

1 GPG – AVANTAGES – INCONVENIENTS

Comme vous l'avez expérimenté dans le laboratoire 3. **GPG** est une implémentation open source gratuite de **PGP** (Pretty Good Privacy de Phil Zimmermann, créé en 1991).

L'utilisation de **GPG** présente certains avantages:

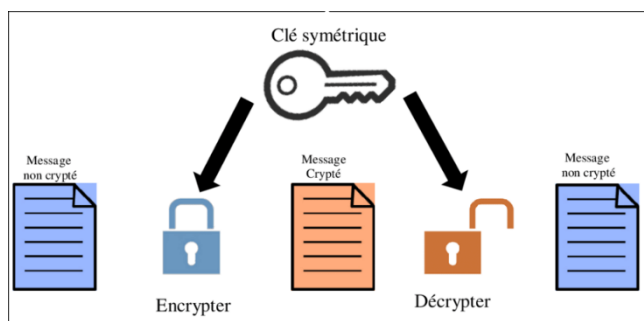
- Il utilise des algorithmes de chiffrement puissants et difficiles à déchiffrer.
- Il utilise le schéma de clé privée / publique, qui élimine le besoin de transférer un mot de passe à un destinataire de message ou de fichier de manière sécurisée. Au lieu de cela, il suffit d'envoyer sa clé publique, qui ne sert à rien d'autre qu'au destinataire ciblé.
- Vous pouvez utiliser **GPG** pour simplement crypter vos propres fichiers pour un usage personnel.
- Il peut être utilisé pour crypter les e-mails, vous permettant d'avoir un véritable cryptage de bout en bout pour les e-mails sensibles. Comme vous l'avez vu aux laboratoire 4, les certificats **S/MIME** sont plus adaptés à cet usage.

Mais, il y a aussi quelques inconvénients:

- Utiliser des clés publiques au lieu de mots de passe est génial lorsque vous travaillez uniquement avec des personnes de votre entourage et donc de confiance. Mais pour tout ce qui va au-delà, la distribution d'une clé publique afin que tout le monde puisse vérifier vos messages signés, rend le système très difficile à mettre en œuvre.
- Pour le chiffrement de bout en bout des e-mails, les destinataires doivent également avoir configuré **GPG** sur leurs systèmes et savoir comment l'utiliser. Cela peut fonctionner dans un environnement d'entreprise, mais ce sera plus délicat pour que votre entourage puisse le mettre en place.
- Si vous utilisez un client de messagerie autonome, tel que Mozilla Thunderbird, vous pouvez installer un plugin qui cryptera et décryptera les messages automatiquement. Mais, à chaque nouvelle mise à jour de Thunderbird, le plugin ne sera plus opérationnel et vous devrez attendre qu'une nouvelle version soit disponible.

Mais, même avec ses nombreuses faiblesses, **GPG** reste l'un des meilleurs moyens de partager des fichiers.

2 GPG - CRYPTAGE SYMETRIQUE



Le cryptage symétrique utilise la même clé pour crypter un fichier que pour décrypter. C'est génial si vous ne faites que crypter des fichiers pour votre propre usage. Mais, si vous avez besoin de partager un fichier crypté avec quelqu'un d'autre, vous devrez trouver un moyen sécurisé de donner le mot de passe à cette personne. Il n'est pas très sécurisant de simplement envoyer le mot de passe dans un e-mail en texte brut.

Mais, vous pouvez crypter vos propres fichiers.. Pour cela, le cryptage symétrique est tout particulièrement recommandé.

Crypterons un fichier super-secret :

```
echo "Ceci est mon plus grand secret !" > secret.txt
ls -l secret.txt
-rw-r--r-- 1 louis louis 33 Dec  3 09:06 secret.txt
gpg -c secret.txt
```

L'option **-c** indique d'utiliser un cryptage symétrique avec une passe-phrase. Cette passe-phrase ne sera utile que pour ce cryptage de fichier, sans aucun lien pour votre clé privée.

Attention que **GPG** fait une copie cryptée du fichier et laisse le fichier original non crypté intact

```
ls -l secret.txt*
-rw-r--r-- 1 louis louis 33 Dec  3 09:06 secret.txt
-rw-r--r-- 1 louis louis 115 Dec  3 09:07 secret.txt.gpg
```

Débarrassons-nous de ce fichier non chiffré avec **shred**. Nous utiliserons l'option **-u** pour supprimer le fichier et l'option **-z** pour écraser toutes données par des zéros sur le système de fichiers (rendant la récupération impossible).

```
shred -u -z secret.txt
```

La commande **shred** ne vous donne aucune sortie. Mais, un **ls -l** prouvera que le fichier a disparu. Pour récupérer mon fichier secret, en entrant la passe-phrase de ma clé privée.

```
less secret.txt.gpg
"secret.txt.gpg" may be a binary file.  See it anyway? Y
(q pour quit)
```

Pour déchiffrer, utilisez simplement **gpg** avec l'option **-d** et **-o** pour spécifier le fichier de sortie)

```
gpg -d secret.txt.gpg
gpg: AES256 encrypted data
gpg: encrypted with 1 passphrase
Ceci est mon plus grand secret !
gpg -o secret.txt -d secret.txt.gpg
gpg: AES256 encrypted data
gpg: encrypted with 1 passphrase
```

Après avoir entré une fois votre passe-phrase, **GPG** ne vous redemandera plus votre phrase secrète.

2.1. Exercice de décryptage

Sur la page du cours, téléchargez le fichier flag.gpg et ma clé publique.

1. Importez ma clé publique
2. Décryptez le fichier flag.gpg. Un indice mon empreinte est la clé.

Répondez dans le Wooclap disponible sur la page du cours. Jouez le jeu, le flag doit rester secret.

2.2. Exercice importation de clés

2.2.1 L'import de clé publique

Comment ajouter une clé publique à votre trousseau ?

Pour pouvoir utiliser la clé publique d'un de vos interlocuteurs, vous devez l'ajouter à votre trousseau grâce à la commande `--import` :

```
gpg --import [fichier]
```

Si aucun nom de fichier n'est passé en paramètre, la clef publique est lue depuis l'entrée standard.

A partir de ma clé publique disponible sur la page du cours. réalisez l'import.

2.2.2 Vérifier l'empreinte de clé

Comment afficher l'empreinte d'une clef publique de votre trousseau de clefs ?

La commande `--fingerprint` affiche les empreintes des clefs publiques de votre trousseau :

```
gpg --fingerprint
```

Demandez-moi mon empreinte de clé publique pour la comparer avec la clé importée.

L'empreinte est-elle identique ?

Dans la négative, retirez la clé de votre trousseau de clés avec la commande `--delete-key` :

```
gpg --delete-key info-clef
```

Sinon signer ma clé publique pour valider l'authenticité de ma clé.

2.2.3 Signer une clé publique

Comment signer une clef publique de votre trousseau de clefs ?

L'authenticité des clés publiques de votre trousseau est essentielle à la sécurité de vos échanges chiffrés. Pour vous assurer de l'authenticité de nouvelles clefs publiques, vous pouvez utiliser les signatures de ces clefs. Vous pouvez également vous porter garant de l'authenticité de certaines clés publiques en les signant avec une de vos clés privées grâce à la commande `--edit-key` :

```
gpg --edit-key info-clef
```

Cette commande vous donne accès à un menu permettant, entre autres, de signer la clef désignée par `info-clef` en tapant `sign`. Une fois la clé publique signée, vous pouvez la rendre publique de la même façon que pour une de vos clés publiques. Une fois de plus, rappelons que vous pouvez totalement compromettre la sécurité de vos échanges et de ceux qui vous font confiance, en accordant votre confiance à la légère. **Vous ne devez donc signer une clé publique que lorsque vous êtes ABSOLUMENT SUR de l'authenticité de la clé que vous signez.**

Ce menu vous permet aussi de modifier le niveau de confiance avec la commande **trust**.

Les niveaux de confiance sont :

- 1 = Je ne sais pas (I Don't know)
- 2 = Je ne fais pas confiance (I do NOT trust)
- 3 = Je fais un peu confiance (I trust marginally)
- 4 = Je fais totalement confiance (I trust fully)

Ces niveaux de confiance sont utilisés lors de la vérification de la signature d'un message. En effet, si vous n'avez pas ou peu confiance en une clé publique, la validité d'une signature basée sur cette clé publique ne peut garantir l'authenticité du message.

2.3. Utilisation des clés asymétriques

2.3.1 Envoyez vos clés publiques

Utilisez l'outil WINSXP pour rapatrier votre clé publique sur votre système Windows (voir le chapitre ci-dessous).






Si votre client mail Outlook permet la signature de vos envois avec le S/MIME. Envoyez votre clé publique en format binaire et ascii à votre enseignant.

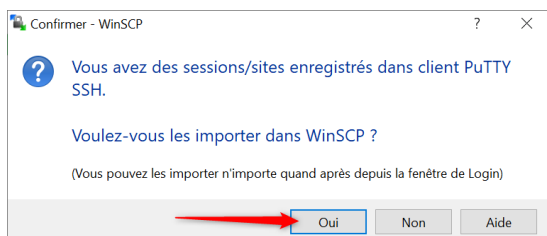
2.3.2 Créez un document crypté et signé

1. Sur votre Kali Linux, créer un document texte avec un message.
2. Crypté ce document texte à destination de votre enseignant et signé le document.
3. Envoyez ce document crypté et signé sur le dépôt sur HELMo Learn.

3 WINSXP

Pour échanger des fichiers avec vos systèmes Linux, voici un moyen très pratique et sécurisé. WinSCP est un client gratuit SFTP/SCP, c'est à dire qu'il permet de se connecter aux serveurs SSH pour transférer des fichiers de manière cryptée. Téléchargez l'outil sur les HELMo Learn <https://learn-technique.helmo.be/course/view.php?id=1336>

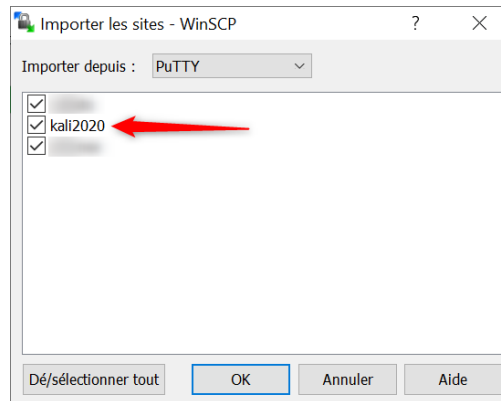
 vlc-3.0.11-win64.exe	2020-07-06 13:24 40M
 winrar-x64-591fr.exe	2020-07-06 13:19 3.2M
 WinSCP-5.17.6-Setup.exe	2020-07-06 13:17 11M
 Wireshark-win64-3.2.6.exe	2020-08-22 00:11 57M
 X2GoClient_latest_mswin32-setup.exe	2020-02-13 12:38 54M



Lors de l'installation, laissez les paramètres par défaut. Si votre PuTTY est correctement configuré (voir laboratoire 2), vous pourrez importer vos sessions PuTTY dans WinSCP.

Sélectionnez votre VM Kali.

Si tout s'est correctement installé, vous pouvez vous connecter sur votre VM Kali en utilisant l'authentification par clé



pouvez vous