Rapport projet :
implémentation El Gamal

Question 1 :

Nous avons choisis d'utiliser le langage Java pour implémenter El Gamal. Pour gérer les nombres entiers de grande taille (1024 bits), nous avons utilisé la classe BigInteger (https://docs.oracle.com/javase/7/docs/api/java/math/BigInteger.html) présent dans la bibliothèque Math de Java. Dans la classe BigInteger il y a déjà d'implémenter les opérations suivantes : addition, soustraction, multiplication, division, modulo, et, ou, xor, not.

Question 2 :

Un nombre aléatoire est cryptographiquement sûr lorsque le générateur utilisé pour le générer est considéré comme un générateur de nombre pseudo-aléatoires cryptographique. C'est à dire que le générateur est capable de générer un nombre proche de l'aléatoire parfait, le nombre généré n'est alors pas possible à prévoir.
Afin de générer ces nombres aléatoires nous utilisons un constructeur fourni dans la classe BigInteger en association avec la classe SecureRandom. (https://docs.oracle.com/javase/7/docs/api/java/security/SecureRandom.html)