TD : Protocoles d'échange de clés

1. Le logarithme discret et les problèmes calculatoire et décisionnel de Diffie-Hellman sont-ils *difficiles* dans le groupe additif $(\mathbb{Z}/n\mathbb{Z}, +)$?

2. Supposons qu'on applique le protocole de Diffie-Hellman avec le groupe $(\mathbb{Z}/p\mathbb{Z}^\star, \times)$, où p est un nombre premier de n bits. Donner la complexité du protocole (complexité des opérations effectuées par les deux protagonistes, nombre de bits échangés), en supposant préalablement fixés le nombre premier p et un générateur g.

3. Montrer que le protocole de Diffie-Hellman est vulnérable à une attaque de type *man-in-the-middle*, c'est-à-dire qu'un attaquant qui peut intercepter et modifier le contenu des communications entre Alice et Bob peut truquer le résultat de l'échange de clé : l'attaquant peut calculer deux clés k_A et k_B et faire en sorte qu'à la fin du protocole, Alice ait la clé k_A et Bob la clé k_B, tout en étant tous deux persuadés que le protocole s'est déroulé sans encombre.

4. On considère le protocole suivant d'échange de clés :

- Alice tire aléatoirement $k, r \in \{0,1\}^n$ et envoie $s = k \oplus r$ à Bob ;
- Bob tire aléatoirement $t \in \{0,1\}^n$ et envoie $u = s \oplus t$ à Alice ;
- Alice calcule $w = u \oplus r$ et l'envoie à Bob ;
- Alice conserve k comme clé, et Bob $w \oplus t$.

i. Montrer qu'Alice et Bob possèdent la même clé en fin de protocole.

ii. Montrer que ce protocole n'est pas sûr.