Arithmétique et DLP

Version du 24 février 2015

TME

Exercice 1 – Arithmétique de base

1. Écrire un programme permettant de calculer un PGCD et une relation de Bézout entre deux entiers (faites afficher les étapes intermédaires comme vu en cours et en TD).
2. Écrire une fonction permettant de calculer des inverses modulaires. En déduire une fonction permettant de calculer tous les inversibles de l'anneau $\mathbb{Z}/N\mathbb{Z}$ pour N un entier donné.
3. On rappelle que l'indicateur d'Euler d'un entier N, noté $\phi(N)$, représente le nombre d'entiers positifs et plus petit que N premier avec N. Écrire une fonction permettant de faire son calcul.
4. Faites la même chose que pour les questions précédentes en utilisant une bibliothèque permettant de gérer de grands entiers (GMP pour le C par exemple).

Exercice 2 – Chiffrement et Arithmétique Modulaire

1. Écrire un programme permettant de réaliser le chiffrement et déchiffrement de type `ADFGVX`.
2. Écrire un programme permettant de réaliser le chiffrement et déchiffrement affine. En particulier, ce programme devra tester si la clé donnée en entrée est cohérente avec ce qui a été vu en cours.
3. Implémenter la cryptanalyse du chiffrement affine comme vu en TD.

Exercice 3 – Logarithme Discret et Cryptologie

Le groupe cyclique support au problème du logarithme discret dans cet exercice sera celui des inverses modulo un nombre premier. Toutes les implémentations devront être réalisées en utilisant des grands entiers.

1. Implémenter la version itérative de l'exponentiation modulaire comme vu en Cours et en TD.

   Dans le reste de cet exercice on s'intéresse au groupe multiplicatif $G = (\mathbb{Z}/p\mathbb{Z})^\times$ avec p un entier premier. On rappelle que ce groupe est cyclique.
2. En utilisant une bibliothèque permettant de tester rapidement si un entier est premier, écrire une fonction, presque brute-force, permettant de factoriser $p-1$ (on pourra par exemple utiliser la fonction GMP `mpz_nextprime`).
3. En utilisant la fonction de la question précédente, écrivez en une permettant de calculer l'ordre d'un élément $g \in G$.
4. Soit g_1 et g_2 deux éléments de G respectivement d'ordre m et n, rappeler quels sont les ordres possibles de $g_1 g_2$. À l'aide de cette propriété, implémenter une fonction permettant de trouver un générateur de ce groupe cyclique.
5. Implèmenter l'algorithme BSGS de Shanks pour la résolution du logarithme discret dans le groupe G.

