# Crypter vos communications : Open PGP : Pretty Good Privacy

Michel Memeteau informatique@millebabords.org

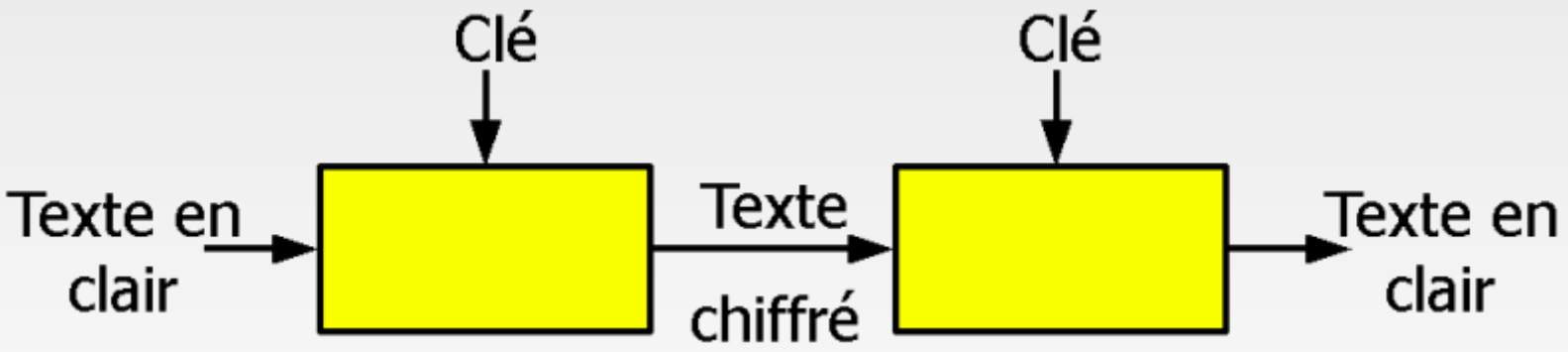
14 Mai 2011 - Ubuntu Natty install Party

# Plan

- Historique/ Principe
- Utilisation sur Ubuntu GNU/Linux
- Utilisation sur Microsoft Windows & Mac OSX
- Application aux messageries instantanées

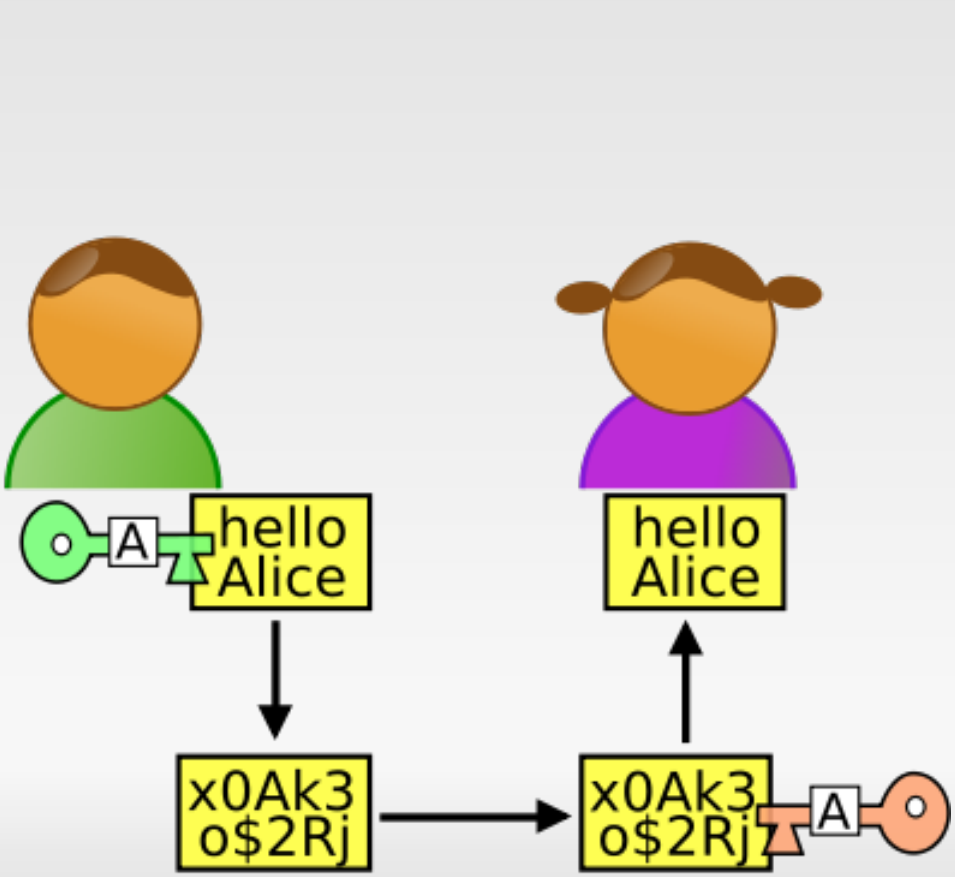
# Historique 1/2

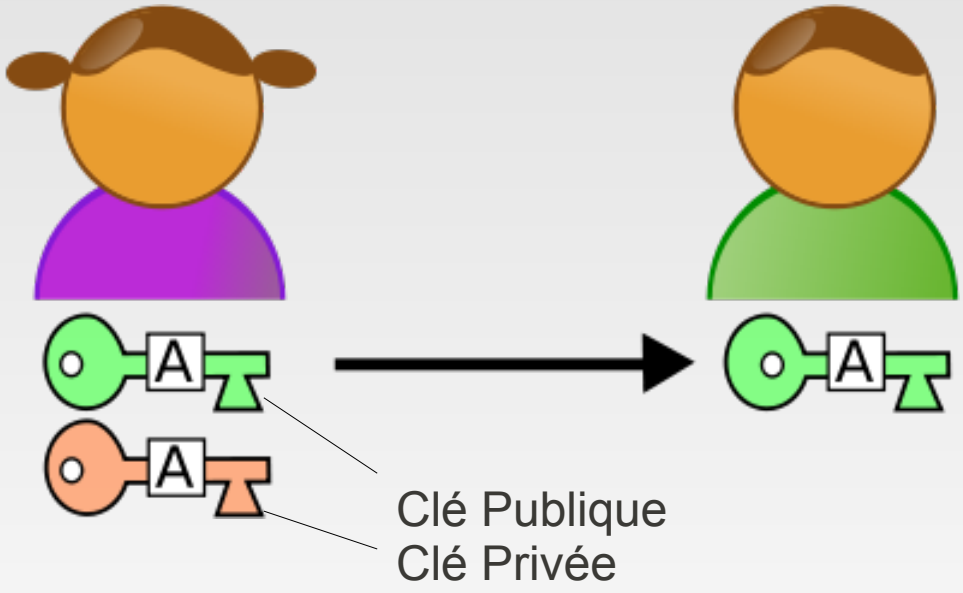
- Avant ~1970 : Cryptographie symmétrique
- Une seule clé secrète que chacun des 2 correspondants doit avoir



# Historique 2/2

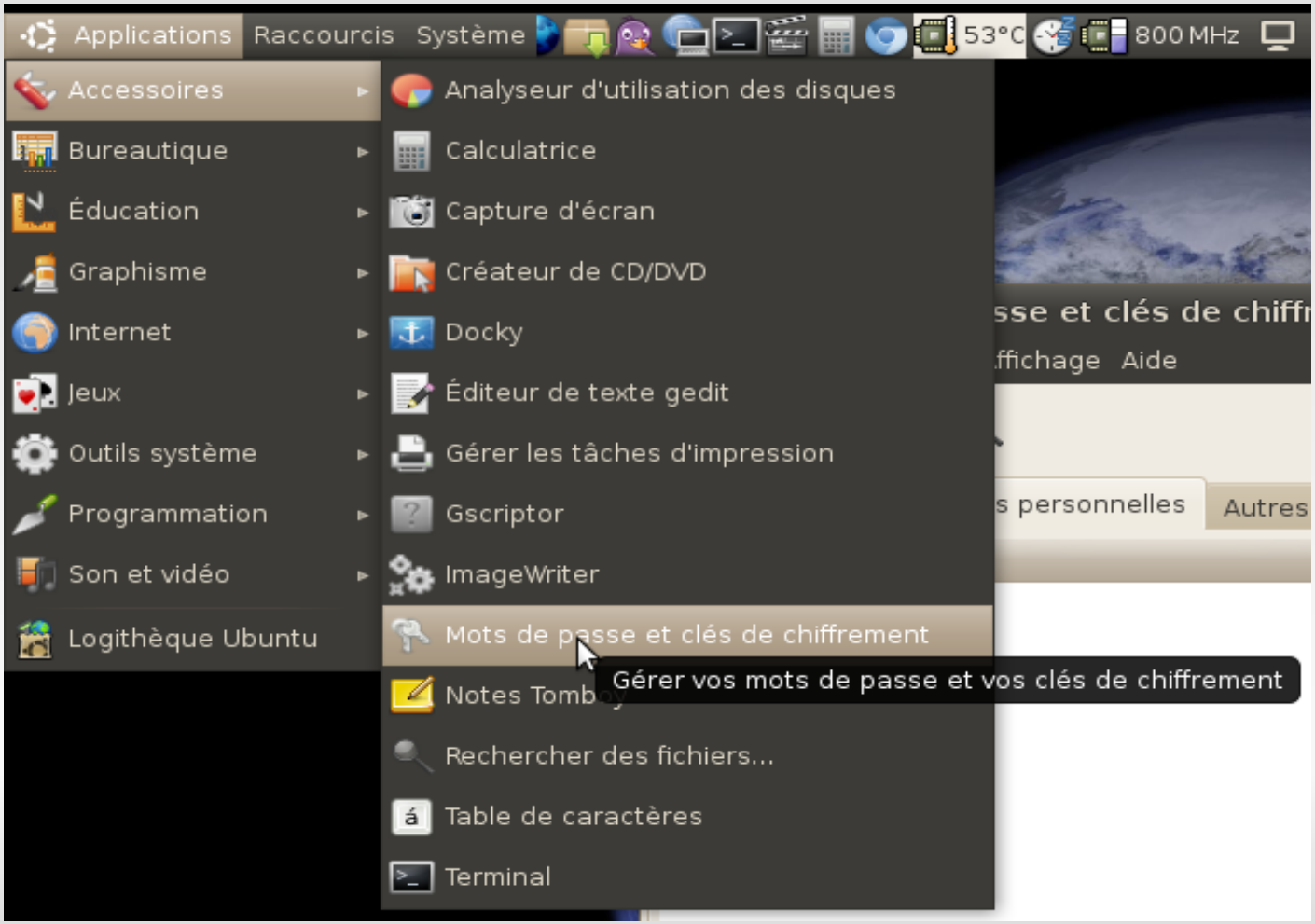
- Après ~1970 : Cryptographie asymmétrique
- ”Paire de clés” : Publique et Privé



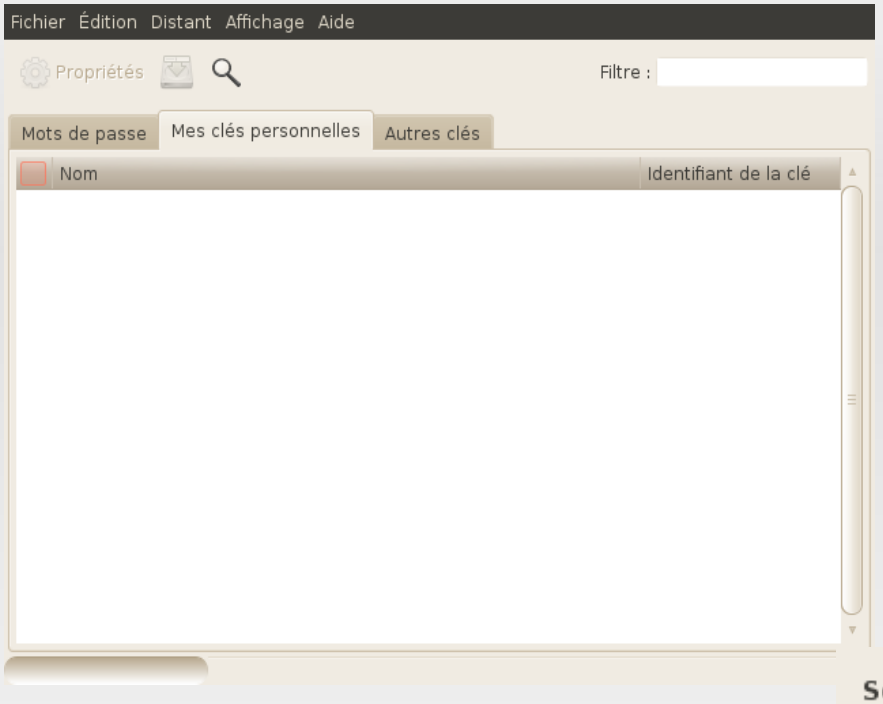



# Créer Une clé avec Ubuntu

- Application Ubuntu préinstallé : SeaHorse
- Nommé : ”Mot de passe et Clés de Chiffement”



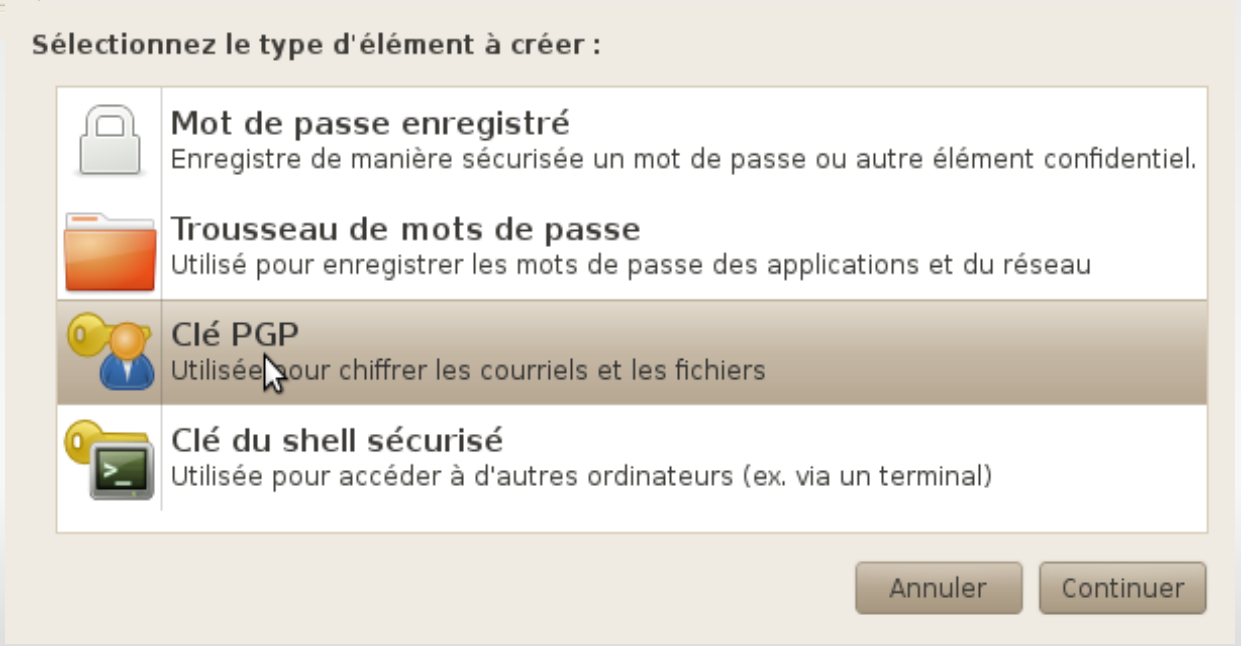
# SeaHorse / Ubuntu




- Onglet ”Mes clés personnelles” : Aucune clé par défaut

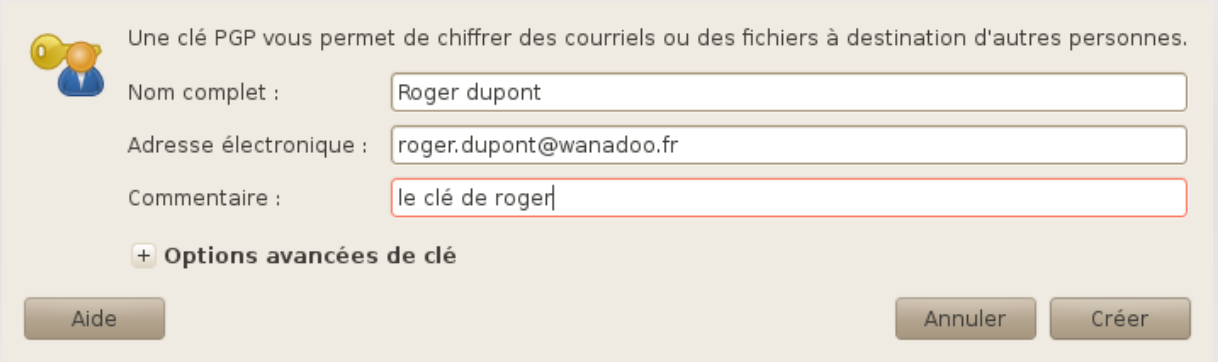
- Menu Fichier

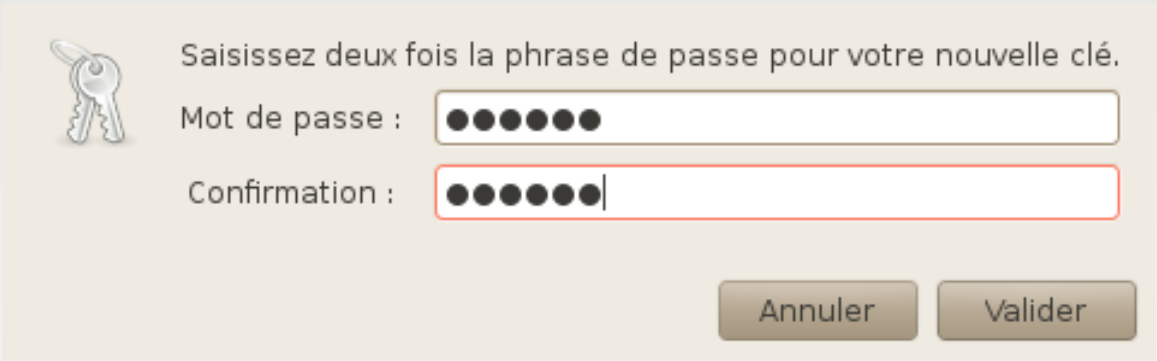
  → Nouveau

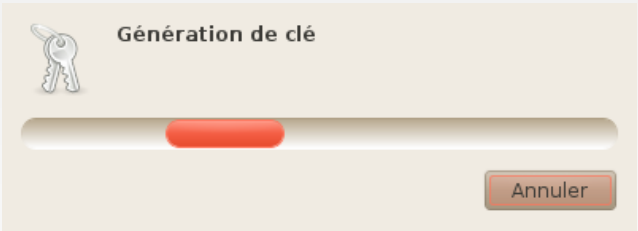


# Ubuntu : création de votre clé GPG

## On associe un email/nom a sa clé



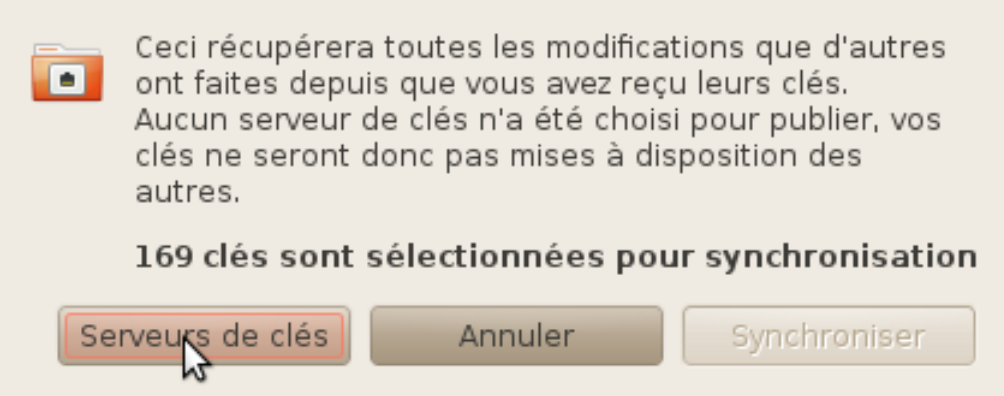



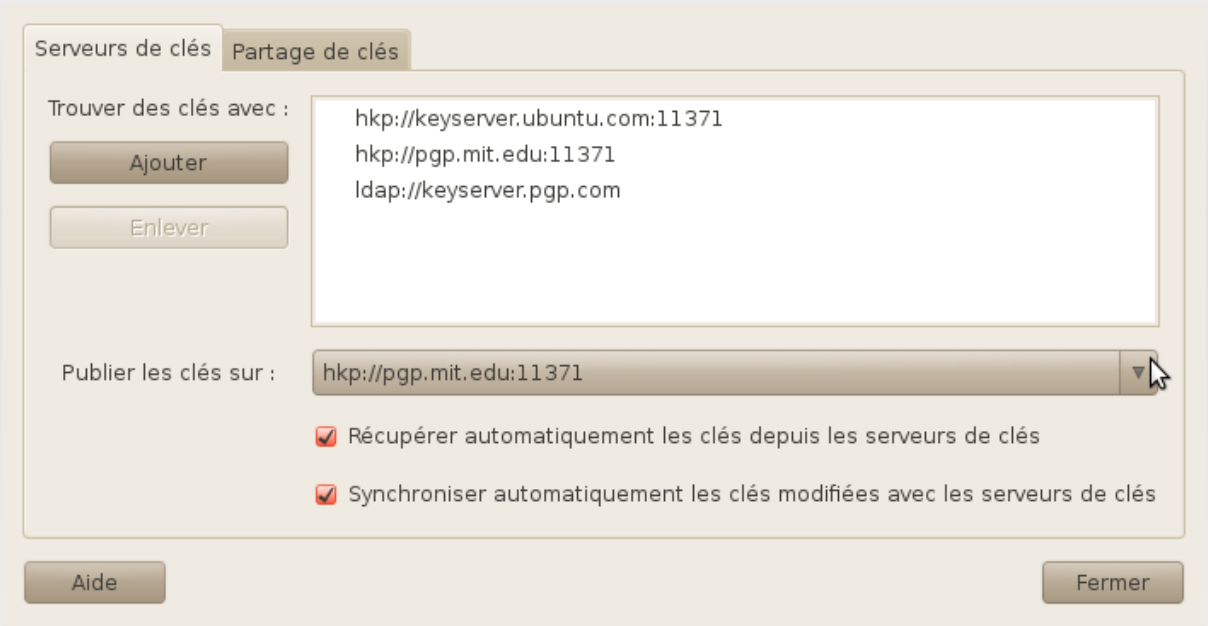

## Et voilà !

# Diffuser sa clé sur internet

- Pour simplifier les choses, les clés publiques sont ”publiées”.
- Menu ”Distant” → Synchroniser et Publier des clés”
- Il faut d'abord cliquer ”Serveur de clés” pour choisir quelques options.....

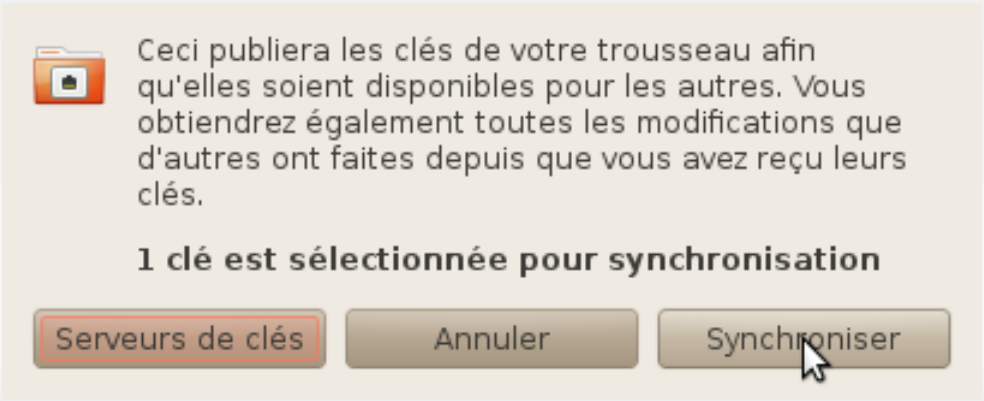


# Options de Publication



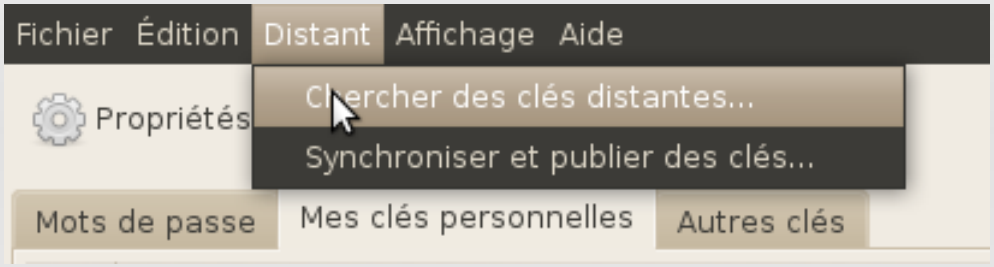

- Pourrait être simplifié ....

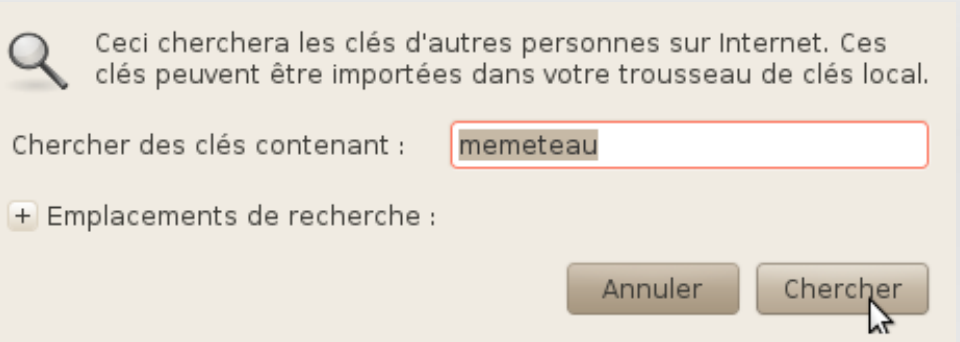
- Le bouton synchroniser est alors actif !

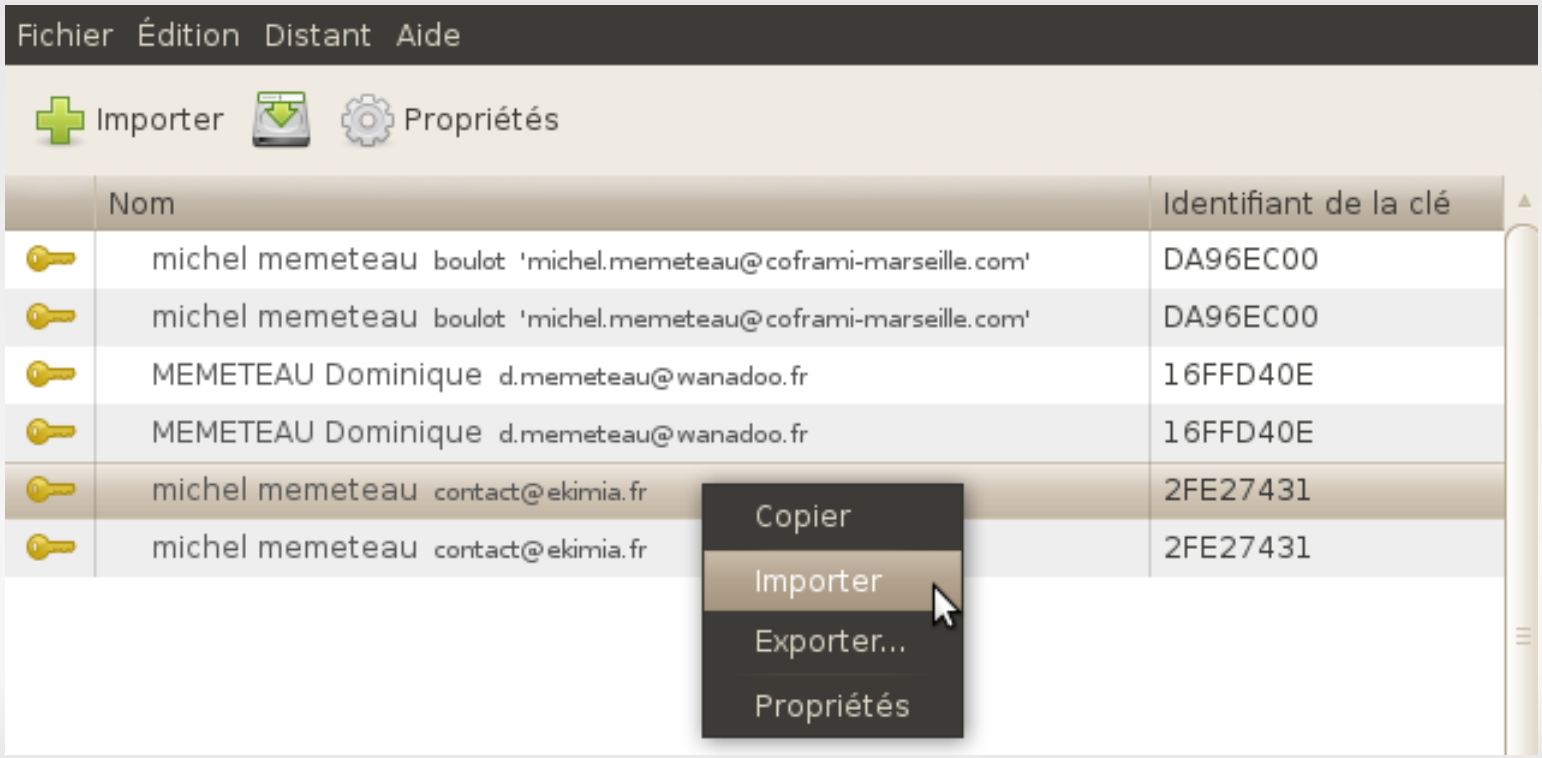


# Chiffrer un fichier 1/3

- Importer les clés de ses amis : email/nom

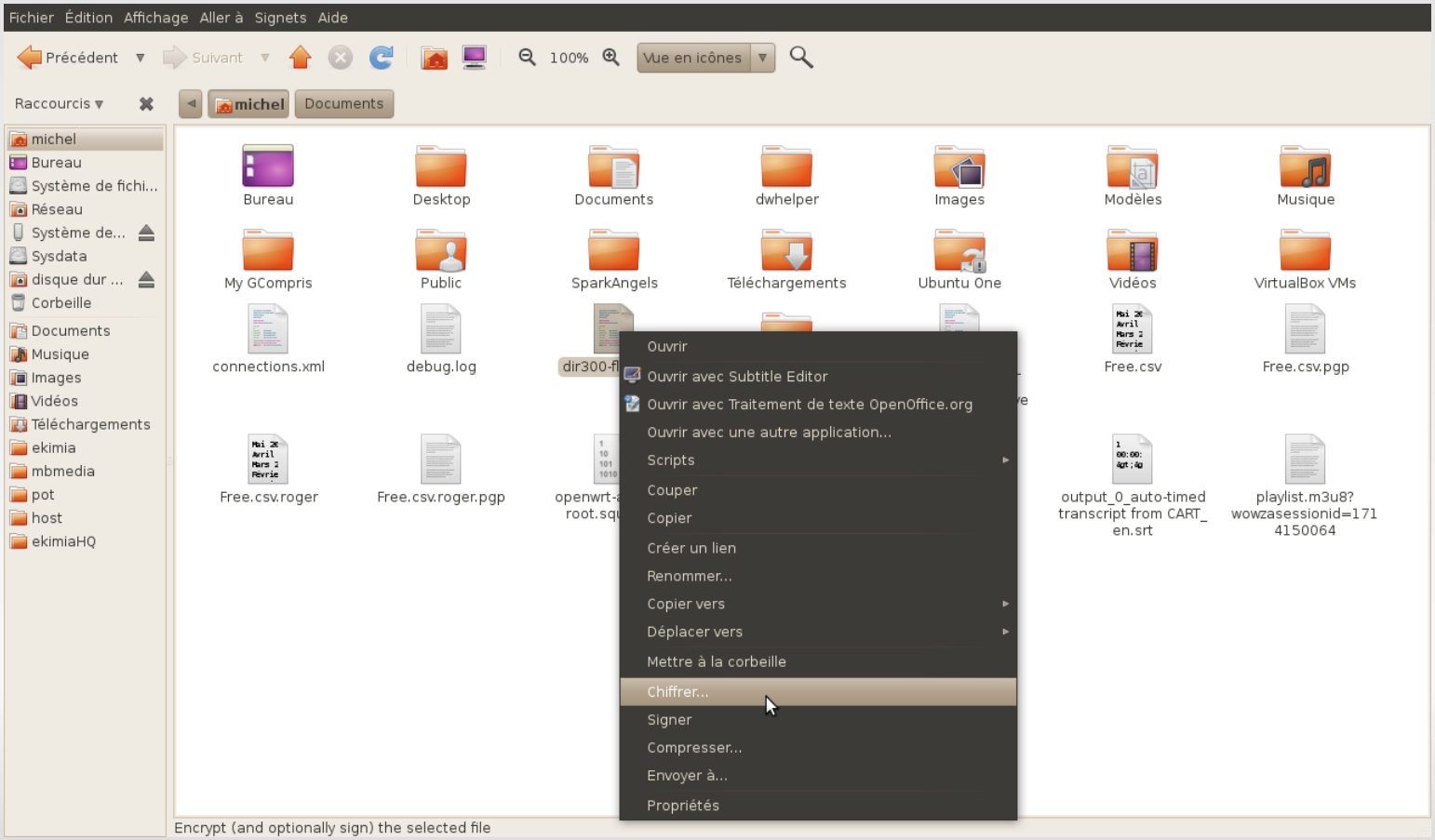


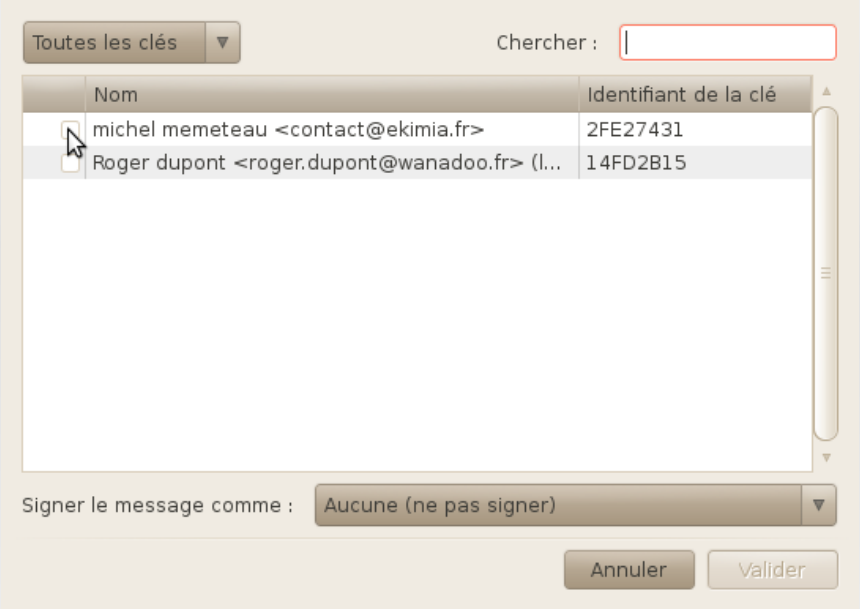
# Chiffrer un Fichier 2/3

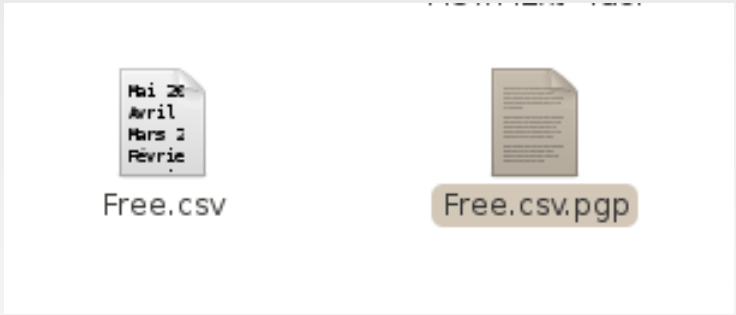
- Installer le logiciel seahorse-plugins
- Fermer/Rouvrir sa session
- Clique droit sur un fichier →Chiffrer



# Chiffrer un Fichier 3/3

- Sélection du destinataire



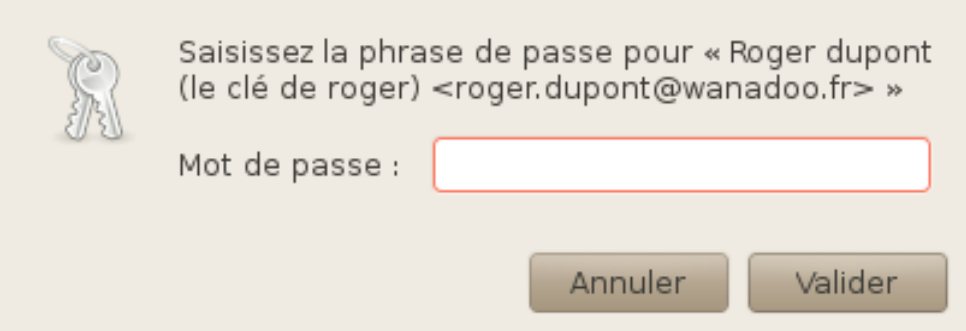




- Nouveau fichier .pgp est crée

- On envoi ce fichier .pgp, seule une personne ayant la clé et le mot de passe pourra le déchiffrer

# Dechiffer un fichier

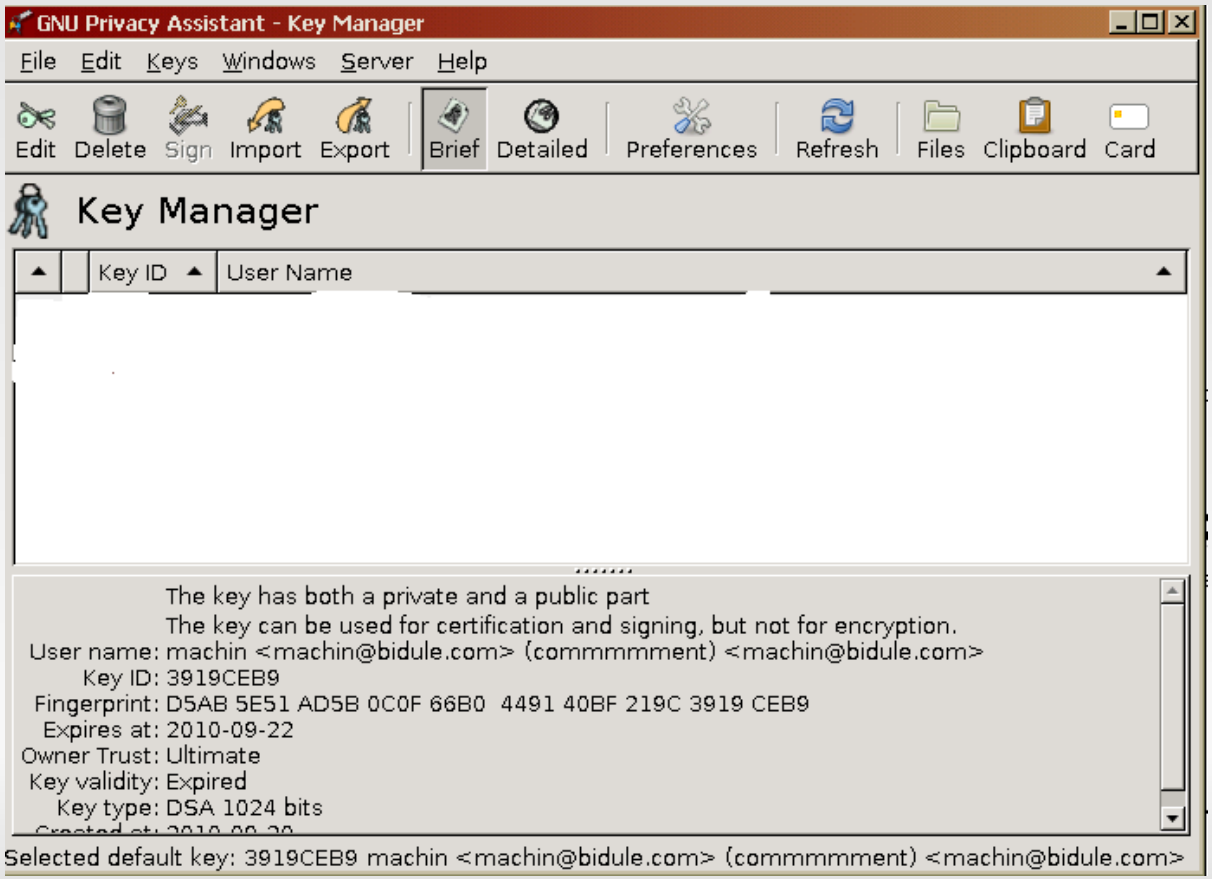
- On reçoit un fichier Free.csv.pgp chiffré
- On DoubleClique pour l'ouvrir
- On tape le mot de passe de la clé




- Le fichier ”en clair” est écrit dans le même repertoire

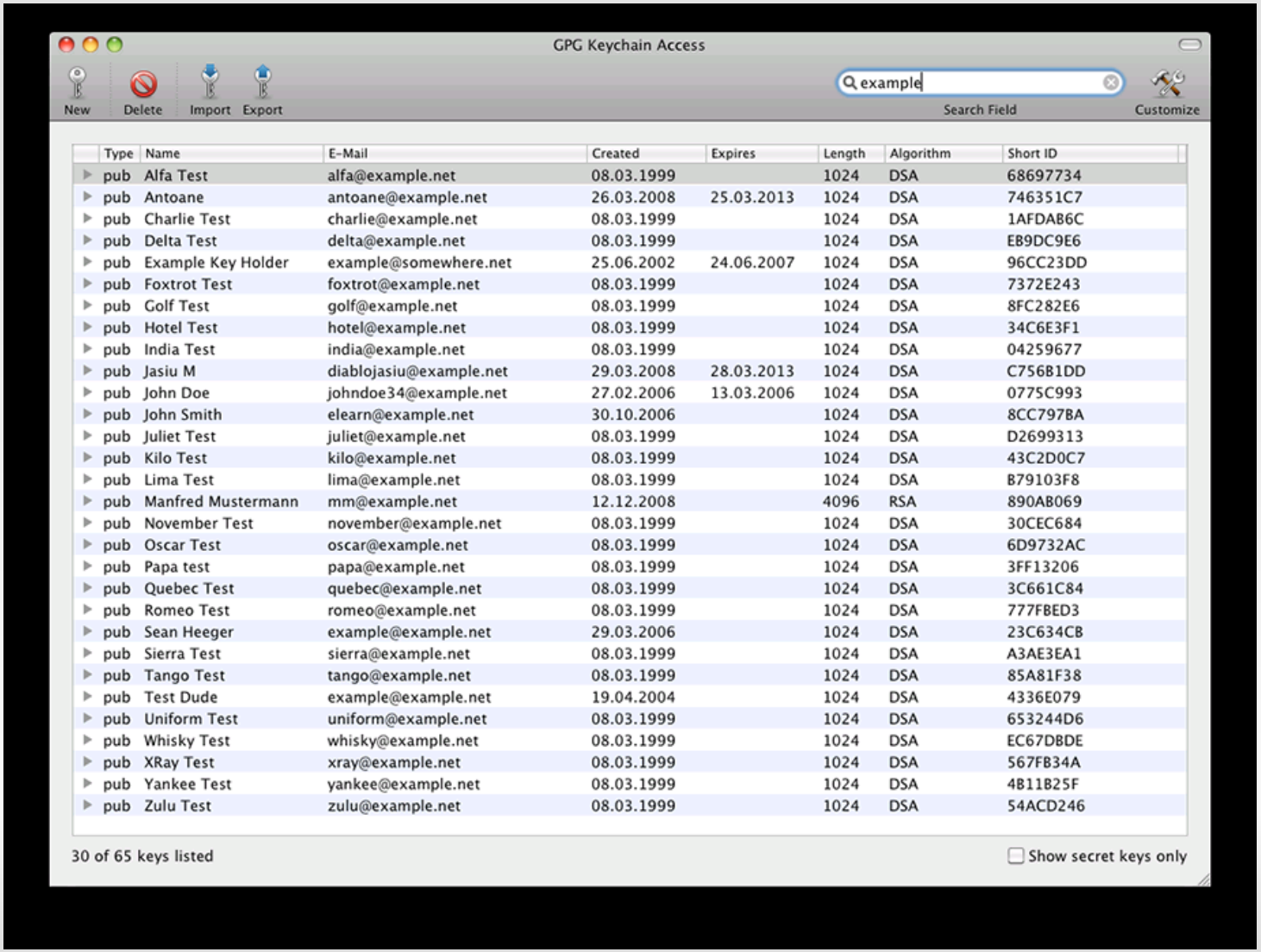
# Sous Microsoft Windows XP

- Rien n'est installé par défaut (on s'en doutait !)
- Outil libre : GPG4win http://www.gpg4win.org



# Sous Mac OSX

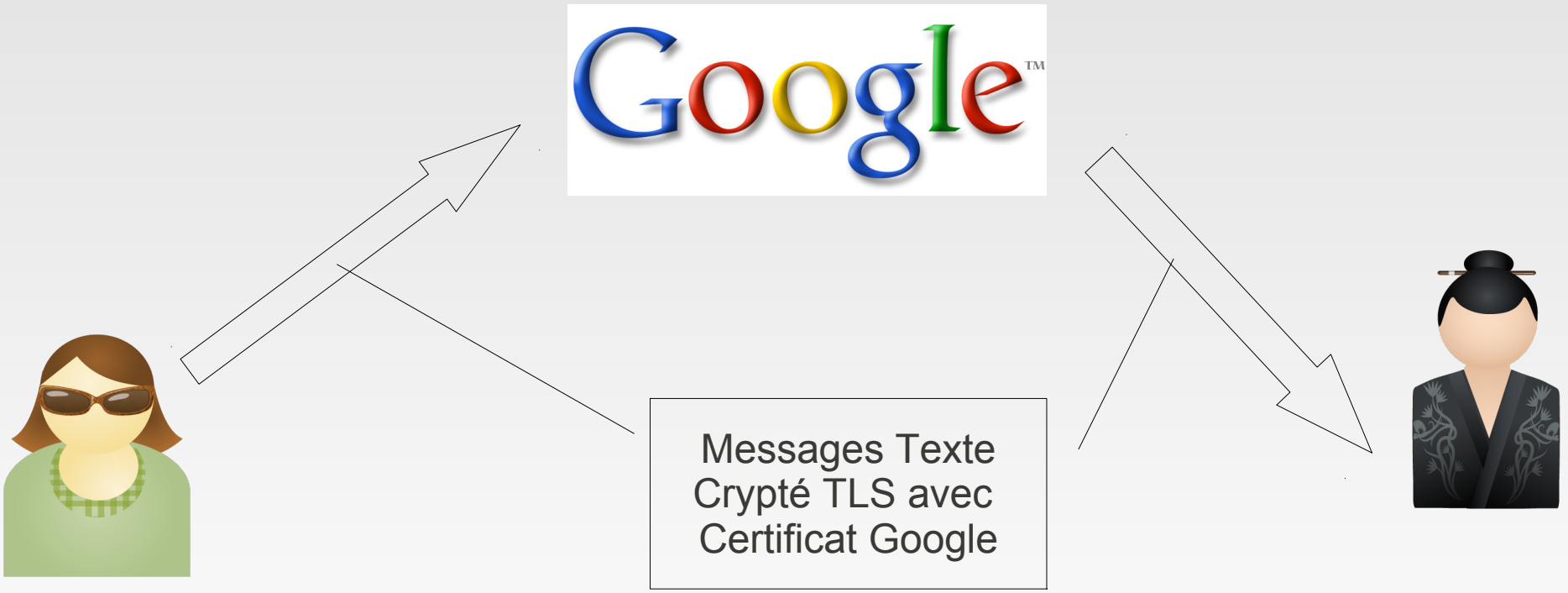
- Outil GPGTools : http://www.gpgtools.org




| Type | Name | E-Mail | Created | Expires | Length | Algorithm | Short ID |
|---|---|---|---|---|---|---|---|
| pub | Alfa Test | alfa@example.net | 08.03.1999 | | 1024 | DSA | 68697734 |
| pub | Antoane | antoane@example.net | 26.03.2008 | 25.03.2013 | 1024 | DSA | 746351C7 |
| pub | Charlie Test | charlie@example.net | 08.03.1999 | | 1024 | DSA | 1AFDAB6C |
| pub | Delta Test | delta@example.net | 08.03.1999 | | 1024 | DSA | EB9DC9E6 |
| pub | Example Key Holder | example@somewhere.net | 25.06.2002 | 24.06.2007 | 1024 | DSA | 96CC23DD |
| pub | Foxtrot Test | foxtrot@example.net | 08.03.1999 | | 1024 | DSA | 7372E243 |
| pub | Golf Test | golf@example.net | 08.03.1999 | | 1024 | DSA | 8FC282E6 |
| pub | Hotel Test | hotel@example.net | 08.03.1999 | | 1024 | DSA | 34C6E3F1 |
| pub | India Test | india@example.net | 08.03.1999 | | 1024 | DSA | 04259677 |
| pub | Jasiu M | diablojasiu@example.net | 29.03.2008 | 28.03.2013 | 1024 | DSA | C756B1DD |
| pub | John Doe | johndoe34@example.net | 27.02.2006 | 13.03.2006 | 1024 | DSA | 0775C993 |
| pub | John Smith | elearn@example.net | 30.10.2006 | | 1024 | DSA | 8CC797BA |
| pub | Juliet Test | juliet@example.net | 08.03.1999 | | 1024 | DSA | D2699313 |
| pub | Kilo Test | kilo@example.net | 08.03.1999 | | 1024 | DSA | 43C2D0C7 |
| pub | Lima Test | lima@example.net | 08.03.1999 | | 1024 | DSA | B79103F8 |
| pub | Manfred Mustermann | mm@example.net | 12.12.2008 | | 4096 | RSA | 890AB069 |
| pub | November Test | november@example.net | 08.03.1999 | | 1024 | DSA | 30CEC684 |
| pub | Oscar Test | oscar@example.net | 08.03.1999 | | 1024 | DSA | 6D9732AC |
| pub | Papa test | papa@example.net | 08.03.1999 | | 1024 | DSA | 3FF13206 |
| pub | Quebec Test | quebec@example.net | 08.03.1999 | | 1024 | DSA | 3C661C84 |
| pub | Romeo Test | romeo@example.net | 08.03.1999 | | 1024 | DSA | 777FBED3 |
| pub | Sean Heeger | example@example.net | 29.03.2006 | | 1024 | DSA | 23C634CB |
| pub | Sierra Test | sierra@example.net | 08.03.1999 | | 1024 | DSA | A3AE3EA1 |
| pub | Tango Test | tango@example.net | 08.03.1999 | | 1024 | DSA | 85A81F38 |
| pub | Test Dude | example@example.net | 19.04.2004 | | 1024 | DSA | 4336E079 |
| pub | Uniform Test | uniform@example.net | 08.03.1999 | | 1024 | DSA | 653244D6 |
| pub | Whisky Test | whisky@example.net | 08.03.1999 | | 1024 | DSA | EC67DBDE |
| pub | XRay Test | xray@example.net | 08.03.1999 | | 1024 | DSA | 567FB34A |
| pub | Yankee Test | yankee@example.net | 08.03.1999 | | 1024 | DSA | 4B11B25F |
| pub | Zulu Test | zulu@example.net | 08.03.1999 | | 1024 | DSA | 54ACD246 |

# Messageries Instantanées

- Envoi de messages textes bidirectionnel en temps réel. Jabber(Gmail), MSN, yahoo, Skype.
- Pratique et rapide : devenues indispensable
- S'annoncent souvent ”sécurisés” (SSL/TLS)



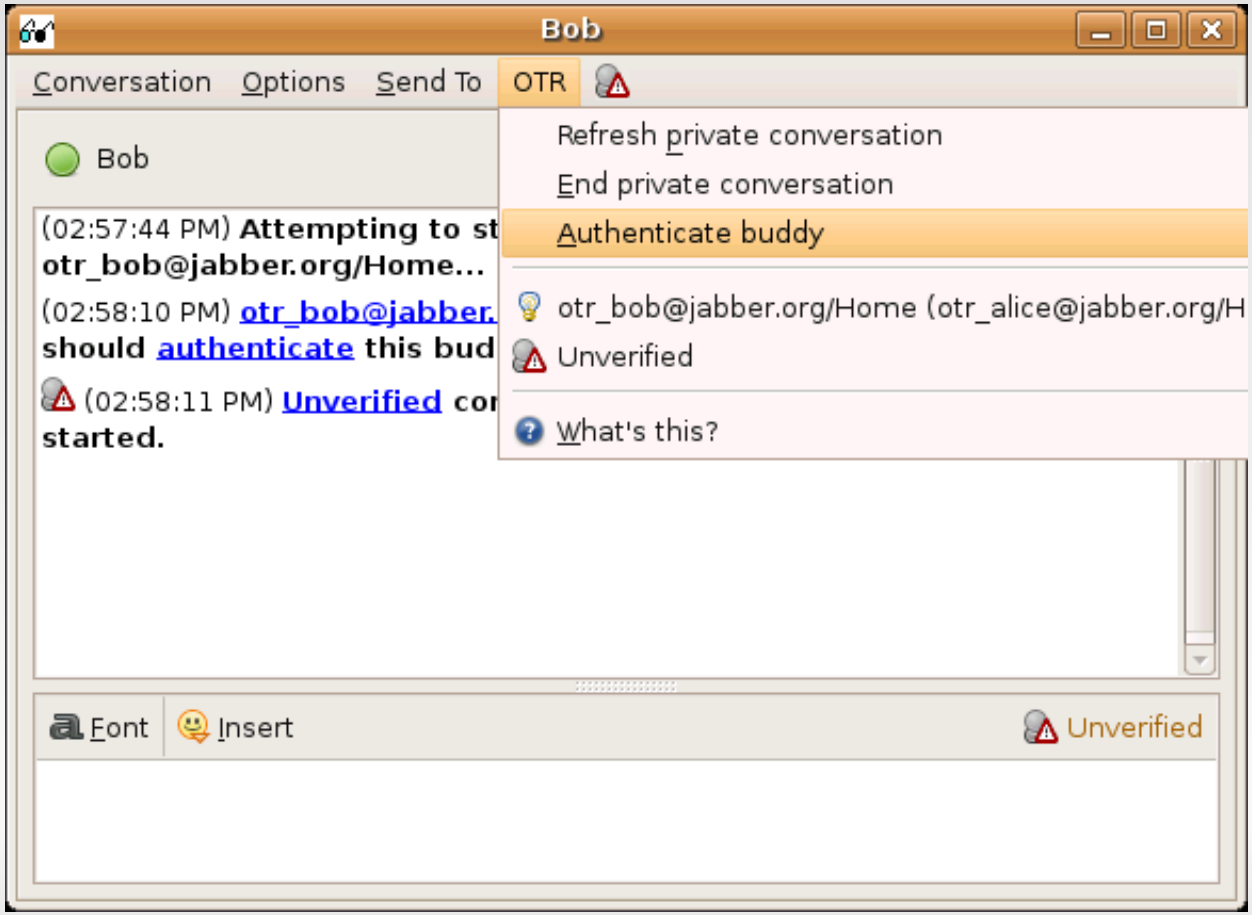

- Fournisseur du service (Google) peut relire en clair les messages.

# OTR : Off the Record

- On utilise le même principe pour crypter chaque message mais en génerant des clés symétriques temporaires : OTR
- Plus adapté qu'une seule clé GPG : les historiques ne sont pas déchiffrables si une clé est compromises (volée).

# OTR

- Pour s'assurer qu'il n'y a pas usurpation, on peut authentifier via une question.



# OTR

- On spécifie la question et la réponse.
- La question va être posée ensuite au correspondant.

# Autres applications

- Email : plugins pour thunderbird/outlook etc...
- Plus ”automatique” :  quand on envoi un mail chiffré à roger.dupont@wanadoo.fr  sa clé publique est automatiquement récupérée.
- Possibilité de stocker la clé privée sur une carte à puce pour plus de sécurité.

# Travaux Pratiques

- Au boulot !