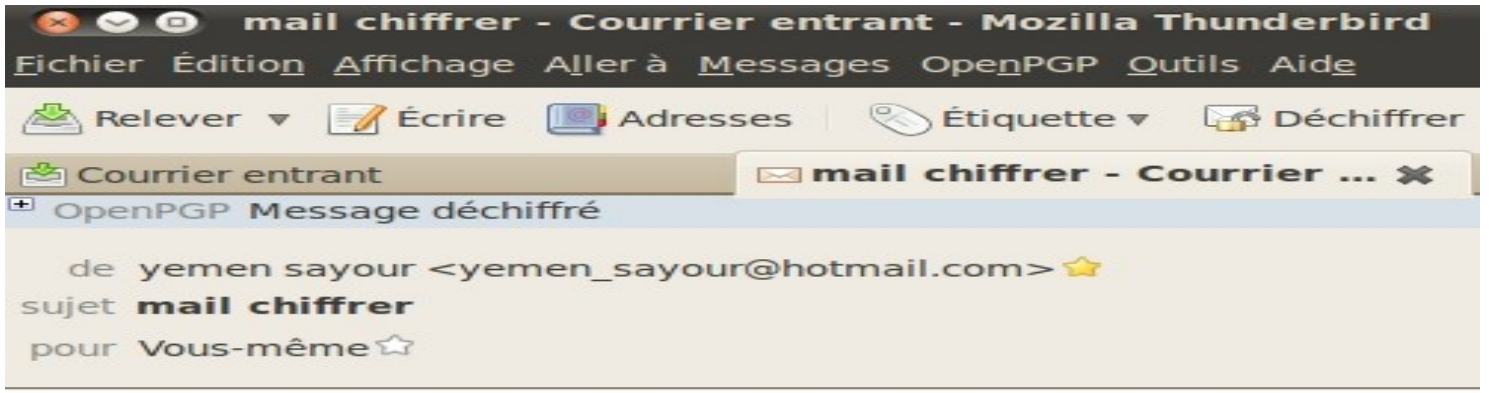
Déverrouillage de la clé secrète par la passephrase



Envoie d'un message signé et chiffré



Déchiffrage d'un message reçu par la phrase de passe de destinataire



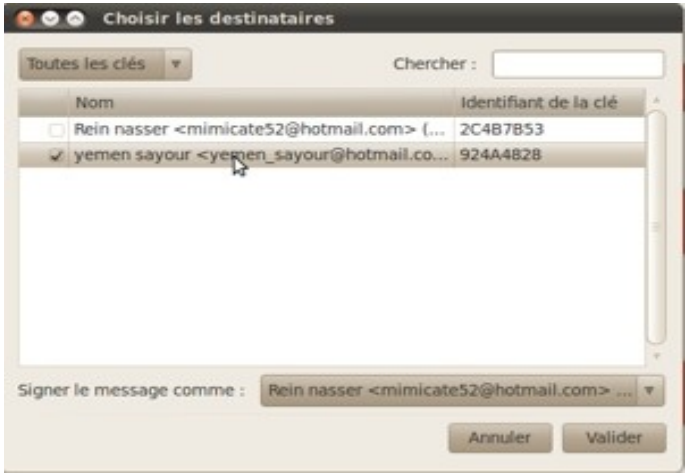
Mail déchiffré

chiffrage d'un mail

Chiffrage d'un dossier ou fichier openoffice

- installer le paquet seahorse-plugins
- clique droit sur le dossier,

Signer le fichier



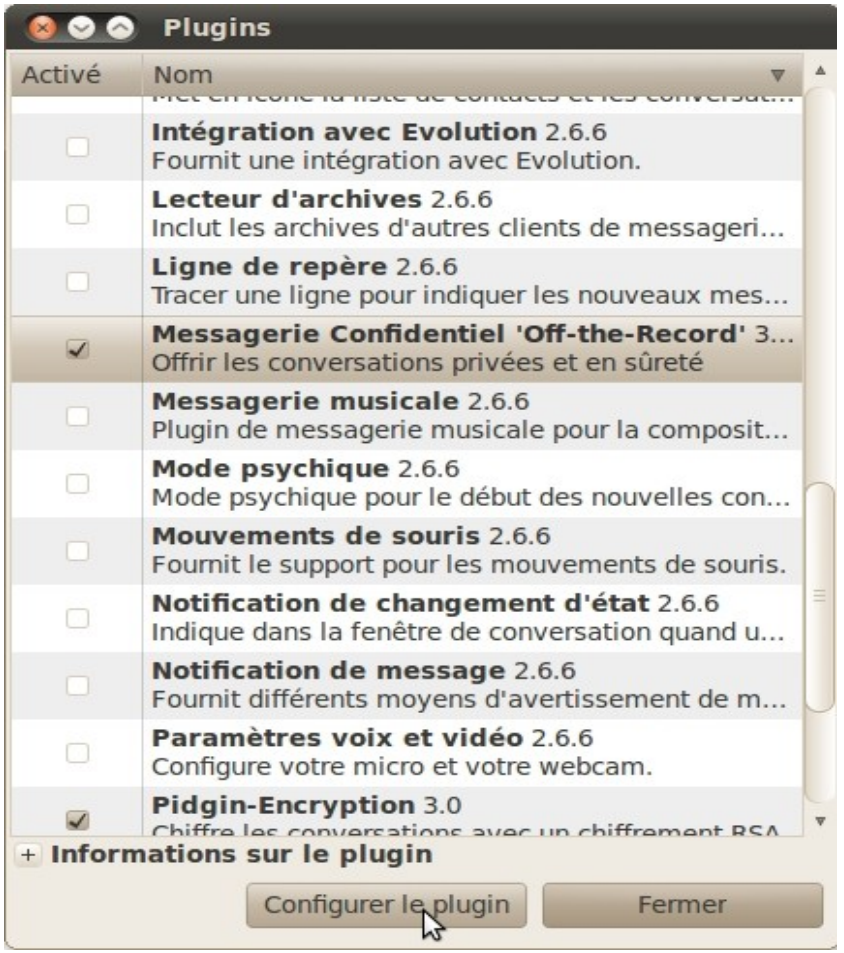
Chiffrer le fichier

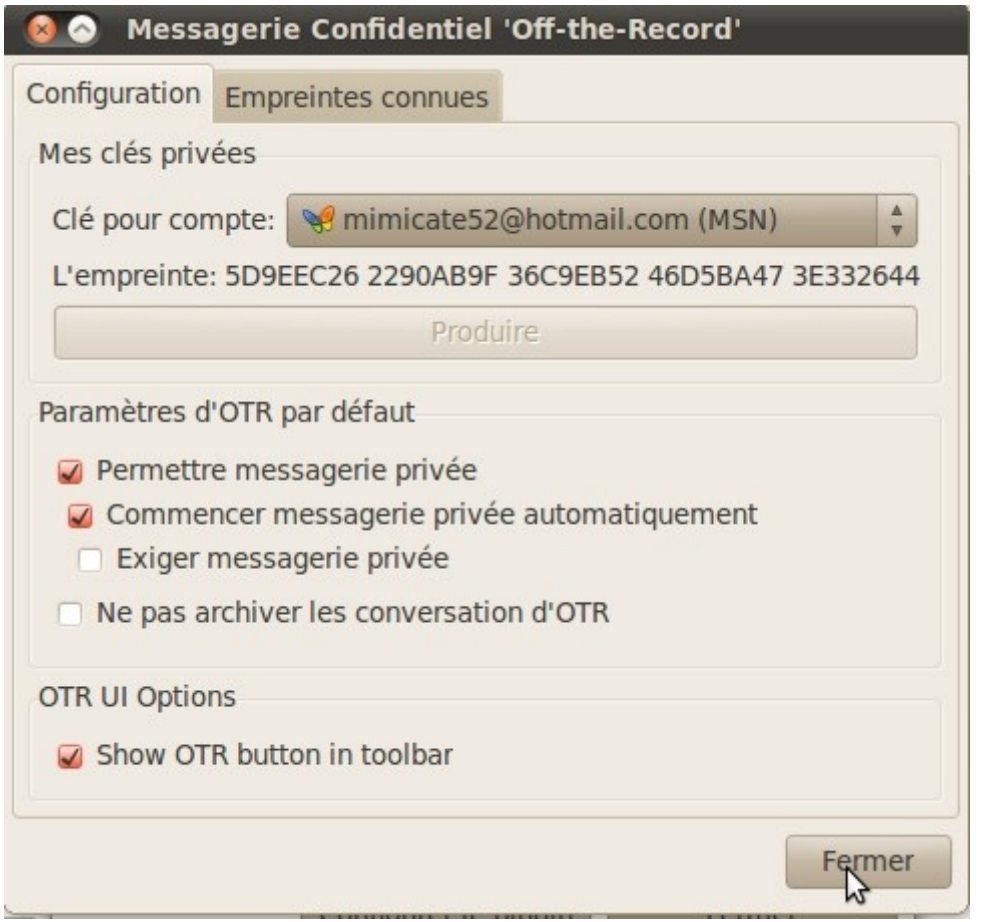
Lors de l'envoie d'un message contenant une pièce jointe chiffrée

Pour déverrouiller une pièce jointe on fait C.D déchiffrer et ouvrir

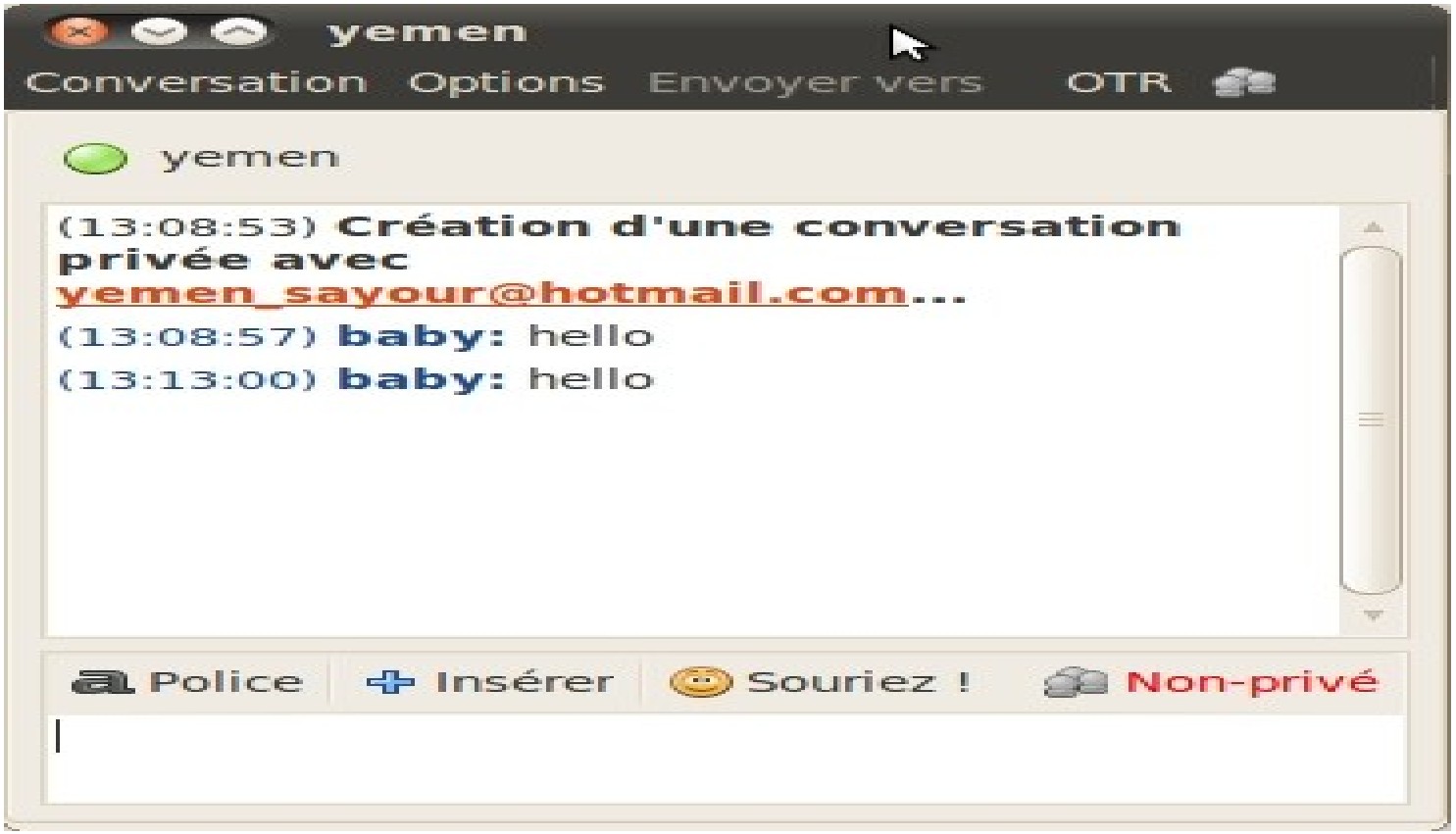
Chiffrer une communication de messagerie instantanée sous Pidgin

- Installation de plugin OTR
- Configuration : outils_plugins_OTR



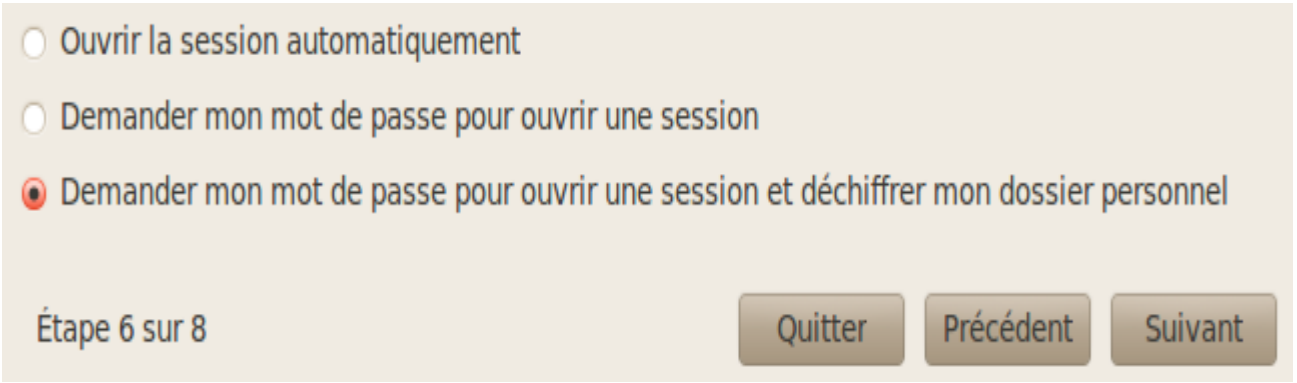


Configuration OTR



Conversation privée

Chiffrer le dossier personnel



Conclusion

Pas besoin, donc, d'être un dieu de l'informatique pour savoir chiffrer les messages. Sous Linux, il existe aussi bien des outils en ligne de commande GPG. Comme quoi, pour protéger vos secrets, ce n'est pas difficile du tout si vous savez cliquer.