

## 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](https://tools.ietf.org/html/rfc4880)) 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	<b>Lubuntu 21.10</b>
CONFIGURATION MACHINE VIRTUELLE	<b>RAM = 2 Go (2 000 Mo)</b> <b>HDD = 10 Go</b> <b>RESEAU = mode « NAT »</b>

### ETAPES DE LA REALISATION

ETAPES	COMMENTAIRES
<b>PARTIE 1 – CREATION MACHINE LUBUNTU/CREATION COMPTE GMAIL/INSTALLATION THUNDERBIRD 91.4</b>	
1	Sous VirtualBox, créez une machine virtuelle « LUBUNTU-LAB ».
2	Créez une adresse GMAIL qui aura la forme suivante : <a href="mailto:labosio.NOM@gmail.com">labosio.NOM@gmail.com</a>
3	<u>Depuis une adresse mail que vous possédez déjà</u> , 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 <b>dernière version de Thunderbird</b> (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 :

## Configurez votre adresse électronique existante

Pour utiliser votre adresse électronique actuelle, remplissez vos identifiants.  
Thunderbird recherchera automatiquement une configuration fonctionnelle et recommandée du serveur

Votre nom complet

LaboProf ⓘ

Adresse électronique

labo.ndlp@gmail.com ⓘ

Mot de passe

●●●●●●●●●● ⓘ

Retenir le mot de passe

[Configuration manuelle](#)

Annuler

Continuer

Renseignez les champs (mail et mot de passe) puis cliquez le bouton « Continuer » pour ajouter ce compte de messagerie dans Thunderbird.

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 contraire de « POP ») :

✓ Configuration trouvée dans la base de données des FAI de Mozilla.

## Configurations disponibles

### IMAP

Gardez vos dossiers et messages synchronisés sur votre serveur

Entrant

**IMAP** imap.gmail.com SSL/TLS

Sortant

**SMTP** smtp.gmail.com SSL/TLS

 **Nom d'utilisateur**  
labo.ndlp@gmail.com

### POP3

Conservez vos dossiers et messages sur votre ordinateur

[Configuration manuelle](#)

Annuler

Terminé

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 :

## Mozilla Thunderbird Email souhaite accéder à votre compte Google

 labo.ndlp@gmail.com

Cela permettra à **Mozilla Thunderbird Email** d'effectuer les actions suivantes :

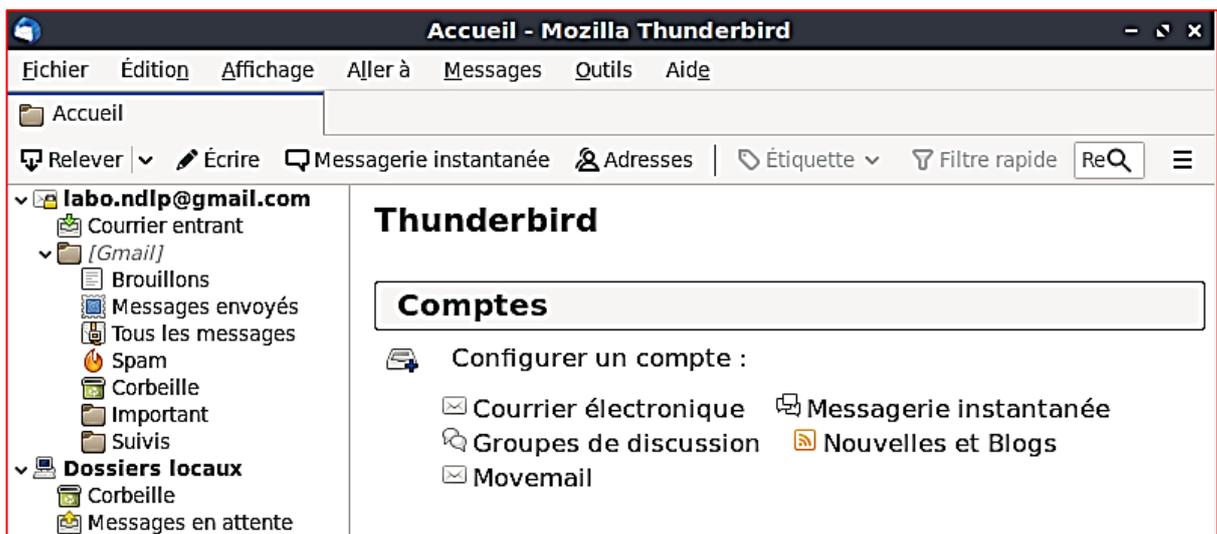
---

 Lire, rédiger, envoyer et supprimer définitivement des e-mails dans Gmail 

---

En cliquant sur "Autoriser", vous autorisez cette application et Google à utiliser vos données conformément à leurs [Règles de confidentialité](#) respectives. Vous pouvez à tout moment modifier ces paramètres, ainsi que d'autres [autorisations associées à votre compte](#).

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



The screenshot shows the 'Accueil - Mozilla Thunderbird' window. The left sidebar shows the account 'labo.ndlp@gmail.com' with folders like 'Courrier entrant', 'Brouillons', 'Messages envoyés', etc. The main pane is titled 'Thunderbird' and contains a 'Comptes' section with the option 'Configurer un compte :'. Under this, there are checkboxes for 'Courrier électronique', 'Messagerie instantanée', 'Groupes de discussion', 'Nouvelles et Blogs', and 'Movemail'. The 'Courrier électronique' checkbox is checked.

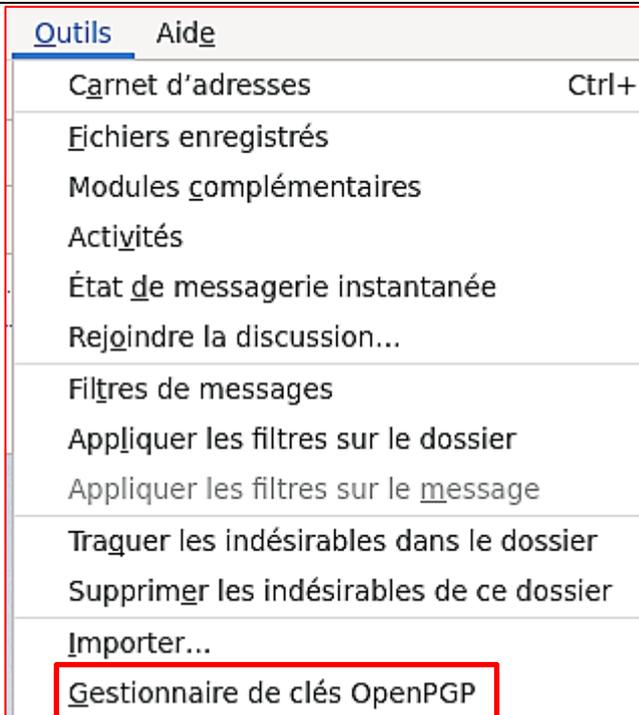
12 Testez le bon fonctionnement de votre compte de messagerie en envoyant un mail depuis cette nouvelle adresse vers une autre adresse que vous possédez :



The screenshot shows the email list in Thunderbird. The selected email is from 'labo.ndlp@gmail.com' with the subject 'Re: test mail' and the sender 'Gilles HOMMET' at '12:25'. The interface includes a search bar and various icons for actions like star, delete, and reply.

### 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 » :

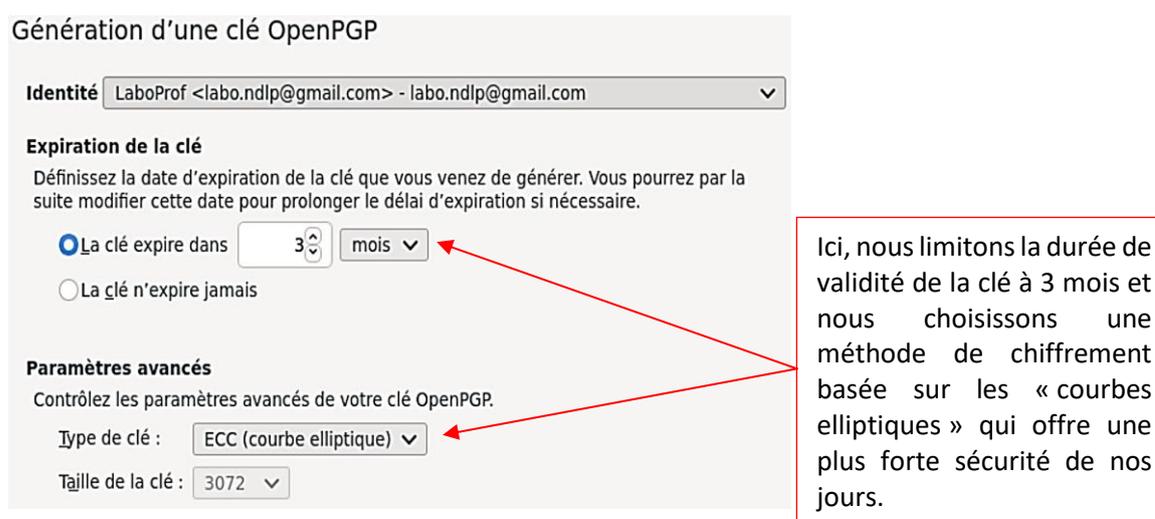


Un assistant Open PGP s'ouvre (gestion Open PGP intégrée par défaut dans Thunderbird depuis la version 78.4). Nous allons maintenant générer la paire de clés (publique et privé) nécessaire à l'utilisation du chiffrement des mails dans Thunderbird.

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



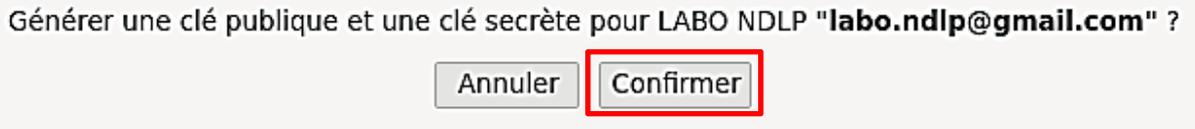
15 Compléter la fenêtre de génération des clés et cliquer sur « Générer la clé » :



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.

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 cryptage fort au niveau de vos clés publiques et privées :

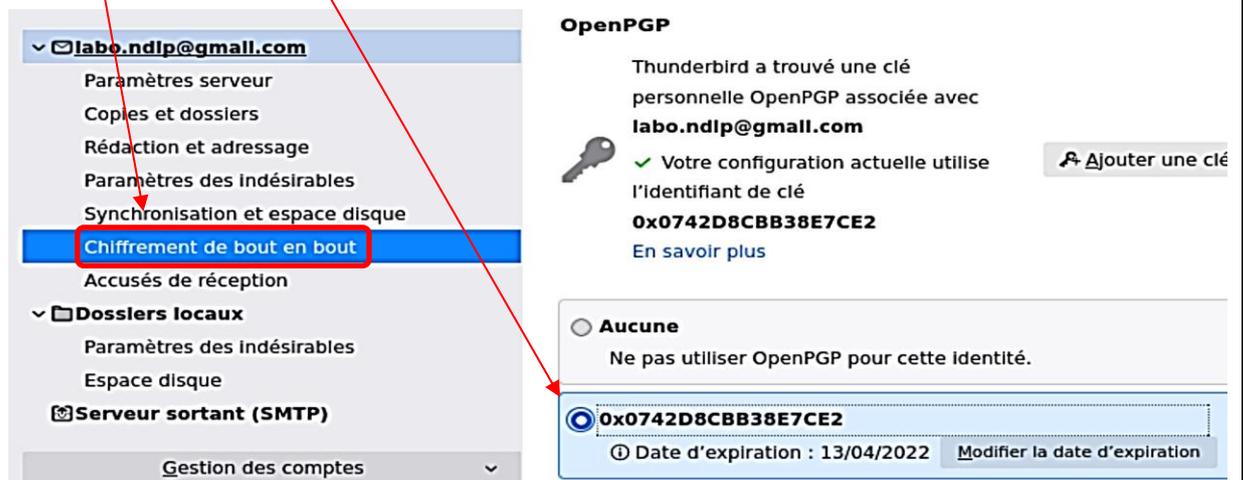


A la fin du processus, la paire de clés est générée :

**LaboProf <labo.ndlp@gmail.com>** **0x0742D8CB...** **13/04/2022**

17

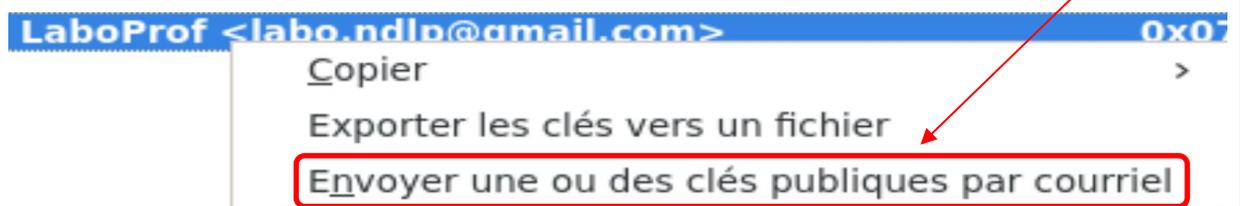
Activez, dans Thunderbird, le mode « chiffrement de bout en bout ». Pour cela, faites un clic droit sur votre compte de messagerie et cliquez « Paramètres ». Sélectionnez ensuite la rubrique « Chiffrement de bout en bout » et validez le chiffrement pour la clé précédemment générée :



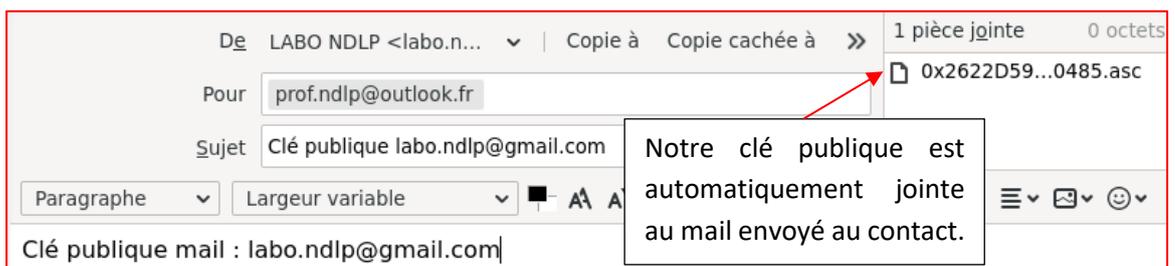
18

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 :

The screenshot shows a Gmail interface. On the left is the navigation pane with folders like 'Courrier entrant', 'Corbeille', and 'Dossiers locaux'. The main area shows an email from 'Gillomet GMAIL <gillomet@gmail.com>' with the subject 'clé publique gillomet GMAIL' and 'Pour Moi'. At the bottom, there is an attachment named '0xEBD3F86D544EEA90.asc' (652 octets). A red arrow points from the attachment name to the next screenshot.

The dialog box is titled 'Importer les clés suivantes ? (1)'. It shows the key ID '3CFAF9AB1365CE833ACB26B5046A0F9D7ABEF8' and the name 'Gillomet GMAIL <gillomet@gmail.com>'. Below this, there is a section 'Clé à importer' with a radio button selected for 'Acceptée (non vérifiée)'. At the bottom, there are 'Annuler' and 'OK' buttons. A red arrow points from the 'Acceptée (non vérifiée)' option to the text below.

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 » :

The dialog box is titled 'Clés correctement importées'. It displays the following information for 'Gillomet GMAIL <gillomet@gmail.com>':  
Bits: 255  
Date de création: 13/01/2022  
Empreinte:  
3CFA F9A8 1365 CE56 13AC  
5B26 8504 6A0F 9D7A 8EF8  
Below this is a link 'Afficher les détails et gérer l'acceptation des clés'. At the bottom right, there is an 'OK' button. A red box highlights the 'OK' button, and a red arrow points from the text below to it.

Cette fenêtre affiche les détails sur la clé publique reçue (empreinte notamment). Il faut ensuite valider et accepter cette clé pour pouvoir l'utiliser par la suite.

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

The screenshot shows the 'Gestionnaire de clés OpenPGP' window. It has a menu bar with 'Fichier', 'Édition', 'Affichage', 'Serveur de clés', and 'Génération'. Below is a search bar 'Rechercher des clés'. A table lists the keys:

Nom	Identifiant de...	Date d'e...
Gillomet GMAIL <gillomet@gmail.com>	0x85046A0F9...	13/04/2022
LaboProf <labo.ndlp@gmail.com>	0x0742D8CB...	13/04/2022

A red arrow points from the text above to the 'Gillomet GMAIL' entry in the table.

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

 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

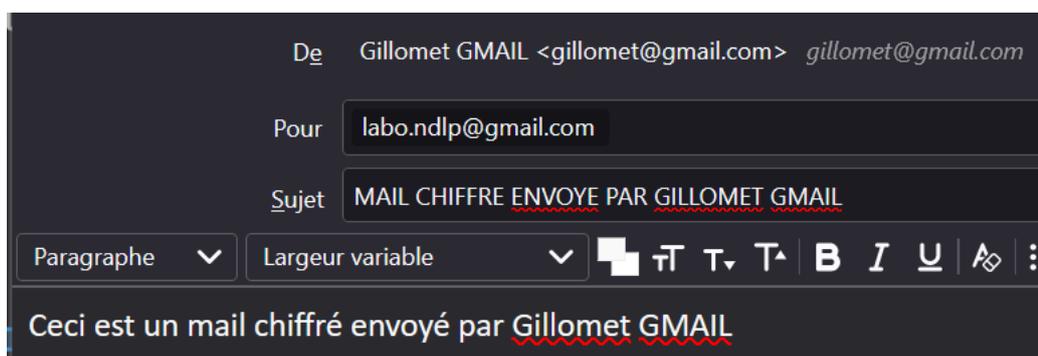
20 Envoyez un mail à l'un de vos contacts **SANS LE CHIFFRER** et en saisissant un texte simple comme, par exemple, « mail non chiffré ».

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) :

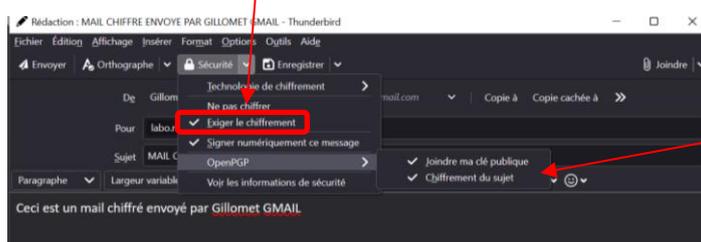
```
To: gillomet@gmail.com
From: LaboProf <labo.ndlp@gmail.com>
Subject: MAIL NON CHIFFRE
Content-Type: text/plain; charset=UTF-8; format=flowed
Content-Transfer-Encoding: 8bit
```

Ceci est un mail non chiffré

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 :

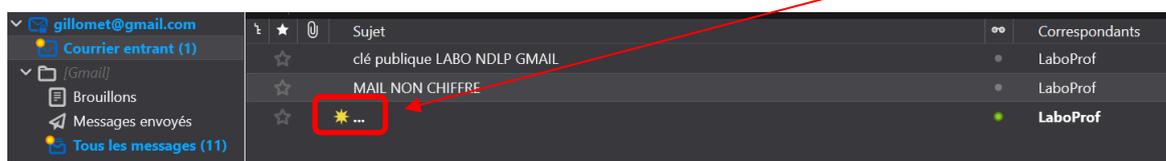


Pour chiffrer le mail avec OpenPGP, cliquez le bouton « Sécurité »  et cliquez l'option « Exiger le chiffrement ».

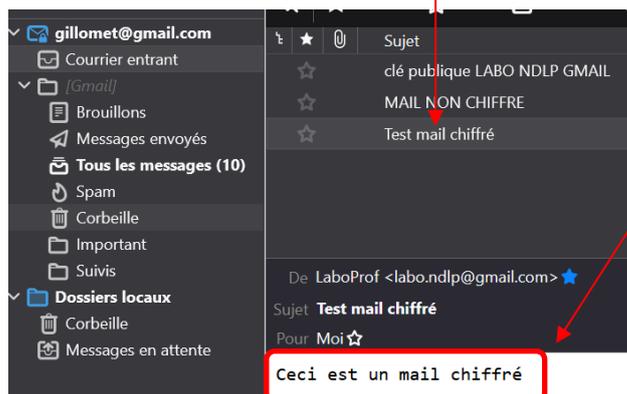


Lorsque l'on sélectionne l'option « OpenPGP », on peut joindre à nouveau notre clé publique si cela n'a pas été fait au préalable sinon le destinataire ne pourra pas déchiffrer le mail. Il est possible aussi de chiffrer le sujet du mail (l'objet).

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)
-----C4TIc1Jp5GRA9ojh1v3GcnS9
Content-Type: application/pgp-encrypted
Content-Description: PGP/MIME version identification

Version: 1

-----C4TIc1Jp5GRA9ojh1v3GcnS9
Content-Type: application/octet-stream; name="encrypted.asc"
Content-Description: OpenPGP encrypted message
Content-Disposition: inline; filename="encrypted.asc"

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

wV4DbjCjq8SjQoSAQdAco9sjaF8H/jst6dhhlLZuBZ6Q0hj6VjA+0tuU9sqLh8w2XjRpg9DW9u4
AYxi1U4su4/d+kgnTsp8fraVfSDCLM1qTejpo7dz5szv/YUF/ScPwV4DKC3tB8qSRY4SAQdAXBV6
1n1EAYD0DgQD5VamfwN/dik520uKkqCRiypWkyAw1EgQzqts6yT59uVMBKf+281030Fcv/8TWa+Y
m+Q8XjEzftJp9sXRb+iIC0wNcDhN0sRXAb2k6BuUVQKhMZJPiN/GpRX0HaMbr8fpcftHf
vd2MF4uZ85RvpAhADR33cJkC00z18sY/20Xoas1nD3m0BkXijVGA57TdzqFUuX4Pmf8ph
tTPBRo4t6Ccu9AYJjakEfjQvUr9DBYlZPgO1DxuQ1/K3Gap/GMR/38HcrS0ddmcUBQp4
mydDzf1LcXbTzks7jwz6ds38HHX+HOq1ud76tckp8Y0E151WTQFt/L3CZ0vTQDgeMvY
DV+cNyMInr0JKuS5tNLskV21b7MFkfkds+/mmnxKaVxruANnTiEVTqqHE5hVB34FReXOS
ECwauF5V1259c2L5mHv/P6KXAix4+XQwYwJdtpX8gN1exBcYnfcEADEK4h412Gtok8PDC
SInKhXk2bIoL2++dP0H2KeqYlJz/vHOY4t1i01bNy6YPI3JST8t4FMtrWmShXDHAiVgI
Vgv2bQdUDCTsUMAZvUuWxwS0H2gZi9yyMhicz9WfmFnbCFEY9P8b5Q0g3c+tQ0uPwp921
k+5P9nu5r7JoIF/Xn5dXjwE/di1sRuUBHAG9bOIJib3qyyDwf/BhM64k11K3iCNrNUiY
K376AzPC9ZiepHwF1ntk9+Ukvg+DCDHVlj2JiNf+Va7rJ4wq5AC/tkv13KU+kZ+nvnuP4
DU67FnY5Jen/eAww+c7wUkeLCM86gyf+tdircR0qNV81Qm0ZeEla9EWi2fmqZY/7u5Rt
AahG5VMcMQbJ7grZ/SN4xQ+317nrRJVkXBEkLbLSZ1x0t+Iko157Kh+2KdQ0JZV2P4i6
rEno6Z48Lbm44ND58rECqfsmX/2kF8/zT1v6w2nsUBhARYid/a3k3xpYw6EZ5tU2QXD2IHx5qD
8DB/eBfQsTi3zrYzdxT3rPgXjuku7ALwIae2Xv2NwoiG2S2tnVVU9IGMXGH0jofASR31h8qXJth
Yx87sdhWDKGCNsr+ifs5jYOWMPBDG2LSIqX1LUTHSwbKqXT00oIZA3RYXg1AKAGnLQ4EHT5gA5
nD5rAYCwLwxH5PyaeJcQdfrF2mbg8wEbs/dwGakEqyptU6Zeiz/sy+vY5GqWzQgUGINzb0rAIzkV
C9NMjrThmxMtkiq9svcb6bnU8A2NGkacwJb/eoohZv+Xv8bdI0Nj7tL/RsTFi27T1uCFoBDPwXbOr
z+o3i+h8jPE+119cGWcsiCEYdI/h18V1xqeMZxXPpab/RH51Z1nh6gPHBqCV3D3BNub6qKYXnXc/
onJ03qDpb21VteC4i2rQK+Xmkrs3x/HEdxSXwXHTDgopcrnnIjwW1QeEWF7W2QJn37e06N/PyxM
YDM+AoAvdeQ0rKqbtzSpgAdscy3icP/W2a3mVUCLCcsvqfcVDjw8i/ddFf+OCe6oiPwxBSdhhLjp
QQM4czHJdsHmIsnoceZgM+ucS0dxzYXx5PmNqujbx/UJFWjYOGepGqfK6i0vC2mQNKd74yHf+
9pTILKSSWht4Ectb/5xy7xTgh6T/cVQVj1Mpj2rc9FULPA5UjJWUJf02QCTR+B1dHS+enIWiH
F/dhqMSvs78r5vsasRAZM417aQ/oqRkyKLWgJx2kp6FLgaN5dGiL1ahg8IAsGzqBLP5mp6Jc518
wPJOeA5qFjwMwogIHSE+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 (chiffage). Ces codes correspondent au texte «Ceci est un mail chiffré »...

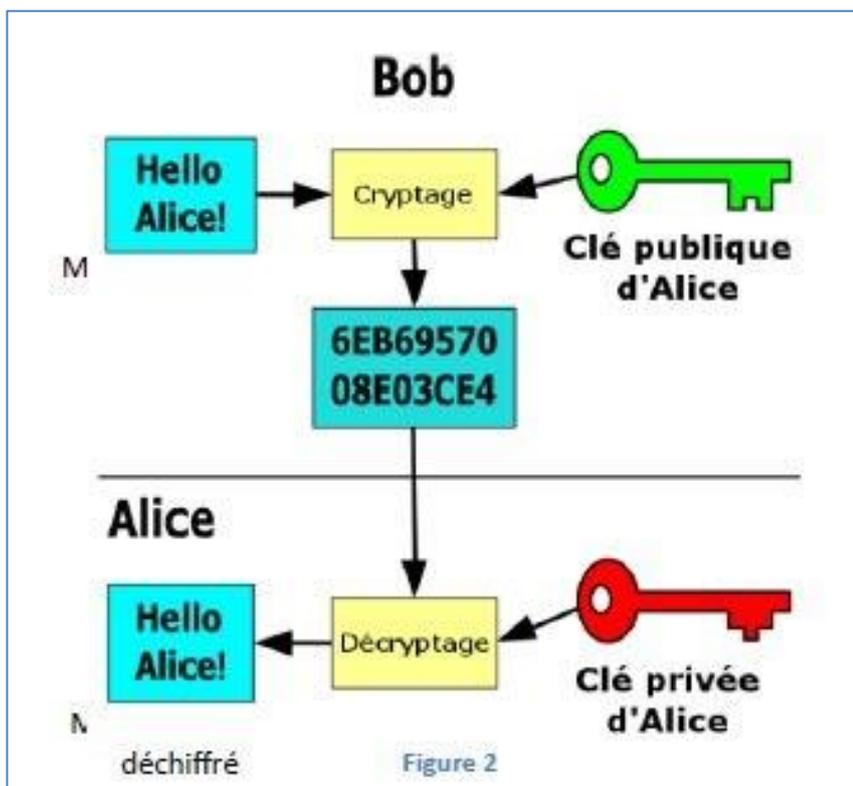
Nous ne présenterons pas dans ce guide la notion de serveurs de clés publics. Ces serveurs ont souvent fait l'objet d'attaques (hacking) ce qui les rend vulnérables (voir attaque des serveurs SKS).

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 chaîne 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.



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 sa 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.