TD7 – Échange de clefs

Exercice 1. *Échange de clef non sûr*

On considère l'échange de clef suivant.

1 Alice tire uniformément k_A, $r \in \{0,1\}^n$ et envoie $s = k_A \oplus r$ à Bob
2 Bob choisit uniformément $t \in \{0,1\}^n$ et envoie $u = s \oplus t$ à Alice
3 Alice calcule $w = u \oplus r$ et envoie w à Bob
4 Bob calcule $k_B = w \oplus t$

1. Montrer qu'Alice et Bob partagent la même clef $k_A = k_B$.
2. Montrer que ce protocole n'est pas sûr : identifier l'ensemble des messages envoyés, et montrer qu'un observateur ayant ces messages peut calculer la clef commune.

Exercice 2. *Algorithme « pas de bébé – pas de géant »*

Soit G un groupe cyclique d'ordre q et g un générateur de G. Étant donné $x \in G$, on cherche l'unique $e \in \{0, \dots, q-1\}$ tel que $g^e = x$. On fixe un entier ℓ tel que $2 < \ell < q$.

1. *Pas de géants.* Écrire un algorithme pour calculer l'ensemble $A = \{g^{\ell t} : 0 \leq t < q/\ell\}$. Combien d'opérations dans G sont nécessaires ?
2. *Pas de bébés.* Écrire un algorithme pour calculer l'ensemble $B = \{xg^t : 0 \leq t < \ell\}$. Combien d'opérations dans G sont nécessaires ?
3. Représenter graphiquement le groupe cyclique G et les ensembles A et B. *Représenter G par un cycle, et considérer un x quelconque, en particulier dessiner un cas où $x \notin A$.*
4. Montrer que $A \cap B \neq \emptyset$. *Indication. Écrire $x = g^e$ et $e = u\ell + v$ la division euclidienne de e par ℓ ; montrer que $g^{(u+1)\ell} \in A \cap B$.*
5. En déduire un algorithme pour calculer le logarithme discret de x. Exprimer sa complexité en fonction de ℓ et q.
6. Trouver une valeur pour ℓ qui minimise la complexité obtenue.
7. Appliquer l'algorithme précédent pour calculer le logarithme de 17 en base 2, dans $\mathbb{Z}/29\mathbb{Z}$.

Exercice 3. *Variante du logarithme discret*

Soit p un nombre premier, x inversible dans $\mathbb{Z}/(p-1)\mathbb{Z}$ et $y = g^x \bmod p$ où g est non nul.

✎ Montrer qu'étant donné p, x et y, on peut calculer g efficacement. *Penser à inverser $x \bmod p-1$.*