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

Exercice 1. ***Difficulté pratique du logarithme discret***

Considérons le problème du logarithme discret dans le groupe $\mathbb{G} = \mathbb{Z}/p\mathbb{Z}^\star$ avec p un nombre premier de 128 bits, pour lequel on se donne un générateur g. Nous supposerons qu'un ordinateur a une fréquence de 1 Ghz, *i.e.* qu'il effectue 10^9 opérations $\{+, -, \times, /\}$ dans $\mathbb{G}$ par seconde.

i. Donner un ordre de grandeur du temps qu'il faut pour calculer g^x avec $0 \leq x < p-1$ dans 2 cas : 1) en utilisant l'algorithme naïf, 2) en utilisant un algorithme rapide (dire quel est le nom de cet algorithme et si besoin redonner son code).

ii. Donner un algorithme naïf pour calculer le logarithme discret de $h \in \mathbb{G}$, *i.e.* l'exposant $0 \leq x < p-1$ tel que $h = g^x$. Donner un ordre de grandeur du temps de calcul de cet algorithme.

Exercice 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.

Exercice 3. ***Générateur de $\mathbb{Z}/p\mathbb{Z}^\star$***

Soit $g \in \mathbb{Z}/p\mathbb{Z}^\star$ et $\mathcal{O} = \{g^i\}_{i\in\mathbb{N}}$ l'orbite de g. On peut voir $\mathcal{O}$ comme un graphe où les sommets sont les g^i et les arêtes sont les $g^i \to g^{i+1}$ pour i entier.
Nous avons admis dans le cours que $\mathbb{Z}/p\mathbb{Z}^\star$ est un groupe cyclique, *i.e.* qu'il existe $g \in \mathbb{Z}/p\mathbb{Z}^\star$ tel que l'orbite de g soit un cycle d'ordre $p-1$. Nous allons montrer dans cet exercice une partie de ce résultat : l'orbite de tout élément g est un cycle dont la longueur divise $p-1$.

i. Montrons que le graphe de $\mathcal{O}$ a une forme de ρ, autrement dit qu'il est ultimement périodique. Pour prouver cela mathématiquement, il faut montrer qu'il existe 2 entiers $u \neq v$ tels que $g^u = g^v$ et en déduire que $g^{u+n} = g^{v+n}$ pour tout entier n.
Indice : Les puissances de g vivent dans un ensemble fini.

Un graphe de $\mathcal{O}$ en ρ se décompose en la queue du ρ puis un cycle. La taille de la queue du ρ est donnée par le plus petit u tel qu'il existe $v \neq u$ avec $g^u = g^v$.

ii. Puisque g est inversible, montrer que la taille de la queue du ρ est nulle, c'est-à-dire que le graphe est juste un cycle.

On appelle *ordre* de g la taille du cycle de $\mathcal{O}$, *i.e.* le plus petit entier $o > 0$ tel que $g^o = 1$.

iii. Montrer que si $g^w = 1$ alors w est un multiple de o.
Indice : Soustraire o à w jusqu'à obtenir un w' tel que $g^{w'} = 1$ et $0 \leq w' < o$.

iv. En utilisant un théorème du cours, montrer que o divise $p-1$.

Exercice 4. ***Exemple de preuve qu'un groupe est cyclique***

La preuve que $\mathbb{Z}/p\mathbb{Z}^\star$ est cyclique pour tout p premier est un peu trop longue pour faire un exercice de TD. Cependant il est plus facile de montrer que les groupes de cardinalité première sont cycliques. On peut appliquer ce théorème au sous-groupe des carrés de $\mathbb{Z}/p\mathbb{Z}^\star$ quand $p = 2q+1$ avec p et q premier.

i. Rappelez l'énoncé du petit théorème de Fermat.

ii. Adaptez la preuve du petit théorème de Fermat pour montrer le théorème d'Euler : Pour tout groupe $(G, \times)$ avec $q = |G|$ et tout élément $x \in G$, on a $x^q = 1$.

iii. En déduire qu'un groupe de cardinalité première est cyclique.

Exercice 5. ***Un exemple de El-Gamal dans*** $\mathbb{G} = \mathbb{Z}/p\mathbb{Z}^\star$

Vous pouvez vous servir de Python pour effectuer les calculs de cet exercice. Nous vous fournissons des classes pour faire les calculs modulo p dans le fichier TD7-ZpZ.py sur Moodle.
Soit $p = 167$ premier et considérons le groupe multiplicatif $\mathbb{G} = (\mathbb{Z}/p\mathbb{Z}^\star)$ avec le générateur $g = 5 \bmod 167$.

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