Chiffrement asymetrique

Je me base sur ce lien pour ma doc

http://arobaseinformatique.eklablog.com/chiffrement-dechiffrement-asymetrique-avec-gnupg-a114562000

Je genere une paire de clés publique et privé avec cette commande :

gpg --gen-key

- Le type de clé souhaité

- La longueur de la clé

- La durée de validité de la clé

Il faudra également entrer quelques informations sur l'utilisateur afin d'associer la clé crée avec une personne physique (ce qui sera important si vous souhaitez signer une clé...)

- Nom

- Adresse email

- Commentaire (facultatif)

Enfin, vous devrez choisir le mot de passe qui servira à chiffrer votre clé privée.

PS : choisissez un mot de passe complexe mais facile à mémoriser pour vous.

Si vous oubliez votre mot de passe, vous ne pourrez plus utiliser vos clés.

J'ai saisi les informations et j'ai utiliser comme mdp pour ma clé privée « siojjr »

L'identifiant de cette clé est ce que j'ai surligner il me semble

```
gpg: /root/.gnupg/trustdb.gpg : base de confiance créée
gpg: clef 613D873980218444 marquée de confiance ultime.
gpg: répertoire « /root/.gnupg/openpgp-revocs.d » créé
gpg: revocation certificate stored as '/root/.gnupg/openpgp-revocs.d/20DEDB7120E
07E1157C49838613D873980218444.rev'
les clefs publique et secrète ont été créées et signées.

pub   rsa3072 2021-05-10 [SC] [expire : 2023-05-10]
      20DEDB7120E07E1157C49838613D873980218444
uid                      Machicouli <machicouli95@gmail.com>
sub   rsa3072 2021-05-10 [E] [expire : 2023-05-10]

root@debian:~#
```

Les clés publiques et privées sont situées dans le répertoire caché **.gnupg** situé dans votre répertoire personnel.

- **pubring.gpg :** clés publiques

- **secring.gpg :** clé privée

- **random_seed :** fichier utilisé pour générer des nombres aléatoires lors de la création des clés.

- **trustdb.gpg :** base de données de confiance.

```
root@debian:~# cd /root/.gnupg
root@debian:~/.gnupg# ls
openpgp-revocs.d   pubring.kbx   random_seed
private-keys-v1.d  pubring.kbx~  trustdb.gpg
```

Pubring.kbx = clé publiques

private-keys-v1 est quand à lui un dossier qui contient 2 fichier comportant 2 clés differente

```
root@debian:~/.gnupg# cd /root/.gnupg/private-keys-v1.d/
root@debian:~/.gnupg/private-keys-v1.d# ls
6C88A94EF1C6A08E426EFAB3B8E88C2DE91F6E13.key
FE93DD3E22E906181B85039F97C3A468C4A1DB86.key
root@debian:~/.gnupg/private-keys-v1.d# ls -l
total 8
-rw------- 1 root root 1608 mai   10 23:43 6C88A94EF1C6A08E426EFAB3B8E88C2DE91F6
E13.key
-rw------- 1 root root 1624 mai   10 23:43 FE93DD3E22E906181B85039F97C3A468C4A1D
B86.key
root@debian:~/.gnupg/private-keys-v1.d#
```

Pour visualiser la liste des clés publiques, utilisez la commande :

gpg --list-keys

Clés privées

gpg --list-secret-keys

Lorsque j’effectue ces 2 commandes voila ce que je trouve

```
pub   rsa3072 2021-05-10 [SC] [expire : 2023-05-10]
      20DEDB7120E07E1157C49838613D873980218444
uid           [  ultime ] Machicouli <machicouli95@gmail.com>
sub   rsa3072 2021-05-10 [E] [expire : 2023-05-10]

root@debian:~/.gnupg/private-keys-v1.d# gpg --list-secret-keys
/root/.gnupg/pubring.kbx
------------------------
sec   rsa3072 2021-05-10 [SC] [expire : 2023-05-10]
      20DEDB7120E07E1157C49838613D873980218444
uid           [  ultime ] Machicouli <machicouli95@gmail.com>
ssb   rsa3072 2021-05-10 [E] [expire : 2023-05-10]

root@debian:~/.gnupg/private-keys-v1.d#
```

Pub signifie clé publiques
et sec signifie secret cad privée

Si vous souhaitez exporter votre clé publique afin de la partager, utilisez la commande :

gpg --armor --export [uid] > nom_souhaité.asc

Je vais maintenant importer ma clé publique dans un fichier

J'ai crée dans le repertoire root un dossier « gpg » j'y ai entreposer ma clé comme ceci

```
root@debian:~/gpg# ls
cléPublique.asc
root@debian:~/gpg# cat cléPublique.asc
-----BEGIN PGP PUBLIC KEY BLOCK-----

mQGNBGCZqN8BDADoCBOAasO4u1CkH8FR8dmn9Mh031gL6yrjuPOVCxmnyAmom7cz
k8+2vh6xIKWhKu7LSmns54S3ExbriU1R/fL6+5PxsjrRoRu0EPEelU1cAqXzAolD
CaTztFB8iCVxvMu05WlpQKc35tCcWH8TC73LW65XXLeWIkKAPigH9mGGzX7U6KU2
7/0HT2BtehJ9uokTocsK6oqIbxaxzEw/mcHJtTdYozMdaV1DYY7BkTpsMLPz64Tp
eZC7zi8serE9WNFyFbhPq2eeRonLw1tV4Y/jrtoaIgPfQAxhieg1/42to6uR6GOo
xys1k6En3NAI8wzhFEBg5iFDgjSy0GKbuOH0OQdiNiaeHDtkTdJn926dvkBELLta
au876delNaSVzSaaQ2JEvNbWIG/oDOr0gTXAv1eEz/TAe8tit81Z2dHc9c8c/b8G
```

La commande de base que j'avais effectuer pour entreposer ma clé publique dans un fichier est celle ci

```
root@debian:~/.gnupg/private-keys-v1.d# gpg --armor --export 20DEDB7120E07E1157C49838613D873980218444 >
 cléPublique.asc
```

Si vous souhaitez importer une clé publique, utilisez la commande :

gpg --import nom_fichier.asc

Chiffrer et dechiffrer des données avec les clés

Chiffrement fichiers : gpg -e -r [uid] -o [fichier sorti] [fichier lu]

-o [fichier sorti] : définit le nom du fichier à la sortie.

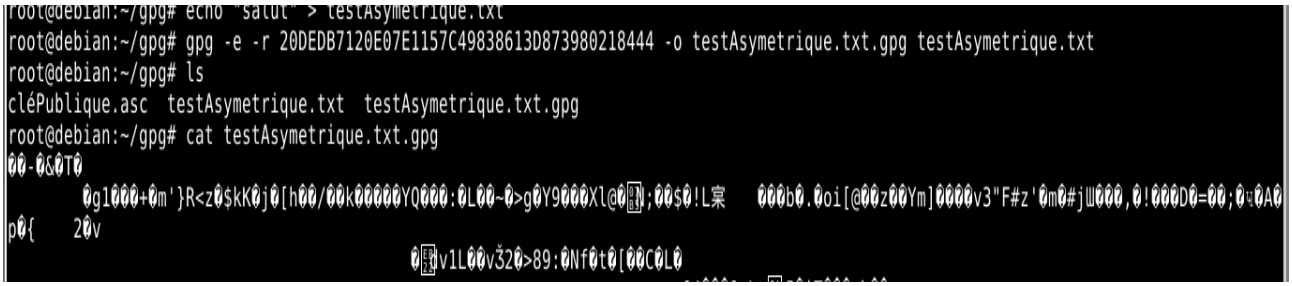
<u>Déchiffrement fichiers</u> : gpg -d -r [uid] -o [fichier sorti] [fichier lu]

-d : indique qu'il faut déchiffrer

-r : spécifie l'identifiant de la clé avec lequel le fichier doit être déchiffré (8 caractères) (16 en 2021)

-o [fichier sorti] : définit le nom du fichier à la sortie.

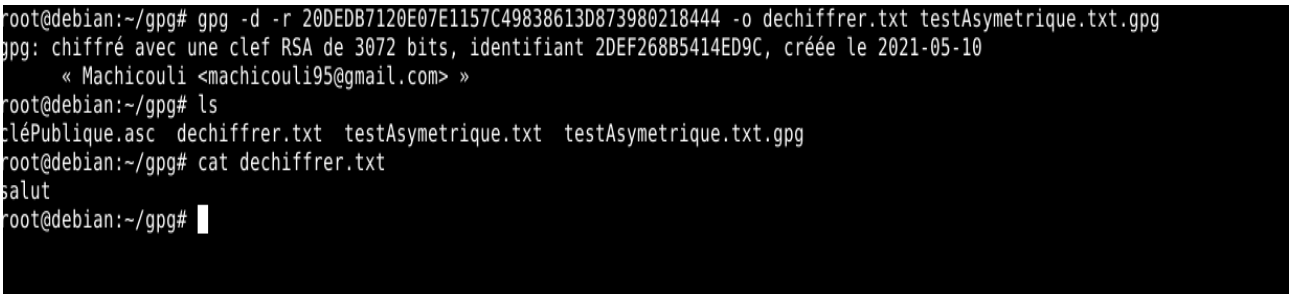
Ok je vais essayer de crypter un fichier avec ma clé publique et le dechiffrer avec ma clé privé



Ici j'ai créer le fichier testAsymetrique.txt j'y ai ecrit salut je l'ai crypter en saissisant l'uid de ma clé publique baser suyr 16 caractère une fois que je fais un « cat » pour consulter l'interieur du fichier

Je trouve que mon « salut » est crypter dans le fichier qui a comme extension « gpg »

Je vais maintenant dechiffrer ce fichier avec les commandes que j'ai mis plus haut dans la doc



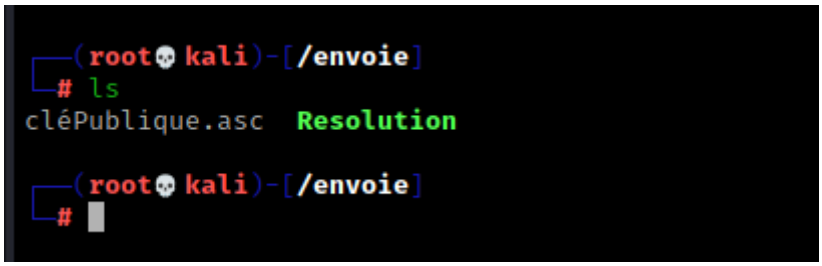
Ici c'est exactement pareil il faut que la clé privé sois presente dans mon trousseau de clé privée

il faut que je renseigne son UID l'UID de la clé publique et privée sont exactement pareil et des que j'ai voulu dechiffrer une fenetre c'est ouverte et m'a demander de saisir la passphrase

C'est excellent !!

Je vais maintenant utiliser une machine kali et envoyer mon fichier de clé publique via le protocole SCP basé sur SSH importer cette clé publique et crypter un message avec et le renvoyer

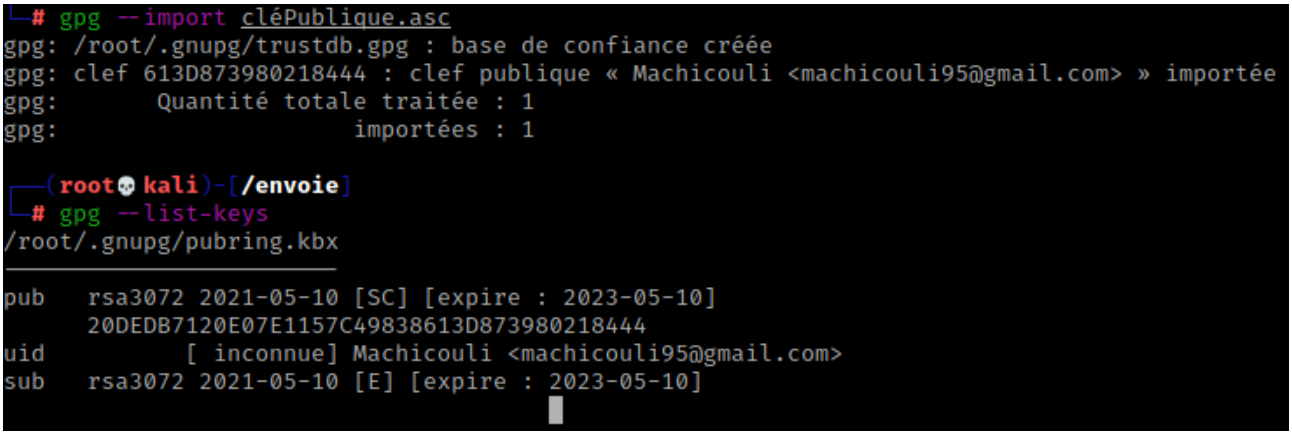
Je suis sur ma machine kali et je me suis envoyer la clé publique



Je vais maintenant l'importer et verifier si elle est présente dans mon trousseau de clé

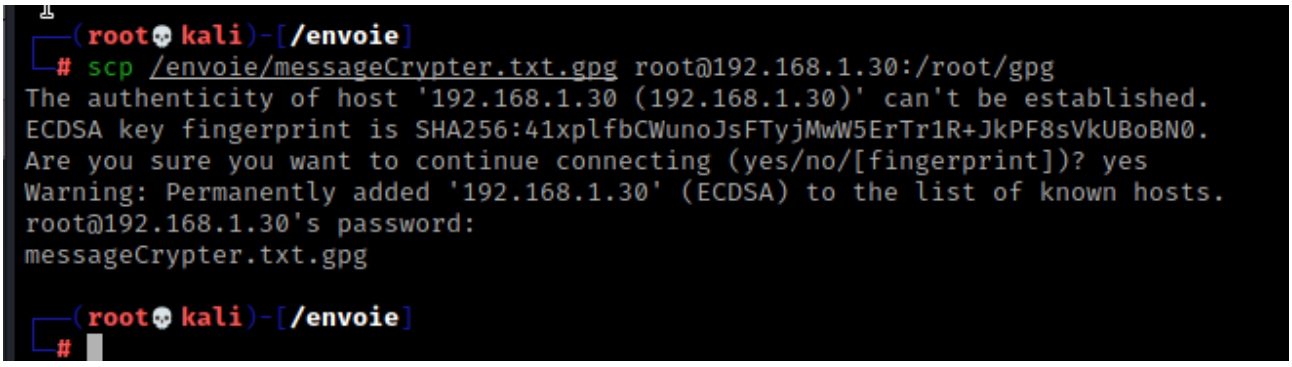
gpg –import cléPublique.asc

ensuite gpg –list-keys



La clé a été correctement importer je vais maintenant cryptée un message qui sera dans un fichier

J'ai crypter le message et je me le suis envoyer



Je decrypte le message et voila le résultat c’est parfait !!

```
root@debian:~/gpg# gpg -d -r 20DEDB7120E07E1157C49838613D873980218444 -o messageDecrypter.txt messageCrypter.txt.gpg
gpg: chiffré avec une clef RSA de 3072 bits, identifiant 2DEF268B5414ED9C, créée le 2021-05-10
      « Machicouli <machicouli95@gmail.com> »
root@debian:~/gpg# cat messageDecrypter.txt
Bonjour comment allez-vous ?
root@debian:~/gpg#
```