Vérifier la version de gpg

1.4.10

Exercice 1

1. symétrique

à l'aide de man gpg et gpg -help, j'ai trouvé que commande –symmetric pour chiffrement symétrique seulement

2. algo supporté

en utilisant la commande gpg --version

clé publique : RSA, RSA-E,RSA-S etc

chiffrement : 3DES, CAST5 etc

hachage : MD5, SHA1 etc

Compression : non compression, ZIP etc

en utilisant la commande gpg -help

outil signature:

commande : -s --sign [ficher] faire une signature

--clearsign [ficher] faire une signature en texte claire

Exercice 2

1-gpg --gen-key

ouvrire mousepad pour taper qqch et des chiffre, déplacer le souris etc

passphrase est une sorte de mot de passe, elle sera demandée à chaque processus de signature ou de chiffrement. elle doit se composer des lettres, des chiffres et des symboles non alpha-numériques, des majuscules et des minuscules.

Elle peut garantir l’accès à un programme

pub : le champ « pub » correspond à la partie publique.

1 nombre + 1 lettre

le nombre est le longeur de bit de clé

les lettres sont :   
 RSA == R  
 DSA == D  
 Elgamal == g (only seen in subkeys)

sub : le champ « sub » correspond à une sous-clé. il est utilisé pour encryptation

uid : le champ « uid » correspond à une adresse email et un nom.

gpg --output zhaomengzi.gpg --armor --export “zhaomengzi” pour exporter la clé publique

gpg --output zhaomengzi.gpg --armor --export-secret-key “zhaomengzi” pour exporter la clé privé

armor : clé doit être exportée dans un format binaire et aussi peut être envoyée par email ou publié sur une page web. donc armor provoque la génération des sorties dans un format ASCII- armored (blindage ASCII) similaire aux documents encodés avec l'algorithme UUE.

En général, toutes les sorties de GnuPG, comme par exemple clés, documents chiffrés, et signatures, peuvent être exportés dans le format ASCII-armored en ajoutant l'option --armor.

gpg --import wangliPubKey.gpg pour importer la clé public des autres personne

gpg --list-key pour vérifier qu’il y a bien deux clés publiques dans la liste

gpg --list-secret il y a une seule clé privé

Exercice 3

gpg --output revoc-key.asc --gen-revoke “zhaomengzi”

pour générer un certificat de révocation

Exercice 4

nano message.txt

gpg --recipient “zhaomengzi” --encrypt message.txt

rejane dalce