# Sécurité des Systèmes d'Information

TP2: Chiffrement asymétrique avec PGP

#### Sommaire

## 1. Introduction

- 2. Utilisation de GnuPG
- 3. Création et échange de clés
- 4. Signature d'un fichier
- 5. Échange de mails cryptés

Introduction : le chiffrement asymétrique

La cryptographie asymétrique, ou cryptographie à clé publique, est une méthode de chiffrement qui repose sur l'utilisation d'une clé publique (qui est diffusée) et d'une clé privée (gardée secrète).

La clé privée permet de coder le message et l'autre de le décoder.

Introduction : le chiffrement asymétrique

L'expéditeur peut utiliser la clé publique du destinataire pour coder un message que seul le destinataire peut décoder, garantissant la **confidentialité** du contenu.

Inversement, l'expéditeur peut utiliser sa propre clé privée pour coder un message que le destinataire peut décoder avec la clé publique.

Introduction : pourquoi utiliser PGP ?

# Problèmes de sécurité liés à la messagerie électronique :

- écoutes : Sniffers ;
- usurpation d'identité : Telnet ;
- litiges : répudiation par l'émetteur ou le destinataire ;
- modification des mails en transit.

<u>Services de sécurité offerts</u> par PGP :

- confidentialité ;
- authentification ;
- non-répudiation de l'émetteur ;
  - intégrité.

<u>Mécanismes de sécurité :</u>

- sécurité au niveau applicatif (complémentaire de SSL au niveau transfert);
- signatures numériques ;
- chiffrement.

Techniques utilisées :

- cryptographie asymétrique ;
- cryptographie symétrique ;
- fonctions de hachage ;
- certification des clés publiques.

Introduction : quels logiciels utiliser ?

<u>Types de logiciels PGP :</u>

- commerciaux : Symantec ;
- libres : GnuPG (GNU Privacy Guard) ;

Intégration dans les agents de messagerie :

- au moyen de modules complémentaires (plugins) ;
- Thunderbird : Enigmail ;
- Outlook, Outlook Express : Gpg4win ;
- Eudora, Lotus Notes, Zimbra...

Utilisation de GnuPG : algorithmes supportés

Pour visualiser les algorithmes supportés :

# gpg --version

Liste des algorithmes disponibles :

- cryptographie symétrique ;
- cryptographie asymétrique ;
- hachage ;
- compression.

#### Création et échange de clé

Tout d'abord, ouvrez le gestionnaire de clé :

Applications R	accourcis	Système 👹 👩 🗾
Accessoires		Calculatrice
Bureautique	> [	Capture d'écran
Graphisme	>[	Dictionnaire
Internet	>	🖌 Éditeur de texte gedit
Outils système	> 👌	Gestionnaire d'archives
Son et vidéo	> [	🚄 Gnote
	6	⊱ Mots de passe et clés de chiffrement
		a Table de caractères
Bureautique Graphisme Internet Outils système Son et vidéo	> [ > [ > [ > [ ]	<ul> <li>Capture d'écran</li> <li>Dictionnaire</li> <li>Éditeur de texte gedit</li> <li>Gestionnaire d'archives</li> <li>Gnote</li> <li>Mots de passe et clés de chiffrement</li> <li>Table de caractères</li> </ul>

6	🥑 М		ots
<u>F</u> ichier	É <u>d</u> ition	<u>D</u> istant	A
<u>N</u> ouv	eau	Ctrl+N	
<u>I</u> mpo	rter	Ctrl+I	
E <u>x</u> po	rter		s <u>p</u>
Quitter		Ctrl+Q	

Ensuite, sélectionnez « Nouveau... »

### Chiffrement asymétrique avec PGP

#### Création et échange de clé



Maintenant que les clés sont générées, li ne reste plus qu'à exporter la clé publique...



... et la transmettre à un autre groupe...

Maintenant que les clés sont générées, li ne reste plus qu'à exporter la clé publique et la transmettre à un groupe...

<u>M</u> ots de passe	Mes clés <u>p</u> ersonnelle	Autres of
Nom		
jcfortor	<u>P</u> ropriétés	lé de test'
	E <u>x</u> porter	
	<u>C</u> opier	
	<u>S</u> upprimer	
	Signer la clé	

... et importer la leur :

ଶ		Mots	de
<u>F</u> ichier	É <u>d</u> ition	<u>D</u> istant <u>A</u>	ffich
<u>N</u> ouveau		Ctrl+N	â
<u>I</u> mpo	rter	Ctrl+I	74
Expo	ter		erso
Signe	r la clé		
Quitte	er	Ctrl+Q	hail.

Faite la même chose avec un serveur PKS :

- Enregistrez votre clé sur le serveur http://keyserver.pgp.com
- Vous recevez un mail de confirmation
- Récupérez la clé d'un autre groupe par ce biais en utilisant l'outil de recherche :

of Mots de passe et clés de chiffrement _ □ ×		
<u>F</u> ichier É <u>d</u> ition	Distant, Affichage Aide	
Propriétés		Filtre :
<u>M</u> ots de passe	Mes clés personnelles <u>A</u> utres clés	
Nom		✓ Identifiant de la clé
Mots of	<b>le passe :</b> login	

Il y a deux trousseaux de clés qui sont enregistrés dans le répertoire *.gnupg* :

- fichier de clés publiques : pubring.gpg ;
- fichier de clés privées : secring.gpg.

Vous pouvez afficher le contenu binaire des clés publiques :

- en détail : # pgpdump -i pubring.gpg
- la synthèse : # gpg ---list-packets pubring.gpg

# Fichier original → **# gpg --clearsign filename** → Fichier signé Phrase de passe pour déverrouiller la clé privée

Fichier signé  $\rightarrow$  **# gpg filename**  $\rightarrow$  Fichier original + résultat

<u>Le résultat :</u>

- bonne signature ;
- mauvaise signature ;
- clé publique non trouvée.

Procédez à un échange de fichier avec un groupe dont vous avez la clé publique et un dont vous n'avez pas la clé publique.

Quels sont les résultats ?

Créez un compte sur Gmail de la sorte : <u>epf.ssi2013.grpX</u> où X correspond au numéro de votre groupe.

Le mail du groupe 1 sera : epf.ssi2013.grp1@gmail.com

Utilisez comme mot de passe : epf2013

Une fois le compte créé, installez Thunderbird :

# yum -y install thunderbird

Enfin, démarrez le :



### Installez le compte que vous venez de créer grâce à l'assistant.



Une fois le mail et le mot de passe entrés, tout est automatique !

Pour pouvoir utiliser PGP dans Thunderbird, il faut installer un module complémentaire :



Ce module s'appelle « Enigmail », vous pouvez préciser sont nom dans la barre de recherche :

980 V	enigmail	*

## Une fois installé, il faut redémarrer Thunderbird :



Ensuite laissez-vous guider par l'assistant de configuration d'Enigmail.

- Envoyer un mail signé à un groupe qui possède votre clé publique et à un groupe qui ne la possède pas.
- Quels sont les résultats ?
- Envoyé un mail crypté à un groupe qui possède votre clé publique et à un groupe qui ne la possède pas.
- Quels sont les résultats ?
- Confirmez ces résultat à l'aide de Wireshark.

- Envoyer un mail signé à un groupe qui possède votre clé publique et à un groupe qui ne la possède pas.
- Quels sont les résultats ?
- Envoyé un mail crypté à un groupe qui possède votre clé publique et à un groupe qui ne la possède pas.
- Quels sont les résultats ?
- Confirmez ces résultat à l'aide de Wireshark.