MATH EN INFO

PROJET N° 2

Projet 2 - RSA

1 Objectif

L'objectif de ce projet est d'implémenter une version complète du protocole SSL basée sur l'algorithme R.S.A. Pour rappel, il s'agit du protocole de cryptographie asymétrique utilisé pour chiffrer les transmissions courtes (https par exemple).

La principale difficulté de l'implémentation de SSL vient de la taille très importante des nombres utilisés. En effet, pour assurer un minimum de sécurité, il convient d'utiliser des nombres dont l'ordre de grandeur avoisine les 2^{128}. L'utilisation des *Integer* et des *Long* n'est donc pas envisageable.

Par conséquent nous devons développer notre propre structure de données capable de gérer des entiers aussi grands soient-ils. Pour cela, nous allons, comme dans le projet précédent, utiliser une représentation binaire (bitset).

2 Organisation

Vu le nombre conséquent de fonctionnalités devant être implémentées, vous êtes invité à travailler en groupe de 6-8 étudiants (environ). Il vous est fortement conseillé de vous répartir le travail et de bien communiquer entre-vous.

Afin de vous aider et de vous guider durant ce projet, vous trouverez sur le commun

- Une version propre du moteur disposant de certaines fonctionnalités déjà implémentées.
- Un programme *ProjetRSA.exe* (compressé en .7z) contenant une série de défis qui vous guideront dans le développement de SSL ainsi qu'une documentation de ces défis.