TD 9 : Protocole Diffie-Hellman

christina.boura@uvsq.fr

3 avril 2018

Exercice 1 *Un peu d'arithmétique*

1. Montrer qu'un élément $a \in \mathbb{Z}_n$ est inversible si et seulement si a est premier avec n.
2. Montrer que si $a, b \in \mathbb{Z}_n$ sont inversibles, alors ab l'est aussi.

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 *Éléments primitifs*

Soit le groupe multiplicatif $\mathbb{Z}_7^*$.

1. Quel est l'ordre (ou la cardinalité) de ce groupe ? Justifier votre réponse.
2. Quels sont les ordres possibles pour un élément dans $\mathbb{Z}_7^*$?
3. Énumérer les éléments primitifs de $\mathbb{Z}_7^*$.

Exercice 4 *Ordre d'un élément dans un groupe*

Soit le groupe multiplicatif $\mathbb{Z}_{53}^*$.

1. Quels sont les ordres possibles pour un élément $a \in \mathbb{Z}_{53}^*$?
2. Vérifier que $a = 2$ est un élément primitif de ce groupe. On peut utiliser le résultat suivant :

   Théorème : Soit p un nombre premier impair et soit a un élément de $\mathbb{Z}_p^*$. Si pour tous les diviseurs premiers q de $p-1$
   $$a^{(p-1)/q} \not\equiv 1 \mod p,$$
   alors a est un élément primitif.

   Pour tester alors si un élément $a \in \mathbb{Z}_p^*$ est primitif on calcule $a^{(p-1)/q} \mod p$ pour tous les diviseurs q de $p-1$. Si aucun de ces calculs ne donne $1 \mod p$, alors a est un élément primitif.

Exercice 5 *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 6 *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 7 *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 $A \cdot B \equiv 7 \mod 71$.