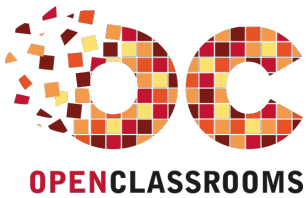
La cryptographie facile avec PGP

Par Perlejade



www.openclassrooms.com

Dernière mise à jour le 23/06/2009

Sommaire

Sommaire 2
La cryptographie facile avec PGP 3
Obtenir GnuPG 3
Sous Linux et *BSD 3
Sous Windows 3
Sous Mac 3
Autres OS, informations, etc. 4
Générer vos clés 4
Chiffrer un message 5
Signer un message 7
Le réseau de confiance 8
Partager 9

La cryptographie facile avec PGP

Par Perlejade
Mise à jour : 23/06/2009
Difficulté : Facile

Si vous avez besoin de communications sûres, la cryptographie est pour vous.

Citation : Wikipédia

> La cryptographie est une des disciplines de la cryptologie s'attachant à protéger des messages (assurant confidentialité et / ou authenticité) en s'aidant souvent de secrets ou clés.

Plus clairement, la cryptographie vous permet d'envoyer un message qui ne pourra être lu que par votre correspondant, et/ou de certifier à votre correspondant que vous êtes bien l'auteur du message. Pour cela, vous **chiffrez** les messages, c'est-à-dire que vous les rendez illisibles à l'aide d'une **clé** (un bout d'information qui sert à ça), et vous les **déchiffrez**, c'est-à-dire que vous les rendez lisibles à nouveau (avec une clé aussi).

Ce tuto a pour but de vous présenter un standard cryptographique puissant, considéré comme fiable et facile à utiliser, **OpenPGP**, et son implémentation libre la plus courante, **GnuPG**.
Sommaire du tutoriel :

- Obtenir GnuPG
- Générer vos clés
- Chiffrer un message
- Signer un message
- Le réseau de confiance

Obtenir GnuPG

Si vous avez déjà votre propre implémentation de PGP, vous pouvez l'utiliser, sinon je vous conseille d'utiliser Gnu Privacy Guard (souvent abrégé GnuPG ou GPG).

Sous Linux et *BSD

GPG est très probablement déjà installé ; tapez

Code : Console

```
gpg --help
```

pour vous en assurer et obtenir la liste des options de GPG.

Sinon, vous pouvez l'obtenir sous la forme de paquets deb ou rpm, ou télécharger le code source.

Sous Windows

Téléchargement de GnuPG pour Windows.

Sous Mac

Téléchargement de GnuPG pour Mac.
Notez que les versions pour Mac sortent avec un peu de retard ; la version actuelle de GnuPG est 1.4.6, mais seule la version 1.4.5 est disponible sous Mac pour le moment.

Autres OS, informations, etc.

Consultez la page de téléchargement principale de GnuPG.

Si un programme propriétaire a accès à vos clés (votre système, votre implémentation de PGP, etc.), n'oubliez pas que vous ne pouvez pas savoir ce qu'il en fait (car vous ne disposez pas du code source). Votre seule garantie est la parole de la compagnie distribuant le programme. Si vous ne lui faites pas confiance, ne le faites pas.

Générer vos clés

Non, vous n'allez pas aller chez le serrurier !
PGP fonctionne par paires de clés, appelées clés asymétriques car tout message chiffré avec une de ces deux clés est déchiffré avec l'autre (et uniquement avec l'autre - vous ne pouvez pas retrouver le message avec la clé avec laquelle vous l'avez chiffré).
Une de ces clés est publique : vous la diffusez à tout le monde ; l'autre est privée, vous devez la garder absolument secrète.

Vous allez demander à votre implémentation de PGP (nous supposerons que c'est GnuPG) de vous fournir ces deux clés. C'est un moment crucial : vous devez le faire sur une machine sûre.

Tapez

Code : Console

```
gpg --gen-key
```

GnuPG vous demande le type de clé que vous voulez, puis sa longueur. En général, les valeurs par défaut devraient convenir (la longueur courante d'une clé est entre 1024 et 2048 bits).
Vous devez ensuite choisir une date d'expiration pour la clé ; à moins que vous ayez une raison particulière de lui donner une durée limitée, choisissez 'jamais'.
Entrez ensuite votre nom (sous la forme Prénom Nom). L'adresse mail et le commentaire sont facultatifs, vous pouvez les laisser vides (il est préférable de toujours donner une adresse mail). GnuPG vous construira un nom d'utilisateur de la forme

Code : Console

```
Prénom Nom (Commentaire) <mail@domaine>
```

ou

Code : Console

```
Prénom Nom <mail@domaine>
```

si vous avez laissé le commentaire vide.

Si vous avez fait une erreur dans le nom d'utilisateur, il est encore temps de changer (voire d'annuler complètement si vous ne voulez finalement pas de clé) ; sinon, confirmez.

Vous choisissez alors une phrase de passe pour accéder à votre clé ; c'est un choix important. Vous devez choisir une phrase à la fois difficile à trouver (pas de mots existants, de noms ou de dates de naissance) et facile à retenir. On conseille en général une phrase d'au moins 12 caractères. Notez cette phrase sur un papier pour le moment (ou sur n'importe quoi de facile à détruire complètement).

Lors de la génération de votre clé, vous devez fournir du hasard : tapez comme un fou sur le clavier.
GnuPG génère alors votre clé privée, et la clé publique qui va avec.
Et voilà, il vous donne votre paire de clés.

Code : Console

```
pub   1024D/1258BA3D 2006-12-29 [expire: 2006-12-30]
```

```
    Empreinte de la clé = 295C 13B3 0E27 5F17 8347  9DE6 350D F3E3 1258 BA3D
uid                  Example (Only an example, do NOT use key)
sub   2048g/DFDA3E9D 2006-12-29 [expire: 2006-12-30]
```

Notez l'identifiant de la clé (ici, 1258BA3D), que vous retrouvez aussi à la fin de l'empreinte de la clé. Lorsque vous voudrez utiliser votre paire de clés, vous la désignerez par cet identifiant.

Il se pourrait bien que vous veniez à perdre cette phrase de passe, ou à ne plus avoir accès à votre clé pour une autre raison. Dans ce cas, il faudra **révoquer** la clé (la marquer comme inutilisable et sans valeur). En prévision, vous allez tout de suite générer un certificat de révocation.

Code : Console

```
gpg --output revoke.asc --gen-revoke id de la clé
```

Vous pouvez choisir la raison de la révocation, plus une description optionnelle.
GnuPG vous demande d'entrer la phrase de passe (que vous avez notée). Vous obtenez le certificat, appelé revoke.asc. Si vous devez l'utiliser, tapez

Code : Console

```
gpg --import revoke.asc
```

Votre clé sera révoquée.

Copiez ce certificat sur des supports sûrs : vous ne devez pas le perdre, et il ne doit pas être obtenu par d'autres. Si quelqu'un met la main dessus, il pourra révoquer votre clé ; ce sera ennuyeux, mais c'est bien préférable à la découverte de votre clé (surtout si vous ne pouvez plus la révoquer).

Détruisez maintenant le papier où vous avez noté la phrase de passe (brûlez-le ou mangez-le). Si vous l'oubliez, vous révoquerez votre clé avec le certificat que vous venez de générer.

Félicitations, vous avez maintenant votre paire de clés !

Chiffrer un message

Vous voulez m'envoyer un message, or vous avez peur que Mallory le lise.

Pour une raison quelconque, en cryptographie, le méchant s'appelle toujours Mallory.

Vous allez donc utiliser ma clé publique pour le chiffrer.

Comment obtenir cette clé ?

C'est moi qui la publie. Pour publier votre clé, il faut que vous l'exportiez

Code : Console

```
gpg --output votrecle.asc --armor --export id de la clé
```

Vous obtenez alors un fichier votrecle.asc contenant quelque chose comme ça

Code : Console

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1.4.3 (GNU/Linux)
```

```
mQGiBEWTfiERBACLUg/A8sHz/6zXZXa8szbr+DEJ3p3eKqmd7Qh7zeCQW+lMpf6I
wTmQ3C7xMv11VVG5ZkTikj0nTyhH2RrETNeA7HCoqsJXAy5DUPw7uhk4i6uJ26Mn
7qeFXFtWbppvc+QAnPblry1mSu9o/cG7Vm3sTAwSPAPEYjivDQ/TJTWMIwCgmAzy
BOMaMZ8WWW+PpzBr9rIH7jEEAIBmiK4X69eyk+iTibQ/SzecllyoGRFazSKUiB1P
3QNfuAX6vOXqS6Cwx6FHqZL0ifc6+t8Aovgbm6v7qOAebiAAHen1aRw4a4Z5i5Il
Fft1TRvNxrKHQ/YOBIsfd7roBF5YrvQfadENnBPJ757RNdeKhbBnPguAAeqrBbWs
vKLxA/91KvoykccLkxTMIKll3FkVsGKdhVdBEuZUlbo567nDOmrCmjGRoVY0H9wm
KPdWlT/ckmB8zK/Epb+yylrxeWP2QqhMwlreJQs/oQo+t8YaskU0UWguZvmaHmlf
JLZI4gqiGpuwLUCXBUk+39xtnKjnD/YaFvM1SY3sZonsHinlwLQ8TWFub24gZGUg
R2FpbGxhbmRlIChSYW5kb20gZ2VlaykgPG1pbG9tYXJvQGNsdWItaW50ZXJuZXQu
ZnI+iGAEExECACAFAkWTfiECGwMGCwkIBwMCBBUCCAMEFgIDAQIeAQIXgAAKCRDY
rKg97NwgFSYgAJ4icjjZChEW4KKs2j/y0mLtEc0uiwCeN6Juhx9SozcsCTq3xcmW
1I0ADxK5Ag0ERZN+OhAIAJ9Y0WyPN8103/qdGKanEjzvsREgWDUAljb4/CquOg/P
zB7EY7QK6U41ZmE5eXX547k1WcG2r1M6cz1WOsNi3NxrYM1Rp8RhNLIWb5CJjg1L
1FQSDiHrAL6uZZJwnLYZX8UIAQhNdq3YhqybhX08bKOnulnRZyd6whLgesLjPAGh
UhgSuOmvfUpqW21PpS3pTzoUr6bLVxNuGTncweEr2pPg8k6DE8uXzdsg5pU5vN2S
KXp8YUBiwKjNK5nHnGgXFVc5+MXy4Jmrjl+XPzvoJKj0E9skeTW+fxBQeJqd6bUN
YlTvA0m+BiifxHxHg3NPBwEopEUwCNKSTpL8GHguCk8AAwcIAJ2rbijNIKIl9Md2
XKbnUa7mlb0JPby1OIsoCU3sBoNGbqp0F+ueLc26SfzDIbhUMgu9s0K/1hcH1pe2
3j+Km9ku/HRPS5MZQC4nVMsObD93FXkc+uKjgvXm5r9I2jGJZX3nz75VqItwh+dL
LSwaZlHciIypweb9NmyA/q1c2qUd2IoUePHmeWiH642nPdzKIUV82OfEibshESlj
mhUe1wBbsWZcO+yd6gFpaCCeD+5XIiHsIsPkGQBv0rVI1KVaFFQZ0uRTu2hc4Xtg
qM/XBRryVlh841VPGsBh91TOE9i55o8CBlYjHB+MXy3DeiKSSAQt8HnyiojvPm2Z
nXGfRTOISQQYEQIACQUCRZN+OgIbDAAKCRDYrKg97NwgFTVtAKCVKqEnouuK++UJ
aXulL3ZRkZhiQACfQVjRepRKPyjcQf+kI5Sdc7ssrBg=
=hAfs
-----END PGP PUBLIC KEY BLOCK-----
```

(Pas très convivial, hein ?)
Vous copiez ce fichier partout où il vous semble bon, notamment sur votre page personnelle, et sur les serveurs de clés (des sites qui stockent des clés publiques, comme Keyserver). Chacun peut alors accéder à votre clé publique et l'utiliser.

Une fois que vous avez obtenu ma clé publique, vous l'ajoutez à votre "trousseau de clés" avec

Code : Console

```
gpg --import macle.asc
```

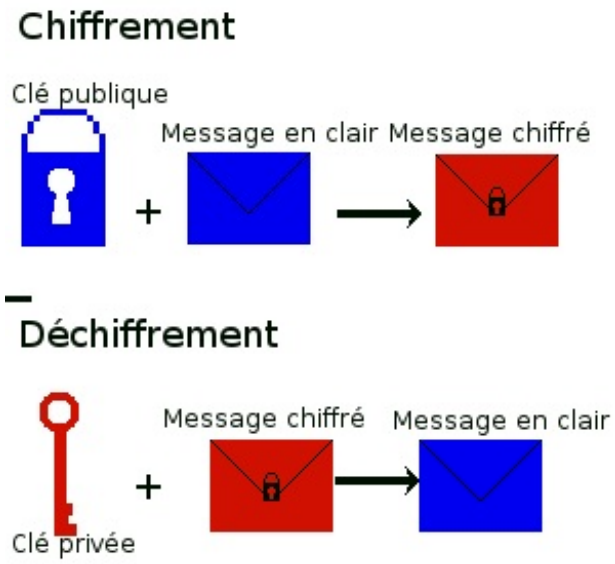
Vous pouvez alors utiliser ma clé publique autant que vous voulez sans avoir à l'importer à nouveau.
Pour chiffrer un message pour moi :

Code : Console

```
gpg --recipient mon nom d'utilisateur --encrypt message
```

Le fichier message.gpg (ou autre si vous utilisez --output) contiendra le message chiffré avec ma clé publique, donc uniquement déchiffrable avec ma clé privée, que je possède et pas Mallory.

Schéma du chiffrement et du déchiffrement



Si vous recevez un message chiffré avec votre clé publique, déchiffrez-le avec

Code : Console

```
gpg --decrypt message.gpg
```

Notez que si ces échanges se font par mail, la plupart des messageries vous proposent de s'en charger automatiquement, à condition que vous fassiez assez confiance à votre messagerie pour lui confier votre clé privée.

Signer un message

Maintenant, le contraire : vous voulez prouver qu'un message vient bien de vous (parce que Mallory envoie des messages en se faisant passer pour vous, ou modifie le contenu de vos messages).

Si vous envoyez en même temps que le message le message chiffré avec votre clé privée (la "**signature**"), il suffira de le déchiffrer avec votre clé publique (connue de tous) et de vérifier qu'on retombe bien sur le même message. Tout le monde pourra alors vérifier que :

- le message vient bien de quelqu'un connaissant votre clé privée (normalement vous) ;
- le message n'a pas été modifié depuis que vous l'avez signé.

En réalité, la signature ne fonctionne pas exactement comme ça (la fonction utilisée est un peu plus complexe), mais c'est le principe.

Pour signer et compresser un message

Code : Console

```
gpg --sign message
```

Pour signer un message en le laissant lisible

Code : Console

```
gpg --clearsign message
```

Pour signer un message avec une signature dans un fichier séparé (si le fichier ne doit pas être modifié)

Code : Console

```
gpg --detach-sign message
```

Pour vérifier la signature d'un message signé

Code : Console

```
gpg --verify message.asc
```

Si le message est aussi compressé

Code : Console

```
gpg --verify message.gpg
```

vérifie la signature, et

Code : Console

```
gpg --decrypt message.gpg
```

permet à la fois de lire le message et de vérifier la signature.
Avec une signature séparée, on utilise

Code : Console

```
gpg --verify signature.sig message
```

Il existe une exception : si le message signé s'appelle message et la signature message.sig, on peut se contenter d'écrire

Code : Console

```
gpg --verify message.sig
```

Bien entendu, on peut à la fois signer et chiffrer un message. Il est même conseillé de signer les messages chiffrés. Il suffit de combiner les options.

Code : Console

```
gpg --recipient 'nom du destinataire' --sign --encrypt message
```

Le réseau de confiance

Ce système permet bien de prouver que vous discutez bien avec la personne possédant la clé appelée "ma clé", mais pas que cette clé est bien la mienne et pas celle de Mallory se faisant passer pour moi.

Pour cela, PGP permet aux possesseurs de clés de signer les clés des autres, c'est-à-dire de certifier qu'elles appartiennent bien à leur propriétaire. Les preuves suffisantes sont en gros d'avoir vu la personne avec une preuve de son identité et l'empreinte et la taille de sa clé.

Normalement, toutes les clés devraient être signées par d'autres, elles-mêmes signées par d'autres, et ainsi de suite jusqu'à arriver à quelques personnes fiables comme Phil Z (l'inventeur de PGP), Linus Torvalds (le créateur de Linux) ou Richard Stallman (le fondateur de GNU) : ce réseau reliant les clés entre elles est appelé réseau de confiance (*web of trust*). En pratique, ça ne se passe pas vraiment comme ça, parce que trop peu de gens ont une clé PGP, et qu'elles sont souvent peu signées.

Pour signer une clé publique (que vous avez importée)

Code : Console

```
gpg --edit-key id de la clé

Commande> sign
```

GnuPG vous demande confirmation, puis votre phrase de passe.
Vous devez ensuite spécifier à quel point vous faites confiance à cette clé.

Code : Console

```
Commande> trust
```

Vous devriez normalement choisir "confiance entière" (4).

Code : Console

```
Commande> q
```

GnuPG vous demande si vous souhaitez enregistrer les changements, répondez oui.

En règle générale, vous ne devriez pas faire confiance à une clé peu signée.
Vous êtes à présent capable de vous servir de votre paire de clés PGP. À condition de bien faire attention à votre clé privée, Mallory ne peut plus rien contre vous.
Si vous voulez en apprendre plus sur GnuPG, consultez le site officiel.

Icône du tuto par MisterMatt sous GNU Free Documentation License.

Ce tutoriel a été corrigé par les zCorrecteurs.