TD : El-Gamal et algorithmes pour le logarithme discret

Romain Lebreton

26 Octobre 2017

Vous pouvez bien sûr vous servir de Python pour effectuer les calculs de ce TD.

1. **Un exemple de El-Gamal dans $\mathbb{Z}/p\mathbb{Z}^\star$:**
   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 $\mathbb{G} = \left\{g^{2i} | 0 \leq i < q\right\}$ le sous-groupe des carrés, qui est d'ordre q premier. Nous choisirons le générateur $g = 4 \bmod 167$ pour $\mathbb{G}$.

   i. Rappelez pourquoi on souhaite que l'ordre du groupe soit premier.
   ii. Supposons que Bob choissise la clé secrète 37. Donnez la clé publique de Bob.
   iii. Alice souhaite envoyer le message $m = 65 = 30^2 \bmod 167$ à Bob. Donnez le chiffré correspondant à l'aléa $y = 71$.
   iv. Déchiffrez le message chiffré c reçu par Bob en indiquant toutes les étapes du calcul.

2. **Preuves de sécurité de El-Gamal**

   i. Montrez que, sous l'hypothèse que le problème calculatoire du logarithme discret est difficile (LD), alors l'attaque TB-CPA est difficile. Pour ceci, veuillez exhiber une réduction polynomiale.
   ii. En fait TB-CPA est équivalent à LD. Montrez donc l'autre réduction.
   iii. Nous avons vu dans le cours que CDH implique OW-CPA. Montrez que ces problèmes sont équivalents en donnant une réduction dans l'autre sens.

3. **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 $g = 3$.

i. 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.

4. **Un exemple de Baby-Step/Giant-Step**
   Considérez le problème du logarithme discret dans $(\mathbb{Z}/p\mathbb{Z}^\star)$ pour $p = 29$, qui est un groupe d'ordre 28 engendré par $g = 2$.

   i. Simulez l'exécution de l'algorithme de Baby-Step/Giant-Step pour l'entrée $h = 17$.