web et sécurité

TP02

Réaliser Par : Guettouche Islam

Mes premières clefs avec GPG

GPG utilise de la cryptographie symétrique et asymétrique. Chaque utilisateur dispose d'une bi-clef publique/privé pour l'authentification, et d'une bi-clef pour le chiffrement.

Pourquoi ?

La clef privée pour l'authentification permet à l'expéditeur de chiffrer le haché du message, ensuite le destinataire va déchiffrer ce message grâce à la clef publique de l'expéditeur et va comparer si les deux hachés correspondent (les hachés du message clair et du message chiffré).

La clef publique pour le chiffrement permet à l'expéditeur de chiffrer le message qu'il veut envoyer au destinataire. La clef privée, gardée par le destinataire lui permettra de déchiffrer le message.

Installation de GPG

La suite de logiciels sous Windows permettant de manipuler des fichiers chiffrés avec GPG, avec une interface conviviale, s'appelle GPG4Win. Sous Windows Téléchargement de GnuPG pour Windows. ftp://ftp.gnupg.org/gcrypt/binary/gnupg-w32cli-1.4.6.exe

S'agissant d'un logiciel libre sous licence GPL, vous pourrez bien évidemment accepter la licence, à moins que vous ne travailliez pour Microsoft. Ensuite, pour ce qui est des composants à installer, cochez les cases :

- GnuPG
- GnuPG2 (attention!)
- GPA (interface pour GPG)
- WinPT
- GPGee (ajout de menu au clic droit)
- ...et accessoirement GPGol qui est un plug-in pour Outlook, mais on s'en passera ici.

Exercice 01

Quelle taille de clef choisissez-vous ? Pour quelles raisons ?

On choisit une taille de 3072 afin de pouvoir avoir des clefs assez forte pour les prochaines années, sachant que le niveau de sécurité (en bits) sera autour de 128 en 2020. C'est donc parfait car 3072 en taille de clef pour DSA-El-Gamal fait 128 bits. De plus, nous avons choisi une durée de vie d'un an.

À quoi servent les données qui vous sont demandées ?

Nous est demandé :

- **Le nom :** afin de montrer réellement qui nous sommes
- **L'adresse email :** permet d'avoir un identifiant unique
- **Un commentaire :** on peut préciser des détails ici, comme pro, perso etc.

Pourquoi est-ce que le processus de génération est lent ?

Car le logiciel doit générer des aléas. Il faut donc favoriser les I/O de la machine. Le processus sera donc plus rapide si la machine est en fonctionnement depuis longtemps. La durée du processus dépend de l'entropie présente sur la machine. On peut voir cette entropie grâce à la commande `cat /dev/random` ou encore la commande `cat /dev/urandom`.

Lisez les informations affichées par `gpg2` lors de la génération.

Aucune information n'apparait lors de la génération.

```
C:\Users\Guettouche>gpg --list-keys
C:/Users/Guettouche/AppData/Roaming/gnupg/pubring.kbx
-------------------------------------------------------
pub   dsa3072 2017-10-24 [SC] [expire : 2018-10-24]
      A3408DE8AA8125E72D2F8BDD038788A23E2A94FC
uid           [  ultime ] GUETTOUCHE (bah oui Morray) <braza92i@gmail.com>
sub   elg3072 2017-10-24 [E] [expire : 2018-10-24]


C:\Users\Guettouche>gpg --list-secret-keys
C:/Users/Guettouche/AppData/Roaming/gnupg/pubring.kbx
-------------------------------------------------------
sec   dsa3072 2017-10-24 [SC] [expire : 2018-10-24]
      A3408DE8AA8125E72D2F8BDD038788A23E2A94FC
uid           [  ultime ] GUETTOUCHE (bah oui Morray) <braza92i@gmail.com>
ssb   elg3072 2017-10-24 [E] [expire : 2018-10-24]
```

```
C:\Users\Guettouche>gpg --full-gen-key
gpg (GnuPG) 2.2.1; Copyright (C) 2017 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Sélectionnez le type de clef désiré :
   (1) RSA et RSA (par défaut)
   (2) DSA et Elgamal
   (3) DSA (signature seule)
   (4) RSA (signature seule)
Quel est votre choix ? 2
les clefs DSA peuvent faire une taille comprise entre 1024 et 3072 bits.
Quelle taille de clef désirez-vous ? (2048) 3072
La taille demandée est 3072 bits
Veuillez indiquer le temps pendant lequel cette clef devrait être valable.
         0 = la clef n'expire pas
      <n>  = la clef expire dans n jours
      <n>w = la clef expire dans n semaines
      <n>m = la clef expire dans n mois
      <n>y = la clef expire dans n ans
Pendant combien de temps la clef est-elle valable ? (0) 1y
La clef expire le 10/24/18 15:08:14 Paris, Madrid (heure dÆÚtÚ)
Est-ce correct ? (o/N) o

GnuPG doit construire une identité pour identifier la clef.

Nom réel : GUETTOUCHE
Adresse électronique : braza92i@gmail.com
Commentaire : bah oui Morray
Vous avez sélectionné cette identité :
    « GUETTOUCHE (bah oui Morray) <braza92i@gmail.com> »
```

```
Changer le (N)om, le (C)ommentaire, l'(A)dresse électronique
ou (O)ui/(Q)uitter ? O
De nombreux octets aléatoires doivent être générés. Vous devriez faire
autre chose (taper au clavier, déplacer la souris, utiliser les disques)
pendant la génération de nombres premiers ; cela donne au générateur de
nombres aléatoires une meilleure chance d'obtenir suffisamment d'entropie.
gpg: Attention : certains programmes OpenPGP ne peuvent pas gérer
          de clef DSA avec cette taille de hachage
De nombreux octets aléatoires doivent être générés. Vous devriez faire
autre chose (taper au clavier, déplacer la souris, utiliser les disques)
pendant la génération de nombres premiers ; cela donne au générateur de
nombres aléatoires une meilleure chance d'obtenir suffisamment d'entropie.
gpg: clef 038788A23E2A94FC marquée de confiance ultime.
gpg: répertoire « C:/Users/Guettouche/AppData/Roaming/gnupg/openpgp-revocs.d » créé
gpg: revocation certificate stored as 'C:/Users/Guettouche/AppData/Roaming/gnupg/openpgp-revocs.d\A3408DE8AA8125E72D2F8BDD038788A23E2A94FC.rev'
les clefs publique et secrète ont été créées et signées.

pub   dsa3072 2017-10-24 [SC] [expire : 2018-10-24]
      A3408DE8AA8125E72D2F8BDD038788A23E2A94FC
uid                   GUETTOUCHE (bah oui Morray) <braza92i@gmail.com>
sub   elg3072 2017-10-24 [E] [expire : 2018-10-24]
```

Exercice 02

```
C:\Users\Guettouche>gpg --edit-key GUETTOUCHE
gpg (GnuPG) 2.2.1; Copyright (C) 2017 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

La clef secrète est disponible.

sec  dsa3072/038788A23E2A94FC
     créé : 2017-10-24  expire : 2018-10-24  utilisation : SC
     confiance : ultime        validité : ultime
ssb  elg3072/F753C440DBC7E2BD
     créé : 2017-10-24  expire : 2018-10-24  utilisation : E
[  ultime ] (1). GUETTOUCHE (bah oui Morray) <braza92i@gmail.com>
```

`showpref`, que signifie les données affichées ?

```
gpg> showpref
[  ultime ] (1). GUETTOUCHE (bah oui Morray) <braza92i@gmail.com>
     Chiffrement : AES256, AES192, AES, 3DES
     Hachage : SHA256, SHA384, SHA512, SHA224, SHA1
     Compression : ZLIB, BZIP2, ZIP, Non compressé
     Fonctionnalités : MDC, Serveur de clefs sans modification
```

Nous avons les différents algorithmes et hachages supportés par la clef.

Chiffrement « Cipher »: sont les algorithmes.

Hachage « Digest » : sont les fonctions de hachage.

`Check`, que pouvez-vous en déduire sur la forme de diffusion des clefs ?

La clef est auto signée. Un système de confiance existe de façon à garantir l'identité. D'autres personnes peuvent signer la clef.

Exercice 03 (Révocation d'une clef)

Expliquez ce qu'est un certificat de révocation ?

```
C:\Users\Guettouche> gpg --output revok_macle.asc --gen-revoke GUETTOUCHE

sec  dsa3072/038788A23E2A94FC 2017-10-24 GUETTOUCHE (bah oui Morray) <braza92i@gmail.com>

Faut-il créer un certificat de révocation pour cette clef ? (o/N) o
choisissez la cause de la révocation :
  0 = Aucune cause indiquée
  1 = La clef a été compromise
  2 = La clef a été remplacée
  3 = La clef n'est plus utilisée
  Q = Annuler
(Vous devriez sûrement sélectionner 1 ici)
Quelle est votre décision ? 1
Entrez une description facultative, en terminant par une ligne vide :
>
Cause de révocation : La clef a été compromise
(Aucune description donnée)
Est-ce d'accord ? (o/N) o
sortie forcée avec armure ASCII.
Certificat de révocation créé.

Veuillez le déplacer sur un support que vous pouvez cacher ; toute personne
accédant à ce certificat peut l'utiliser pour rendre votre clef inutilisable.
Imprimer ce certificat et le stocker ailleurs est une bonne idée, au cas où le
support devienne illisible. Attention tout de même : le système d'impression
utilisé pourrait stocker ces données et les rendre accessibles à d'autres.
```

Un certificat de révocation permet de révoquer une clef. Imaginons que la machine prenne feu, il faut pouvoir dire que nous n'avons plus accès à la clef et que donc la clef est invalide. Cela peut également permettre de prévenir les utilisateurs que l'authenticité de notre clef est corrompue.

Il faut conserver le certificat dans un endroit sûr afin d'éviter toute perte ou tout vol de la clef.

Gestion de son trousseau de clefs

Exercice 04 (Distribution de clefs)

Lorsque vous importez des clefs publiques comme ci-dessous, vous n'avez aucune raison de penser que ce sont les bonnes clefs.

Détailler `man in the middle`

Les clefs pourraient être des fausses clefs mise en place par quelqu'un au centre du réseau. **« man in the middle »** est quelqu'un qui se place entre deux interlocuteurs (qu'ils soient client ou serveur) pour intercepter les messages d'un expéditeur, de les modifier et les envoyer au destinataire.

Quel est le lien entre l'identifiant de la clef et le _fingerprint_ ?

L'identifiant de la clef est la fin du _fingerprint_. Cela permet de vérifier l'intégrité de la clef. Il faudrait un énorme hasard pour que les deux correspondant.

```
C:\Users\Guettouche>gpg --import clef.asc
key D0BF9D6A1310163F:
4 signatures not checked due to missing keys
gpg: clef D0BF9D6A1310163F : clef publique « Cécile Gonçalves <cecile.goncalves@univ-rouen.fr> » importée
gpg:       Quantité totale traitée : 1
gpg:                    importées : 1
gpg: marginals needed: 3  completes needed: 1  trust model: pgp
gpg: profondeur : 0  valables :   1  signées :   0
     confiance : 0 i., 0 n.d., 0 j., 0 m., 0 t., 1 u.
gpg: la prochaine vérification de la base de confiance aura lieu le 2018-10-24
```

```
C:\Users\Guettouche>gpg --edit-key cecile.goncalves@univ-rouen.fr
gpg (GnuPG) 2.2.1; Copyright (C) 2017 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.


pub  dsa3072/D0BF9D6A1310163F
     créé : 2016-11-10  expire : jamais      utilisation : SC
     confiance : inconnu       validité : inconnu
sub  elg3072/5B8688C8920F1B89
     créé : 2016-11-10  expire : jamais      utilisation : E
[ inconnue] (1). Cécile Gonçalves <cecile.goncalves@univ-rouen.fr>

gpg> fpr
pub   dsa3072/D0BF9D6A1310163F 2016-11-10 Cécile Gonçalves <cecile.goncalves@univ-rouen.fr>
Empreinte clef princip. : 3CDA C867 6AF9 3763 E9AA  B7A2 D0BF 9D6A 1310 163F
```

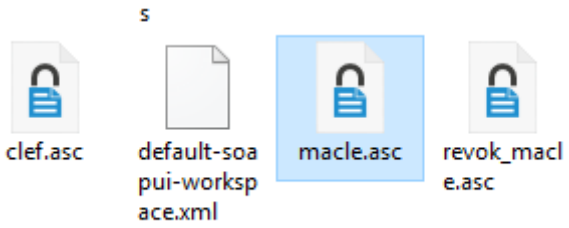
```
gpg> sign

pub  dsa3072/D0BF9D6A1310163F
     créé : 2016-11-10  expire : jamais      utilisation : SC
     confiance : inconnu       validité : inconnu
Empreinte clef princip. : 3CDA C867 6AF9 3763 E9AA  B7A2 D0BF 9D6A 1310 163F

     Cécile Gonçalves <cecile.goncalves@univ-rouen.fr>

Voulez-vous vraiment signer cette clef avec votre
clef « GUETTOUCHE (bah oui Morray) <braza92i@gmail.com> » (038788A23E2A94FC)

Voulez-vous vraiment signer ? (o/N) o
```

Exercice 05 (Confiance et validité)

```
gpg> trust
pub  dsa3072/D0BF9D6A1310163F
     créé : 2016-11-10  expire : jamais      utilisation : SC
     confiance : inconnu       validité : inconnu
sub  elg3072/5B8688C8920F1B89
     créé : 2016-11-10  expire : jamais      utilisation : E
[ inconnue] (1). Cécile Gonçalves <cecile.goncalves@univ-rouen.fr>

Décidez maintenant de la confiance que vous portez en cet utilisateur pour
vérifier les clefs des autres utilisateurs (en regardant les passeports, en
vérifiant les empreintes depuis diverses sources, etc.)

  1 = je ne sais pas ou n'ai pas d'avis
  2 = je ne fais PAS confiance
  3 = je fais très légèrement confiance
  4 = je fais entièrement confiance
  5 = j'attribue une confiance ultime
  m = retour au menu principal

Quelle est votre décision ? 4

pub  dsa3072/D0BF9D6A1310163F
     créé : 2016-11-10  expire : jamais      utilisation : SC
     confiance : totale        validité : inconnu
sub  elg3072/5B8688C8920F1B89
     créé : 2016-11-10  expire : jamais      utilisation : E
[ inconnue] (1). Cécile Gonçalves <cecile.goncalves@univ-rouen.fr>
Veuillez remarquer que la validité affichée pour la clef n'est pas
forcément correcte avant d'avoir relancé le programme.
```

Exercice 06

```
C:\Users\Guettouche>gpg --output macle.asc --armor --export GUETTOUCHE
```



GPG et messagerie

Exercice 7 (Messagerie)

Pouvez-vous déchiffrer les documents que vous envoyez ?

Oui, fort heureusement, comme on dispose des clefs nécessaire, on peut déchiffrer les messages que l'on envoie.

Ceux que vous recevez ?

Cela dépend. Si nous disposons de la clef publique de la personne qui nous envoie le message, alors on peut déchiffrer ce message, sinon il nous est impossible de voir le contenu du message.

De qui proviennent-ils ?

Ils proviennent des camarades de la promotion. Pour certains, nous en sommes sûr car nous avons leurs clefs. Pour d'autres, c'est à voir, il faudrait que nous vérifiions et qu'ensuite nous signons leurs clefs histoire d'être sûr pour la suite.

Quel est le chiffrement utilisé ? Quelle est la clef de signature ?

Le message est signé avec la clef privée. Le destinataire se servira de la clef publique pour vérifier l'authenticité de l'expéditeur.