**Cryptographie : TP\_Final GNU Privacy Guard 26/03/2019**

1. GlobalSign Extended Validation CA – SHA256 – G3
2. GlobalSign Root CA – R3
3. Chiffrement RSA
4. 2048 bits, exposant 24 bits
5. Pas après 21 septembre 2026

Hachage

1)

Man gpg > aide\_gpg.txt

Gpg -h | more

Liste : MD5, SHA1, SHA256, SHA384, SHA512, SHA224, RIPEMD160

2)

Echo -n ESIEA | gpg –print-md (+OPTION)

PIPE == |

**OPTION :**

SHA1

MD5

SHA512

SHA256

3)

Pour hacher une image/un fichier :

Gpg --print-md SHA256 Original.bmp Tatouee.bmp

nb bit utilisé pour coder un chiffre en hexadécimal (=4) \* nb de chiffres

Pour MD5 : 128 bits car 4\*32 = 128

Pour SHA256 : 256 bits car 4\*64=256

4) Les images sont quasiment identique, et le haché par contre est totalement différent.

Chiffrement symétrique

1. Gpg -c --armor Original.bmp (--armor permet de chiffrer en ASCII)
2. Gpg -d -o coucou.bmp Original.bmp.asc (on déchiffre Original.bmp.asc et on créé un fichier coucou.bmp)
3. Gpg -c Original.bmp
4. Gpg -d -o coucou.bmp Original.bmp.gpg

Génération de clé publique/privée

1. gpg–-gen-key

Ou

Gpg –-full-generate-key

1. pour lister : gpg –-list-keys
2. pub :

uid :

sub :

1. Pour générer la clé et la mettre dans un fichier texte :

Gpg –-export -a [monadresse@et.esiea.fr](mailto:monadresse@et.esiea.fr) > nom\_pk.gpg

1. Pour supprimer un une clé :

Gpg -o revoke.asc –gen-revoke identifiant\_de\_votre\_cle

1. Pour importer une clé :

Gpg –-import Bob\_pk.gpg

1. Pour chiffrer avec la clé publique du destinataire :

Utiliser : gpg --list-keys –with-colons (pour récuperer le pub du destinataire (sans la date))

Gpg –encrypt –armor -r (Boris / ou pub) fichier\_a\_chiffrer

1. Pour déchiffrer avec la clé privé du receveur :

Utiliser pour un texte : gpg –-decrypt -r nom\_clé\_privé fichier\_a\_dechiffrer -r permet de lire la clé privé

Pour un autre type : Gpg –-decrypt -r nom\_clé\_privé -o name.jpeg fichier\_a\_dechiffrer.jpeg

Permet de créer un fichier contenant le déchiffré.

Signature RSA

1. Gpg –-clearsign nom\_fichier\_a\_signer