TP 8 – Utilisation de la librairie pycrypto

Yann.Esposito@lif.univ-mrs.fr
28 novembre 2005

☞ Le but va être de se familiariser avec la librairie de cryptographie pycrypto. Cette librairie peut-être importée avec la commande `import Crypto`. Attention la majuscule est importante.

1 Cryptographie symmétrique (AES)

Les algorithmes d'encryptions peuvent être importer avec la commande `import Crypto.Cipher`. Les algorithme d'encrytions transforme des données d'entrées (généralement des chaînes de caractères) de façon dépendante d'une variable `cle` produisant ainsi le `ciphertext`. Cette transformation peut aisément être inversée si (et, espérons-le, seulement si) on connaît la clé.

Pour une encryption sécurisée, il doit être très difficile de trouver le texte original sans connaissance de la clé.

Les `Block ciphers` prennent des entrées de taille fixe (généralement 8 ou 16 octects de long) et les chiffre. Les `Block cipher` peuvent fonctionner en utilisant plusieurs modes. Le plus simple est `Electronic Code Book` (ou mode `ECB`). Dans ce mode, chaque bloc est simplement chiffré pour produire le `ciphertext`. Ce mode peut-être dangereux parce que beaucoup de fichier contiennent des messages connus de longueur supérieure à la taille des blocs. Par exemple, dans un fichier contenant du code C, il y a souvent des commentaires ne contenant que des astérixes. Tous ces messages identiques seront alors encryptés de manière identique. Un adversaire pourrait alors être capable d'utiliser cette structure pour obtenir des informations sur le texte.

Pour éliminer cette faiblesse, il y a d'autres modes dans lesquels le texte est combiné avec le `ciphertext` précédent avant l'encryption. Cette façon de procéder permet d'éviter les structures répétitives.

Un de ces mode est le `Cipher Block Chaining` (ou mode CBC) et un autre est le `Cipher FeedBack` (ou mode CFB). Le mode CBC encrypte toujours par blocks and par conséquent est à peine plus lent que le mode ECB. Le mode CFB encrypte en mode octet par octet et est beaucoup plus lent que les deux autres modes. De plus le mode CFB demande une chaine de caractère d'initialisation d'une longueur de 8 ou 16 octects (cela dépend de l'algorithme).

1.1. téléchargez le fichier exemple et observez comment marche les trois modes.

1.2. Vérifiez la vitesse de chiffrement et de déchiffrement des données en modifiant légèrement le programme et en lui permettant de chiffrer des fichiers.

2 Chiffrement avec clés publiques

Dans le chiffrement avec clés publiques. Un individu qui voudra recevoir des fichier qu'il sera le seul à pouvoir lire crée un couple de clé ; clé publique clé privée. La clé publique peut-être diffusée à tous. Mais le message ne pourra être déchiffrée que par la personne possédant la clé privée.

2.1. Téléchargez les fichiers d'encryption par clé publique. Comprenez le fonctionnement de ces programmes. Vous utiliserez ceux-ci pour chiffrer vos comptes-rendus hebdomadaires. Les clés publiques de vos responsables de TP sont disponibles en lignes.

2.2. Générez un couple de clés (publique et privée).

2.3. Vérifiez le temps que prend le décryptage d'un fichier en fonction de la taille de la clé. Essayez avec une clé de taille 256, 512, 1024 et 4096.

2.4. Pourquoi ne faut-il pas construire un tunnel par connexion ?

❦