Université Côte d'Azur — L3 Info, L3 MI, L3 ST
Cryptographie et calcul symbolique — 2023-24

TP n° 11

# Messagerie sécurisée avec PGP

PRETTY GOOD PRIVACY (PGP) a été développé au début des années 90. Il permet à ses utilisateurs de s'échanger des messages chiffrés et/ou signés par la messagerie électronique classique. Chiffrement et signature s'appuient sur de la cryptographie à clef publique et à clef secrète : c'est un système hybride (*cf.* Cours 10). L'authenticité des clefs publiques est assurée par les certificats PGP dont le système est, par comparaison avec `x.509`, entièrement décentralisé. GPG (GNU PRIVACY GUARD) implémente le standard OPENPGP.
Le but de ce TP est de prendre en main l'interface en ligne de commandes de GPG en vue de savoir l'utiliser par exemple dans votre messagerie. Il y a 2 ans, OPENPGP a été intégré à THUNDERBIRD, auparavant, c'est un plug-in (`Enigmail` dans ce cas) qui en simplifiait l'utilisation. C'est toujours le cas pour certains webmails. Quoi qu'il en soit, il est utile de comprendre le fonctionnement basique de cet outil.

## Introduction

**Exercice 1)** Voici l'adresse du site officiel de GPG :

`https://www.gnupg.org`

Pour toutes les questions suivantes, reportez-vous à la documentation de GPG, voir par exemple :

`http://www.gnupg.org/howtos/fr/index.html`

Pensez à utiliser l'option `--armor` abrégée en `-a` de GPG pour éviter les problèmes de codage de caractères dans la mesure où elle permet le codage sur 7 bits des caractères.

**Travaillez impérativement en binôme** (ici Alice et Bob)

Ce TP est rédigé du point de vue d'Alice mais bien-sûr, Bob doit effectuer rigoureusement la même chose en symétrique !

## Génération de clefs

**Exercice 2)**

1. Ouvrez une fenêtre auxiliaire afin de constater les modifications au contenu du répertoire `.gnupg` à la racine de votre compte.
2. Testez l'option `--version` de GPG, vous apprendrez quels sont les algorithmes proposés.
3. Alice crée sa clef privée (appelée secrète par GPG) puis en extrait sa clef publique. Elle retrouve ses clefs en listant le contenu de son trousseau. Elle peut également choisir de ne lister que sa clef secrète.
4. Alice transmet alors sa clef publique à Bob par courriel.
5. Alice importe la clef publique de Bob qu'elle vient de recevoir par mail.
6. Alice vérifie son trousseau où la clef publique de Bob, fraîchement importée, doit être visible.
7. Faites afficher en outre les empreintes des clefs affichées avec l'option `--fingerprint`. Parmi les informations, vous trouverez la taille en binaire des clefs.

## Chiffrement

**Exercice 3)**

1. Alice rédige un premier message, le chiffre avec la clef publique de Bob qu'elle a dans son trousseau GPG puis l'envoie par mail à Bob.
2. Alice envoie à Bob un second message mais cette fois-ci, elle essaye de préciser d'emblée le destinataire avec l'option `-r` pour *recipient*.
3. Alice recueille et déchiffre grâce à sa clef secrète les deux messages qu'elle vient de recevoir de Bob.

## Signature et intégrité

**Exercice 4)**

1. Alice souhaite envoyer à Bob un message signé mais non chiffré. Le message est *haché* avant d'être signé. Utilisez tour à tour les deux options `--sign` ou bien `--clearsign`.
   Visualisez dans chaque cas le produit de la signature et remarquez la différence entre les deux. Quelle est donc la fonction de hachage utilisée ?
2. Alice vient de recevoir les 2 messages différemment signés de Bob. Elle vérifie avec `--verify` l'intégrité de chacun et l'authenticité de leur signature. Pour voir le contenu des messages, il faut utiliser `--decrypt` (et pourtant, il n'y a pas de chiffrement ici ...).
3. Quel avertissement Alice a-t-elle obtenu lors de la vérification d'une signature ?

## Confiance et certification

**Exercice 5)**

1. Pour se fier à la signature de Bob, Alice décide de certifier la clef publique de Bob dans son trousseau en la signant. Utilisez pour cela la commande `sign` du dialogue interactif initié par l'option `--edit-key`.
2. Tentez à nouveau de vérifier la validité de la signature du message de Bob. Qu'est-ce qui a changé ?

## Chiffrement, signature et intégrité

**Exercice 6)**

1. Cette fois, Alice décide d'envoyer à Bob un message à la fois chiffré et signé.
2. Réciproquement, Alice reçoit de la part de Bob un message chiffré et signé. Procédez tout à la fois au déchiffrement, à la vérification de l'intégrité et de la signature du message de Bob.
   *Bonne signature ?*

## Diffusion de clefs

Il existe des serveurs de clefs PGP qui contiennent les clefs publiques des utilisateurs comme :

`https://keys.openpgp.org`

On peut à la fois y enregistrer des clefs et l'interroger pour retrouver la clef publique d'un utilisateur.