TD El-Gamal : preuves de sécurité et difficulté du logarithme discret

Vous pouvez vous servir de Python pour effectuer les calculs de ce TD. Nous vous fournissons des classes pour faire les calculs modulo p dans le fichier TD7-ZpZ.py sur Moodle.

Exercice 1. ***Un exemple pour Pohlig-Hellman***
Considérons le problème du logarithme discret dans $(\mathbb{Z}/p\mathbb{Z}^\star)$ pour $p = 31$, qui est un groupe d'ordre $\varphi(p) = p - 1 = 30 = 5 \cdot 3 \cdot 2$ engendré par $g = 3$.
Simulez l'algorithme de Pohlig-Hellman pour réduire le calcul du logarithme discret de $h = 26$ à des logarithmes discrets dans des plus petits groupes. Détaillez les calculs, sauf ceux des logarithmes discrets dans les plus petits groupes où les résultats suffisent.

Exercice 2. ***Un exemple de Baby-Step/Giant-Step***
Considérez le problème du logarithme discret dans $(\mathbb{Z}/p\mathbb{Z}^\star)$ pour $p = 37$, qui est un groupe engendré par $g = 2$.
Simulez l'exécution de l'algorithme de Baby-Step/Giant-Step pour l'entrée $h = 6$.

Exercice 3. ***Un exemple de El-Gamal dans*** $\mathbb{G} \subsetneq \mathbb{Z}/p\mathbb{Z}^\star$
Soient $q = 83$ et $p = 2q + 1$ premier et considérons le groupe multiplicatif $(\mathbb{Z}/p\mathbb{Z}^\star)$. Comme le cardinal de ce groupe n'est pas premier et que c'était l'une des recommandations du cours, nous allons considérer un sous-groupe $\mathbb{G}$ de $(\mathbb{Z}/p\mathbb{Z}^\star)$. Posons $\mathbb{G} = \{g^{2i} | 0 \leq i < q\}$ le sous-groupe des carrés, qui est d'ordre q premier. Nous choisirons le générateur $g' = 4 \bmod 167$ pour $\mathbb{G}$.

1. Rappelez pourquoi on souhaite que l'ordre du groupe soit premier.
2. Expliquez pourquoi $\mathbb{G}$ est un groupe, c'est-à-dire que $1 \in \mathbb{G}$, $g \cdot g' \in \mathbb{G}$ et que $g^{-1} \in \mathbb{G}$ pour tout $g, g' \in \mathbb{G}$.
3. Supposons que Bob choissise la clé secrète 37. Donnez la clé publique de Bob.
4. Alice souhaite envoyer le message $m = 65 \bmod 167 \in \mathbb{G}$ à Bob. Donnez le chiffré correspondant à l'aléa $y = 71$.
5. Déchiffrez le message chiffré c reçu par Bob en indiquant toutes les étapes du calcul.