


# Installer GPG et Enigmail sur Mozilla en 12 étapes

*(Windows, Linux, MacOS X)*

1. Pour Windows et MacOS X, vérifier que le programme GnuPG (WinPT ou MacGPG) est installé sur l'ordinateur (version Windows, version MacOS X)

2. Vérifier que le programme Enigmail est installé sur l'ordinateur

2.1 Vous pouvez aussi installer le module de traduction française pour Mozilla ainsi que pour Enigmail 

3. Si le compte courrier n'a pas encore été créé dans Mozilla, le faire:



Assistant de création de compte

### Paramétrage du nouveau compte

Pour recevoir des messages, vous devez d'abord créer et paramétrer un compte Courrier ou Forums.

Cet assistant va collecter les informations nécessaires à la création d'un compte Courrier ou Forums. Si vous êtes incapable de répondre à certaines questions, veuillez contacter votre Administrateur Système ou votre Fournisseur d'Accès Internet.

Sélectionnez le type de compte que vous voulez créer :

☒ Compte Courrier

☐ Compte Forums

< Précédent   Suivant >   Annuler

Assistant de création de compte

### Information sur le serveur

Sélectionnez le type du serveur de réception.

☒ POP   ☐ IMAP

Entrez le nom du serveur de réception (par exemple, « pop.exemple.fr »).

Nom du serveur :

Entrez le nom du serveur d'envoi (SMTP) (par exemple, « smtp.exemple.fr »).

Nom du serveur :

< Précédent   Suivant >   Annuler

Assistant de création de compte

**Nom d'utilisateur**

Entrez le nom d'utilisateur donné par votre fournisseur de courrier (par exemple, « pmartin »).

Nom d'utilisateur :

< Précédent   Suivant >   Annuler

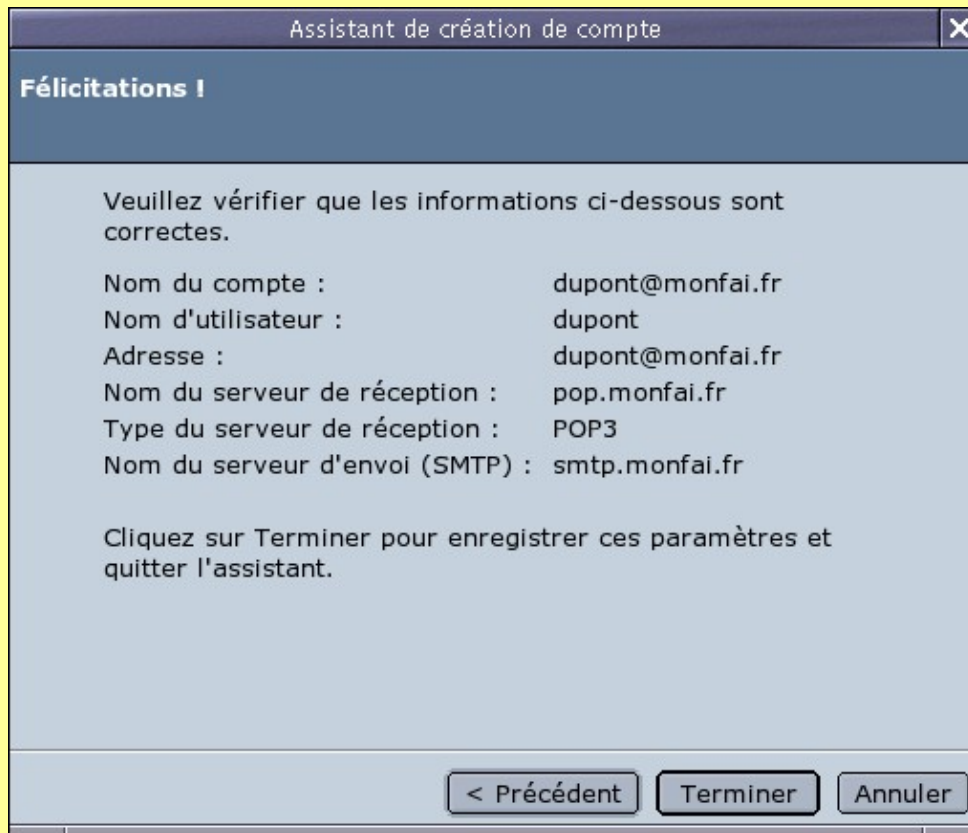
Assistant de création de compte

**Nom du compte**

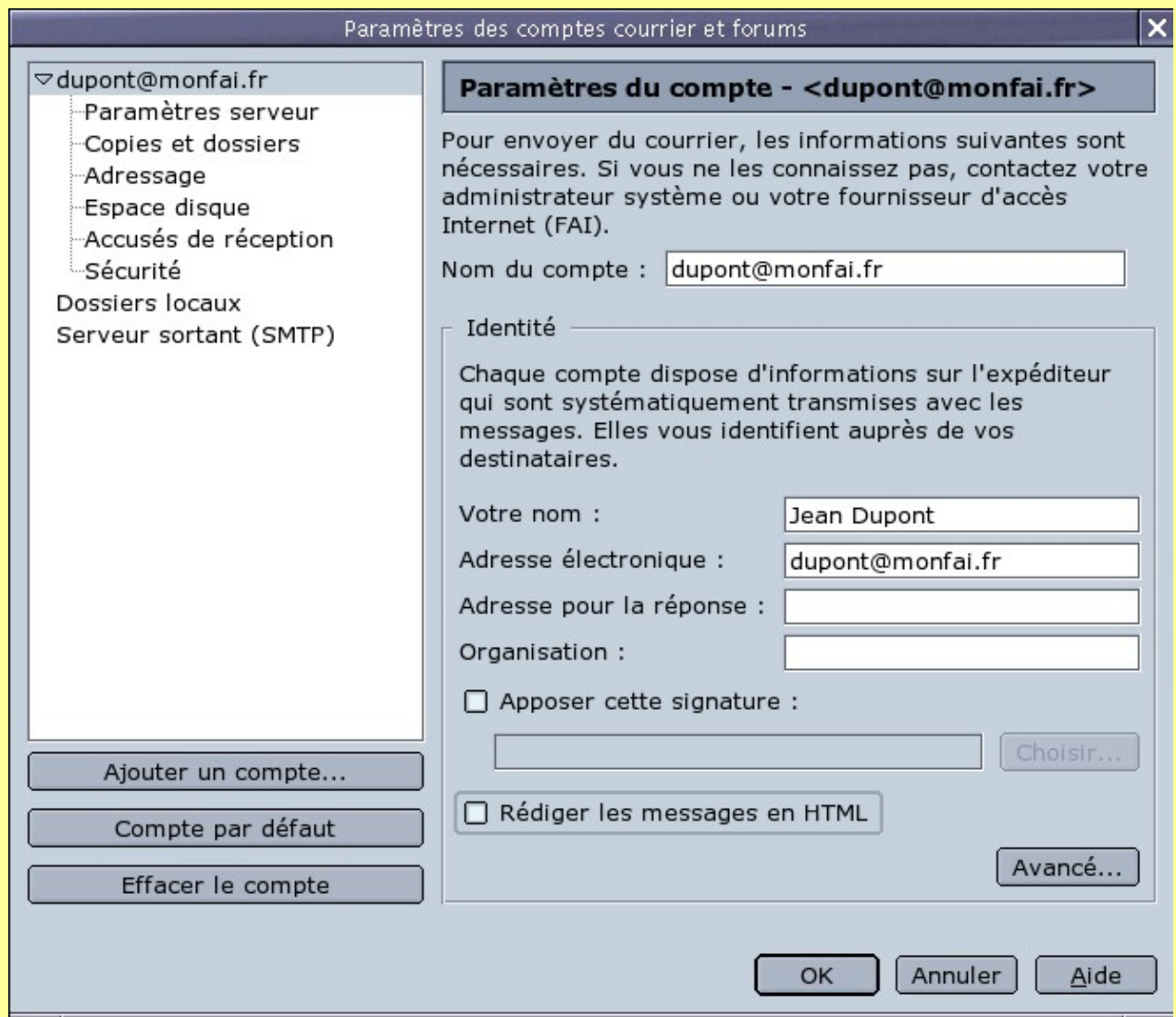
Entrez le nom avec lequel vous souhaitez vous référer à ce compte (par exemple « Compte Travail », « Compte personnel » ou « Compte Forums »).

Nom du compte :

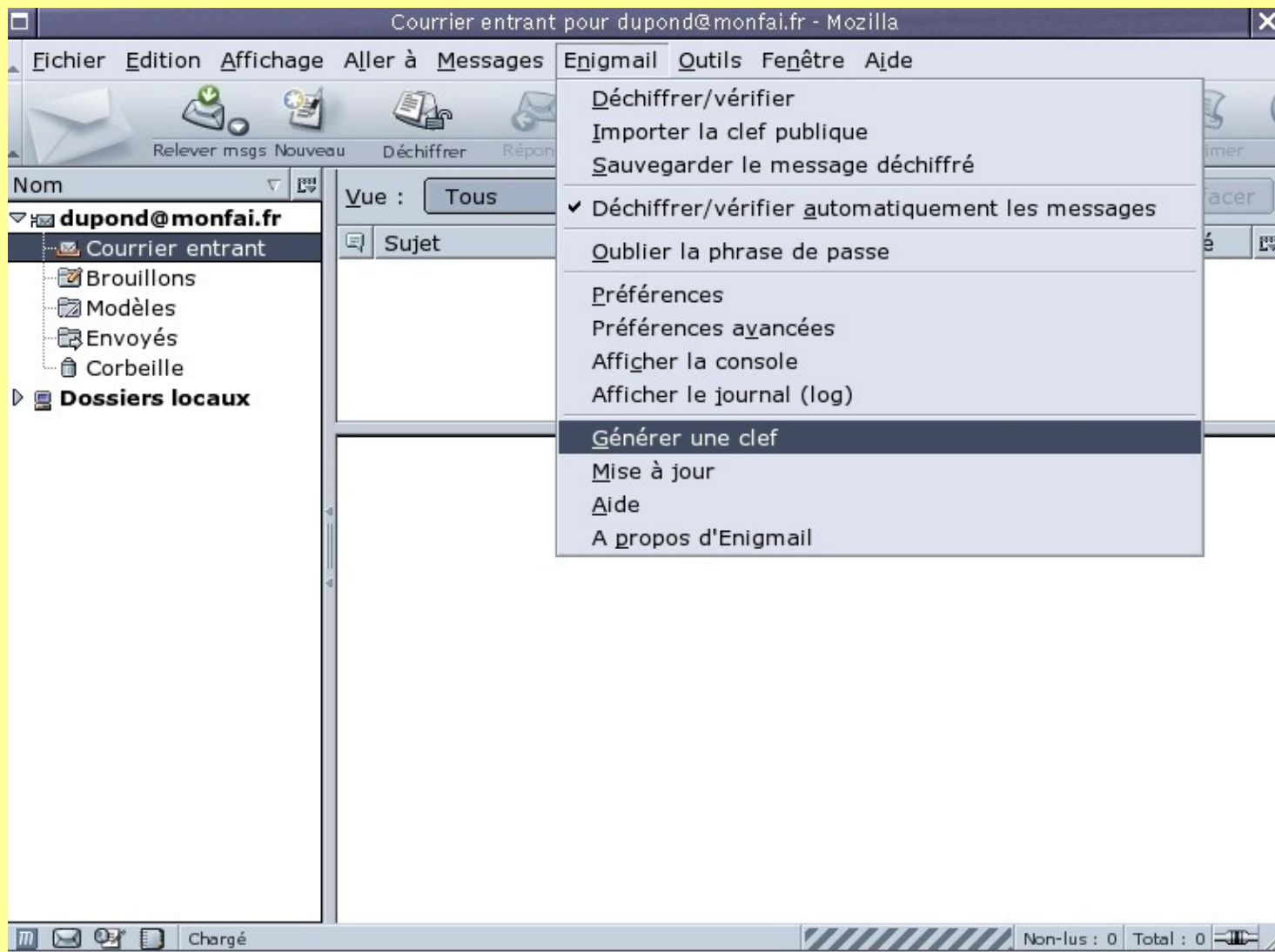
< Précédent   Suivant >   Annuler



**4. Dans les paramètres courrier, décocher l'option "Rédiger les messages en HTML":**



## 5. Générer sa paire de clefs OpenPGP (clef publique / clef privée):



## 5.1 La paire de clefs peut aussi être générée dans un terminal avec la commande:

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



```
dupont@localhost.localdomain: /home/dupont
[dupont@localhost dupont]$ gpg --gen-key
gpg (GnuPG) 1.2.1; Copyright (C) 2002 Free Software Foundation, Inc.
This program comes with ABSOLUTELY NO WARRANTY.
This is free software, and you are welcome to redistribute it
under certain conditions. See the file COPYING for details.

Sélectionnez le type de clé désiré:
  (1) DSA et ElGamal (par défaut)
  (2) DSA (signature seule)
  (5) RSA (signature seule)
Votre choix ? █
```

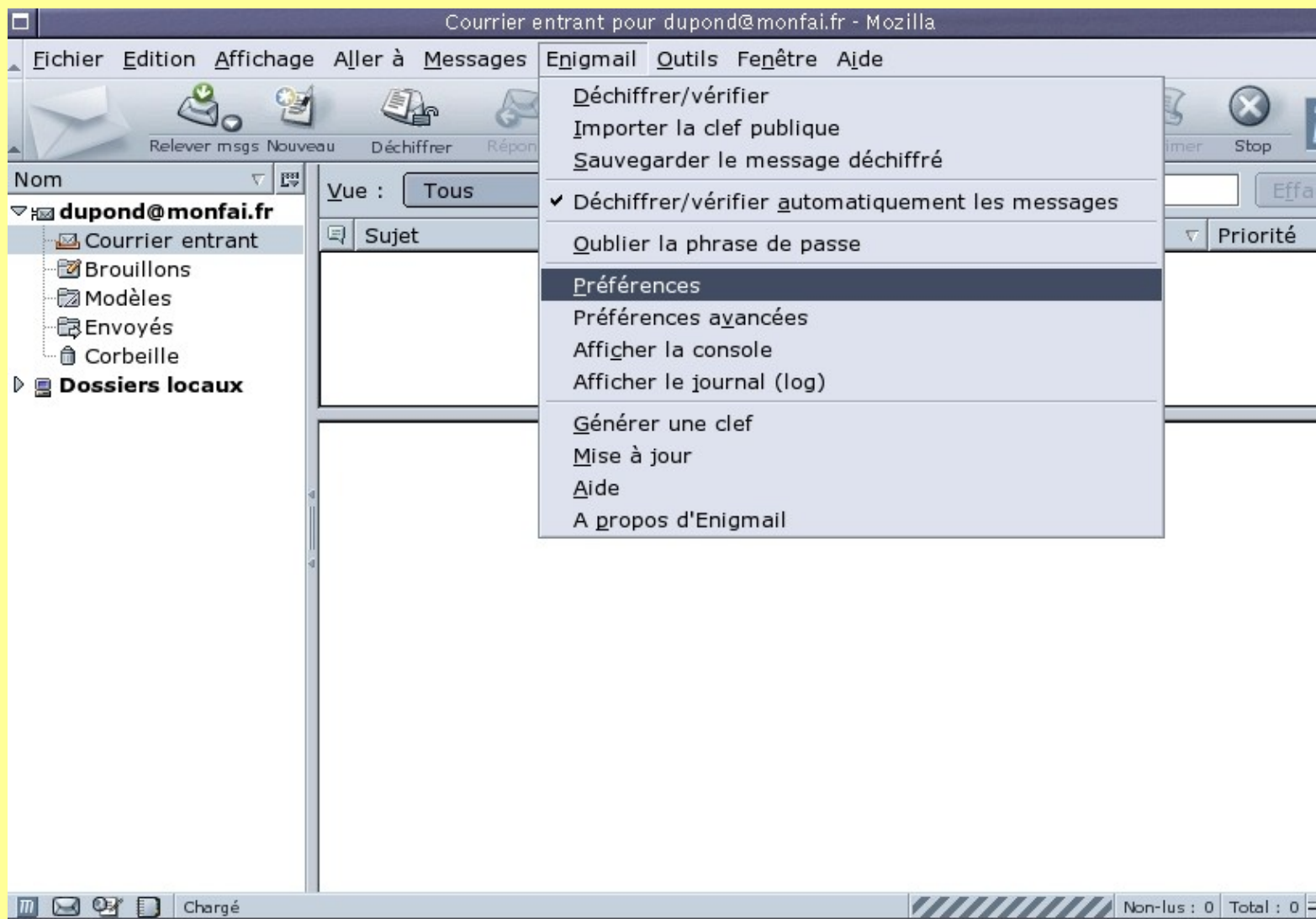
6. La paire de clefs OpenPGP contient une clef publique (pour chiffrer) et une clef secrète (pour déchiffrer).

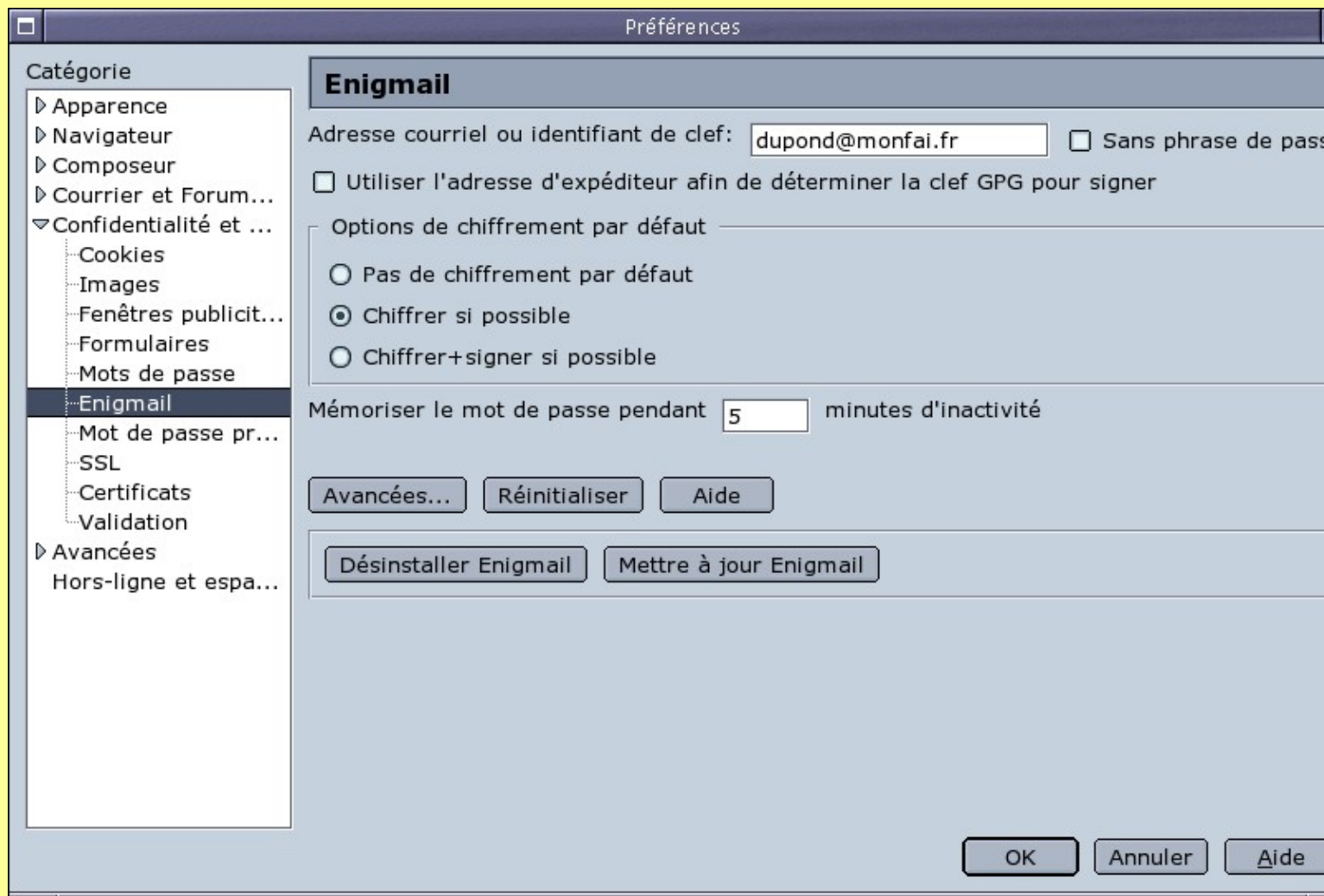
Les "trousseaux" contenant toutes les clefs sont les fichiers **pubring.gpg** et **secring.gpg** du répertoire "gnupg":

```
dupont@localhost.localdomain: /home/dupont
[dupont@localhost dupont]$ ll ~/.gnupg
total 32
-rw-r--r-- 1 dupont dupont 7736 jui 17 19:22 gpg.conf
-rw-r--r-- 1 dupont dupont 10573 jui 18 10:28 pubring.gpg
-rw-r--r-- 1 dupont dupont 600 jui 17 19:26 random_seed
-rw-r--r-- 1 dupont dupont 1048 jui 17 19:24 secring.gpg
-rw-r--r-- 1 dupont dupont 1280 jui 18 10:28 trustdb.gpg
[dupont@localhost dupont]$ █
```

7. Paramétrer Enigmail:







Préférences avancées d'Enigmail

Chemin d'accès de l'exécutable GPG

Lors de l'envoi d'un courrier

- ☐ Signer les messages par défaut
- ☐ Signer les messages dans les forums par défaut
- ☒ Chiffrer pour moi-même
- ☒ Toujours avoir confiance en l'identifiant utilisateur
- ☒ Autoriser le format texte coulé (RFC 2646)

Options supplémentaires

- ☐ Toujours confirmer avant l'envoi
- ☒ Utiliser le commentaire par défaut dans la signature
- ☒ Cacher les boutons/menus SMIME
- ☐ Treat '--' as signature separator
- ☐ Capturer le webmail (expérimental)

Options PGP/MIME

- ☐ Ne jamais utiliser PGP/MIME
- ☒ Utiliser PGP/MIME si possible
- ☐ Toujours utiliser PGP/MIME

Algorithme de hachage:

Serveur de clefs:

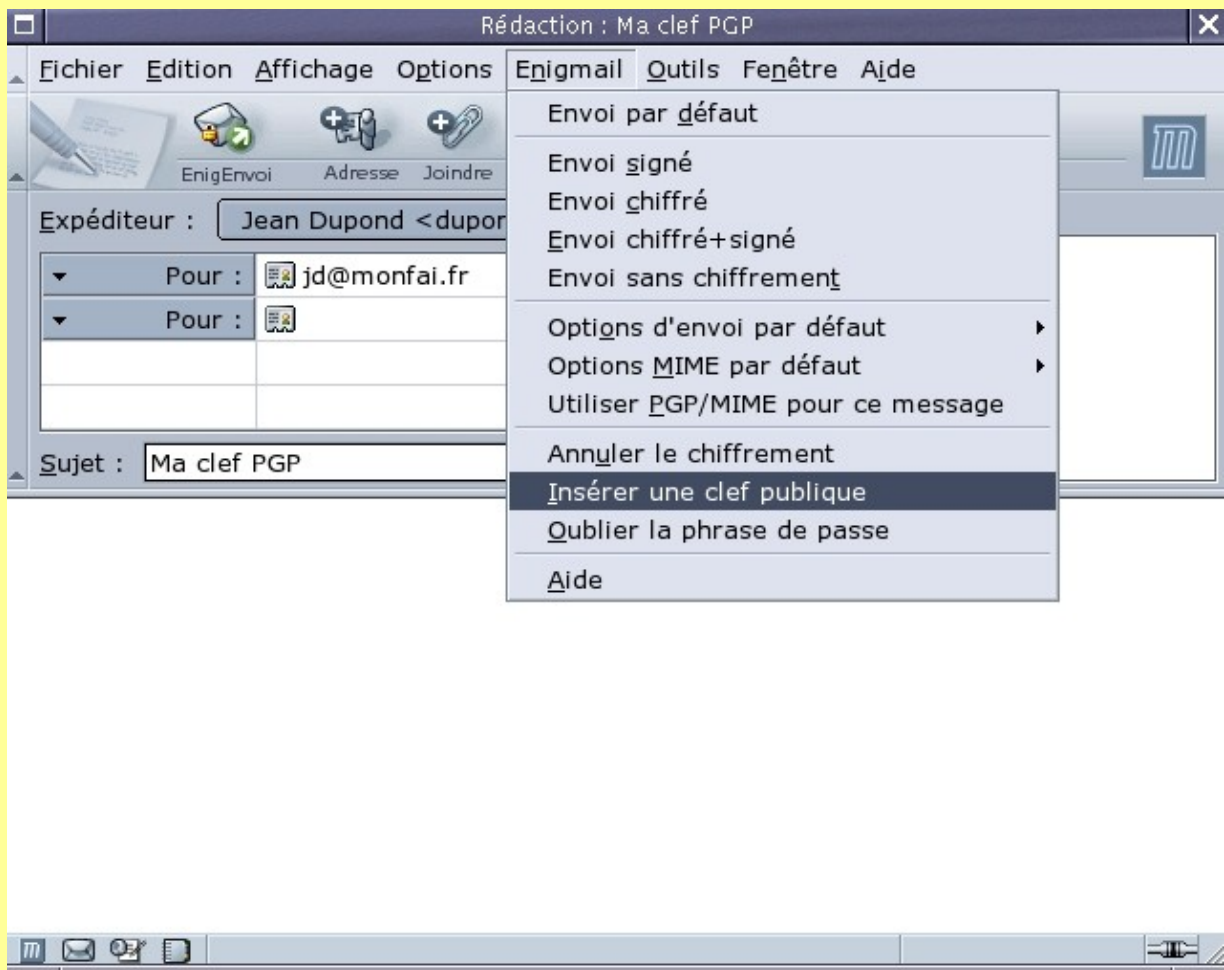
Déboguage d'Enigmail

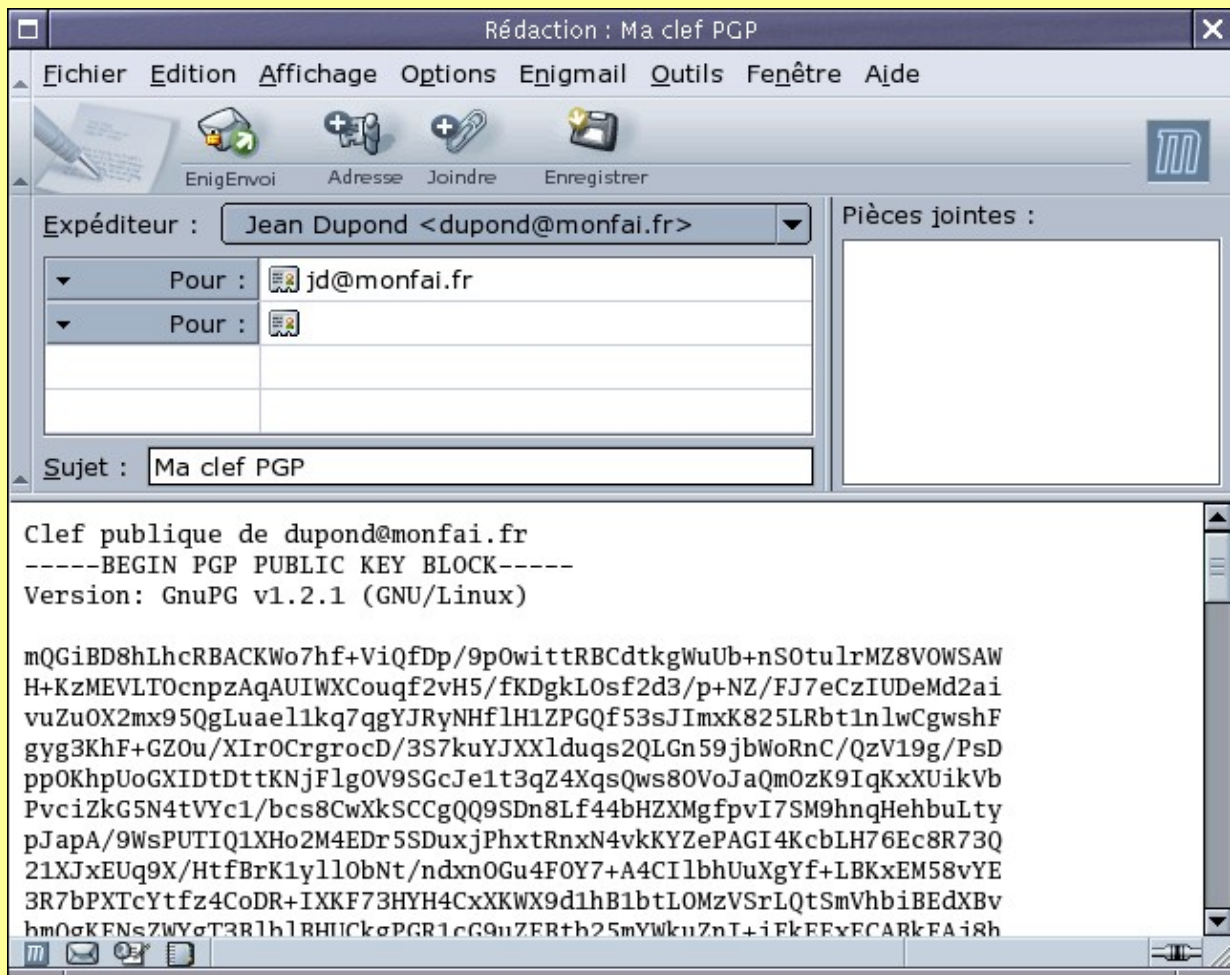
Répertoire du journal (log)

Adresse de messagerie de test

☐ Utiliser la signature et le chiffrement à la volée (expérimental)

**8. Exporter sa clef publique OpenPGP et l'insérer dans un message pour l'envoyer à ses correspondants:**



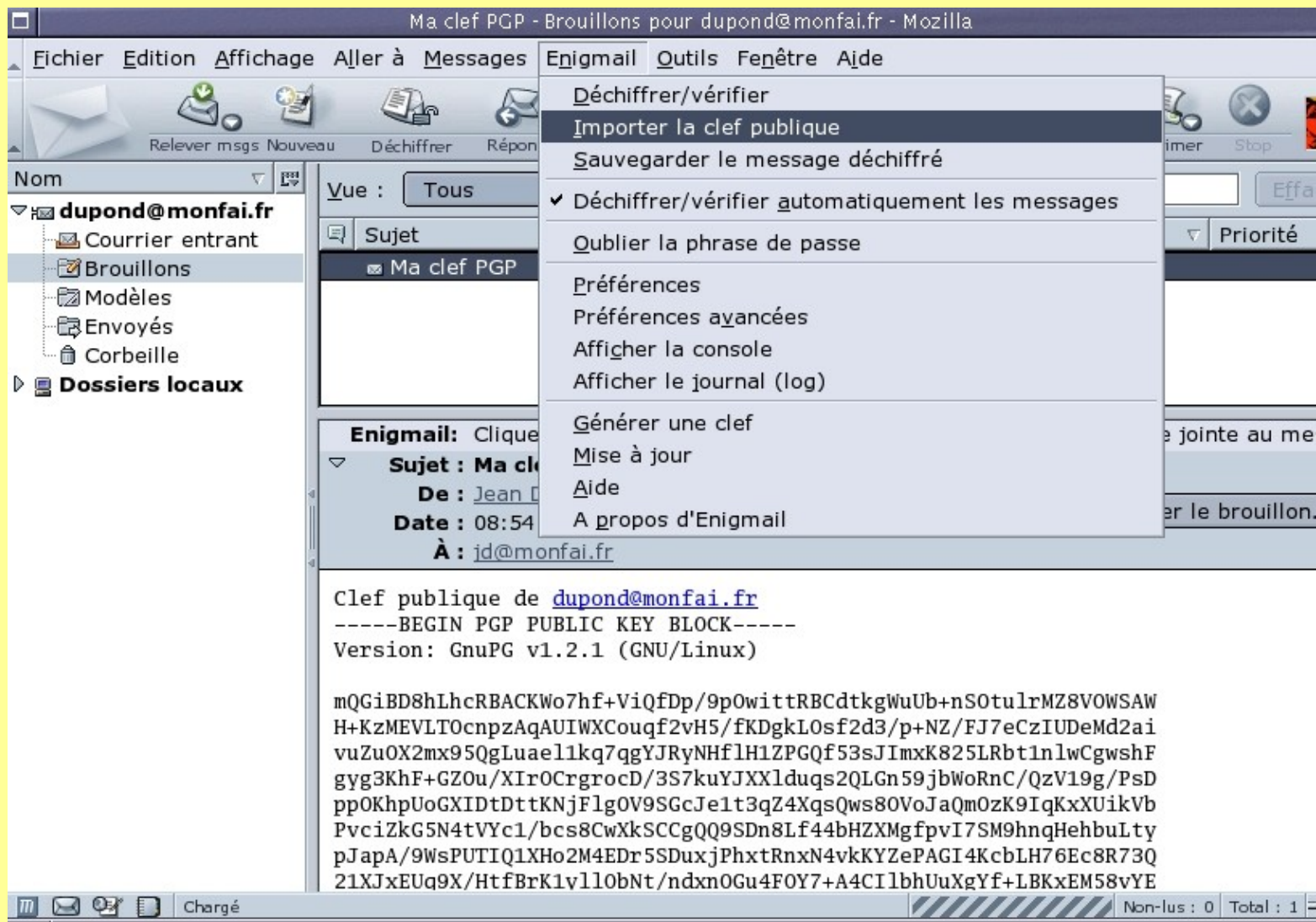


**8.1 La clef publique OpenPGP peut aussi être copiée dans un fichier "maclef.asc" en tapant dans un terminal la commande:**

```
gpg --export -a dupont@monfai.fr > maclef.asc
```

**9. Importer une clef publique envoyée par un correspondant:**





10. Pour lister les clefs de son trousseau OpenPGP, dans un terminal taper la commande:

```
gpg --list-keys
```

```
dupont@localhost.localdomain: /home/dupont
[dupont@localhost dupont]$ gpg --list-keys
/home/dupont/.gnupg/pubring.gpg
-----
pub 1024D/83217383 2003-07-17 Jean Dupont (Clef OpenPGP) <dupont@monfai.fr>
sub 1024g/C7A4EDDD 2003-07-17

pub 1024D/B2D7795E 2001-01-04 Philip R. Zimmermann <prz@mit.edu>
uid                               Philip R. Zimmermann <prz@acm.org>
uid                               [jpeg image of size 3457]
sub 3072g/A8E92834 2001-01-04

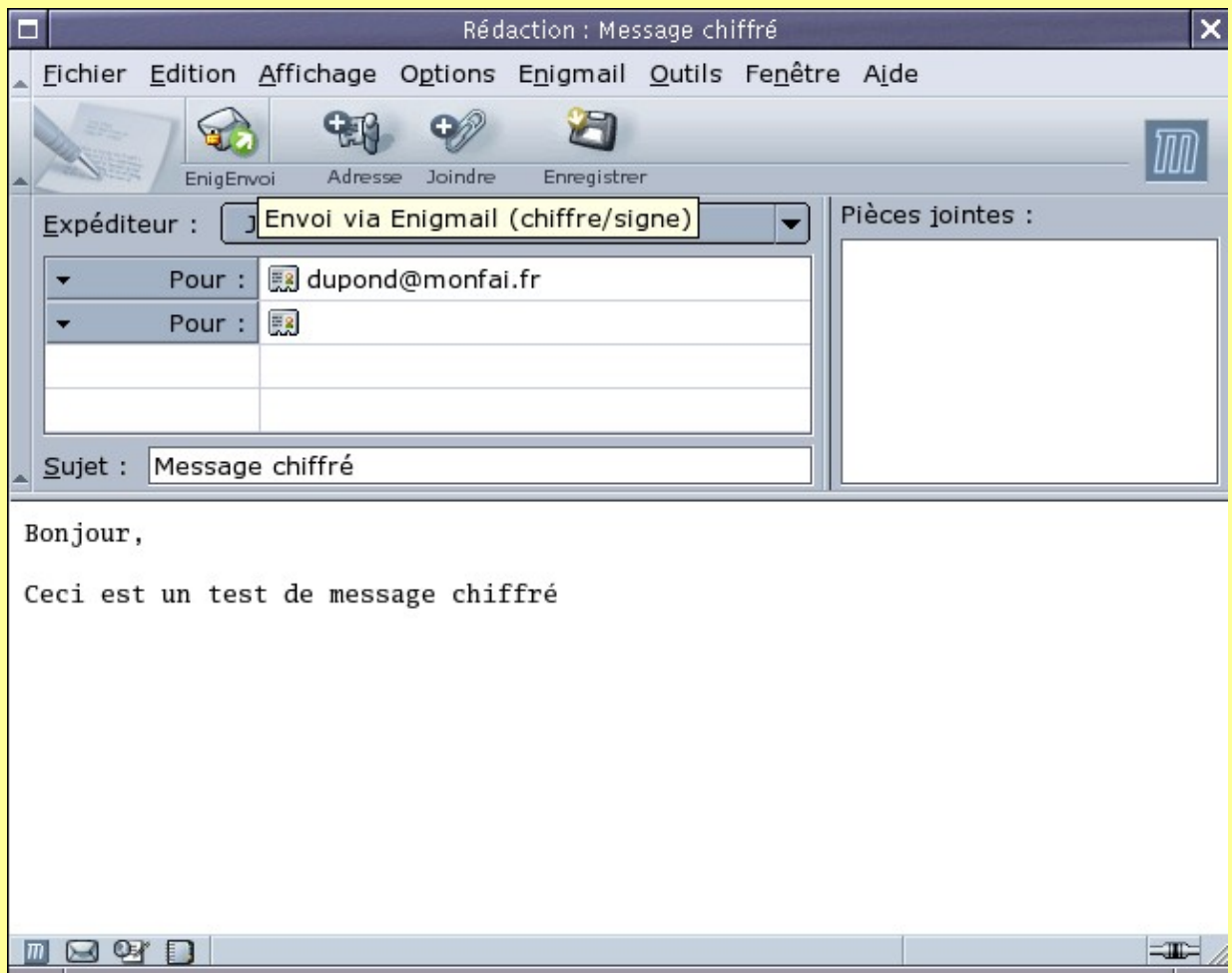
pub 1024D/FAEBD5FC 1997-04-07 Philip R. Zimmermann <prz@pgp.com>
sub 2048g/42F0A0A0 1997-04-07

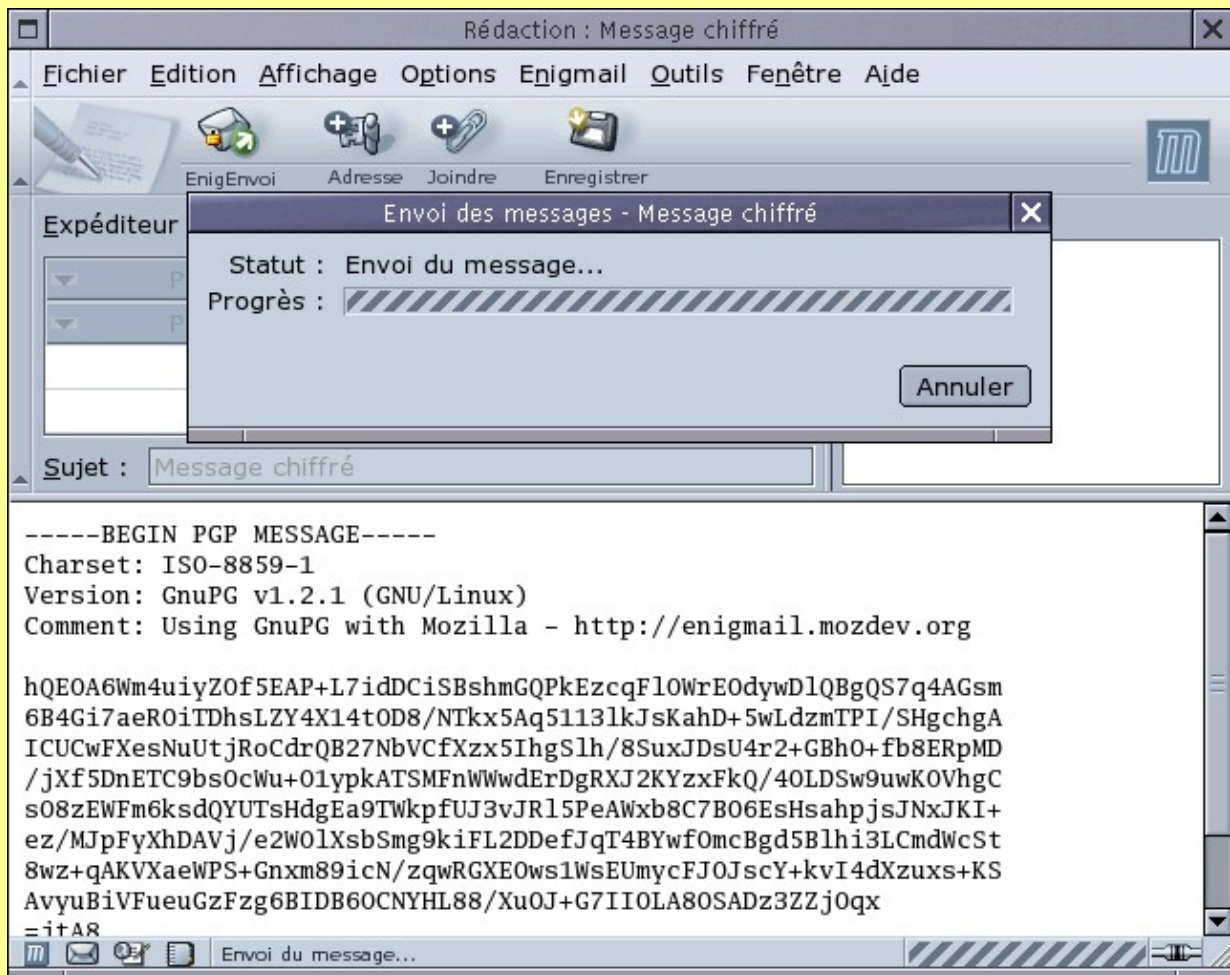
pub 1024R/C7A966DD 1993-05-21 Philip R. Zimmermann <prz@acm.org>

[dupont@localhost dupont]$ █
```

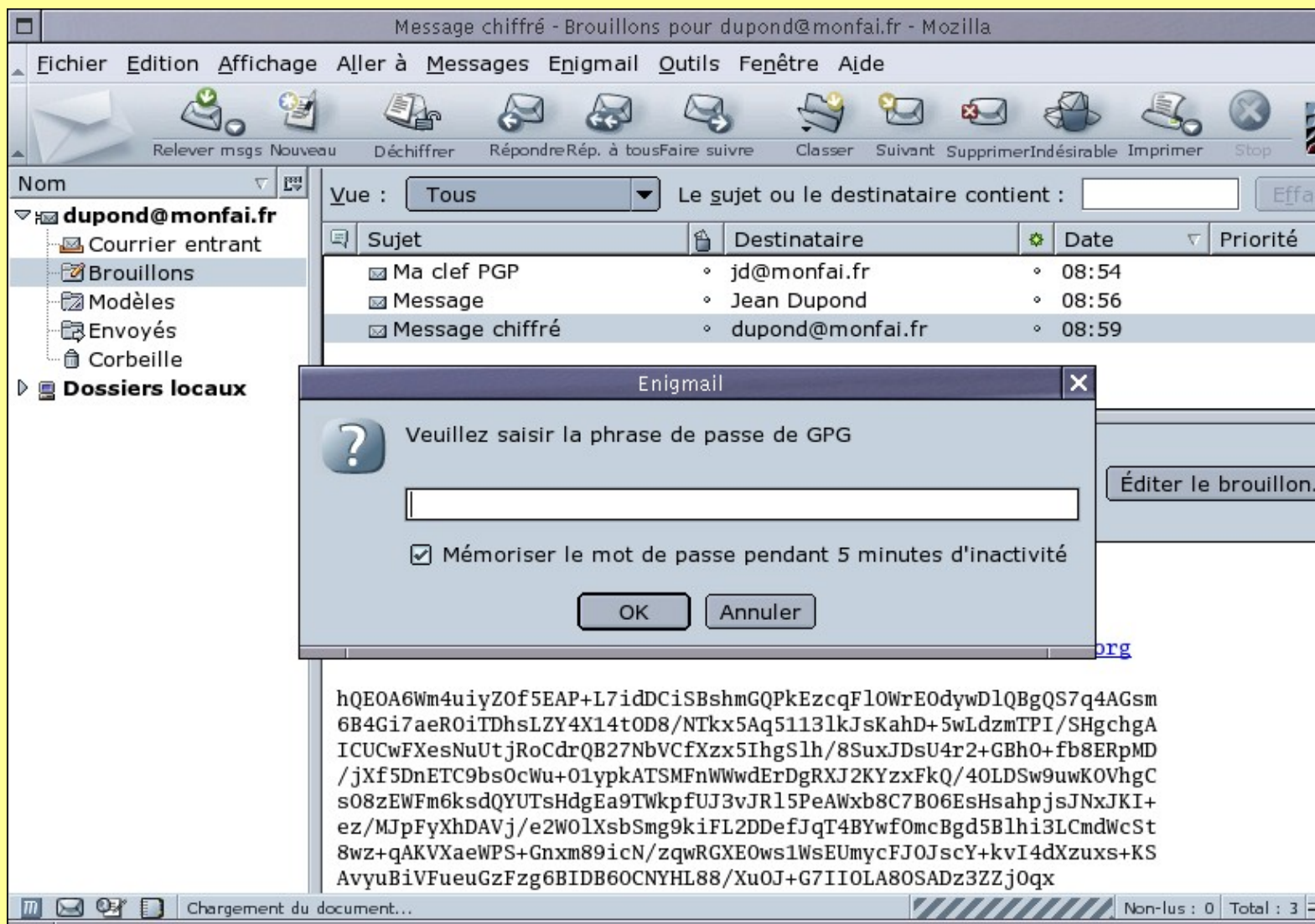
## 11. Envoyer un message chiffré au format OpenPGP :







## 12. Déchiffrer un message chiffré en OpenPGP :



Copyright (c) 2003, pplf