Projet Sécrypt - Info 3

Sujet

Le projet consiste à implanter, dans le langage de programmation de votre choix, deux procédés de chiffrement, l'un à clef secrète, l'autre étant l'algorithme RSA. La seule contrainte étant que vos programmes doivent s'exécuter sur les ordinateurs sous linux en salle de tp de l'institut Galilée. **Un projet est réalisé soit par un monôme, soit par un binôme.**

Lors de la remise du projet, en salle machine, la bonne implantation des procédés de chiffrement sera testée. Vous serez évaluer en fonction des points suivants :
– Compilation / exécution des programmes ;
– Connaissance de votre code ;
– Tests sur certaines entrées.
Il ne vous est demandé aucune documentation ni d'effectuer une présentation. Lors de la remise des projets, vous serez tous en salle tp et le correcteur (moi !) évaluera les binômes (ou monômes) les uns après les autres en testant les programmes et en interrogeant les développeurs.

Procédé de chiffrement à clef secrète

Écrire un programme qui implante l'un des procédés de chiffrement suivants : DES, IDEA ou AES. Il vous faudra ainsi coder les algorithmes de chiffrement, de déchiffrement et l'algorithme de dérivation des clefs. Ce programme prendra en entrée un texte (qu'il vous faudra convertir en une chaîne de bits de la longueur spécifiée dans l'algorithme choisi) ainsi qu'une clef secrète principale (qui sera un bloc d'un certain nombre de bits ; ce nombre étant également spécifié dans la description du procédé).

Implantation de RSA

Écrire un programme qui implante le procédé de chiffrement RSA. Il vous faudra coder l'algorithme de génération des clefs (publiques et privées) qui prend en entrée deux nombres premiers p et q, ainsi que les algorithmes de chiffrement et de déchiffrement proprement dits qui prennent en entrée un entier $m \in \mathbb{Z}_{pq}$ ainsi que la clef publique pour le premier, et la clef privée pour le second.