GPG (GnuPG – GNU Privacy Guard)
Présentation

- Commande line tool
- Implémentation du standard OpenPGP (PGP)
- Permet de chiffrer et signer des données et communications
- Garantie authenticité, intégrité et confidentialité
- Chiffrement asymétrique : inconvénient : devoir stocker quelque part la clé privée
- Inclus dans Enigmail (extension pour Thunderbird)

Cryptographie asymétrique

- Donnée publique (clé publique)
- Donnée privée (clé privée)
- Garder confidentialité
- « Asymétrique » car 2 clés mises en jeu
- Clé de chiffrement = clé publique
- Clé de déchiffrement = clé privée
- Clé privée transmise à personne, alors que clé publique transmise sans restriction

Signature numérique
Expéditeur utilise sa clef privée pour coder un message que le destinataire peut décoder avec la clef publique de l'expéditeur. S'il réussit à le déchiffrer, cela veut dire que c'est bien Alice qui est l'expéditeur.

Cryptographie asymétrique : fondée sur les fonctions à sens unique et à brèche secrète.

- Fonctions à sens unique : fonctions mathématiques telles qu'une fois appliquées à un message, il est extrêmement difficile de retrouver le message original = clé publique
- L'existence d'une brèche secrète permet cependant à la personne qui a conçu la fonction à sens unique de décoder facilement le message grâce à un élément d'information qu'elle possède = clef privée.

En réalité, on utilise une fonction classique pour le chiffrement, ce qui fait la différence, c'est le paramètre que l'on donne à cette fonction. Dans notre cas, c'est la clé publique ou la clé privée qui est donnée en paramètre.

La connaissance d'une clé ne permet pas d'en déduire l'autre.

Inconvénient et limites

- Moins performant que le chiffrement symétrique car temps de traitement plus long
- Les clés doivent être beaucoup plus longue
- Transmission initiale de la clé publique sur canal non sécurisé expose des attaques de l'homme du milieu, on fait généralement appel à une infrastructure à clefs publiques

On peut utiliser le chiffrement asymétrique pour protéger la mise en place d'un chiffrement symétrique car partage de l'unique clé secrète.

Mécanisme d'authentification : s'assurer que l'expéditeur est bien celui que l'on pense.

- Bob -> Alice : Bob chiffre avec sa clé privée un condensat, puis le chiffre avec clé publique de Alice

- Alice <- Bob : Alice déchiffre le message avec sa clé privée, ensuite déchiffre le condensant avec la clé publique de Bob pour s'assurer que c'est bien Bob qui l'a envoyé.
- Cela utilise la propriété des paires de clés asymétriques, on peut chiffrer avec clé publique et déchiffrer avec clé privée, on peut aussi chiffrer avec clé privée et déchiffré avec clé publique.

gpg ou pgp : paire de clé, asymétrique, privée et publique

gpg --gen-key
gpg --full-gen-key

gpg -K : clés secrètes disponibles
gpg -k : clés privées disponibles

gpg --encrypt-files test.txt
gpg --decrypt-files test.txt.gpg

gpg -e -s -r alfonse.spoutnik@urss.ru
gpg –encrypt –sign –recipent alfonse.spoutnik@urss.ru