PENSE-BÊTE

UTILISER OPEN PGP AVEC THUNDERBIRD

MISE EN PLACE DU LABO (VirtualBox)

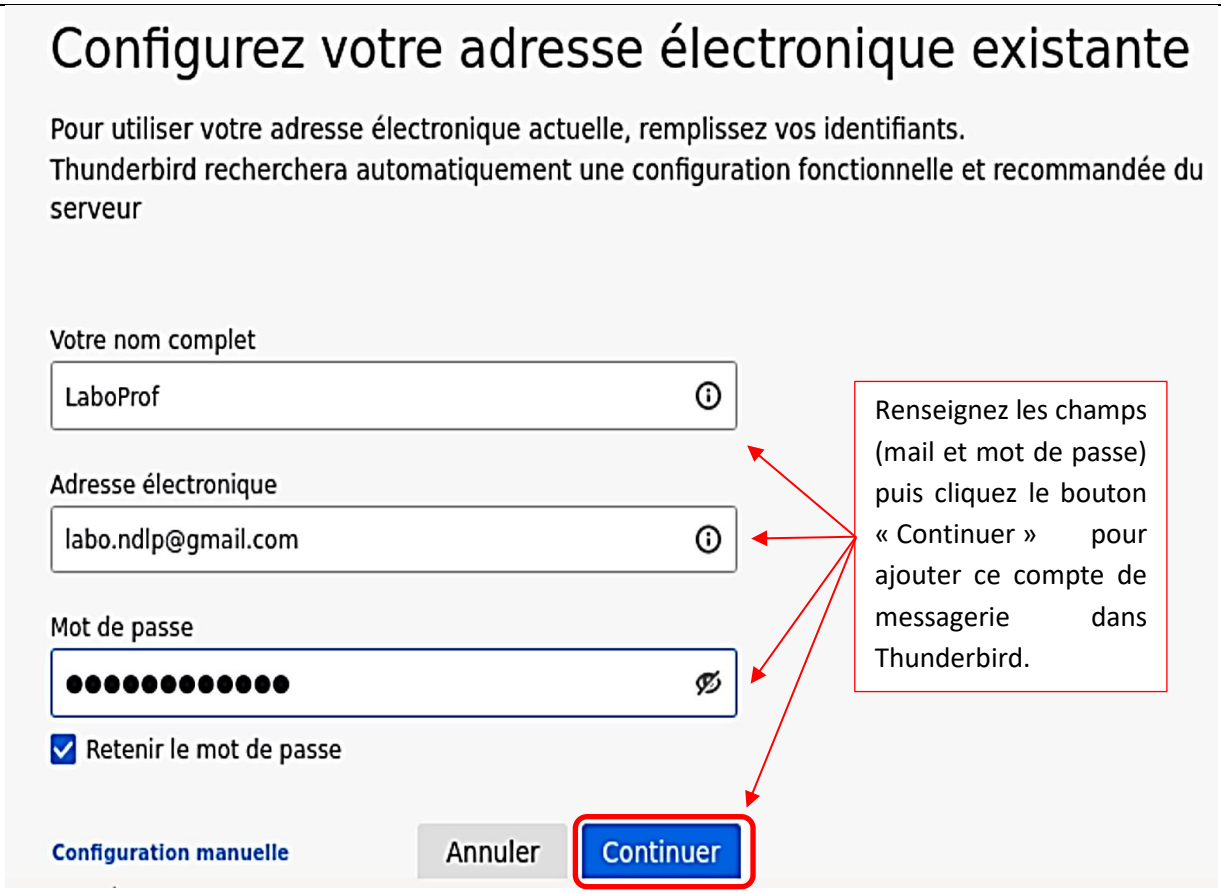
Mozilla a annoncé la **prise en charge native** du standard de chiffrement de courriel OpenPGP dans **Thunderbird** à compter de la **version 78**.

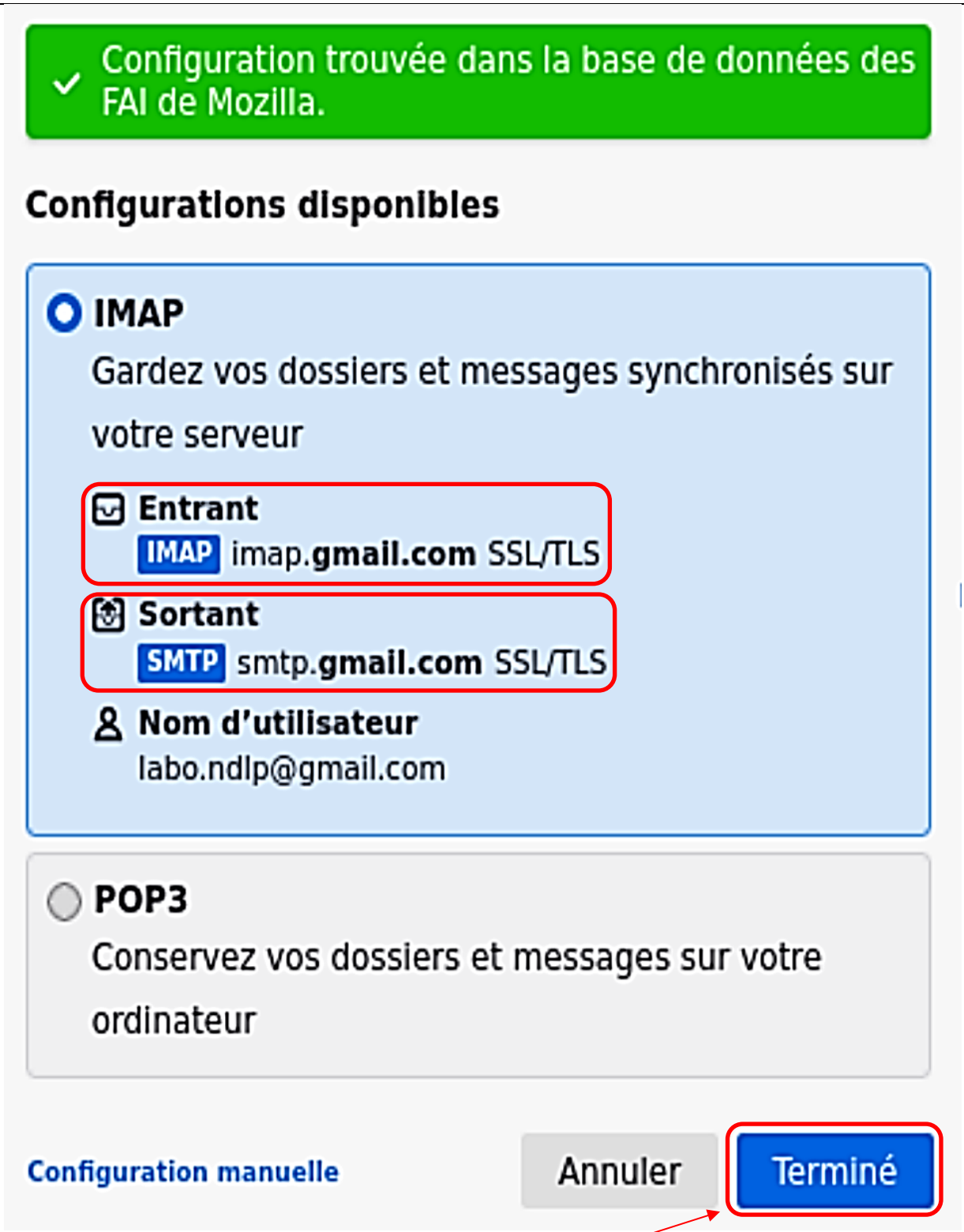
OpenPGP est une norme de chiffrement de courriels (IETF RFC 4880) dérivée de Pretty Good Privacy (PGP), une application logicielle développée au début des années 1990 et conçue pour chiffrer les courriels.

Auparavant, le chiffrement des mails avec Thunderbird (versions antérieures à la 8) se faisait via un module complémentaire appelé « ENIGMAIL ».

CONFIGURATION DE LA MACHINE DE TEST	
MACHINE VIRTUELLE A INSTALLER	**Lubuntu 21.10**
CONFIGURATION MACHINE VIRTUELLE	**RAM = 2 Go (2 000 Mo)** **HDD = 10 Go** **RESEAU = mode « NAT »**

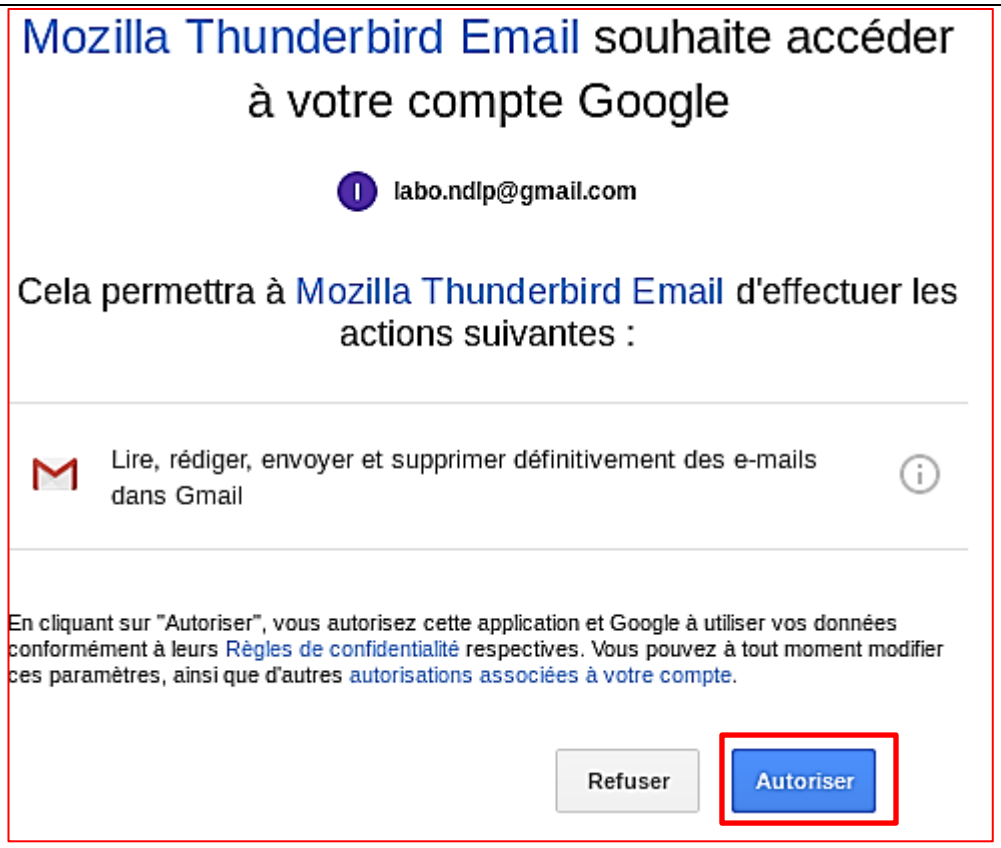
ETAPES DE LA REALISATION	
ETAPES	**COMMENTAIRES**
PARTIE 1 – CREATION MACHINE LUBUNTU/CREATION COMPTE GMAIL/INSTALLATION THUNDERBIRD 91.4	
1	Sous VirtualBox, créez une machine virtuelle « LUBUNTU-LAB ».
2	Créez une adresse GMAIL qui aura la forme suivante : labosio.NOM@gmail.com
3	Depuis une adresse mail que vous possédez déjà, envoyez un mail de test à cette nouvelle adresse GMAIL afin de vérifier le bon fonctionnement. Faites le test en répondant au mail depuis cette nouvelle adresse.
4	Lancez votre machine Lubuntu.
5	Depuis Firefox (installé nativement), téléchargez la **dernière version de Thunderbird** (91.4).
6	Une fois la version téléchargée, décompressez-la en faisant un clic droit sur le fichier compressé.
7	Lancez Thunderbird et faites afficher la barre des menus en faisant un clic droit à côté d'un onglet de navigation et en cochant la case « Menu Bar ».
8	Lors du premier lancement, Thunderbird vous demande de paramétrer un nouveau compte de messagerie ; saisissez les coordonnées du compte Gmail créé pour ce labo :

	
9	Si les paramètres de votre compte Gmail sont corrects, Thunderbird affiche la fenêtre de configuration des serveurs entrants et sortants. Si vos identifiants de messagerie sont corrects, Thunderbird retrouve automatiquement les paramètres des serveurs entrants et sortants de votre hébergeur. Ici, Thunderbird propose de configurer la messagerie à l'aide du protocole « IMAP ». Nous conservons cette configuration qui permet de stocker les mails chez le fournisseur (au contraitre de « POP ») :



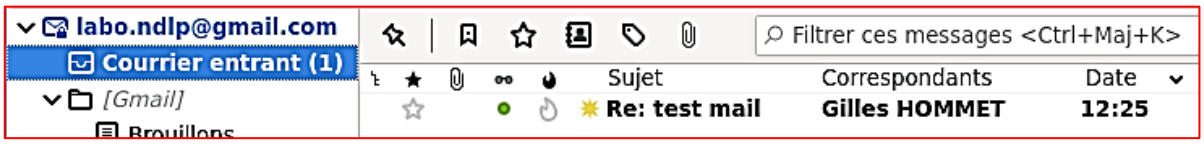
Si ces paramètres vous conviennent, il suffit de cliquer « Terminer » pour valider la création du compte de messagerie sur Thunderbird.

10	Vous devrez valider l'autorisation d'accès au compte GMAIL par Thunderbird :



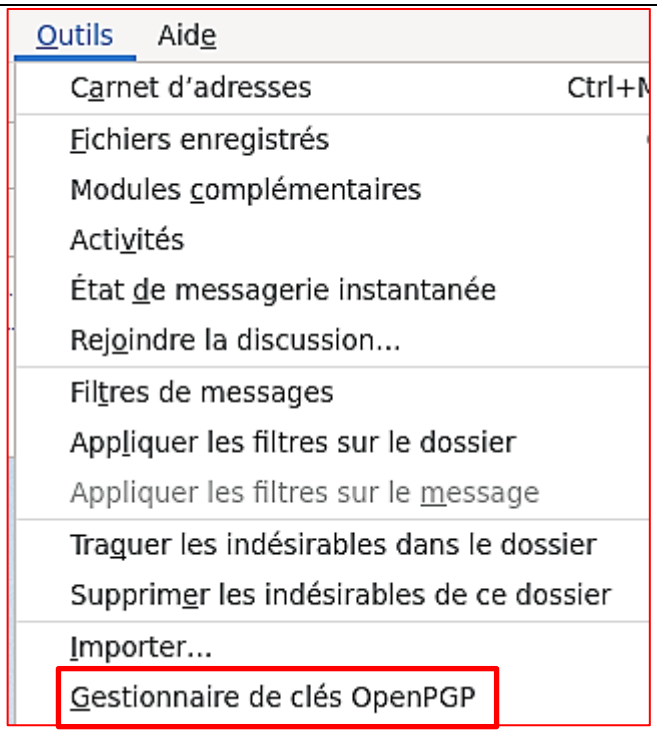
11 Votre compte est prêt et vous devriez obtenir ceci à partir de la page d'accueil :

12 Testez le bon fonctionnement de votre compte de messagerie en envoyant un mail depuis cette nouvelle adresse vers une autre adresse que vous possédez :



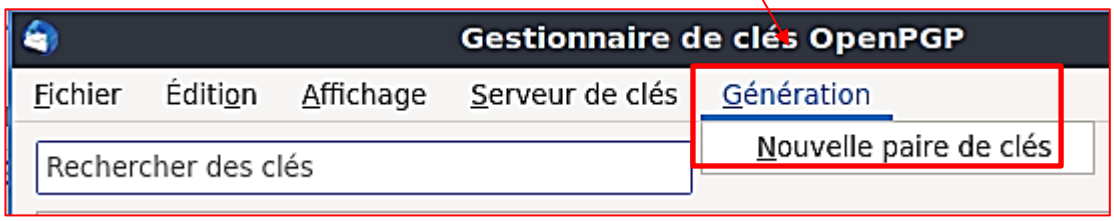
UTILISATION DU MODULE « OPEN PGP » DE THUNDERBIRD

13 Dans un premier temps, il faut créer la paire de clés (privé et publique) à l'aide du gestionnaire Open PGP du client de messagerie.
Cliquez sur « Outils » et « Gestionnaire de clés Open PGP » :

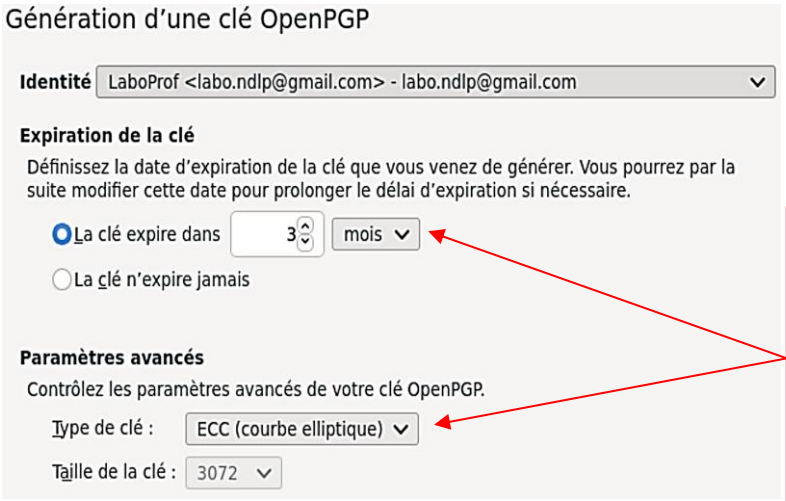


Un assistant Open PGP s'ouvre (gestion Open PGP intégrée par défaut dans Thunderbird depuis la version 78.4). Nous allons maintenant générer la paire de clés (publique et privé) nécessaire à l'utilisation du chiffrement des mails dans Thunderbird.

14 Générer la paire de clés en cliquant « Génération » et « Nouvelle paire de clés » :

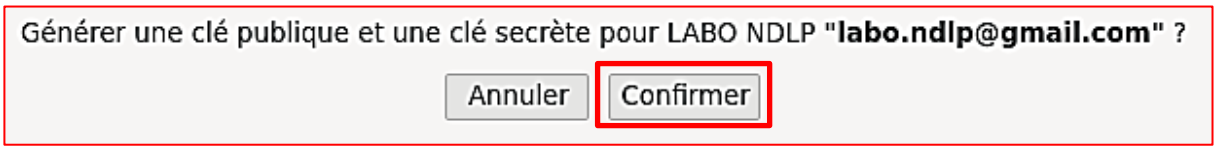
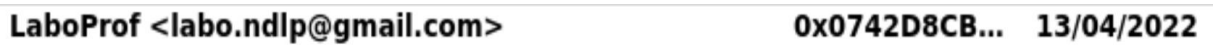
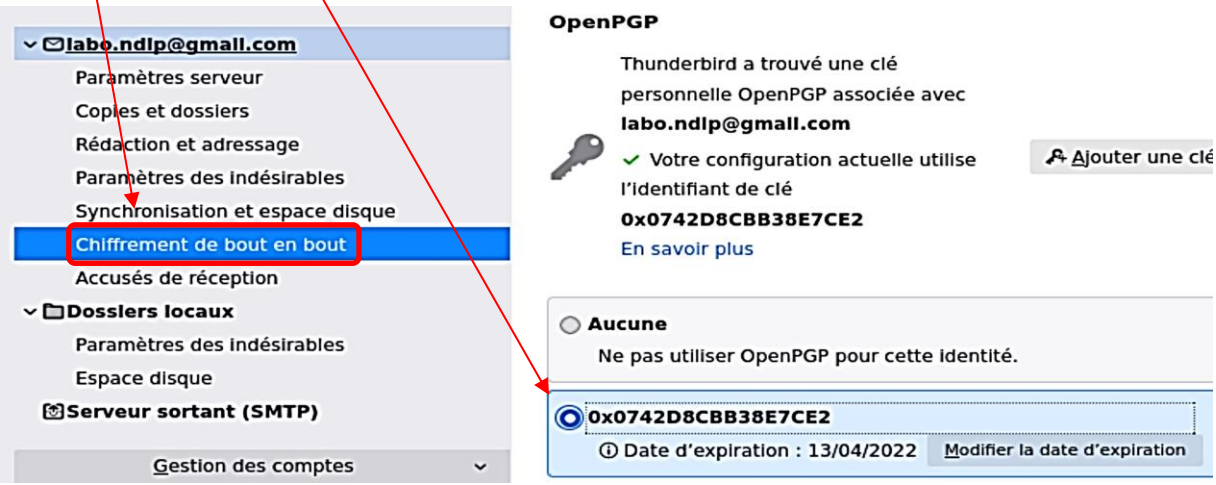
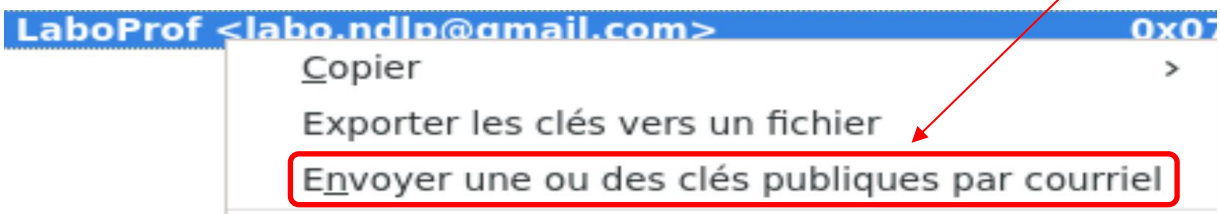
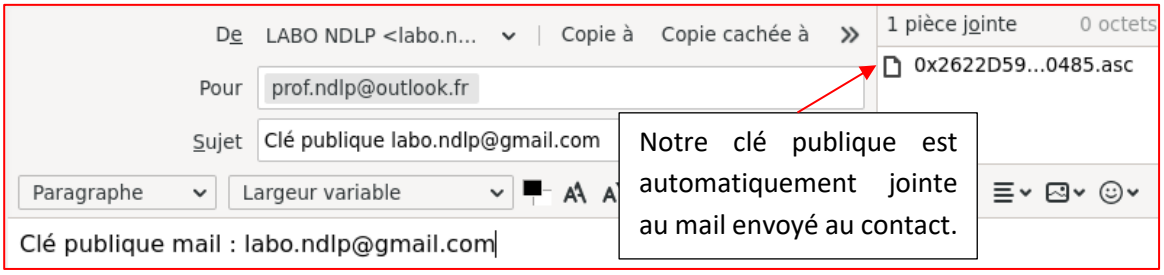


15 Compléter la fenêtre de génération des clés et cliquer sur « Générer la clé » :

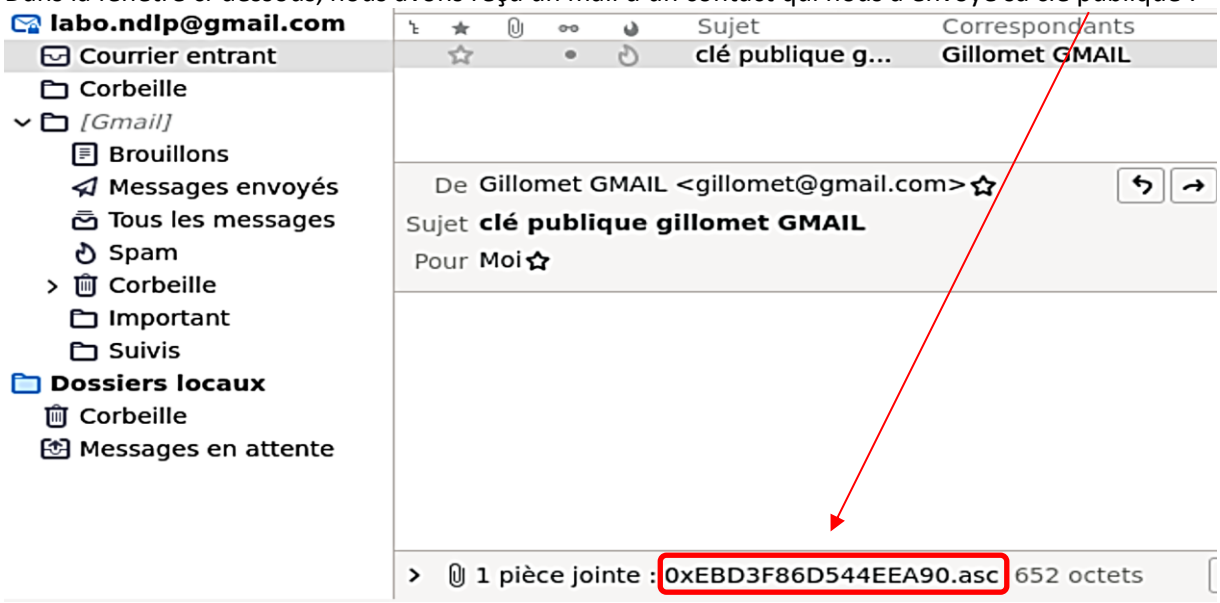


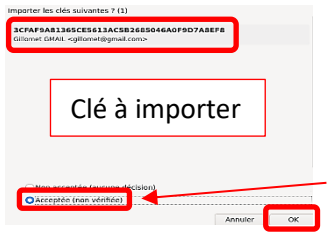
Ici, nous limitons la durée de validité de la clé à 3 mois et nous choisissons une méthode de chiffrement basée sur les « courbes elliptiques » qui offre une plus forte sécurité de nos jours.

Ici, nous avons indiqué un délai

16	Cliquez sur « Générer la clé » et « Confirmer » pour générer la paire de clés et ne pas hésiter à utiliser votre machine pendant l'opération afin de multiplier les calculs aléatoires et, ainsi, générer un crypage fort au niveau de vos clés publiques et privées :  A la fin du processus, la paire de clés est générée : 
17	Activez, dans Thunderbird, le mode « chiffrement de bout en bout ». Pour cela, faites un clic droit sur votre compte de messagerie et cliquez « Paramètres ». Sélectionnez ensuite la rubrique « Chiffrement de bout en bout » et validez le chiffrement pour la clé précédemment générée : 
18	Afin de pouvoir envoyer des mails avec OpenPGP, **il faut que le destinataire de votre mail possède votre clé publique**. Ouvrez le gestionnaire de clés OpenPGP et faites un clic droit sur votre clé. Cliquez sur « Envoyer une ou des clés publiques par courriel » :  La clé est automatiquement ajoutée en pièce jointe dans un nouveau mail : il vous suffit d'envoyer le mail à vos contacts pour leur transmettre cette clé. 

	Attention, il faudra demander à votre contact de vous envoyer sa clé publique si vous voulez échanger des mails avec OpenPGP.
19	Dans la fenêtre ci-dessous, nous avons reçu un mail d'un contact qui nous a envoyé sa clé publique :



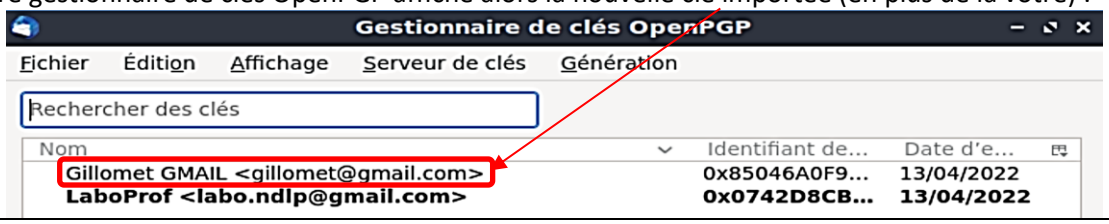


Il faut importer cette clé publique reçue dans notre gestionnaire de clés OpenPGP. Enregistrez la pièce jointe contenant la clé publique dans un emplacement de votre disque dur. Ouvrez le gestionnaire de clés de Thunderbird et cliquez « Fichier » - « Importer ».

Acceptez l'importation de cette nouvelle clé publique en cliquant l'option « Acceptée (non vérifiée) et cliquez le bouton « OK ».

Une fenêtre affiche alors les détails de la clé importée, cliquez « OK » :

Votre gestionnaire de clés OpenPGP affiche alors la nouvelle clé importée (en plus de la vôtre) :



Double-cliquez la clé reçue et cliquez l'option « Oui, j'ai vérifié en personne que l'empreinte de cette clé est correcte » :

TESTS D'ENVOI DE MAILS NON CHIFFRES ET CHIFFRES AVEC OPEN PGP

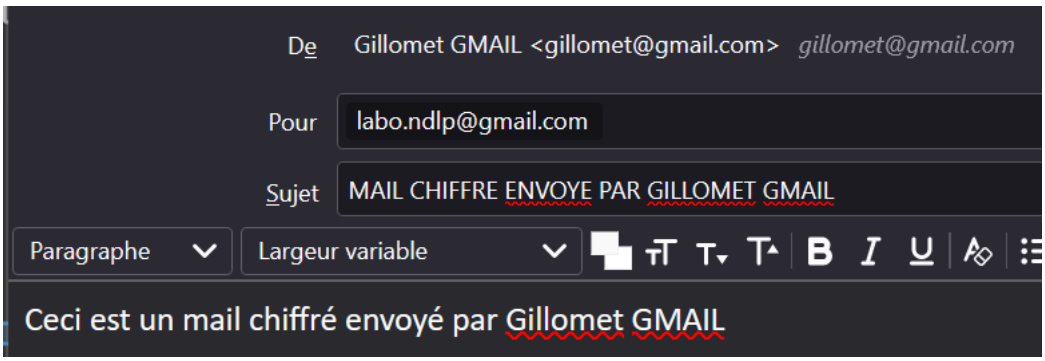
20 Envoyez un mail à l'un de vos contacts **SANS LE CHIFFRER** et en saisissant un texte simple comme, par exemple, « mail non chiffré ».

Si nous faisons afficher la source du mail, en cliquant sur « Affichage » - « Code source du message », nous constatons que le texte du mail envoyé est bien affiché en clair (voir en bas du code source) :

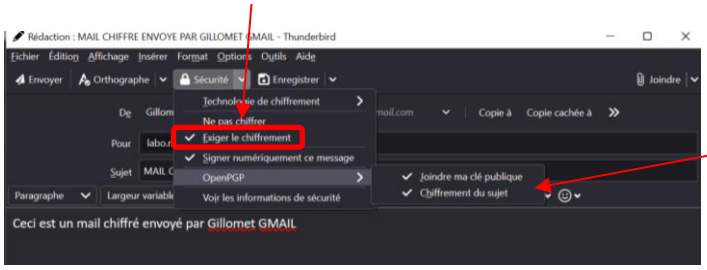
```
To: gillomet@gmail.com
From: LaboProf <labo.ndlp@gmail.com>
Subject: MAIL NON CHIFFRE
Content-Type: text/plain; charset=UTF-8; format=flowed
Content-Transfer-Encoding: 8bit

Ceci est un mail non chiffrÃ©
```

21 Envoyez un autre mail mais, cette fois, **en le chiffrant** avec Open PGP. Rédigez le message en saisissant par exemple « Ceci est un mail chiffré » dans le corps du message, comme ci-dessous :

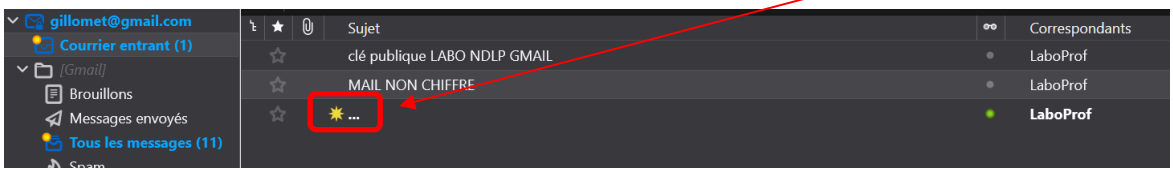


Pour chiffrer le mail avec OpenPGP, cliquez le bouton « Sécurité »  et cliquez l'option « Exiger le chiffrement ».

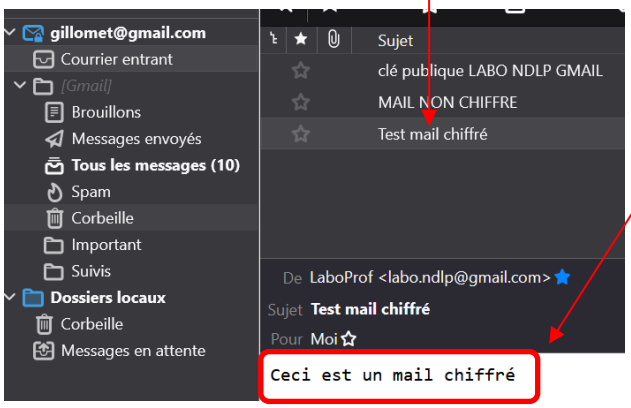


Lorsque l'on sélectionne l'option « OpenPGP », on peut joindre à nouveau notre clé publique si cela n'a pas été fait au préalable sinon le destinataire ne pourra pas déchiffrer le mail. Il est possible aussi de chiffrer le sujet du mail (l'objet).

Le destinataire reçoit le mail. On note ici que le sujet (l'objet) est bien masqué :



Si le destinataire clique sur le sujet du mail, il verra le mail en clair car il a déjà importé la clé publique de l'expéditeur :



Le destinataire ayant déjà importé la clé publique de l'expéditeur peut lire le contenu du mail.

En affichant le code source du message, on constate bien que le corps du message (texte) n'est absolument pas lisible :

```
This is an OpenPGP/MIME encrypted message (RFC 4880 and 3156)
--------------C4TIclJp5GRA9ojhlv3GcnS9
Content-Type: application/pgp-encrypted
Content-Description: PGP/MIME version identification

Version: 1

--------------C4TIclJp5GRA9ojhlv3GcnS9
Content-Type: application/octet-stream; name="encrypted.asc"
Content-Description: OpenPGP encrypted message
Content-Disposition: inline; filename="encrypted.asc"

-----BEGIN PGP MESSAGE-----

wV4DbjCjq8SJqjoSAQdAco9sjaf8H/jst6dhhLLZuBZ6QQhj6VjA+0tuU9sqLh8w2XjRPg9DW9u4
AYXilU4su4/d+kgnTsp8fraVFSDCLM1qTejpo7dz5szv/YUF/ScPwV4DKC3tB8qSRy4SAQdAXBV6
1nlEAyD0DgQD5VamfwN/dik52OuKkqCRiypWkyAw1EgQzqts6yTS9uVMBKf+281O30FcV/8TwA+Y
m+Q8XjEzfTjp9sXRb+iIC0wNcDhN0sRXAb2k6BuUVQKhMZJPiN/GpRX0HaMbr8fpctfHF
vd2MF4uZ85RvpAhADR33cjKcOOzl8sY/20Xoas1nD3mOBKXijVGA57TdzqFUUx4Pmf8pH
tTPbRo4t6Ccu9AYJjakEfjQvUr9DByYLzPgO1DxuQl/K3Gap/GMR/38HcrS0ddmcUBQp4
mydDzf1LcXbTzkscs7jwz6ds38HHX+HOq1ud76tckp8Y0EI51WTQFt/L3CZ0vTQDgeMvY
DV+cNYmInr0JKuS5tNLSkV2ib7MFkfKdS+/mmnxKaVxruANnTiEVTqqHE5hVB34FRexOS
ECwauF5Vl259c2L5mHv/P6KXAix4+XQwYwjDtpX8gNlexBcYNfcEADEKh4Bl2Gtok8PDc
SInKhXKk2bIoL2++dP0H2KeqYlJz/vHOY4tli0lbNy6YPI3JST8t4FMtrWmShXDHAiVgM
Vgv2bQdUDCTsUMAZvUuWxwsOH2gZi9yyMhicz9WfmFnbCfEY9P8b5Qbg3c+tQUoPwp92I
k+5P9nu5r7JoIF/Xn5dXjwE/di1sRuXUBHAG9bOIJib3qyyDwf/BhM64k1lK3iCNRnUIY
K376AzPC9ZiepHWflNtk9+Ukvg+DCDHvLj2JiNf+Va7rJ4wq5AC/tkv13KU+kZ+nvnUp4
DU67FnY5Jen/eAwv+c7w7UkeLCM86gYf+TdircR0qNV8lQm0ZeEla9EWi2fmqZY/7u5Rb
AaHg5VMCvMQbJ7gRz/SN4xQ+317ntRJVkXBEdKbLSZ1xOt+Ikoi57Kh+2KdQ0JZV2P4i6
rEno6Z48Lbm44NDS8rECqfsmX/2kF8/zT1v6w2nsUBhaRYid/a3k3xpYw6EZ5tU2QXD2IHxfF5qD
8DB/eBfQsTi3zrYzdxT3rPgXjukv7ALwIae2Xv2NwoiG2S2tnVVU9IGMXGH0JoftASR31h8qXJth
YxB7sdhWDKKGCNNsr+iFs5jJYOwMPBDG2LSIqXlUTHsWbKqXTO0oIZA3RYXglAKAGnLQ4EHT5gA5
nD5rAYCwLwxH5PyaeJCqdfrF2mbg8wEbs/dwGakEqyptU6ZeiZ/sy+vY5GqwzQgUGINzb0rAIzkV
C9NMjrThmxMtkiq9svc6bnU8A2NGkacwJb/eoohZv+xv8bdI0Nj7tL/RsTFi27T1uCfoBDPwXbOr
z+o3i+h8jPE+Ll9cGWcsicEYdI/hi8Vlxqe MZxXPpab/RH51Z1nh6gPHBqCV3D3BNUb6qKYXnXc/
onJO3qDpb2iVteC4i2rQK+Xmkrs3x/HEhdxSXwXHTDgopcrnnIjWWlQeEWF7W2QJn37e06N/PyxM
YDM+AoAvdeQOrKqbtzSpgAdscy3icP/W2a3mVUCLCcsvqfcVDjw8i/ddFf+OCe6oipwxBsDhhLjp
QQM4czHJdsH+mIsnoceZ4gM+ucS0dxzYXx5PmNqujbx/UJFWjYOgEpGqqfK6iovC2mQNKd74yH+f
9pTlLKSSWHbt4EcctB/5xy7xTgh6T/cVQVjlMpj2rC9fULpA5UjjWMUJfo2QCTR+B1dHS+enIWiH
F/dhqMSvs78r5vsasRAZM417aQ/oqRkyKLwGZjx2kp6FLgaN5dGiLlahg8IAsGZqBLPSmp6Jc518
wPJ0eA5qFjwMwogIHSE+4Q==
=Zj7/
-----END PGP MESSAGE-----
```

Ici, on constate bien que le corps du mail a été chiffré puisqu'il est totalement impossible de voir son contenu (chiffrage). Ces codes correspondent au texte «Ceci est un mail chiffré »…

Nous ne présenterons pas dans ce guide la notion de serveurs de clés publics. Ces serveurs ont souvent fait l'objet d'attaques (hacking) ce qui les rend vulnérables (voir attaque des serveurs SKS).

FICHE MEMO 2

LE CHIFFREMENT PAR CLE ASYMETRIQUE

La cryptographie asymétrique, ou cryptographie à clé publique, est une méthode de chiffrement qui repose sur l'utilisation de fonctions à sens unique : il est simple d'appliquer cette fonction à un message, mais extrêmement difficile de retrouver ce message à partir du moment où on l'a transformé.

Pour inverser la fonction, il faut disposer d'une information tenue secrète, appelée clé privée. Pour mettre en oeuvre cette technique de cryptographie, il faut donc posséder deux clés, l'une publique, qui est connue de tous, et l'autre privée.

Alice désire sécuriser ses communications à l'aide de la cryptographie asymétrique. Elle a donc besoin d'une paire de clé, qu'elle va générer à l'aide d'un logiciel de cryptographie (PGP par exemple). Ce logiciel génère un grand nombre aléatoire, qui servira de paramètre d'entrée à la fonction de génération de clés. Cette fonction varie selon l'algorithme cryptographique utilisé. Alice peut alors distribuer sa clé publique à ses correspondants, sous forme de fichier ou sous forme de chaine de caractère (au sein d'un e-mail par exemple).

Il faut donc que l'émetteur du message encrypte celui-ci avec la clé publique du destinataire, qui décodera le message avec sa clé privée. Ainsi, l'émetteur est sûr que seul le destinataire voulu pourra prendre connaissance du contenu du message.

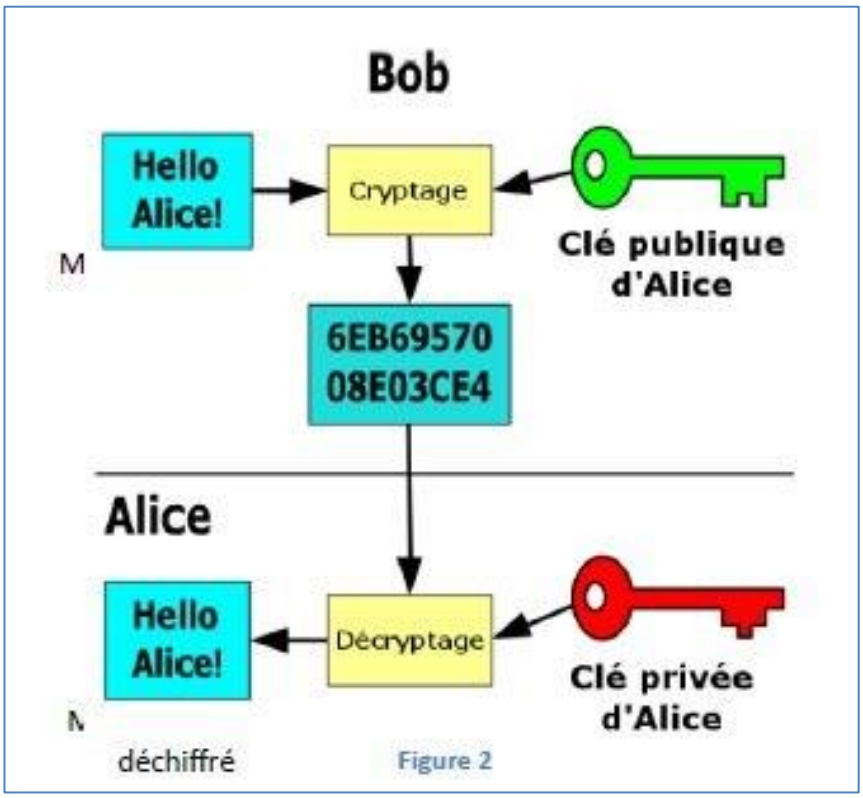


Figure 2

1

BOB crypte son mail à l'aide de la clé publique d'Alice (clé qui lui avait envoyée précédemment ou importée depuis un serveur de clés).

2

ALICE pourra décrypter le message envoyé par BOB car le message a été crypté avec se clé publique. Le logiciel d'ALICE se servira de sa clé privée.

Une clé est une valeur utilisée dans un algorithme de cryptographie, afin de générer un texte chiffré. Les clés sont en réalité des nombres extrêmement importants. La taille d'une clé se mesure en bits et le nombre correspondant à une clé de 1 024 bits est gigantesque. Dans la cryptographie de clé publique, plus la clé est grande, plus la sécurité du texte chiffré est élevée.