TD 10 : Protocole Diffie-Hellman

Christina Boura

Exercice 1 *Diffie-Hellman*

Alice et Bob souhaitent échanger une clé secrète en utilisant le protocole d'échange de clés Diffie-Hellman. Ils se mettent d'accord sur le nombre premier $p = 17$. Afin d'exécuter le protocole, Alice et Bob ont également besoin de se mettre d'accord sur un élément générateur de $\mathbb{Z}_{17}^*$, qu'on notera α.

1. Calculer le plus petit élément générateur de $\mathbb{Z}_{17}^*$.
2. Alice choisit comme clé secrète $a = 5$ tandis que Bob choisit comme clé secrète $b = 7$. Calculer la clé publique A d'Alice et la clé publique B de Bob, en utilisant l'élément générateur α calculé dans la question précédente.
3. Calculer la clé secrète commune k_{AB} qu'établissent Alice et Bob après l'exécution du protocole.

Exercice 2 *L'ordre d'un élément divise la cardinalité du groupe*

Montrer que l'ordre d'un élément de $\mathbb{Z}_p^*$, où p est un nombre premier, divise la cardinalité du groupe.

Exercice 3 *Diffie-Hellman et l'attaque de l'homme du milieu*

Alice et Bob veulent échanger une clé secrète commune en utilisant le protocole Diffie-Hellman avec le nombre premier $p = 11$.

1. Trouver le plus petit élément primitif $\alpha \in \mathbb{Z}_p^*$.
2. Supposons qu'Alice choisit $a = 5$ et que Bob choisit $b = 9$. Calculer la clé commune qu'Alice et Bob partageront à la fin de l'exécution du protocole en utilisant l'élément primitif de l'étape précédente.
3. Supposons qu'Oscar réussit à faire une attaque en choisissant comme exposant pour son communication avec Alice $o = 4$ et pour celui avec Bob $o = 4$ également. Calculer les clés d'Alice de Bob et d'Oscar dans cette attaque.

Exercice 4 *Diffie-Hellman, valeurs faibles*

Pour l'échange de clés Diffie-Hellman, les clés privées sont choisies dans l'ensemble $\{2, ..., p-2\}$. Pourquoi, sont les valeurs 1 et $p-1$ exclues ? Décrire leur faiblesse.

Exercice 5 *Diffie-Hellman, Éve devine les clés privées*

Pour un échange de clés Diffie-Hellman avec paramètres $\alpha = 7$ et $p = 71$, les clés privées sont notées a et b. Les clés publiques calculées et transmises sont $A \equiv \alpha^a \mod p$ et $B \equiv \alpha^b \mod p$.

1. Donner des couples (a, b) possibles tels que la clé K calculée à la fin de la communication soit $K = 1$.
2. Donner des couples (a, b) possibles si on sait que $A \cdot B \equiv 7 \mod 71$.