Courbes elliptiques — N1MA8W04

Responsables : G. Castagnos, D. Robert

Le logarithme discret

1 Écrire une fonction prenant en entrée k et ressortant (p, q, g) tels que q soit un nombre premier de k bits et p un premier tels que $p - 1 = 2q$ et g un élément de $(\mathbf{Z}/p\mathbf{Z})^\times$ d'ordre q.

2 Implanter la méthode naïve de calcul du logarithme discret. Tester sur des exemples à l'aide de la fonction de l'exercice précédent.

3 Implanter et tester la méthode *Baby Step / Giant Step*.

4 Implanter la méthode ρ de Pollard dans $\mathbf{Z}/p\mathbf{Z}$. Pour calculer x dans $h = g^x$, on partionnera $\mathbf{Z}/p\mathbf{Z}$ en S_0, S_1, S_2 avec $S_i = \{X \in \mathbf{Z}/p\mathbf{Z}, X \equiv i \ (mod\ 3)\}$. On utilisera la fonction d'itération définie par

$$f(X) = \begin{cases} X^2 \text{ si } X \in S_0, \\ hX \text{ si } X \in S_1, \\ gX \text{ si } X \in S_2. \end{cases}$$

5 Implanter la méthode de Pohlig–Hellman. Tester dans $(\mathbf{Z}/p\mathbf{Z})^\times$. Puis adapter le code pour travailler dans un corps fini.