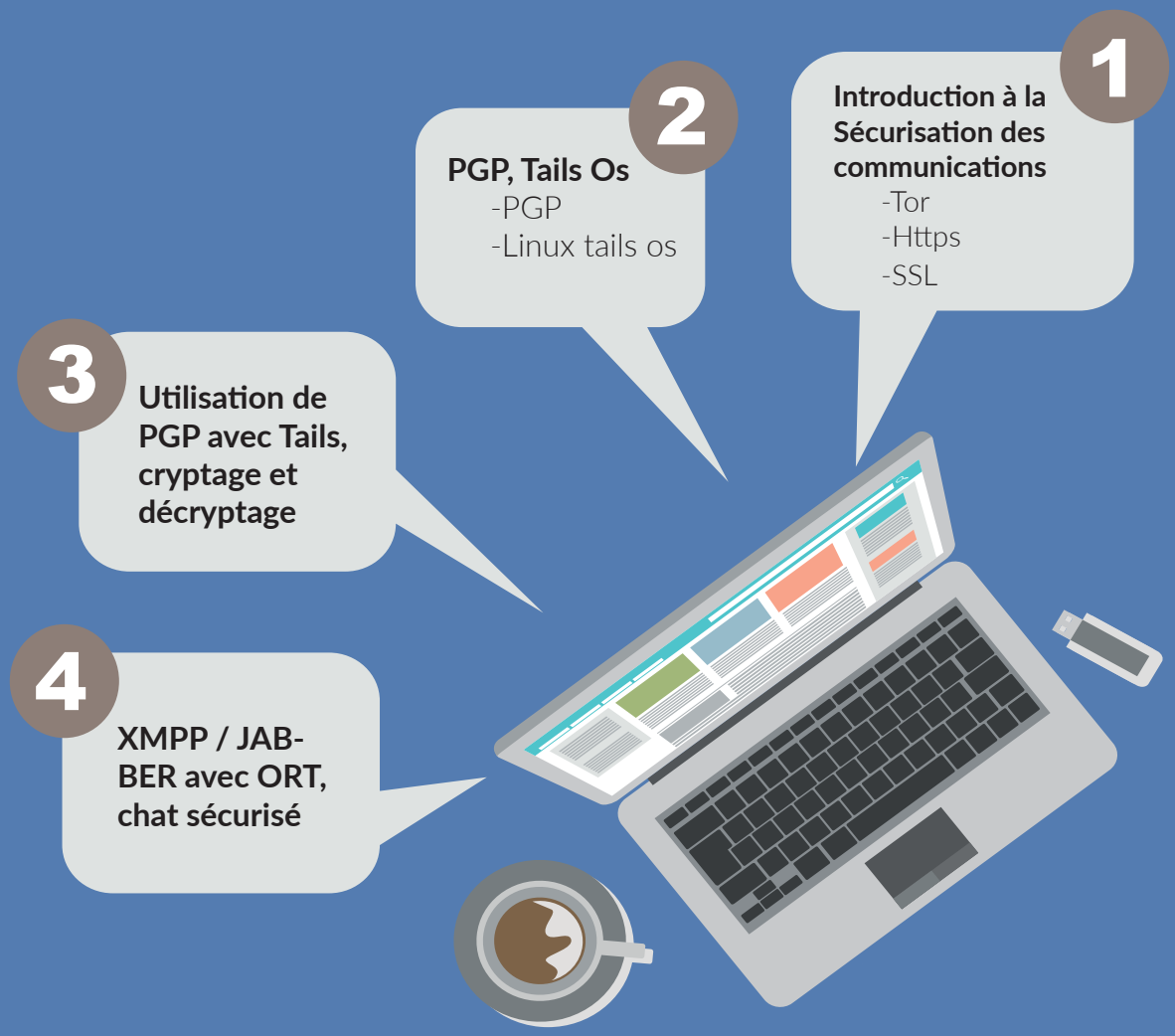



# SÉCURITÉ INFORMATIQUE

## > CHAPITRE 1 - INTRODUCTION A LA SÉCURISATION DES COMMUNICATIONS

TOR, HTTPS et SSL

### 1.1 TOR

Tor est un navigateur dissimulant votre **adresse IP** ainsi que votre **adresse MAC** lors de votre connexion internet et va vous fournir un certain degré d'anonymat en utilisant un système de cryptage de type ed25519 (courbe elliptique).

Quant à savoir si la NSA peut casser ce code, la réponse est probablement oui. Voilà pourquoi il ne faut jamais rien envoyer sur **Tor** qui soit personnel, sensible ou dont vous ne souhaitez pas voir le contenu intercepté. Excepté si vous utilisez un **cryptage PGP** dont nous allons parler plus tard dans ce dossier.

Les communications internet de votre ordinateur reposent sur un nœud d'entrée qui fondamentalement « entre dans votre ordinateur » sur le réseau **Tor**. Ce nœud d'entrée communique avec votre ordinateur et connaît votre **adresse IP** donc votre localisation réelle. Le nœud d'entrée fait une demande cryptée à un second nœud « le nœud de relais ». Le nœud relais communique avec le nœud d'entrée et le nœud de sortie mais ne connaît pas votre **adresse IP**.

Le nœud de sortie est l'endroit où votre demande est décryptée et envoyée à l'Internet. Le nœud de sortie ne connaît pas non plus votre **adresse IP**, il a connaissance uniquement de l'IP du nœud de relais.

En utilisant ce modèle de 3 nœuds, cela rend plus difficile, mais pas impossible de faire coïncider vos consultations sur internet à votre adresse IP d'origine.

Le problème réside dans le fait que lorsque vous saisissez des informations sensibles en clair sur **TOR**, il se peut que le nœud de sortie soit mis en place par les services de renseignement mécréants ou une personne malveillante souhaitant vous voler ces informations car tout le monde peut mettre en place un nœud de sortie.

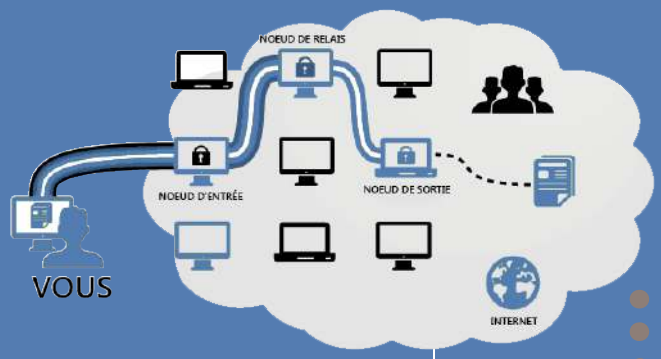



Schéma des noeuds TOR

## 1.2- HTTPS « HIDDEN SERVICE »

Depuis peu, des serveurs qui offrent ce qu'on appelle les services cachés (« **Hidden Service** ») se sont mis en place. Vous pouvez facilement reconnaître ces services par l'adresse d'un site web finissant par .onion contrairement aux autres sites classiques terminant par .com, .fr, etc.

Ces services offrent ce qu'on appelle le chiffrement de bout-en-bout, qui permet de prendre possession des nœuds de sortie compromis et donc de les contrôler. Le serveur web du service caché devient donc votre nœud de sortie, ce qui signifie que le site que vous visitez est celui qui décrypte vos messages et non un espion à la solde des mécréants.

Rappelez-vous, le nœud de sortie possède la clé pour décrypter votre demande d'accès à un site web. Le nœud de sortie peut voir ce que vous envoyez en texte clair une fois qu'il est déchiffré. Ainsi, si vous entrez votre nom et votre adresse dans un champ, le nœud de sortie obtient vos informations. Si vous mettez un numéro de carte de crédit, un compte bancaire, votre vrai nom, même vos informations de connexion, alors vous compromettez votre identité.

Une autre précaution que vous pouvez prendre est de visiter uniquement les sites web qui utilisent ce qu'on appelle le **protocole HTTPS** sécurisé que l'on voit avant l'adresse du site (ex. https://votresiteinternet.com). Si vous voyez https:// alors votre site web utilise le **protocole HTTPS** sécurisé.

Cela crypte votre demande d'accès à un site web de telle manière que seulement le serveur du site web puisse décrypter votre demande et non une personne restant en surveillance sur le nœud de sortie de **Tor**.

Si quelqu'un devait intercepter votre demande via le **protocole HTTPS** sécurisé, ils verraient les données chiffrées et prendra du temps afin de le décrypter.

C'est pour cette raison que vous ne devriez pas entrer de données sensibles ou personnelles sur tout site web, en particulier lorsque vous y accédez avec **TOR**.
Si l'un des nœuds de la chaîne est compromis alors les personnes en charge de ces nœuds compromis ont la technologie pour déchiffrer votre navigation. Il est préférable que les informations ne soient pas sensibles. Face à cela, que pouvons-nous faire pour résoudre ce problème de sécurité ?

Une autre raison pour laquelle vous devez utiliser **HTTPS** chaque fois que cela est possible est que les nœuds malveillants de **Tor** peuvent endommager ou modifier le contenu avec une connexion **HTTP** non sécurisée et injecter des logiciels malveillants dans la connexion. Ceci est particulièrement facile lorsque vous envoyez des demandes de connexion non sécurisée mais **HTTPS** réduit cette possibilité.

## 1.3- CERTIFICAT SSL

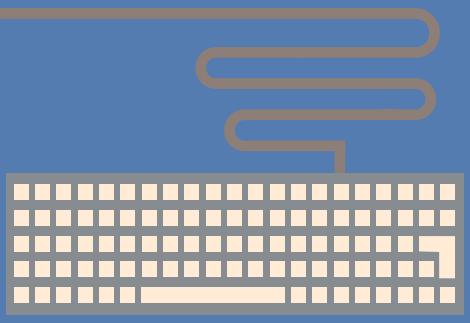
Vous devez savoir, cependant, que HTTPS peut également être craqué en fonction du niveau de la clé de chiffrage. Lorsque vous visitez un site utilisant le **protocole HTTPS**, vous cryptez votre demande en utilisant sa clé publique et elle est décryptée en utilisant la clé privée du serveur abritant le site en **HTTPS**. Voilà comment fonctionne la cryptographie.

Une clé publique est prévue pour ceux qui veulent envoyer un message chiffré ou se connecter en **HTTPS** et le seul qui peut décrypter est celui qui est en possession de la clé privée. Malheureusement, de nombreux sites Web aujourd'hui utilisent des clés privées **1024 bits** et cela n'est plus très performant.

Vous devez donc vous assurer de trouver quel niveau de cryptage le site que vous visitez utilise pour vous assurer qu'il utilise des clés de **2048 bits** ou **4096 bits**. Même après tout cela, la faille n'est toujours pas complètement comblée parce que nous avons un autre problème. Qu'advient-il si le serveur web lui-même est compromis ?

Il se peut que vos nœuds **TOR** ne soient pas compromis et que vous utilisiez **HTTPS** lors de toutes vos demandes de connexion aux sites web. Mais si le serveur web lui-même du site que vous visitez a été compromis, alors toutes vos demandes sont à nouveau décryptables facilement et visible par tous.

Par la grâce d'Allah, il existe des solutions pour combler les failles. Cela dit, nous allons procéder aux explications afin de sécuriser vos connexions après avoir mentionné les risques et les mesures que nous pouvons prendre pour protéger notre vie privée en ligne et rester anonyme.



# > CHAPITRE 2 - PGP ET TAILS OS

## PGP & linux Tails os

Encore une fois, gardez à l'esprit que si vous souhaitez garder votre anonymat, vous ne devez jamais saisir des détails d'identification personnelle en ligne. Faites en sorte que, même si les chiens du *ṭâghût* interceptent et déchiffrent, ou compromettent votre circuit, la seule information qu'ils puissent trouver soit votre nom d'utilisateur et mot de passe.

Comment être sûr que le nom d'utilisateur et mot de passe que j'utilise sont sûrs ? Est-ce que votre mot de passe contient une information d'identification ? Est-ce le même mot de passe que vous utilisez pour votre e-mail personnel ? Contient-il un nom de quelqu'un que vous connaissez personnellement ? Toujours garder tous ces facteurs à l'esprit.

Une autre étape que vous devez prendre en compte, en particulier lors de la communication avec d'autres utilisateurs sur des sites non sécurisés tels que les réseaux sociaux, forum ou encore Telegram (qui est loin d'être totalement sécurisé), c'est que ces utilisateurs utilisent le **cryptage PGP**.

Cela n'est pas toujours possible comme dans le cas où vous vous connectez à un site web, en remplissant un formulaire, en entrant dans une boîte mail, etc.

Considérons comme potentiellement compromis tout type d'informations que vous entrez dans un site web en utilisant le texte brut (c'est-à-dire sans **cryptage PGP**). Evitez donc de mettre tout type de format de texte brut sensible en ligne.

### 2.1- PGP

Pourquoi **PGP** ?

Car **PGP** utilise une très forte méthode de cryptage appelé cryptographie asymétrique.

**PGP** signifie Pretty Good Privacy. Il est utilisé pour chiffrer, déchiffrer et signer (rendre authentique) des textes, des e-mails, des fichiers, des répertoires, des partitions entières de disque et à accroître la sécurité des communications par email.

Pour les lecteurs plus avisés, il utilise une combinaison de série de hachage, la compression de données, la cryptographie à clé symétrique, et la cryptographie à clé publique. Pour les lecteurs moins avisés, le processus de cryptage des messages avec **PGP** est le suivant.

Vous créez une clé privée et une clé publique. Votre clé publique est la clé que vous donnez aux personnes à qui vous souhaitez envoyer des messages cryptés. Votre clé privée est détenue uniquement par vous. Cette clé privée est la seule clé qui peut ouvrir les messages qui ont été précédemment cryptés avec votre clé publique.

Pour illustrer cela : Abû Bakr doit recevoir un message de 'Umar mais il ne fait pas confiance au facteur qui pourrait ouvrir sa lettre. Comment peut-il être sûr de recevoir ce message sans qu'il soit lu ? Abû Bakr va d'abord envoyer à 'Umar un cadenas ouvert dont lui seul possède la clé. Ensuite, 'Umar va placer son message dans une boîte qu'il fermera à l'aide de ce cadenas avant de l'envoyer à Abû Bakr. Le facteur ne pourra donc pas ouvrir la boîte puisque seule Abû Bakr possède la clé !

Pareillement, si vous souhaitez envoyer un message crypté à un utilisateur, vous utiliserai sa clé publique et l'utilisateur utilisera sa clé privée pour décrypter votre message. Ceci est appelé la cryptographie asymétrique et a été conçu afin que si une personne intercepte votre message, il soit dans l'incapacité de décrypter le message sans votre clé privée. Même si vous perdez votre clé privée, il n'y a aucun moyen de récupération de clé. Vous pouvez considérer que le message est verrouillé définitivement, sans avoir la possibilité de lire son contenu.

Alors, comment utiliser **PGP** ?

Avant d'en arriver là, nous allons vous présenter un système d'exploitation live qui rend l'utilisation du **cryptage PGP** très facile.

Un système d'exploitation en temps réel (live) est un système d'exploitation que vous pouvez exécuter sur votre système d'exploitation actuel. Ainsi, par exemple, si vous êtes un utilisateur Windows, vous avez deux choix.

Vous pouvez télécharger le système d'exploitation live, le graver sur un CD ou un DVD, puis démarrer votre ordinateur à partir de ce CD ou DVD. Votre ordinateur fonctionnera sur le CD ou le DVD comme si vous avez ce système d'exploitation installé sur votre ordinateur.

Toutefois, si vous retirez le CD ou le DVD ou qu'il redémarre, votre ordinateur va redémarrer normalement avec un retour sur Windows sans avoir affecter ou altérer quoi que ce soit sur votre ordinateur.

Vous pouvez également utiliser une clé USB ou Carte SD pour effectuer cette même installation, ou bien exécuter ce système d'exploitation en live avec ce qu'on appelle **Virtual Box**. Les avantages sont que vous pouvez exécuter **Windows** simultanément avec cet autre système d'exploitation et vous pouvez facilement basculer entre eux sans avoir à redémarrer l'ordinateur. Les deux méthodes ont leurs avantages et inconvénients.

Les avantages en passant par un support externe (CD, DVD, USB, Carte SD) sont de réduire le risque d'avoir votre ordinateur compromis par un virus, logiciels malveillants et **keylogger** (enregistreur de frappe de clavier) qui reposent sur des vulnérabilités de **Windows** pour fonctionner.

Enfin, le système d'exploitation en Live, celui que nous allons vous présenter est **Tails**.

La raison pour laquelle nous vous présentons le système d'exploitation **Linux Tails** est qu'il a beaucoup de spécificités de sécurité dont vous avez besoin pour rester anonyme et qui sont déjà installées de base. Cela vous donne presque tous les éléments de sécurité prêts à l'emploi.

Assurez-vous de télécharger le fichier **ISO Tails** à partir du site web officiel de **Tails** et vous pouvez l'installer dans **Virtual Box** ou l'installer sur une clé USB ou le graver sur un DVD et démarrer votre ordinateur à partir de ce lecteur.

Nous vous suggérons une clé USB ou Carte SD pour des raisons de sécurité car bien plus pratiques à enlever et à détruire par la suite si les chiens du ṭâghût aboient à votre porte. Nous partons donc du principe que vous opterez pour la méthode d'installation sur USB ou Carte SD. Si ce n'est pas le cas, de nombreux tutoriels sont disponibles en ligne sur l'installation de **Virtual Box**.

Mais fondamentalement, **Virtual Box** fonctionne directement sur votre disque dur, il crée un disque dur virtuel qui est utilisé comme un disque dur temporaire pendant que **Tails** est en marche. Une fois que **Tails** est fermé, ce disque dur virtuel est supprimé, mais il n'est pas supprimé définitivement. Comme nous le savons, avec la puissance des outils de récupération de nos jours, les fichiers supprimés sont facilement récupérables et donc cela ne reste pas très fiable.

Nous allons montrer la façon de protéger vos fichiers des outils de récupération de données au fil de ce document. Pour le moment, effectuez l'installation de Tails sur une clé USB ou une carte SD.

Même chose lors du démarrage de votre ordinateur sur Tails, à partir d'une clé USB ou d'un DVD, votre disque dur sera utilisé pour stocker les fichiers utilisés par Tails, alors assurez-vous que tous les fichiers qui sont enregistrés ou accessibles par Tails le sont à partir d'une clé USB ou une carte SD, sinon ils vont être aussi récupérables.

## 2.2- LE SYSTÈME D'EXPLOITATION TAILS :

Prérequis : L'installeur de **Tails** peut uniquement l'installer sur une clé USB ou une carte SD/Micro SD d'au moins 4 Go.

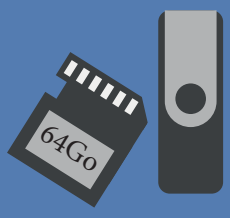
Tails nécessite une clé USB ou une carte SD dédiée. Il est impossible d'ajouter un autre système d'exploitation ou une autre partition sur le même périphérique si vous voulez bénéficier des mises à jour automatiques.

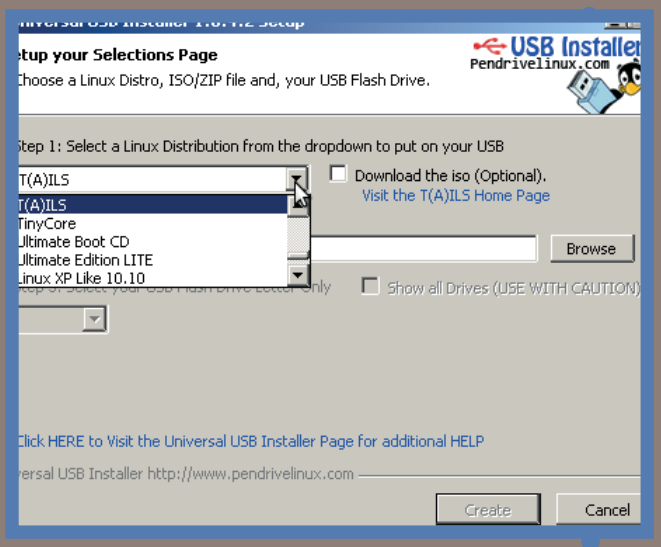
### Comment l'installer sur USB, carte SD ou DVD

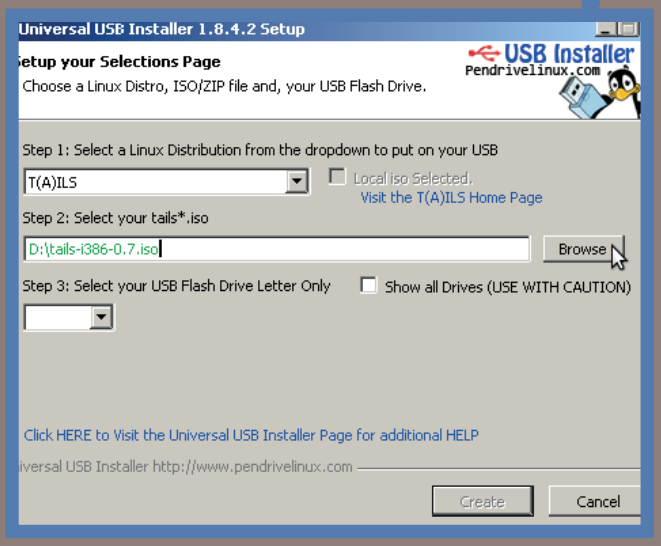
**?**

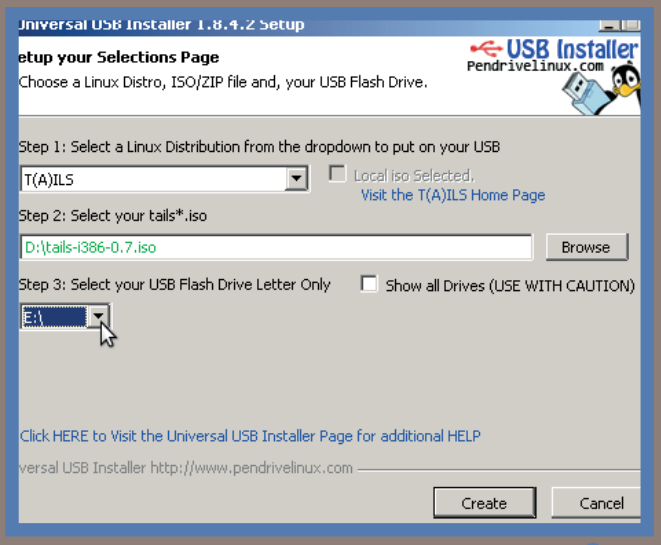
Processus d'installation sur **Windows** et **Macintosh** :

1. Téléchargez la dernière version de Tails disponible à cette adresse :
https://tails.boum.org/download/index.fr.html
2. Selon que vous utilisez Windows ou Mac
   - **a** Le Guide d'installation complet pour **Windows**
   - **b** Le Guide d'installation complet pour **Mac**
3. Démarrez avec **Tails**






### *a) Sur PC Windows :*

Cette méthode utilise l'Universal USB Installer (l'installateur universel USB) téléchargeable a cette adresse : http://www.pendrivelinux.com/universal-usb-installer-easy-as-1-2-3/

Lancez le logiciel. Une fois ouvert, dans le menu déroulant, sélectionnez **T(A)ILS** et cliquez sur « *Browse* » pour sélectionner votre fichier Tails.iso et sélectionner votre clé USB. Selon sa lettre d'appartenance, D, E, F ou autre, en allant sur votre Poste de travail ou Ordinateur vous verrez quelle lettre lui est associée.

Cliquez sur « *Create* » pour créer votre clé USB Tails.

Ensuite, éteignez l'ordinateur, branchez votre clé USB et démarrez l'ordinateur. Vous devriez voir apparaître le menu de démarrage de **Tails**. Si le menu n'apparaît pas, vous pourriez avoir besoin d'effectuer quelques manipulations supplémentaires.

Démarrage avancé :

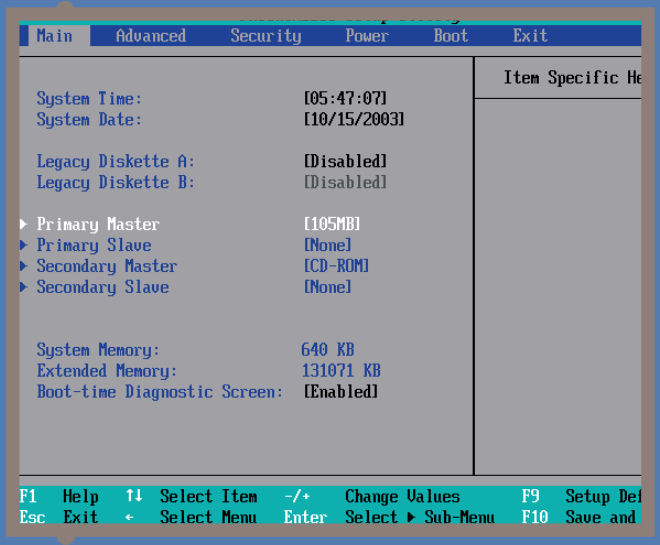
Pour cela, redémarrez votre ordinateur puis un message au démarrage devrait vous indiquer la touche à presser afin d'accéder au démarrage avancé. Une fois entré dans les réglages avancés, choisissez de démarrer sur la clé USB correspondant à l'installation de Tails.

Si cela n'est toujours pas concluant voici une méthode pour régler le problème.

Modification de la séquence de démarrage du **BIOS** :

Au démarrage de votre ordinateur, pressez la touche vous permettant d'accéder au **BIOS**. Souvent l'une des touches suivantes : F1, F2, Suppr, Echap ou F10. Pressez cette touche au démarrage de votre ordinateur pour éditer les paramètres de votre **BIOS**.

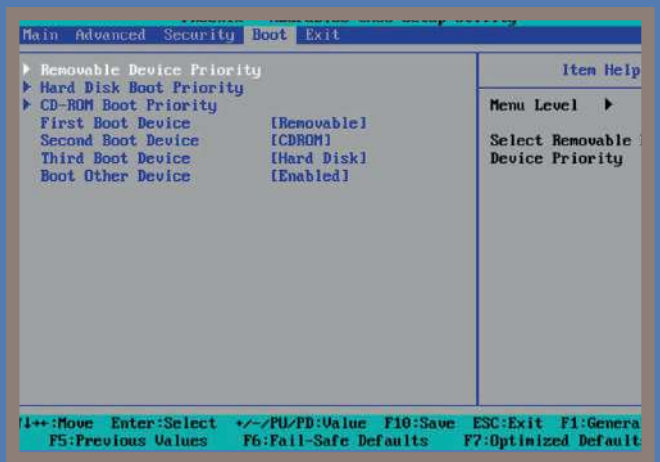
Vous devez changer l'ordre de démarrage. En fonction de votre ordinateur, vous devriez voir une ligne contenant périphériques externes ou média USB. Déplacez cette ligne au sommet de la liste pour forcer l'ordinateur à essayer de démarrer à partir de votre périphérique avant le disque interne. Enregistrez vos modifications et redémarrer.




Déplacez-vous jusqu'à l'onglet Boot à l'aide des flèches, vous obtenez comme dans l'image 2, il ne vous reste plus qu'à choisir l'ordre :

**1st Boot Device :** *Périphériques externes ou média USB*
**2nd Boot Device :** *CD ou DVD*
**3rd Boot Device :** *HDD*

Sélectionnez la clé USB et tapez sur la touche entrée de votre clavier pour valider.



***b) Sur Macintosh :***

Pour ce qui concerne les **Macintosh**, l'installation devra s'effectuer via l'application Terminal. Pour l'ouvrir il suffira d'aller dans le dossier Applications, Utilitaires, Teminal.app et le lancer.

Débrancher votre clé USB et lancer l'application Terminal, puis exécutez la commande suivante :

*diskutil list*

Ceci renvoie la liste des périphériques de stockages actuels. *(voir l'image 1)*

Une fois la liste analysée, branchez la clé USB ou l'on veut installer **Tails**, exécuter une nouvelle fois la commande diskutil list afin de voir quel périphérique de stockage est apparu par rapport à la liste précédente et en fonction de la taille de votre clé USB. Par exemple, une fois une clé USB branchée cela donnerait quelque chose comme dans *l'image 2*.

Dans cet exemple votre clé USB est nommée /dev/disk2. Cela varie selon les périphériques donc il est très important de bien noter la liste avant et après avoir branché la clé voulue afin de voir le nom correct.

Maintenant, il suffit de démonter la clé USB avec la commande suivante, et en remplaçant [device] par le nom du périphérique (/dev/votrecléusb) à la place :

*diskutil unmountDisk [device]*

Il faut ensuite installer **Tails** sur la clé USB avec une commande toute simple. Il y a deux champs à remplacer [tails.iso] par votre fichier à vous ainsi que son chemin d'accès. Pour faire plus rapide il vous suffit de faire glisser le fichier Tails.iso directement à la suite pour que l'application Terminal note le chemin automatiquement et remplacer aussi [device] de la même façon que précédemment. La commande :

*dd if=[tails.iso] of=[device] bs=16m && sync*

Ce qui donnerait quelque chose comme ceci en exemple :

*dd if=/Users/AbouHamza/Downloads/Tails.iso of=/dev/votrecléusb bs=16m && sync*

Si un message « *Permission denied* » apparait, il suffit alors de rajouter au début de la commande : *sudo* et il sera alors demandé le mot de passe pour effectuer la commande avec les droit d'administrateur.

Exemple :

*sudo dd if=/Users/AbouHamza/Downloads/Tails.iso of=/dev/votrecléusb bs=16m && sync*

Si aucun message d'erreur n'apparaît, c'est alors que **Tails** est en train d'être copié vers la clé USB. Ce processus peut prendre quelques minutes, l'installation est complète lorsque l'invite de commande réapparaît.

Ensuite, éteignez l'ordinateur, branchez votre clé USB, démarrez l'ordinateur et appuyez immédiatement sur la touche Option « *cmd* ». Maintenez cette touche enfoncée jusqu'à ce qu'un menu de démarrage apparaisse. Dans ce menu de démarrage, choisissez l'entrée qui indique **Boot EFI** et qui a l'apparence d'une clé USB.

Vous devriez alors voir le menu de démarrage de **Tails** se lancer. Si cela ne

1

```
$ diskutil list
/dev/disk0 (internal, physical):
   #:                       TYPE NAME                    SIZE       IDENTIFIER
   0:      GUID_partition_scheme                        *500.1 GB   disk0
   1:                        EFI EFI                     209.7 MB   disk0s1
   2:                  Apple_HFS Mac OSX System          499.2 GB   disk0s2
   3:                 Apple_Boot Recovery HD             650.0 MB   disk0s3
```

2

```
# diskutil list
/dev/disk0 (internal, physical):
   #:                       TYPE NAME                    SIZE       IDENTIFIER
   0:      GUID_partition_scheme                        *500.1 GB   disk0
   1:                        EFI EFI                     209.7 MB   disk0s1
   2:                  Apple_HFS Mac OSX System          499.2 GB   disk0s2
   3:                 Apple_Boot Recovery HD             650.0 MB   disk0s3
/dev/disk2 (external, physical):
   #:                       TYPE NAME                    SIZE       IDENTIFIER
   0:      FDisk_partition_scheme                       *31.5 GB    disk2
   1:                Windows FAT 32 SONY32GD            31.5 GB    disk2s1
```

fonctionne pas, vous aurez besoin d'installer **Refit**. Il vous permet d'effectuer un démarrage avancé sur **Mac** mais reste bloqué par Apple dans ses nouvelles versions.

http://refit.sourceforge.net/#download

**1.** Téléchargez et montez l'image de disque rEFIt-0.14.dmg.

*a.* Double-cliquez sur le paquet « rEFIt.mpkg ».
*b.* Suivez les instructions et sélectionnez le volume de votre installation de Mac OS X comme volume de destination pour l'installation.

**2.** Si tout s'est déroulé correctement, vous verrez lors du redémarrage de l'ordinateur le menu rEFIt. Sélectionnez **Boot Efi** avec les flèches de direction de votre clavier afin de lancer **Tails**.

Il est à noter que parfois la clé USB ou la carte SD n'est pas détectée. Dans ce cas, un redémarrage supplémentaire corrigera ce problème. Sélectionnez simplement avec votre clavier l'icône flèche descendance en bas de votre écran pour redémarrer l'ordinateur.

### *3. Démarrer Tails*

A ce Stade, vous devriez avoir ceci à l'Écran :

Sélectionnez « *Live* » et tapez sur la touche Entrée.

Ensuite, choisissez la langue en bas de page ainsi que la langue du clavier a droite, puis cliquez sur Login pour lancer **Tails** sans option avancée. Si vous souhaitez paramétrer plus d'options, rendez-vous sur : https://tails.boum.org/doc/first_steps/startup_options/index.fr.html

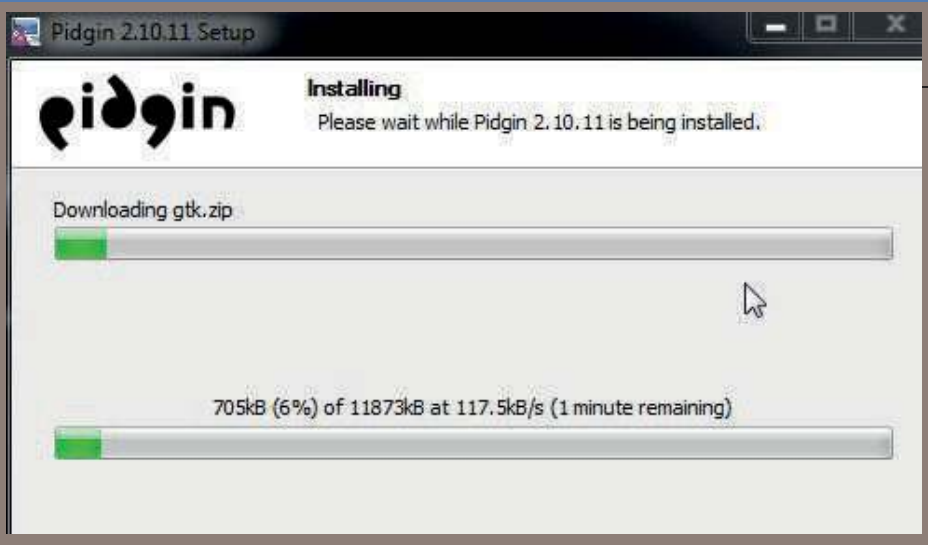
Vous voici donc sur le Bureau de **Tails**. Avant de lancer internet, une notification vous prévient lorsque **TOR** est prêt à être utilisé en toute sécurité.

Une fois que vous avez terminé d'utiliser **Tails**, il ne vous reste plus qu'à éteindre votre ordinateur et toutes vos traces s'effaceront automatiquement.

Pour réutiliser **Tails**, il vous suffit de redémarrer de nouveau sur la clé USB ou votre carte SD.

Gardez autant que possible les fichiers sensibles hors de votre disque dur personnel. Il est possible de détruire des fichiers de sorte qu'ils soient irrécupérables par les technologies de récupération et il est certes plus aisé de le faire sur une clé USB ou carte SD de 16GO que sur un Disque Dur de 1To.

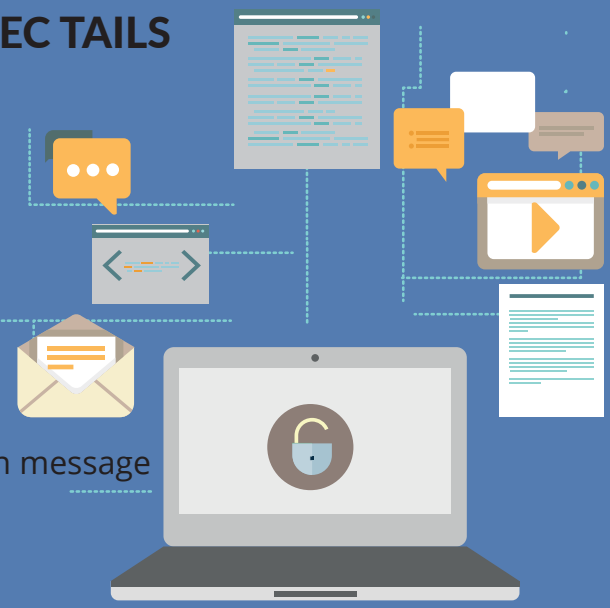
Nous reviendrons sur le sujet de destruction sécurisée de fichiers, il est temps pour nous d'apprendre à utiliser **PGP**.




Capture d'écran du bureau de Tails os

# > CHAPITRE 3 - UTILISATION DE PGP AVEC TAILS

## Cryptage & Décryptage





Maintenant, nous supposons que vous avez installé **Tails** et que vous êtes sur le bureau de votre nouveau système d'exploitation.

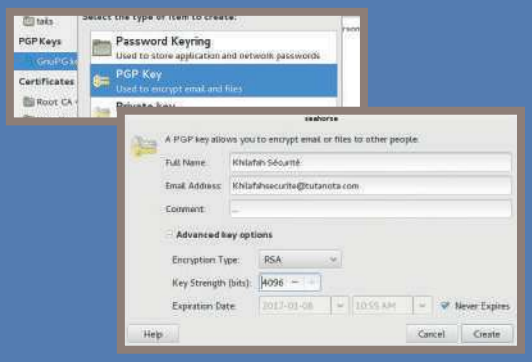
### Comment utiliser PGP dans Tails

?

La première chose à faire est de créer votre propre clé PGP personnelle qui se compose de votre clé publique que vous pouvez donner à des personnes ou poster dans vos profils en ligne. Comme mentionné précédemment, c'est cette clé que les personnes utilisent pour crypter les messages à vous envoyer. Votre clé personnelle se compose également de votre clé privée que vous pouvez utiliser pour déchiffrer les messages cryptés à l'aide de votre clé publique **PGP**.

### 3.1- PROCÉDURE D'OBTENTION D'UNE CLÉ PGP :

Commençons par aller vers la zone en haut à droite de votre écran, vous verrez une liste d'icônes dont l'une d'entre elles ressemble à un presse-papier. Vous devez cliquer sur ce presse-papier, puis cliquez sur Gérer les clés

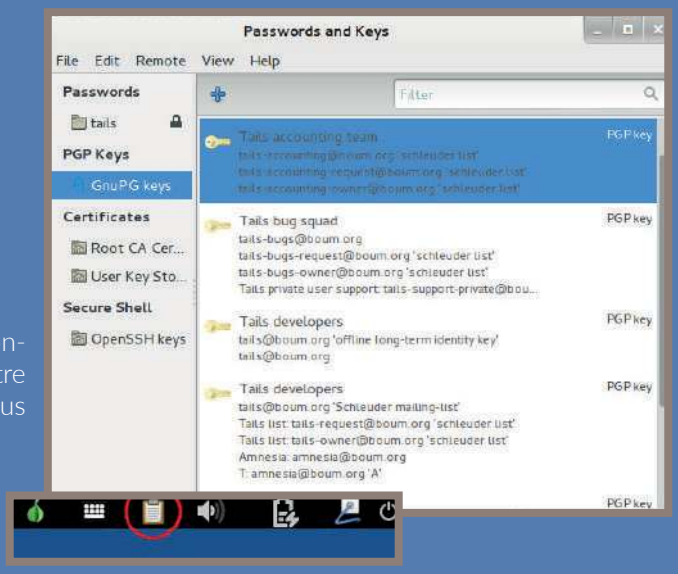



Ensuite, cliquez sur Fichier > Nouveau
Sélectionnez > **Clé PGP** et cliquez sur Continuerv

Remplissez votre nom complet (utilisez un pseudonyme et non pas votre identité réelle), optionnellement un e-mail et un commentaire. Ensuite, cliquez sur Options avancées clés.

Assurez-vous que le type de cryptage est réglé au **RSA** et mis en force clé de **4096 bits**. Une fois que vous avez fait cela, cliquez sur créer (Create) et cela va générer votre clé. Suite à cela, votre clé personnelle est affichée dans la fenêtre de gestion des clés. Vous avez créé votre clé personnelle !

Pour trouver votre clé publique **PGP**, cliquez sur votre clé personnelle, puis cliquez sur Editer « haut de la fenêtre » et Copier. Votre clé publique **PGP** sera copiée dans votre presse-papier mais vous pouvez la coller ou vous le souhaitez.




## ÉTAPE IMPORTANTE :

Pour sauvegarder votre clé privée sur une clé USB ou une carte SD secondaire.

Si vous utilisez **Tails** à partir d'une clé USB, vous devez utiliser un disque séparé pour y stocker votre clé privée. Encore une fois, ne jamais stocker vos clés privées sur votre disque dur, les garder en dehors de votre ordinateur.

Pour enregistrer votre clé privée, cliquez droit sur votre clé personnelle et cliquez sur Propriétés, puis Onglet (détails) et Exportation de clé complète.

Rappel : Si vous perdez votre clé privée, vous ne pourrez jamais la récupérer même si vous en créez une autre en utilisant le même mot de passe.

Une fois que vous avez fait cela, vous avez enregistré votre clé personnelle pour une utilisation future lorsque vous redémarrez **Tails**. Gardez à l'esprit que **Tails** n'est pas installé sur votre disque dur, donc à chaque redémarrage de **Tails** vous perdez toutes vos clés ainsi que tous les dossiers et fichiers non stockés dessus.

En enregistrant vos clés sur une clé USB ou une carte SD, vous pouvez importer vos clés et les utiliser chaque fois que vous redémarrez **Tails**. Les clés publiques appartenant à d'autres utilisateurs, vous pouvez les sauvegarder dans un fichier texte en allant dans Application > Accessoires > Gedit éditeur de texte. Collez la clé publique d'un utilisateur et sauvegardez.

Ensuite, revenez à la gestion des Clés (presse-papier) et cliquez sur l'onglet Fichier > Importer et sélectionnez le fichier. La clé publique de cette personne va être importée dans votre trousseau de clés.

Pour ajouter les clés publiques futures à votre trousseau de clés, il est plus facile d'utiliser le même fichier et juste ajouter la clé suivante en dessous de la clé précédente. À chaque importation du fichier, toutes les nouvelles clés seront ajoutées. De cette façon, vous pourrez garder toutes les clés publiques **PGP** ensemble dans un fichier et l'enregistrer sur votre carte SD ou une clé USB pour une utilisation future.

Enfin, nous allons apprendre à crypter et décrypter les messages à l'aide de **PGP**.

## 3.2- PROCÉDURE DE CRYPTAGE D'UN MESSAGE AVEC UNE CLÉ PGP SUR TAILS

Avec l'applet **OpenPGP** de **Tails** vous pouvez chiffrer ou signer du texte en utilisant le chiffrement par clé publique d'**OpenPGP**.

Attention : écrire un texte confidentiel dans un navigateur web n'est pas sécurisé car des attaques JavaScript peuvent y accéder depuis ce même navigateur. Vous devriez plutôt écrire votre texte dans une autre application, le chiffrer en utilisant l'applet **OpenPGP** de Tails, et coller votre texte chiffré dans votre navigateur, avant de l'envoyer par email par exemple.

Lorsque vous utilisez l'Applet **OpenPGP** de Tails pour chiffrer des emails, les caractères non-**ASCII** (par exemple les caractères non-Latin ou avec des accents) peuvent ne pas s'afficher correctement pour le destinataire de l'email.

Si vous allez souvent crypter vos e-mails, nous vous recommandons d'utiliser « Icedove » qui se trouve dans les applications de **Tails**. C'est un logiciel de messagerie comme Thunderbird.

**1-** Ecrivez votre texte dans un éditeur de texte. Ne l'écrivez pas dans le navigateur web ! Cliquez sur l'Applet **OpenPGP** de Tails et choisir Ouvrir l'Éditeur de Texte pour ouvrir Gedit.

**2-** Sélectionnez avec la souris le texte que vous voulez crypter ou signer. Pour le copier dans le presse-papier, faire clic droit sur le texte sélectionné et choisir Copier dans le menu. L'Applet **OpenPGP** de Tails affiche désormais des lignes de texte, signifiant que le presse-papier contient du texte non-chiffré.

**3-** Cliquez sur l'Applet **OpenPGP** de Tails et choisir Signer/Chiffrer le presse-papier avec une clé publique dans le menu. Si vous obtenez le message d'erreur « Le presse-papier ne contient pas de données valides. », réessayez de copier votre texte depuis l'étape 2.

**4-** Si vous voulez chiffrer le texte, sélectionnez une ou plusieurs clés publiques pour les destinataires du texte chiffré dans la boîte de dialogue. Choisissez les clés des destinataires. Pour sélectionner une clé publique, double-cliquez sur la ligne correspondante dans la liste : Sélectionnez les destinataires.

**5-** Si vous voulez signer le texte, sélectionnez la clé privée avec laquelle vous voulez signer le texte dans le menu déroulant : Signer le message en tant que.

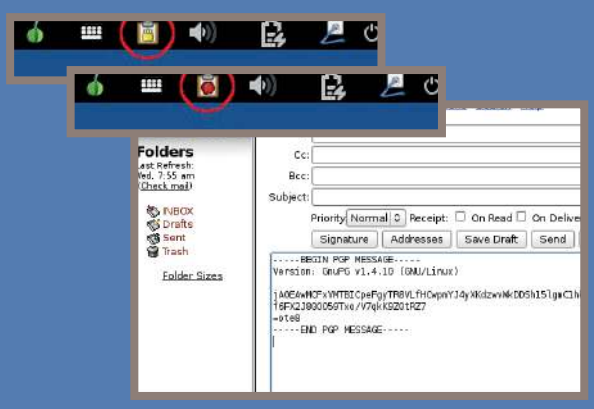
**6-** Si vous voulez masquer les destinataires du texte chiffré, cochez Cacher les destinataires. Sans quoi n'importe qui voyant le texte chiffré peut savoir qui en sont les destinataires.

**7-** Cliquez sur le bouton OK. Si vous obtenez l'avertissement Faites-vous confiance à ces clés ? Répondez-y en conséquence.

**8-** Si vous avez sélectionné une ou plusieurs clés publiques pour crypter le texte, l'Applet **OpenPGP** de **Tails** affiche désormais un cadenas signifiant que le presse-papier contient du texte chiffré.

Si vous avez seulement sélectionné une clé privée pour signer le texte, l'Applet **OpenPGP** de Tails affiche désormais un sceau, signifiant que le presse-papier contient du texte signé.

**9-** Pour coller le texte crypté ou signé dans une autre application, faire clic droit dans l'application où vous voulez le coller et choisir Coller dans le menu. Par exemple, vous pouvez le coller dans le navigateur web pour l'envoyer par email.



## 3.3- PROCÉDURE DE DÉRYPTAGE D'UN MESSAGE AVEC UNE CLÉ PGP SUR TAILS

Avec l'Applet **OpenPGP** de Tails vous pouvez décrypter du texte qui a été chiffré via **OpenPGP** ou vérifier du texte signé via **OpenPGP**.

1- Sélectionnez avec la souris le texte chiffré que vous voulez déchiffrer ou le texte signé que vous voulez vérifier en y incluant les lignes :

« -----BEGIN PGP MESSAGE----- » et « -----END PGP MESSAGE----- »

Pour le copier dans le presse-papier, faire clic droit sur le texte sélectionné et choisir Copier dans le menu.

**2-** Si le texte que vous avez sélectionné est chiffré, l'Applet **GnuPG** de **Tails** affiche désormais un cadenas, signifiant que le presse-papier contient du texte chiffré.

Si le texte que vous avez sélectionné est signé, mais pas chiffré, l'applet **GnuPG** de **Tails** affiche désormais un sceau, signifiant que le presse-papier contient du texte signé.

**3-** Cliquez sur l'applet **GnuPG** de **Tails** et choisir Déchiffrer/Vérifier le presse-papier dans le menu.

**4-** Si le texte que vous avez sélectionné est seulement signé et que la signature est valide, la fenêtre Résultat de **GnuPG** décrite à l'étape 6 apparaît directement.

Si le texte est signé et que la signature est invalide, vous obtiendrez un message Erreur de **GnuPG** qui mentionne MAUVAISE signature de…

Si le texte est chiffré avec une phrase de passe, une boîte de dialogue Phrase de passe apparaît. Entrez la phrase de passe qui a été utilisée pour chiffrer le texte et cliquez sur Valider.

Si le texte a été chiffré avec une clé publique, deux boîtes de dialogue différentes peuvent apparaître.

*a.* Si la phrase de passe pour la clé privée correspondante n'est pas déjà stockée en mémoire, une boîte de dialogue apparaît avec le message suivant : Vous avez besoin d'une phrase de passe pour déverrouiller la clé secrète pour l'utilisateur. Tapez la phrase de passe pour cette clé privée et cliquez sur Valider.

*b.* Si aucune clé privée pour laquelle le texte est chiffré n'est disponible dans votre trousseau, un message d'erreur **GnuPG** apparaît, mentionnant que le déchiffrement a échoué : la clé secrète n'est pas disponible.

**5-** Si la phrase de passe renseignée à l'étape 4 est incorrecte, une Erreur **GnuPG** apparaît, mentionnant que le déchiffrement a échoué : mauvaise clé.

**6-** Si la phrase de passe renseignée à l'étape 4 est correcte, ou si la signature du texte est valide, ou les deux, une fenêtre Résultat de **GnuPG** apparaît.

Le texte déchiffré apparaît dans une boîte de texte Voici la sortie de **GnuPG**.

Dans la partie Autres messages de **GnuPG** de la fenêtre, le message Bonne signature de… confirme que la signature du texte est valide.

# > CHAPITRE 3 - XMPP, JABBER, OTR
## Chat sécurisé

Communiquer en chat en ligne en toute sécurité via le protocole de messagerie **XMPP**/**Jabber**. L'explication qui suit va être faite pour windows7 mais la configuration est la même dans les autres distributions Macintosh ou encore Linux.

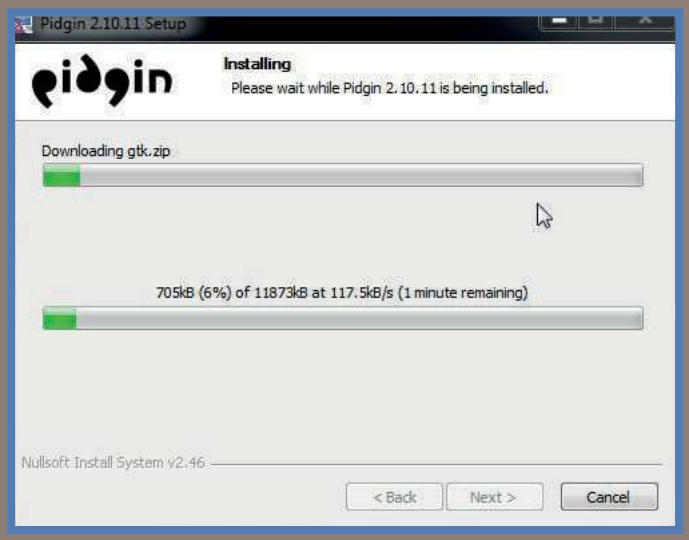
Pour **Tails**, inutile de l'installer, il est déjà intégré en haut a gauche de votre écran. Pour les autres distributions, voici le lien de téléchargement :

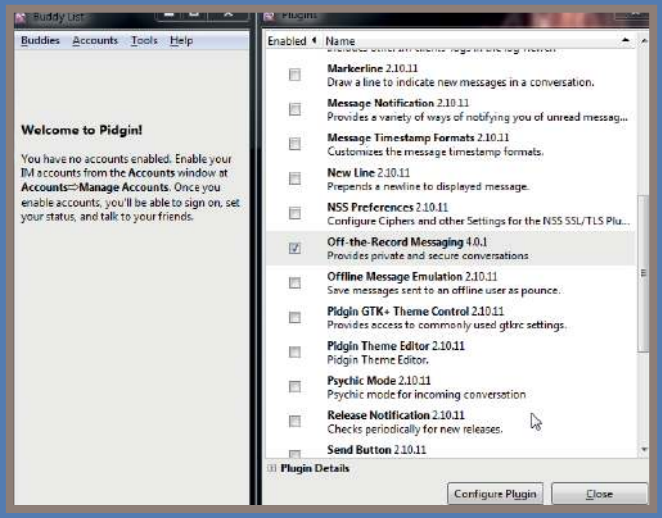
https://www.pidgin.im/download/

La première chose à faire est de télécharger le client **XMPP** appelé pidgin. Une fois téléchargé, effectuez l'installation comme un logiciel classique.

Une fois qu'il est installé, ne démarrez pas encore Pidgin. Deux fenêtres différentes vous seront présentées. Ignorez-les pour le moment. Nous devons d'abord télécharger et installer un second logiciel complémentaire qui nous permettra de chatter en toute sécurité. Il se nomme **OTR** « *Off-The-Record* » et peut être téléchargé via ce lien : https://otr.cypherpunks.ca/

Une fois téléchargé, installez-le. Assurez-vous que l'application Pidgin soit fermée, vérifiez aussi la barre des tâches en bas à droite de votre écran avant d'installer **OTR**.




**OTR** et Pidgin sont maintenant installés. Il ne nous reste plus qu'à effectuer quelques configurations simples sur Pidgin. La première chose que nous devons faire est de mettre le plugin **OTR** actif dans Pidgin.

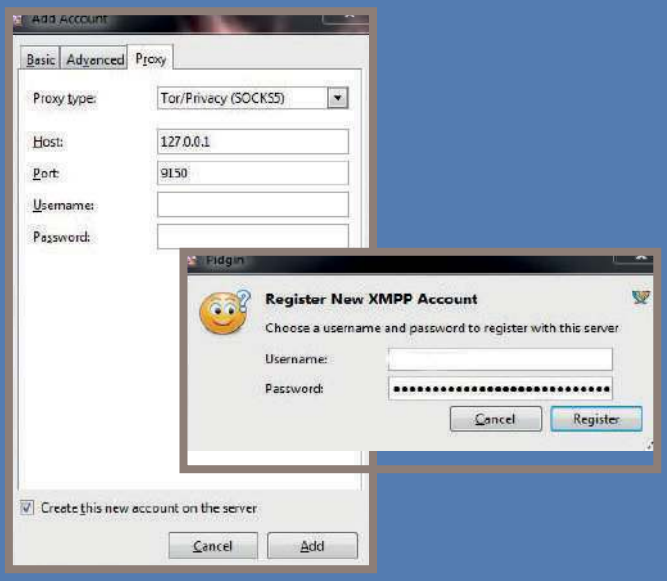
Ouvrez Pidgin, allez dans « Outils », choisissez « Plugins » et cochez la case de « *Off-The-Record Messaging* ». Il nous reste plus qu'a créer un nouveau compte **XMPP**. Pour l'exemple, je vais créer un nouveau compte avec le service de wtfismyip.com. Vous pouvez vous inscrire sans sortir de Pidgin.


La première étape pour vous enregistrer à partir du client sera d'entrer le nom d'utilisateur, mot de passe et le domaine. Le nom d'utilisateur et mot de passe seront ceux que vous souhaitez mais le domaine sera « wtfismyip.com » sans les guillemets. « Ressources » doit être laissé vide. Ensuite, cochez la case « Créer ce nouveau compte sur le serveur » au bas de l'écran. Comme sur l'illustration.

Si vous avez besoin d'une liste des fournisseurs de services gratuits **XMPP**, suivez le lien suivant : https://list.jabber.at/

Les prochaines étapes serviront à rendre encore plus sûres nos communications. Nous allons ajouter **TOR** comme un **proxy SOCKS5**, de sorte que non seulement les messages soient cryptés avec **OTR** mais aussi que le trafic soit chiffré avec **TOR**. Pour ce faire, cliquez sur l'onglet « ***Proxy*** » et définir votre « *hôte* » et « Port » en conséquence. Assurez-vous que **TOR** fonctionne bien, sinon vous aurez des erreurs de connexion.

Une fois ceci fait, cliquez sur le bouton « Ajouter », revenir à la « Liste d'amis », cliquez sur le menu « Comptes » vers le bas. Ensuite sur « Gérer les comptes » et enfin cliquez sur la case à côté de votre compte.





Ceci enverra la demande au serveur et vous demandera de confirmer votre nouveau compte. Si vous obtenez une erreur avec votre compte malgré avoir effectué toutes les étapes convenablement, il peut arriver que des erreurs se produisent avec le serveur. Pour résoudre ce souci, il suffit de vous inscrire en ligne sur le site Web de l'hôte **XMPP** que vous utilisez. (Comme vu via le lien fourni au-dessus). Il ne vous reste plus qu'à ajouter une personne avec qui chatter.

Pour sécuriser vos échanges, cliquez sur le bouton « **OTR** » dans la salle de chat, et cliquez sur « Démarrer avec une conversation privée ». Patientez quelques secondes et vous serez en conversation sécurisée via **XMPP**.

Vous pouvez également ajouter une sécurité supplémentaire : « Créer une question dont seul votre destinataire connait la réponse » et vous êtes sûr que votre interlocuteur est celui qu'il prétend être.

Dans tous ces différents sujets, nous avons appris comment se prémunir des adorateurs du ṭâghût en modifiant nos habitudes par différentes techniques simples à mettre en œuvre sur internet. Que vous vous trouviez en terre de mécréance ou en terre de fierté, ces précautions font parti de votre arsenal avec lequel vous pourrez combattre pour la vérité. Bien entendu, peu importe les moyens mis en place par les adorateurs du ṭâghût, nul ne peut nous nuire si ce n'est par la permission de Celui qui détient nos âmes entre Ses mains, le Seul garant de notre protection.

## > LEXIQUE

> CHAPITRE 1 :

**Adresse IP :** Une adresse IP est un numéro d'identification qui est attribué de façon permanente ou provisoire à chaque appareil connecté à un réseau informatique utilisant l'Internet Protocol.

**Adresse MAC :** Une adresse MAC est un identifiant physique stocké dans une carte réseau ou une interface réseau similaire et utilisé pour attribuer mondialement une adresse unique au niveau de la couche de liaison.

**TOR :** Tor est un réseau informatique superposé mondial et décentralisé. Il se compose d'un certain nombre de serveurs, dont la liste est publique, appelés nœuds du réseau, et permet d'anonymiser l'origine des connexions.

**Cryptage :** Le chiffrement est un procédé de cryptographie grâce auquel on souhaite rendre la compréhension d'un document impossible à toute personne qui n'a pas la clé de chiffrement.

**PGP :** «Pretty good privacy» est un système de cryptage populaire sur internet. En raison de l'architecture d'internet, les courriers électroniques peuvent être lus par n'importe quel ordinateur entre le destinataire et vous. PGP résoud ce problème en cryptant les données.

**Nœud :** Les nœuds sont des liens entre plusieurs machines sur un réseau.

**Protocole http, https :** L'HyperText Transfer Protocol, plus connu sous l'abréviation HTTP — littéralement « protocole de transfert hypertexte » — est un protocole de communication client-serveur développé pour le World Wide Web. HTTPS est la variante du HTTP sécurisée par l'usage des protocoles SSL ou TLS.

**Clé de chiffrage :** Une clé est un paramètre utilisé en entrée d'une opération cryptographique (chiffrement, déchiffrement, scellement, signature numérique, vérification de signature).

**Clé RSA :** Le chiffrement RSA (nommé par les initiales de ses trois inventeurs) est un algorithme de cryptographie asymétrique, très utilisé dans le commerce électronique, et plus généralement pour échanger des données confidentielles sur Internet.

> CHAPITRE 2 :

**Système Live :** Un live CD ou USB autonome - selon la traduction proposée par le projet Debian - est un CD/USB qui contient un système d'exploitation exécutable sans installation, qui se lance au démarrage de l'ordinateur.

**Virtual Box :** Logiciel de virtualisation permettant d'installer un système d'exploitation en parallèle au vôtre.

**Fichier ISO :** Le fichier ISO est une image virtuelle d'un CD/DVD.

**Linux** : Linux est le nom couramment donné à tout système d'exploitation libre fonctionnant avec le noyau Linux. C'est une implémentation libre du système UNIX.

**Bios :** Le Basic Input Output System (BIOS, en français : « système élémentaire d'entrée/sortie ») est, au sens strict, un ensemble de fonctions, contenu dans la mémoire morte (ROM) de la carte mère d'un ordinateur, lui permettant d'effectuer des opérations élémentaires lors de sa mise sous tension. Par exemple, la lecture d'un secteur sur un disque. Par extension, le terme est souvent utilisé pour décrire l'ensemble du micrologiciel de la carte mère.

**Boot :** Il s'agit du processus de démarrage de l'ordinateur.

**Terminal (console) :** interface de gestion en ligne de commande permettant d'effectuer des tâches diverses.

> CHAPITRE 3 :

**ASCII :** L'American Standard Code for Information Interchange, plus connu sous l'acronyme ASCII est une norme de codage de caractères en informatique ancienne et connue pour son influence incontournable sur les codages de caractères qui lui ont succédé.

**GnuPG :** GnuPG est l'implémentation GNU du standard OpenPGP défini dans la RFC 4880. Il est distribué selon les termes de la GNU GPL. Il permet à ses utilisateurs de transmettre des messages signés ou chiffrés.

**XMPP :** Extensible Messaging and Presence Protocol, souvent abrégé en XMPP, est un ensemble de protocoles standards ouverts de l'Internet Engineering Task Force pour la messagerie instantanée, et plus généralement une architecture décentralisée d'échange de données.

**Jabber :** Jabber est un protocole de messagerie instantanée.

**OTR :** Off-the-Record Messaging, appelé communément OTR, est un protocole cryptographique.

**Proxy :** Un proxy est un composant logiciel qui joue le rôle d'intermédiaire en se plaçant entre deux autres pour faciliter ou surveiller leurs échanges.

**SOCKS :** SOCKS est un protocole réseau qui permet à des applications client-serveur d'employer d'une manière transparente les services d'un pare-feu. SOCKS est l'abréviation du terme anglophone « sockets » et « Secured Over Credential-based Kerberos ».