Programmation de RSA

Votre travail doit être rendu le mercredi 30 novembre. Le travail est effectué en binôme. Tous les fichiers utiles doivent être envoyés par mèl (avec une description de ces fichiers) à `coulbois@cmi.univ-mrs.fr`. Le code doit être lisible et bien documenté.

L'objectif de ce travail est de programmer RSA en Java.

Les API Java contiennent des classes qui faciliteront votre travail. La classe `BigInteger` contient en particulier, toutes les opérations mathématiques dont vous avez besoin. Plus généralement, la `Java cryptography extension` vous aidera à faire l'interface avec d'autres sytèmes cryptographiques. Vous êtes invités à minimiser votre effort de programmation en utilisant les fonctionnalités de Java.

L'objectif minimal de ces 4 séances (deux TP et deux TD) est de proposer :

1. une fonction de génération et de vérification de clés RSA
2. les fonctions de chiffrement et déchiffrement RSA ;
3. une interface pour chiffrer et déchiffrer un texte de longueur arbitraire en mode CBC ;
4. une fonction d'importation de clés RSA de SSH ou GPG (utiliser `java.security`).

Pour le dernier point vous serez amenés à lire les RFC correspondant à SSH et à ses fichiers de stockage de clés.

NB : Les étudiants non-familiers de Java, peuvent programmer en C, C++, etc.