TP7 : Cryptographie asymétrique

1 Boîte à outils

On va d'abord constituer une petite bibliothèque de calcul modulo un nombre premier, permettant de réaliser :

- L'inversion modulo p (via l'algorithme d'Euclide étendu)
- Un crible pour construire la liste des nombres premiers inférieurs à une certaine borne. L'algorithme classique est le suivant : partir d'un tableau de taille n, et marquer les cases multiples de i où $i > 1$ est le numéro de la plus petite case non marquée. À la fin, les cases non marquées sont aux positions premières. Vous pourrez générer la liste des premiers jusqu'à 1000000 et la stocker dans un fichier.
- Un test de primalité
- Le calcul des diviseurs premiers d'un entier donné
- Le calcul d'un générateur de $\mathbb{Z}/p\mathbb{Z}^*$ (on pourra tirer un élément au hasard tant qu'on ne trouve pas de générateur)
- L'exponentiation modulo un nombre premier

2 Diffie-Hellman

Implémenter une communication entre Arielle et Bertrand sous TCP (on pourra considérer que l'un des deux est un serveur et l'autre un client) permettant d'appliquer le protocole de Diffie-Hellman. Faites afficher à chaque participant les étapes du protocole sur sa sortie standard.

3 L'homme du milieu

On se place maintenant dans le cadre d'une attaque par l'homme du milieu. Pour ne pas rentrer dans les détails techniques de comment l'attaquant peut intercepter les communications, on va se placer dans le cadre où les clients sur les machines d'Arielle et Bertrand communiquent avec un serveur sur la machine de l'attaquant Laurent.

Arielle et Bertrand veulent communiquer en utilisant RSA. Implémenter le serveur de Laurent pour qu'il se fasse passer pour Bertrand auprès d'Arielle (et inversement). Laurent affichera sur la sortie standard les messages échangés par Arielle et Bertrand (sous forme déchiffrée).

4 Malléabilité et signature

Laurent n'a pas eu le temps de mettre en place sa stratégie d'attaque par homme du milieu, mais il peut cependant intercepter les messages transmis (il ne peut juste pas les déchiffrer). Il a accès aux clés publiques RSA d'Arielle et Bertrand, ainsi qu'aux messages chiffrés, qu'il peut intercepter, modifier et retransmettre.

Implémenter Laurent pour que, lorsqu'il intercepte un message chiffré c correspondant au message m (qu'il ne peut retrouver), il transmette à l'autre participant un message c' correspondant au message $2m$.