



## La cryptographie avec GnuPG Sous Linux

Campus Numérique Francophone de Tripoli

Yemen.sayour@auf.org

# GnuPG



## Fonctionnement

## Exemple d'utilisation

# Présentation

- GnuPG est la version GNU de PGP permet de transmettre des messages signés et/ou chiffrés.
- il existe deux types de chiffrement : à clés asymétriques et à clés symétriques, GPG permet de chiffrer des communications par le biais d'un algorithme de chiffrement à clés asymétriques en assurant la confidentialité
- La signature numérique est un mécanisme permettant de garantir l'intégrité d'un document électronique et d'en authentifier l'auteur

# Fonctionnement



## **Installation Gnugp**

L'installation de GnuPG passe par les étapes suivants :

► Installation de programme GnuPG.

\$ sudo aptitude install gnupg

Génération des clefs

- Décider votre passphrase
- Générez votre propre paire de clés
- Générer la paire de clés
- Confirmer la paire de clés
- Une sauvegarde de votre porte-clés



## Serveurs des clés

Les types par defaut sont :

\* HKP pour les serveurs de type Horowitz ou compatible.
\* LDAP pour les serveurs de type NAI LDAP.
\*MAILTO pour les serveurs de clés par mail de type Horowitz.

\$ gpg --send-keys maclé --keyserver ldap://serveurdeclef permet d'exporter la clé maclé vers un serveur de clés.

#### Créer un certificat de révocation

La clé de révocation permet d'annuler la validité d'une clé.

\$ gpg --gen-revoke maclé --output certificat

#### Exporter la clé publique

\$ gpg --armor --export Nom d'utilisateur --output cle\_utilisateur

### Importer une clé publique

\$ gpg --import blake.gpg

### Chiffrer le courriel avec Mozilla Thunderbird et Enigmail

Thunderbird grâce à l'extension Enigmail permet de lire et d'envoyer des courriels chiffrés.

- \* Thunderbird, le client de messagerie
- \* GnuPG, le programme de chiffrement
- \* Enigmail, l'extension nécessaire au chiffrement de courriels





## Enigmail

1- Installation du paquet **enigmail** depuis le gestionnaire de paquets synaptic

#### 2- Configuration deTthunderbird

#### • vérification de la liaison entre enigmail et gpg.

Dans Thunderbird, Ouvrez le menu OpenPGP  $\rightarrow$  Préférences.Dans l'onglet Général, assurez-vous d'avoir un message comme GnuPG trouvé dans /usr/bin/gpg.

#### • Activer Enigmail pour un compte

Allez dans la sous-catégorie Sécurité OpenPGP et choisissez Activer le support OpenPGP (Enigmail) pour ce compte.

## **Configuration Enigmail**

Baramètres des comptes Cour	rier et Groupes		
– mimicate52@hotmail.com Paramètres serveur	Options OpenPGP (Enigmail)		
Copies et dossiers Rédaction et adressage Paramètres des indésirables Espace disque OpenPGP Accuses de réception Sécurité Dossiers locaux Paramètres des indésirables Espace disque Serveur sortant (SMTP)	Enigmail fournit le support OpenPGP pour le chiffrement et la signature de messages. Il est nécessaire d'avoir le logiciel GnuPG (gpg) pour utiliser cette fonctionnalité.		
<u>G</u> estion des comptes	▼ ⊗Annuler ⊘OK		

### Sélection des clés des destinataires

Préférences OpenPGP		
Général Envoi Sélection clef	Avancé Serveur de clefs	Débogage
Comportement du choix d O Suivant les règles établie O Suivant les règles et les	<b>les clefs</b> es uniquement adresses de messagerie	
Suivant les adresses de l	messagerie	
🖰 Manuellement		
<ul> <li>Pas de sélection manuell</li> </ul>	le	
		Modifier les règles
		🔞 Annuler 🛛 🎻 OK

<b>E</b> ichier Édition <u>Affichage</u> <u>Insérer Format</u> <u>Options</u> Ope <u>n</u> PGP O <u>u</u> tils Aid <u>e</u>	
Envoyer 🖉 Orthographe 🔻 🖉 Joindre 🔻 🙀 OpenPGP 🔻 🖴 S/MIME 🔻	Enregistrer 🔻
Expéditeur : Rein nasser <mimicate52@hotmail.com></mimicate52@hotmail.com>	1170.
Pour :      yemen_sayour@hotmail.com	
Sujet : signer et chiffrer un message	
Texte principal v Largeur variable v K A a a	Chiffrement Open
	Chiffr <u>e</u> r le message
	Utiliser PGP/MIME
	⊗Annuler  ⊘OK
Sélection de clef OpenPGP	N
Sélectionnez la ou les clefs OpenPGP à utiliser pour	
Compte / ID utilisateur Confia	Expi Identifi 🛤
<ul> <li>Rein nasser (tester gpg) <mimicate52@hotmail.com> confiance</mimicate52@hotmail.com></li> <li>yemen sayour (signer des mails) <yemen_sayour@hotma< li=""> </yemen_sayour@hotma<></li></ul>	. 2C4B7B53 924A4828

Télécharger les clefs manquantes

Annuler

JOK

Rafraîchir la liste des clefs

Chiffrer et signer le message Envoyé en même temps

#### Sélection du clé qui va chiffrer le message



Déverrouillage de la clé secrète par la passephrase

	S En	voi des messages - signer un message 🛛 🕺
BEGIN PGP SIGNED Hash: SHA1	Statut : Progression :	Connecté à smtp.live.com
signer un message BEGIN PGP SIGNAT		Annuler
Version: GnuPG v1.4.1	0 (GNU/Linux)	
Comment: Using GnuF	G with Mozilla	a - http://enigmail.mozdev.org/

iJwEAQECAAYFAk5YfJ0ACgkQg3BdMJJKSCgUUgQAniPqUov3JOUOwBylwmmApAlf pY+6rSA3+MIPIvQxHrqzFWduLi/A0zCFswC+5hBXz4OiEwMTvsC53Uqm2GtHAhjt wObtUepzaPZEa4JPeOitWTUrseVSW7s/QIvq2+t8HB1QY3gWyOAzleJJVHKYd6GN blcn44PXymbnocfsF3s= =ODP8 -----END PGP SIGNATURE----- Envoie d'un message signé et chiffré

chiffrer le message	pinentry	
de Rein nasser <mimicate52@ho sujet chiffrer le message pour Vous-mêmeta</mimicate52@ho 	Vous avez besoin d'une phrase de passe pour la clé secrète pour l'utilisateur: "yemen sayour (signer des mails) <yemen_sayour@hotmail.com>" clé 1024 bits RSA, ID DDA22356, créée 2011-0 principale 924A4828)</yemen_sayour@hotmail.com>	Déchiffrage d'un message
Charset: ISO-8859-1 Charset: ISO-8859-1 Version: GnuPG v1.4.10 (GNU/Linux) Comment: Using GnuPG with Mozilla hIwDrSLjmt2iIIYBBACQgTY+oZxAEfn7R ktgiCscbpP55scFldG8uIAFofORoeIWY4 Snl96q0EcHGotyGJ8LhfWiOU9n2/EZptBjQ25 Axow6600YtDSAQP/WudoyoGzc99kCXJL7at5 yKrzwMNTfJzlXNx4b2vMu9zgsUMJsuktqYD6 I2TESdCYTr/LZeGsZOQbhdOnaYO082zX3VI1 vc44eirQWhYLJ+7RYiYtSQQkuOilJT2VZJPr Jku0WrQpqGKRuwlChFi5K2r6ET7azQixrsDx =SZKh	Passphrase Annuler PkLUGINb5CtXrRUplBsnONmYi4SM NEnryvCG8LTnwpxLBRU3/aBAyOlz pu7ozMrjXk2uXlgflBwZjijgeaBV IFwLE5JdPgCZ95y11UxDBdLSWQEz NRyfQwdypNhcuHRCbXyKqusgFzBI Ao7i/S2syA+W5YSO	reçu par la phrase de passe de destinataire



Mail déchiffré

chiffrage d'un mail

## Chiffrage d'un dossier ou fichier openoffice

- ► installer le paquet seahorse-plugins
- clique droit sur le dossier,

#### Signer le fichier



				_
	Nom		Identifiant de la clé	
	Rein nasser <min< td=""><td>nicate52@hotmail.com&gt; (</td><td>2C4B7B53</td><td></td></min<>	nicate52@hotmail.com> (	2C4B7B53	
2	yemen sayour <y< td=""><td>emen_sayour@hotmail.co</td><td>924A4828</td><td></td></y<>	emen_sayour@hotmail.co	924A4828	
				11 J. P.



#### Question OpenPGP

Ce message contient des pièces jointes. Comment souhaitez-vous les chiffrer/signer ?

- Ohiffrer uniquement le texte du message mais pas les pièces jointes
- Chiffrer chaque pièce jointe séparément et envoyer le message en utilisant PGP à la volée
- O Chiffer/signer le message en entier et l'envoyer en utilisant PGP/MIME

PGP/MIME n'est supporté que par un nombre limité de logiciels de messagerie ! Sous Windows seuls Mozilla/Thunderbird, Sylpheed, Pegasus et Mulberry sont connus pour supporter ce standard; sous Linux, UNIX et MacOS X la plupart des logiciels de messagerie le supporte. Dans le doute, sélectionnez la seconde option.

Utiliser dorénavant la méthode sélectionnée pour toutes les pièces jointes



Lors de l'envoie d'un message contenant une pièce jointe chiffrée

Pour déverrouiller une pièce jointe on fait C.D déchiffrer et ouvrir

#### Chiffrer une communication de messagerie instantanée sous Pidgin

► Installation de plugin OTR

Configuration : outils\_plugins\_OTR

$\underline{\otimes} \odot \odot$	Plugins	
Activé	Nom 🔻	*
	Intégration avec Evolution 2.6.6 Fournit une intégration avec Evolution.	
	Lecteur d'archives 2.6.6 Inclut les archives d'autres clients de messageri	
	<b>Ligne de repère</b> 2.6.6 Tracer une ligne pour indiquer les nouveaux mes	
2	Messagerie Confidentiel 'Off-the-Record' 3 Offrir les conversations privées et en sûreté	
	Messagerie musicale 2.6.6 Plugin de messagerie musicale pour la composit	
	Mode psychique 2.6.6 Mode psychique pour le début des nouvelles con	~
	Mouvements de souris 2.6.6 Fournit le support pour les mouvements de souris.	
	Notification de changement d'état 2.6.6 Indique dans la fenêtre de conversation quand u	111
	Notification de message 2.6.6 Fournit différents moyens d'avertissement de m	
	Paramètres voix et vidéo 2.6.6 Configure votre micro et votre webcam.	
✓ + Inform	Pidgin-Encryption 3.0 Chiffre les conversations avec un chiffrement RSA nations sur le plugin	*
	Configurer le plugin Fermer	



#### **Configuration OTR**



#### Conversation privée

## Chiffrer le dossier personnel

Ouvrir la session automatiquement

- O Demander mon mot de passe pour ouvrir une session
- Demander mon mot de passe pour ouvrir une session et déchiffrer mon dossier personnel

Étape 6 sur 8

Quitter Précédent

Suivant

## Conclusion

Pas besoin, donc, d'être un dieu de l'informatique pour savoir chiffrer les messages. Sous Linux, il existe aussi bien des outils en ligne de commande GPG. Comme quoi, pour protéger vos secrets, ce n'est pas difficile du tout si vous savez cliquer.