SÉCURITÉ INFORMATIQUE

> CHAPITRE 1 - CRYPTER ENTIÈREMENT SON TÉLÉPHONE

Si vous possédez des données sensibles dans votre smartphone, il serait dommage de les laisser à la portée de tous et, en particulier, des autorités. Il est alors possible de crypter entièrement le contenu de votre smartphone Android, ce qui s'avère très utile en cas de perquisition, de garde à vue ou, tout simplement, de personnes indiscrètes dans votre entourage. Il faut tout de même prendre en compte que pour les smartphones Android de la version inférieure à 5.0, il y a des risques et donc il ne faut pas se fier entièrement à cette méthode. Mais à partir d'Android 5.0, Google a renforcé son système de cryptage en utilisant des clés **128bits** ensuite **hashées (SHA256)**, ce qui reste correctement fiable de nos jours. Le fait de crypter votre téléphone vous permettra de rentrer un **code PIN** à chaque fois que vous allumerez votre téléphone. Voyons maintenant comment procéder.

Il est important de noter qu'une fois que vous commencerez le processus de chiffrage de votre smartphone, vous ne pourrez plus faire machine arrière à moins de réinitialiser votre smartphone dans sa valeur d'usine. Le cas échéant, vous perdrez toutes vos données par la suite.

1- OPTIONS DE SECURITE :

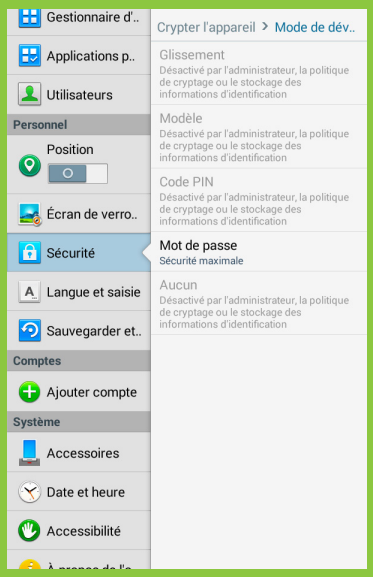
Avant de commencer l'opération, vous pouvez faire une sauvegarde de vos données. Ensuite, allez dans « *Paramètres* » puis sélectionnez « *Sécurité* ». En fonction de la version d'Android ou de la marque de votre téléphone, sélectionnez « *Chiffrer l'appareil* » ou « *Crypter le téléphone* », les deux signifiant la même chose.

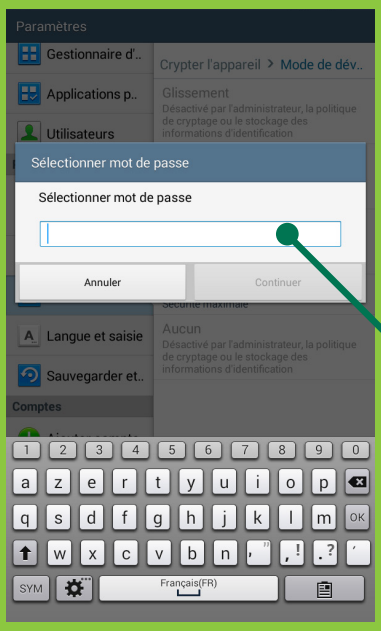
PRECAUTIONS :

Assurez-vous que votre téléphone a au **minimum 80-90% de batterie** ou qu'il soit **branché sur la prise secteur.** Si le téléphone s'éteint en plein milieu de l'opération, **vous perdrez alors toutes vos données.** Le processus de cryptage de l'appareil peut durer plus d'une heure selon le modèle et la puissance.

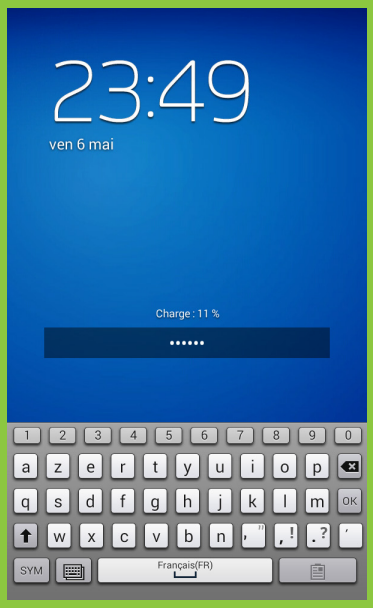
2- METHODE DE VERROUILLAGE :

Vous serez par la suite invité à choisir une méthode de verrouillage du téléphone. Une fois encore, les options divergent selon la version d'Android mais une des meilleures méthodes reste celle du « *mot de passe* ». Cela donnera du fil à retordre aux petits malins utilisant des méthodes de **Force Brute** pour casser vos codes. Choisissez un mot de passe assez long avec caractères variés.





Choisissez alors votre mot de passe, il vous sera ensuite demander de le confirmer pour éviter les erreurs de frappe.



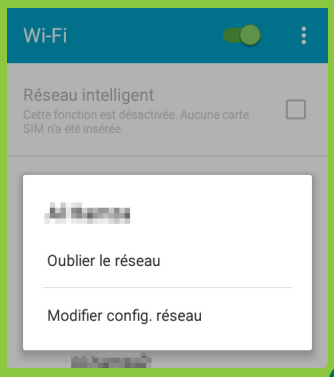
À ce moment-là, cliquez sur « *Crypter l'appareil* » et patienter jusqu'à la fin. Le processus peut prendre beaucoup de temps et votre smartphone est susceptible de redémarrer à plusieurs reprises durant l'opération. Laissez-le processus avancer et, une fois fini, vous devriez voir votre appareil qui vous demande le mot de passe choisi précédemment. Et voilà, votre smartphone Android est crypté ! Ne fournissez votre mot de passe à personne et faites en sorte qu'il ne comprenne aucune information personnelle (date de naissance, nom, ou autres).

> CHAPITRE 2 - UTILISATION DES COMMUNICATIONS SÉCURISÉES

Installation & utilisation d'ORBOT et ORFOX (Tor), Appel via le protocole ZRTP, Discussions avec le protocole XMPP via ChatSecure

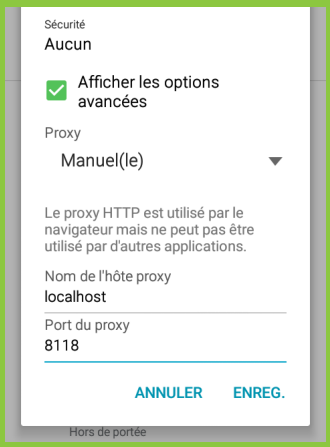
1- INSTALLATION & UTILISATION D'ORBOT ET ORFOX

Si vous utilisez un réseau wifi avec votre smartphone Android, il faut, au préalable, modifier un paramètre. Allez donc dans le menu wifi et, en laissant votre doigt appuyé sur le réseau wifi de votre choix, un menu va apparaître. Sélectionnez ainsi « *Modifier le réseau* ».



1

Cochez la case « *Afficher les options avancées* » afin de laisser apparaître le menu souhaité. Dans la section « ***Proxy*** », sélectionnez « *Manuel* ». Puis, dans « Nom du Proxy », écrivez « *localhost* » et dans « ***Port*** », écrivez « *8118* ».



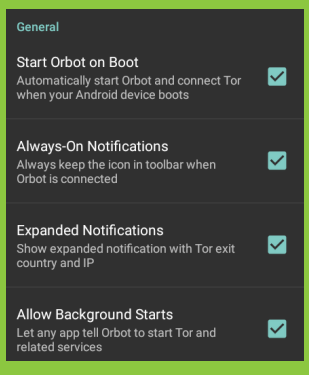
2

Téléchargez maintenant l'application **ORBOT** via le lien suivant : https://copy.com/k9DtKdlEJdx-qbSpN/ORBOT.apk?download=1

Installez-la et lancez-la. Afin d'activer **ORBOT**, il vous faut tout simplement laisser votre doigt appuyé sur le milieu de l'application. Quand cela devient coloré, l'application est activée. Si elle est grisée, elle est alors désactivée.

Cliquez ensuite sur « ***VPN*** » qui cryptera la connexion de vos applications lorsqu'il est activé.

3



Appuyez sur l'icône « *Paramètre* » en haut à droite de l'application et cochez les options suivantes : « *Start Orbot on boot* » (Démarrer Orbot au démarrage) ; « *Always on notification* » (Toujours dans les notifications) ; « *Expanded notification* » (Permet de montrer les IPs utilisées ainsi que les pays) ; « *Transparent proxying* » (Fait passer les applications par le réseau **TOR** automatiquement. Cette option nécessite d'avoir rooté le smartphone).

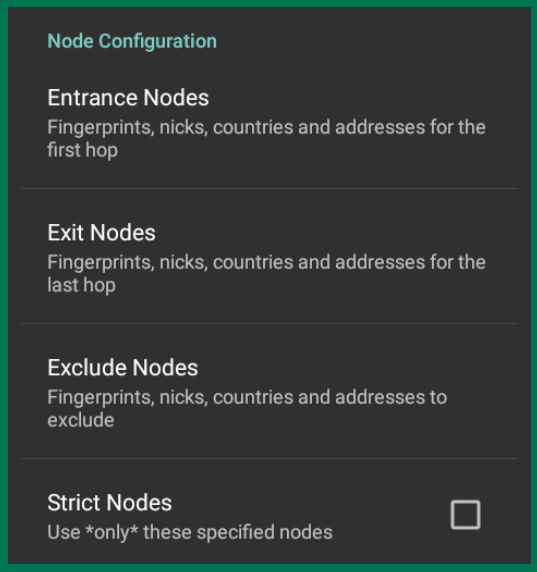
4

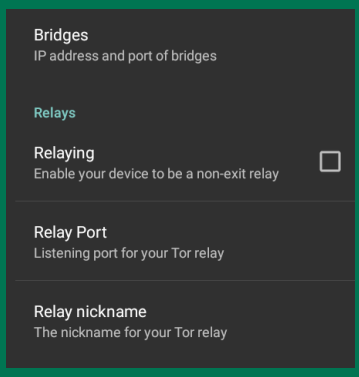
5

La partie qui suit est un peu plus complexe que la précédente. Allez dans « *Entrance Nodes* » (Nœuds d'entrés) et coller ceci **{ch}, {fi}, {ro}, {no}, {au}**. Cette option permet de limiter les pays par lesquels va passer votre réseau tels que la Suisse, la Roumanie ainsi que d'autres.

Allez maintenant dans « *Exit Nodes* » (Nœuds de sorties). Cela se réfère à la fin du trafic du réseau qui se fera uniquement par les pays sélectionnés. Ajouter alors **{ch}, {fi}, {ro}, {no}, {au}**.

Ensuite, sélectionnez « *Exclude Nodes* » (Nœuds exclus) pour définir les pays à exclure du trafic. Ajoutez alors **{fr}, {be}** pour la France et la Belgique, par exemple. Vous pouvez trouver la liste des codes des pays que vous souhaitez ajouter aux listes d'exclusion via le lien suivant : https://b3rn3d.herokuapp.com/blog/2014/03/05/tor-country-codes





Maintenant, afin de diminuer les failles de sécurité, sélectionnez « *Use **Bridges*** » (Utiliser des ponts).

6

7

Rendez-vous sur le lien suivant pour obtenir vos bridges, https://bridges.torproject.org. Cliquez ensuite sur « *Récupérez les adresses de **bridge*** ». Puis, « *Donnez-moi juste des bridges !* »

Une fois récupérés, vous devez copier uniquement la section de l'adresse IP, c'est-à-dire, par exemple, comme sur l'image : **37.218.246.200 :17706**, et collez-la dans « ***Bridges*** ». Redémarrez ensuite le téléphone afin que les bridges soient pris en compte.

```
37.218.246.200:17706 DD21A53C559121FA9AEE684FD51767816A0C9495
194.132.208.40:21359 081F47EE4831F19CB85B32C44D0C60500DC30B77
107.191.58.23:443 225A895211B179FDE2E8F8E35BE8EE5C8BECC0B0
```

Maintenant, vous devez installer l'application **ORFOX** (un navigateur **TOR**), disponible via le lien suivant ou ailleurs sur internet : http://www.apkmirror.com/wp-content/themes/APKMirror/download.php?id=16661, ce navigateur fonctionne uniquement sous le réseau **TOR** donc si l'application **ORBOT** n'est pas active, le navigateur **ORFOX** ne fonctionnera pas.

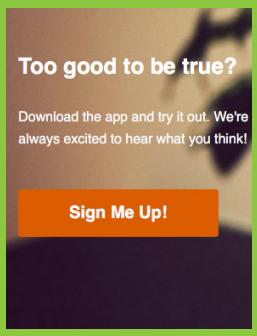
8

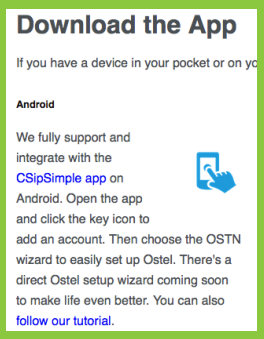
Vous devriez maintenant avoir un **VPN** (**ORBOT**) et un navigateur **TOR** (**ORFOX**).

2- APPELS VIA LE PROTOCOLE ZRTP

1

Inscrivez-vous sur le site ostel.co. En bas de la page, sélectionnez « *Sign up* » (s'inscrire). Vos informations vous seront alors envoyées par e-mail à la fin du processus d'inscription.





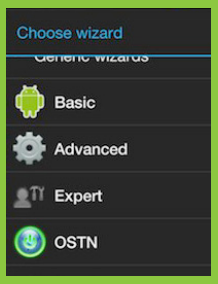
Téléchargez ensuite l'application **CSipSimple**. Changez alors votre adresse IP pour plus d'anonymat. Allez dans **ORBOT**/Paramètres/Select Apps/ (cochez **csipsimple**) afin que l'application utilise le réseau **TOR** pour fonctionner. Vous pouvez tout aussi bien utiliser un **VPN** lors de l'utilisation de l'application si vous ne possédez pas **TOR** sur votre smartphone.

Google play

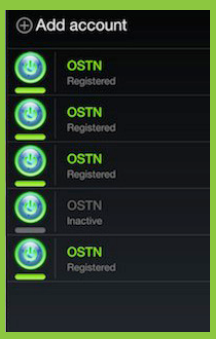
2

3

Ouvrez **CSipSimple.** Sélectionnez « *Ajouter un compte* » en haut à droite et choisissez « ***OSTN*** » (Open Secure Telephony Network) en mode expert.



4

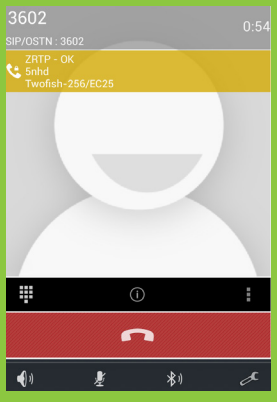


Entrez alors les informations reçus par e-mail lors de votre inscription sur le site internet d'*Ostel*. Pour confirmer que votre compte est actif et enregistré, vous devez voir **OSTN** devenir vert.

5

Vous pouvez effectuer un test en appelant le *9196* pour tester la ligne. Il s'agit d'un écho test afin de confirmer que la communication est bien établie. Vous devez être en mesure d'entendre votre voix en retour durant cet appel.

Pour communiquer, ajouter une personne, en entrant son nom d'utilisateur exemple « *votreami@ostel.co* ». Avant la connexion, une petite fenêtre s'ouvrira sur votre écran, vous confirmant un code. Votre interlocuteur recevra ensuite le même code afin de vous assurer que votre connexion est opérationnelle et sécurisée.



3- DISCUSSIONS AVEC LE PROTOCOLES XMPP VIA CHATSECURE

ChatSecure est une application libre pour téléphones iPhone et Android permettant aux utilisateurs de communiquer en toute confidentialité. **ChatSecure** permet aux utilisateurs d'envoyer des messages instantanés et de chatter en utilisant un téléphone portable, au lieu de l'ordinateur traditionnel de bureau ou portable.

ChatSecure admet le chiffrement **OTR** (OFF The Record, vu dans le numéro précédent de *DAR AL-ISLAM*) moyennant **XMPP**. Tous les messages envoyés via ChatSecure sont totalement privés, sous réserve que la personne avec qui vous chattez utilise également un client de messagerie instantanée compatible **OTR** comme **ChatSecure** (Android), **Adium** (Mac OS X), **Pidgin** (Windows & Linux). L'application permet d'envoyer des messages audio, des photos, des fichiers ou du texte.

Lorsque vous envoyez un message en utilisant **ChatSecure**, il n'est pas stocké dans la mémoire du système du téléphone. **ChatSecure**, utilisée avec le module de confidentialité **ORBOT**, doit être capable de contourner tous les pare-feu, les restrictions du réseau et les listes noires. L'application peut gérer des comptes multiples. Vous pouvez donc chatter avec vos amis sur Facebook, vos contacts de Google ou autres utilisateurs soucieux de leur intimité à condition qu'ils utilisent aussi un programme de messagerie instantanée admettant le chiffrement **OTR**.

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

Une fois votre compte ajouté, saisissez votre nom d'utilisateur (ou adresse e-mail) et mot de passe afin de vous inscrire. Vos contacts devraient automatiquement être exportés.

Afin d'ajouter un deuxième ou un troisième compte, cliquez sur l'onglet « *Comptes* » du menu. En haut à droite, cliquez sur le signe « + ». Vous pouvez choisir d'ajouter un compte existant par exemple celui que vous avez créé dans **Pidgin** sous **Tails OS** (vu dans le numéro précédent de *DAR AL-ISLAM*) ou de créer un nouveau compte.

a. Télécharger et installer ChatSecure

Visitez Google Play Store et cherchez ChatSecure par The Guardian Project. Sélectionnez « *Installer* » et accepter les Conditions du Service en cliquant sur « *Accepter* ». L'application se téléchargera et s'installera automatiquement.

https://play.google.com/store/apps/details?id=info.guardianproject.otr.app.im

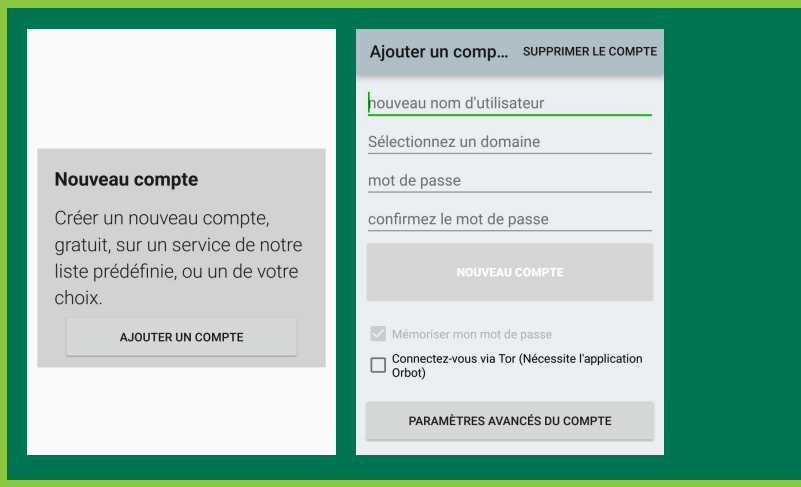
b. Ouvrez l'application et configurez votre mot de passe

Lorsque vous ouvrez l'application, il vous sera proposé de configurer un mot de passe. Vous devrez également créer une phrase de passe afin de chiffrer vos données localement. Si vous choisissez cette technique, vos données seront chiffrées en transit, ainsi que localement sur votre téléphone.

Si vous choisissez de passer outre cette étape, vos messages seront toujours chiffrés en transit, mais ne seront pas protégés sur votre téléphone.

c. Configurer vos comptes

Vous pouvez ajouter une variété de différents comptes à votre application **ChatSecure**. Afin d'ajouter un service de messagerie **XMPP** ou **Jabber**, choisissez « *Jabber (XMPP)*. »

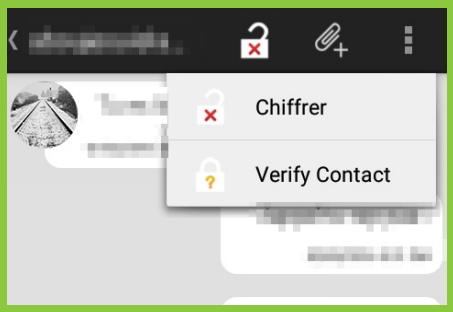


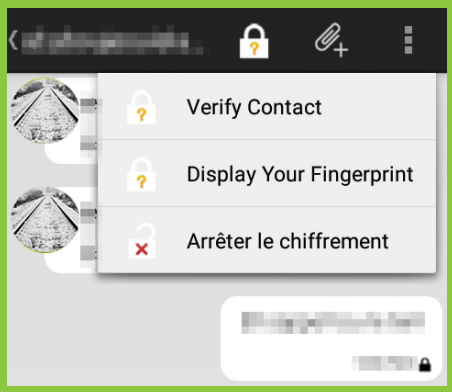
d. Enregistrer vos comptes

Afin de procéder à l'enregistrerement votre compte, cliquez sur l'onglet « *comptes* » du menu et activez les comptes que vous souhaitez utiliser. Une fois connecté, quiconque peut communiquer avec vous à partir d'un téléphone portable ou une application de messagerie instantanée sur un ordinateur de bureau.

e) Démarrer le chiffrement global

Une fois que vous avez commencé à chatter avec quelqu'un, cliquez sur l'icône déverrouillé en haut de la barre du menu affiché. Choisissez « *Chiffrer* » Si la personne avec qui vous chattez possède un système de messagerie instantanée compatible **OTR**, vous disposerez de l'option « *Vérifier votre empreinte digitale* » (et la sienne).





ChatSecure offre trois manières de vérifier les empreintes digitales **OTR**, mais si vous chattez avec quelqu'un sur la messagerie instantanée d'un ordinateur de bureau et non moyennant **ChatSecure**, la meilleure manière de vérifier une empreinte digitale **OTR** est de communiquer via un autre réseau.

Vous pouvez renvoyer votre empreinte digitale par SMS (TextSecure), la communiquer par téléphone si vous reconnaissez la voix des autres, utiliser **PGP** ou la vérifier en personne. Cliquez sur « *vérification manuelle* » et **ChatSecure** affichera votre empreinte digitale, ainsi que celle de vos amis. Si vous pouvez tous confirmer que vous disposez de la même information en posant une question dont la réponse est connue seulement de l'interlocuteur à vérifier, alors vous pouvez cliquer sur « *vérifier* »

ChatSecure admet la vérification manuelle ou au moyen d'un scanner de code-barres de l'autre utilisateur (**QR**). Si vous vous trouvez dans la même pièce que l'autre personne, vous pouvez aisément scanner le code-barres sur son téléphone ou lire vos codes à haute voix l'un à l'autre.

f) Connaître vos options

Tout comme le service de messagerie instantanée d'un ordinateur de bureau, **ChatSecure** vous offre l'option d'apparaître hors ligne, occupé, inoccupé ou parti. Afin de modifier cette configuration, cliquez sur votre nom en haut de la liste de vos amis.

ChatSecure vous permet également de créer des groupes de chat et d'ajouter de nouveaux contacts, ce qui peut se faire à partir du menu principal. (Tenez compte du fait que les chats de groupe ne sont pas sécurisés comme les chats privés étant donné les limitations du protocole **OTR**).

L'Application permet aussi la messagerie multimédia, prise de photos, ainsi qu'envoyer des photos et des fichiers de manière sécurisée si vos amis utilisent le chiffrement global et que vous pouvez vérifier leur identité.

ChatSecure vous offre l'option de créer un nouveau compte de messagerie **XMPP** ou **Jabber** permettant le chiffrement **OTR**.

Dans « *Settings* » (Paramètres) de l'application, vous pouvez activer le passage par **ORBOT** afin que vos communications **ChatSecure** passent par le réseau **TOR** et ainsi ajouter une couche de sécurité supplémentaire.

Chiffrez vos SMS avec SMS Secure **Lien :** https://goo.gl/tEKD3v

SMS Secure se rajoute à l'application de base d'envoi de SMS de l'appareil et vous propose de chiffrer en **256bits** vos SMS/MMS avant de les envoyer. Ce qui rend la tâche un peut plus difficile à toutes personnes qui souhaiteraient intercepter vos messages, en remplaçant les caractères par des caractères incompréhensibles. Pour que l'application fonctionne, il faut que le destinataire du SMS/MMS ai lui aussi l'application d'installé sur son smartphone.

> CHAPITRE 3 - UTILISATION DES MESSAGES CRYPTÉS PGP POUR ANDROID

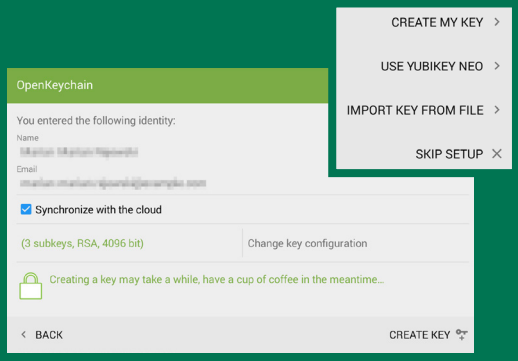
Téléchargez l'application **OpenKeychain** via le **GooglePlay Store** ou via internet et installez-la.
https://play.google.com/store/apps/details?id=org.sufficientlysecure.keychain

Créer votre clé PGP personnelle :

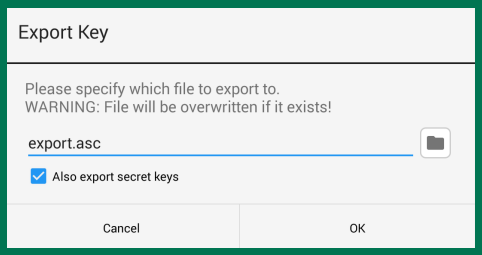
1

En créant votre clé **PGP** personnelle, vous serez en mesure de lire des fichiers ou textes cryptés afin de rendre votre correspondance complétement illisible par les ṭawâghît. Cliquez sur « *Create my key* » (Créer ma clé).

Entrez toutes les informations demandées et cliquez ensuite sur « *Create key* » (Créer la clé). Aucun changement de paramètres n'est nécessaire ici. Patientez ensuite quelques instants et votre clé sera enfin créée.



Exporter votre clé personnelle :



2

Attention : vous ne devez en aucun cas perdre votre clé privée personnelle.

Il faut absolument l'exporter et la stocker dans un endroit sûr. Cliquez pour cela sur votre clé et sélectionnez « *export* » (exporter). Sélectionnez également « *Export also secret keys* » (exporter aussi les clés secrètes).

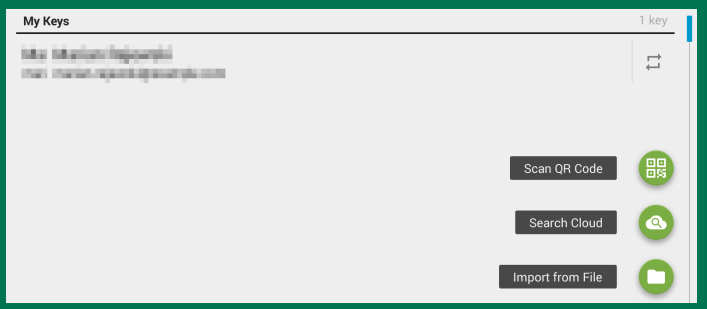
Ce fichier doit être stocké dans un endroit sûr, c'est-à-dire une clé USB ou une carte SD que vous dissimulerez dans un endroit auquel personne d'autre que vous ne pourrait penser.

Importer les clés de vos interlocuteurs :

3

Avant de chiffrer ou de déchiffrer des éléments, vous devez obtenir la clé publique de votre interlocuteur (comme vu dans le numéro précédent de *DAR AL-ISLAM*).

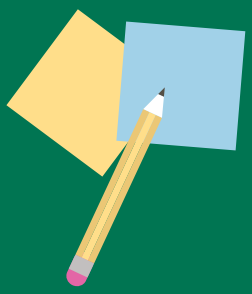
Vous pouvez importer une clé d'un fichier si celle-ci vous est envoyée par un de vos interlocuteurs en suivant les mêmes étapes, mais en choisissant « *Import from file* » (importer à partir d'un fichier).



Encrypter et Décrypter :

4

Vous pouvez chiffrer des fichiers ou des textes dans le menu en haut à gauche de l'application « *Chiffrer / Déchiffrer* » et ensuite sélectionnez le fichier désiré.



> LEXIQUE

> CHAPITRE 1 :

Hachage (SHA 256) : On nomme fonction de hachage une fonction particulière qui, à partir d'une donnée fournie en entrée, calcule une empreinte servant à identifier rapidement, bien qu'incomplètement, la donnée initiale. Les fonctions de hachage sont utilisées en informatique et en cryptographie.

Bits : Le bit est l'unité binaire de quantité d'information la plus simple dans un système de numération, ne pouvant prendre que deux valeurs, désignées le plus souvent par les chiffres 0 et 1.

Code PIN : Le code PIN (Personal Identification Number ou numéro d'identification personnel) est un code d'identification personnel qui permet de sécuriser l'accès à votre appareil.

Force Brute : L'attaque par force brute est une méthode utilisée en cryptanalyse pour trouver un mot de passe ou une clé. Il s'agit de tester, une à une, toutes les combinaisons possibles. Cette méthode est en général considérée comme la plus simple concevable.

> CHAPITRE 2 :

VPN : Définition du VPN. Le terme VPN (Virtual Private Network) ou réseau privé virtuel

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.

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.

Port : Composant du réseau TCP/IP (connection Internet) qui permet de diviser les types de communication que l'on veut avoir entre les ordinateurs. Les connections actuelles permettent d'en avoir 65536.

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.

QR code : QR code est l'acronyme de Quick Response Code ou code barre 2D. Alors que le code barre classique ne permet qu'un codage horizontal, le QR code est en deux dimensions et comprend donc plus d'informations.

> CHAPITRE 3 :

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.