

GnuPG : chiffrer et signer sous Ubuntu pour les nuls

22/05/2009

Ce billet présente l'utilisation de **GnuPG** sous Ubuntu pour chiffrer ses fichiers, ses mails ou sa messagerie instantanée. Tout ceci **sans jamais passer par la ligne de commande**.

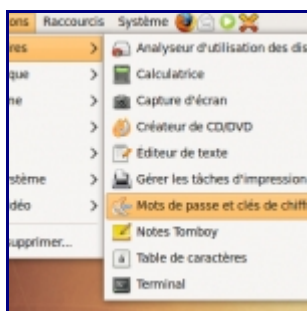
Principe

Je ne vais pas expliquer comment fonctionne le chiffrement, c'est déjà bien expliqué sur wikipedia. **Il est important de comprendre le principe.**

Pour résumer, si A possède une clé publique *Apub* et une clé privée *Apriv*, si B possède une clé publique *Bpub* et une clé privée *Bpriv*. et si A envoie un message à B :

- A peut chiffrer son message pour B en utilisant *Bpub* ;
- A peut signer son message en utilisant *Apriv* ;
- B peut déchiffrer le message reçu de A en utilisant *Bpriv* ;
- B peut vérifier la signature du message reçu de A en utilisant *Apub*.

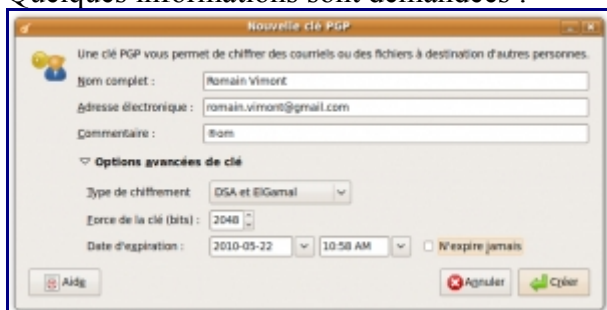
Créer sa paire de clés



Pour créer sa paire de clés (une clé publique et une clé privée) :

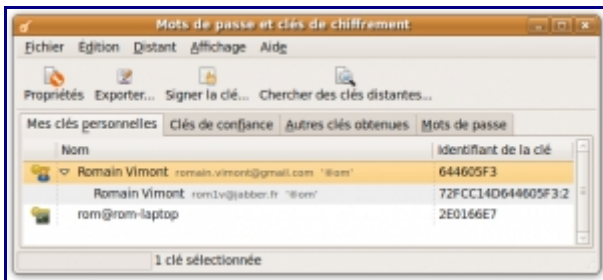
- ouvrir Applications → Accessoires → Mots de passe et clés de chiffrement ;
- dans la fenêtre qui s'ouvre, cliquer sur Fichier → Nouveau... (Ctrl+N) ;
- choisir « *Clé PGP (utilisée pour chiffrer les courriels et les fichiers)* » et cliquer sur *Continuer*.

Quelques informations sont demandées :



Personnellement, je préfère décocher « *N'expire jamais* », et faire expirer la clé au bout de deux ans, on ne sait jamais...

Il ne reste plus qu'à cliquer sur *Créer*, une *phrase de passe* (un long mot de passe) est demandée, et les clés sont générées. Une nouvelle ligne apparaît alors dans « *Mes clés personnelles* » :



Si vous avez plusieurs e-mails et/ou adresses Jabber, vous pouvez les rajouter en cliquant droit sur votre clé, Propriétés, Noms et signatures.

Une fois créée, je vous conseille de garder une copie du répertoire `~/.gnupg`, qui contient votre clé privée, sur un support externe (une clé USB).

Exporter sa clé publique

Maintenant que nous avons créé notre paire de clés, il faut que notre clé publique soit accessible à ceux avec qui nous souhaitons communiquer.

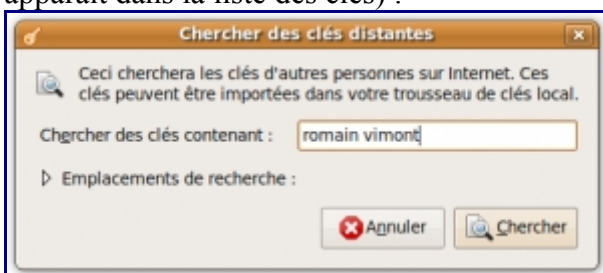
Il suffit pour cela de sélectionner la clé et de cliquer sur le bouton *Exporter...* : la clé publique sera alors exportée dans un fichier portant l'extension `.asc`. Il ne reste plus qu'à envoyer ce fichier par n'importe quel moyen (mail, messagerie instantanée, clé USB...). Une fois ce fichier reçu, notre contact n'aura qu'à double-cliquer dessus (à partir du navigateur de fichiers) ou l'importer dans Fichier → Importer... (Ctrl+I).

Pour une diffusion plus globale, il existe des **serveurs de clés** : ils répertorient les clés publiques de tout le monde. Par exemple, il est possible de publier sa clé sur <http://pgp.mit.edu>, en y copiant le contenu du fichier `.asc` exporté.

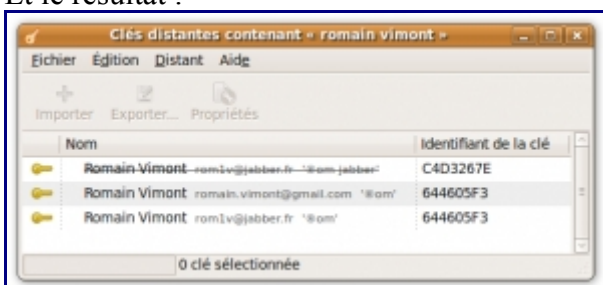
Attention : une clé publiée ne sera jamais supprimée du serveur, elle pourra simplement être révoquée, en créant un certificat de révocation, indiquant à tous que votre clé est invalide. Ne publiez donc que votre clé "définitive".

Il est également possible de configurer le gestionnaire de clés pour qu'il les publie et synchronise directement, en activant dans Édition → Préférences → Serveurs de clés → « Publier les clés sur... ».

Grâce à ces serveurs de clés, il est facile de trouver la clé publique d'une personne directement dans le gestionnaire de clés. Il faut ouvrir le menu Distant → Chercher des clés distantes... et taper le nom de la personne, son mail ou l'identifiant de sa clé (la suite de 8 caractères hexadécimale qui apparaît dans la liste des clés) :



Et le résultat :



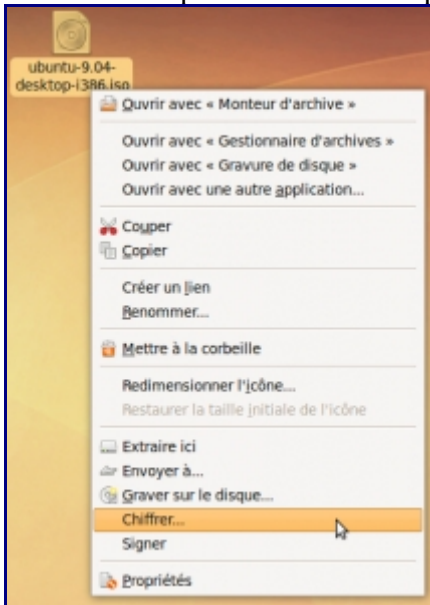
(la première est barrée car c'était mon ancienne clé, que j'ai révoquée lorsque mon ordinateur a été volé)

Il ne reste plus qu'à cliquer sur *Importer*.

Voilà, maintenant tout est en place, nous pouvons commencer à chiffrer et à signer.

Chiffrer et signer des fichiers

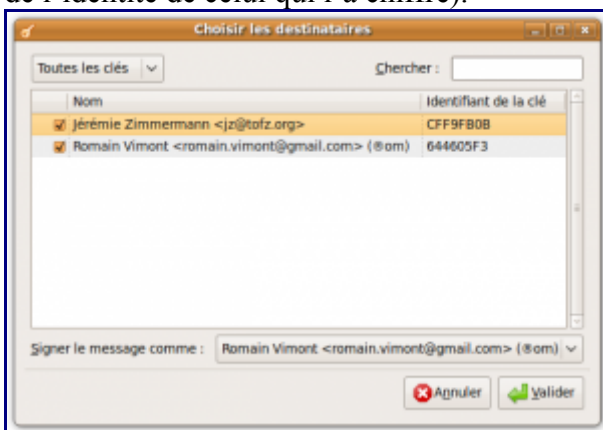
C'est très simple : il suffit de cliquer-droit sur un fichier, et de choisir *Chiffrer* ou *Signer* :



Chiffrer

L'outil de chiffrement demande les destinataires qui pourront déchiffrer le fichier (avec leur clé privée). Tous ceux n'étant pas dans la liste des destinataire n'auront aucun moyen de déchiffrer le fichier ; en particulier, il peut être utile de s'ajouter en destinataire.

Il est également possible de signer le fichier en même temps (pour que celui qui le déchiffre soit sûr de l'identité de celui qui l'a chiffré).



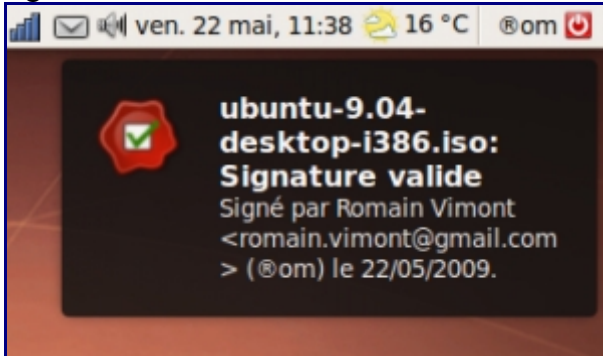
Il ne reste plus qu'à cliquer sur *Valider*. Lorsque l'on choisit de signer le fichier en même temps, la phrase de passe de la clé privée est demandée. Ensuite, le fichier est chiffré dans un nouveau fichier portant l'extension *.pgp* (alors qu'en ligne de commande, cela crée un fichier *.gpg*, mais peu importe).

Pour le déchiffrer, il suffit de double-cliquer dessus.

Signer uniquement

L'outil de signature demande avec quelle clé nous souhaitons signer (utile si plusieurs utilisateurs utilisent chacun une clé), demande ensuite la phrase de passe (pour déverrouiller la clé), et crée la signature dans un fichier portant l'extension *.sig*.

Pour vérifier la signature, il suffit de double-cliquer sur ce *.sig*, une notification indiquera si la signature est valide :

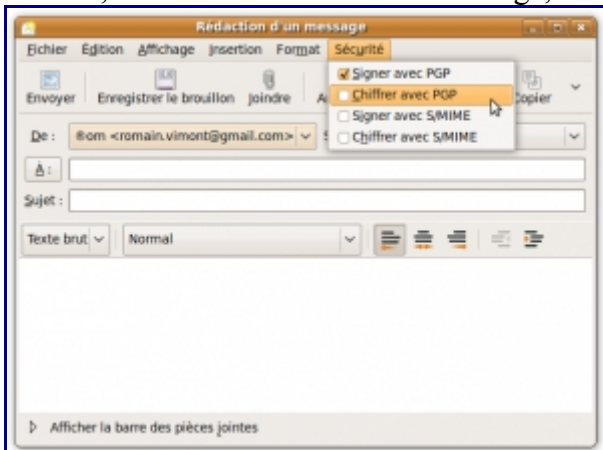


Si le fichier est assez volumineux, cela peut prendre un moment (20 ou 30 secondes), et parfois aucune fenêtre ne s'ouvre indiquant que la vérification est en cours, ce qui est assez perturbant ; mais le processeur, lui, tourne bien à plein régime pour vérifier la signature.

Chiffrer et signer des e-mails (avec Evolution)

Dans **Evolution** (le gestionnaire de mails par défaut sous Ubuntu), il faut associer la clé que nous avons créée avec le compte mail. Pour cela, ouvrir le menu Édition → Préférences → Comptes de messagerie, sélectionner le compte de messagerie auquel associer la clé, et cliquer sur *Édition*. Dans l'onglet « *Sécurité* », recopier l'identifiant de la clé en question, et valider.

Ensuite, lors de la rédaction d'un message, il est possible d'activer la signature et le chiffrement :



Pour que le chiffrement fonctionne, il faut évidemment avoir dans le trousseau de clés les clés publiques de tous les destinataires du mail.

Lorsque nous recevons un message chiffré et/ou signé, Evolution vérifie la signature et déchiffre le mail. Pour l'illustrer, je me suis envoyé à moi-même un message chiffré et signé, lorsque je l'ouvre, Evolution me demande la phrase de passe (pour déchiffrer le message), et ensuite me l'affiche de cette manière :

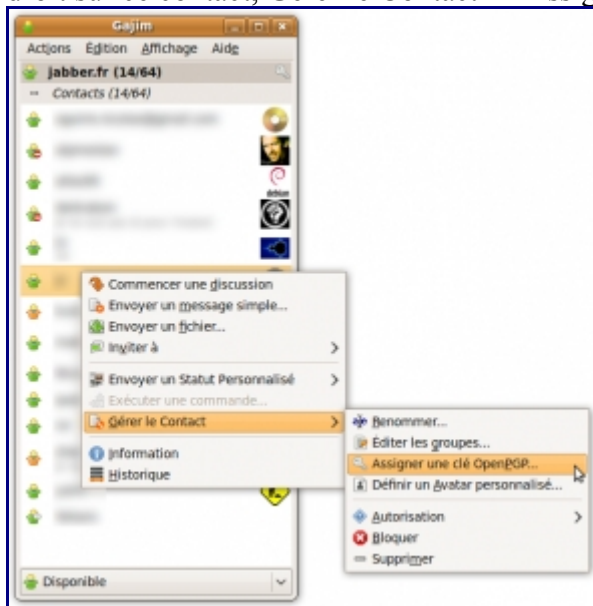


Chiffrer ses communications Jabber (avec Gajim)

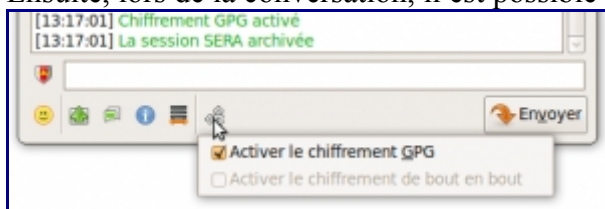
Dans [gajim](#) (le client Jabber de référence), il faut associer la clé avec le compte Jabber. Pour cela, ouvrir le menu Édition → Comptes, sélectionner le compte, et dans l'onglet « Informations personnelles », choisir la clé à associer.

*Une fois la clé associée au compte, **gajim** va toujours se connecter en « signant la présence ». Et qui dit signature dit déverrouillage de la clé privée, et donc demande de la phrase de passe à chaque démarrage de gajim. Il est possible de désactiver la signature de la présence : Édition → Préférences, onglet « Avancées » → « Éditeur de configuration avancé » → Ouvrir... et faire passer **gpg_sign_presence** à « Désactivé ».*

Ensuite, il faut avoir la clé publique des contacts avec qui nous souhaitons communiquer de manière chiffrée (leur clé doit absolument contenir l'adresse Jabber dans la liste des e-mails associés). Une fois récupérée et ajoutée dans le trousseau de clés, il faut l'assigner au contact. Pour cela, cliquer droit sur ce contact, Gérer le Contact → Assigner une clé OpenPGP... :



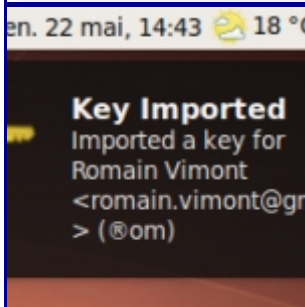
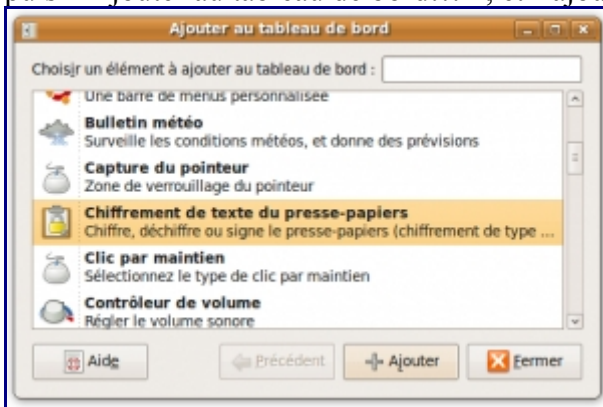
Ensuite, lors de la conversation, il est possible d'activer le chiffrement :



Seahorse-applet : l'applet Gnome

Un applet *Gnome* permet de chiffrer, déchiffrer et signer le presse-papier. Sachant que le presse-

papier contient ce qui est surligné avec la souris (ou ce qui est copié avec Ctrl+C), c'est parfois bien pratique. Pour l'ajouter, il faut cliquer droit sur un panel de Gnome (la barre du haut par exemple), puis « Ajouter au tableau de bord... », et l'ajouter :



Petit plus, lorsque le presse-papiers contient une clé, l'applet permet de l'importer directement dans le trousseau de clés. Une fois que vous avez ajouté l'applet, essayez de sélectionner tout ceci (c'est ma clé publique) :

```
-----BEGIN PGP PUBLIC KEY BLOCK-----  
Version: GnuPG v1.4.9 (GNU/Linux)
```

```
mQGibEmnHMERBADvj+LL49rQCMmSaf1AdxLfl6VZgGHHzh4WqzwEnBDJSfSziJ7A  
tkGN5MxsTnB/C5Dnb6MAEskqBDBjHvJEaVvql7M7HeYSiz+fqwVRNx/s3M3HwMzV  
AlWlMq7xi9rmcKBHNJZzQN7EU/w5nfRnKEUvKlBMTABrF//HgH6EdeSXswCg73CA  
Uv0xx+BncZFCY6KBmgvEg2sD/R8Wuv4L1HIV00bJIP+C8JcHu07aMn6j9KutlHs9  
W84dyVE2MW394G6Bxa439kUKljC4zpx46xD8JR06e5wst00W5K5F2qICxM0M2FZF  
o2KwcAwHfFbFzXmowjXP6+TKmsfz8m0xUdec6JVikFkjkdXv03kzbtCA2YFkktSM6  
1CdJBADGKfWRZaZpR75Gp+EjJvuomWrJ6rDiGwL0n/8DlIWcsvK56yVqtWkgDIwF  
NBLBicxdakAGX1EmmQq1G5mANwiQLZw57L6e89sMt2Fbx3u3+8YUCDYiR0ci5FIK  
2BZqFzDhUnF6mgX5RtCb8edEtA6zMXyVa+CBYP/HB70nRD6k0bQmUm9tYwluIFZp  
bW9udCAowq5vbSkgPHJvbTF2QGphYmJlci5mcj6IZgQTEQIAJgUCSacepAIbAwUJ  
A8JnAAYLcQgHawIEFQIIAwQWAgMBAh4BAheAAoJEHL8wU1kRgXzZVsAni1/vaBd  
+b1mYzXBVogjZs3+CZTAKDR8UzESgtqtud0zFzN86r7IQo0a7QuUm9tYwluIFZp  
bW9udCAowq5vbSkgPHJvbWfPbi52aW1vbnRAZ21haWwuY29tPohpBBMRagApAhsD  
BQkDwmcABgsJCACdAgQVAggDBBYCAwECHgECF4AFakmHrICGQEACgkQcvzBTWRG  
BfMq9ACgk2zdtiR21LmnFfaivKwNaA+WuesAnjmwFa+I92I4zut5EwvTp+B1R7zF  
uQINBEmnHMEQCACJ40osiY+jbwzJQKxyaYCbNGE4DKUgoz+q9yMy0+Hlpsfu70lR  
p/z/dnLVhQ/K020chDnqcBNBL5d7TV+QXmhC9/EIvsYZrnunJoJT+jpRPM7qtrMJ  
ftt5R/5ku3MiHnR1G2YmqDF604qhVqHmShRxpS4Gp28K9E5cLUtY+AENY7eS8LKq  
CTAJYaHR8AAgC3wb6LKA9dd+7LHT/mjbbdjKGCPrd0X+bNnplVH2zr5d44wu2DRf  
aWvySKnhjs1pab4tfkEE/YdtGqqxovYrClR778BIU3r9SJupki0s0ByYcrVp5zZ8  
m9Zk1PNlCmPLUMA/ZCXAfA+VmhmEgXD0WzL3AAMFB/9teF5/S000yVRPVuKwchgS  
SKTEDjjnrBHeFsg9qxvv/QfclaI/3/x6D7eg1zGMjzuwY8Iry50teNHDqAdSuyy7  
3HibcE9d3iw/Ib2cjrYo7FVa9esf3Dh2Z/y2XtyHfE26r0No+T38hIlw1hI6I2g3  
nH7QM0t010JC8x9kdLsyDIdnvtKlD9jsoA5WBUZ/aMMaRmAb7mSDGS3sN8x1o+hA  
23lEz1Sr7d2PLZpxc9i5bk2xXDNI0ugJusxHwi19VKvcEkK7tB6M3q0KdR+93TWB  
lMf94lFJLerjno+M0p0ZiLviXmGrrUhrbXWyWb0b1dIh/mt16BkR1W+UBPAsW2F  
iE8EGBECAA8FAkmnHMECGwWFCQPCZwAACgkQcvzBTWRGBf04JACcCX6SB21n7R4X  
ByQ17kGVuyHz9zUAoNqQqaR8EIRM1kNzr4Yq5c3F07+t  
=/uRd
```

-----END PGP PUBLIC KEY BLOCK-----

Ensuite, cliquez sur le bouton de l'applet : vous pourrez importer ma clé directement.

Merci à cyril pour cette astuce



Aller plus loin

Pour plus d'infos sur l'outil **gpg**, rendez-vous sur [le site officiel \(en anglais\)](#) sur sur la [doc ubuntu-fr](#).

Vous pouvez également consulter **man gpg** pour l'utiliser en ligne de commande.