CRYPTOGRAPHIE
TP N°3

Objectif du TP : *Nous abordons ici questions de chiffrement et de signatures "réels". Ces programmes seront les premiers programmes de cryptographie que nous feront et qui seront réellement utilisables : les algorithmes, les spécifications des clefs sont sécurisés et standards. Les algorithmes seront DSA pour la signature, RSA pour le transfert des clefs de sessions, Blowfish pour le chiffrement des messages. L'algo de calcul de digest est SHA1 (un peu dépassé en fait). Notez cependant que la classe java.securite est bridée conformément à la législation américaine...Idéalement, il faudrait utiliser la librairie Bounty Castle....*

ENONCE :

Exercice 1 :
Il s'agit ici de faire les programmes permettant de chiffrer et déchiffrer des fichiers en utilisant un véritable algorithme (ici Blowfish). Nous allons de plus chiffrer la clef secrete avec la clef publique du recepteur en utilisant RSA avant de la sauvegarder...

- Un premier programme génère des couples clefs publiques, clefs privées et les sauve dans des fichiers separes (KeyPubAlice, KprivAlice.....) pour un utilisateur (ici Alice). Contrairement a ce qu'il faudrait faire, nous ne chiffrons pas la clef privée...
- Le second programme devra permettre de chiffrer un fichier quelconque en utilisant une clef de session. La clef de session est chiffrée avec la clef publique du recepteur, lue dans un fichier. le programme génère donc deux fichiers, un correspondant au fichier chiffré, l'autre au fichier contenant la clef de session chiffrée.
- Le troisième programme devra permettre de déchiffrer un fichier à l'aide de deux autres fichiers : celui contenant la clef privée et celui contenant la clef de session.

Testez vos programmes en créant trois couples de clefs pour Alice, Bob et Mallory et personnifiez chaque acteur lors de l'envoie d'un message.....

Exercice 2 :
Il s'agira ici de signer des messages en utilisant les clefs précédentes.
- Le premier programme devra permettre de signer un fichier.
- Le second programme devra permettre de vérifier la signature du message.

Ici aussi, personnifiez Alice, Bob et Mallory.

Exercice 3 :
Utilisez ce que vous avez fait précédemment pour faire les deux programmes suivants :
- Le premier signe un message avec la clef d'Alice, et chiffre le message + sa signature avec la clef publique de Bob.
- Le second devra permettre a Bob de déchiffrer le message et de vérifier qu'Alice en est bien a l'origine.

Ici aussi, personnifiez Alice, Bob et Mallory.

Remarquez que le problème à ce stade est de gérer les trousseaux de clef. En particulier, Bob devra être capable de sortir la clef d'Alice si il reçoit un message prétendument d'Alice. Pour cela, il nous faudrait des certificats qui feront l'objet du TP suivant.