Groupes cycliques et protocole Diffie-Hellman

christina.boura@uvsq.fr

1 Le protocole d'échange de clés de Diffie et Hellman

Whitfield Diffie et Martin Hellman ont proposé en 1976 le premier protocole cryptographique à clé publique. Leur découverte à été largement influencée par les idées de Ralph Merkle. Le protocole Diffie-Hellman (ou Diffie-Hellman-Merkle) fourni une solution pratique au problème de la distribution des clés à travers un canal non-sécurisé. Or, il permet à deux personnes d'établir une clé secrète commune sans devoir se rencontrer physiquement. Cette découverte a révolutionné le monde de la cryptographie en le forçant à réviser les règles du chiffrement.

Le système Diffie-Hellman, implanté aujourd'hui dans des nombreux protocoles cryptographiques libres ou commerciaux (SSH, TLS, IPSec, ...) est basé sur le problème du logarithme discret. Avant d'introduire ce concept mathématique, nous commençons par introduire cet algorithme d'échange de clés.

Pour établir une clé secrète commune, Alice et Bob commencent par se mettre d'accord sur deux valeurs publiques ; un très grand nombre premier p et un entier $\alpha \in \mathbb{Z}_p^* = \{1, 2, \ldots, p-1\}$. Nous verrons plus tard que α doit être un élément *primitif*. Alice choisit ensuite une valeur secrète a et calcule $A = \alpha^a \mod p$ et envoie A à Bob. De son côté, Bob choisit aussi une valeur secrète b et calcule $B = \alpha^b \mod p$. Il envoie ensuite B à Alice. Alice calcule maintenant $K := B^a \mod p$ pendant que Bob calcule $K' := A^b \mod p$. On peut maintenant voir que les deux côtés se sont mis d'accord sur une même valeur secrète $K = K'$.

En effet,

$$K \equiv B^a \mod p \equiv (\alpha^b)^a \equiv \alpha^{ab} \equiv (\alpha^a)^b \equiv A^b \equiv K' \mod p.$$

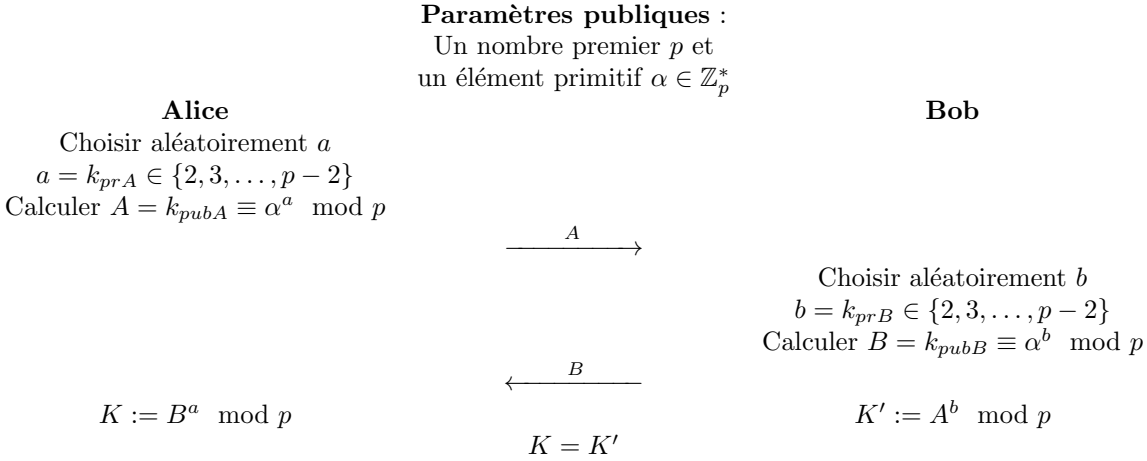

FIGURE 1 – Le protocole d'échange de clés de Diffie et Hellman

La phase de mise en place du protocole Diffie-Hellman est très similaire à celle du cryptosystème RSA. Comme pour RSA, un très grand nombre premier doit être généré avec un générateur aléatoire et ensuite testé par un algorithme probabiliste de primalité. La taille de l'entier p doit avoir une longueur similaire au module RSA, c'est-à-dire 2048 bits ou plus. La clé secrète K calculée à l'aide de ce protocole a le même nombre de bits que p. Si on souhaite l'utiliser comme la clé secrète d'un algorithme de chiffrement par bloc, par exemple le `3DES`, on peut utiliser que les 112 ou 168 bits de poids fort. Quelques fois, une fonction de hachage est appliquée à la clé générée et le résultat du hachage (c.-à.-d. l'empreinte) est utilisée comme

la clé secrète pour le chiffrement symétrique. Les clés privées a et b doivent être également générées à l'aide d'un bon générateur aléatoire, afin d'éviter qu'un attaquant puisse facilement les deviner. Les clés publiques A et B peuvent être calculées à l'aide de l'algorithme `square and multiply`. Dans la pratique elles sont souvent pré-calculées, en conséquence les calculs principaux qui doivent être effectués sont $B^a \mod p$ ou $A^b \mod p$. Ces calculs pouvaient être accélérés pour RSA en utilisant des exposants publiques de petite taille. Ceci n'est pas applicable dans le cas de Diffie-Hellman.

2 Groupes finis

On commence par la définition formelle d'un groupe.

Définition 2.1. Un groupe $(G, \circ)$ est un ensemble G muni d'une loi de composition interne, c'est-à-dire d'une application

$$\begin{array}{rcl} G \times G & \to & G \\ (a, b) & \mapsto & a \circ b \end{array}$$

vérifiant les propriétés suivantes :

1. La loi $\circ$ est associative : pour tous $a, b, c \in G$, $(a \circ b) \circ c = a \circ (b \circ c)$.
2. Il existe un élément neutre $e \in G$, tel que $a \circ e = e \circ a = a$, pour tout $a \in G$.
3. Pour tout élément $a \in G$ il existe un élément $a^{-1} \in G$, appelé *l'inverse de* a, tel que $a \circ a^{-1} = a^{-1} \circ a = e$.

Le groupe G est dit *abélien*, si de plus la loi $\circ$ est commutative, c'est-à-dire $a \circ b = b \circ a$ pour tous $a, b \in G$.

En cryptographie on utilise à la fois des groupes multiplicatifs ($\circ$ désigne la multiplication) et des groupes additifs ($\circ$ désigne l'addition).

Question : $\mathbb{Z}_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$ est-il un groupe fini pour la multiplication ?

Réponse : No. Plus précisément, on observe que la condition 3 de la définition 2.1 n'est pas vérifiée, puisque tous les éléments de $\mathbb{Z}_8$ ne possèdent pas un inverse multiplicatif. Les seuls éléments possédant un inverse multiplicatif dans cet exemple sont les éléments a tels que $\text{pgcd}(a, 8) = 1$, or les éléments $0, 2, 4, 6$ ne sont pas inversibles.

Cependant, on peut vérifier que l'ensemble $\mathbb{Z}_8 \setminus \{0, 2, 4, 6\} = \{1, 3, 5, 7\}$ forme un groupe abélien pour la multiplication modulo 8. De façon générale, nous avons le théorème suivant.

Théorème 2.2. *L'ensemble $\mathbb{Z}_n^*$ de tous les entiers $a \in \mathbb{Z}_n$ tels que pgcd$(a, n) = 1$ forme un groupe abélien pour la multiplication modulo n. L'élément neutre est $e = 1$.*

En cryptographie, on s'intéresse qu'aux groupes contenant un nombre fini d'éléments. On parle alors de *groupes finis*.

Définition 2.3. (Ordre d'un groupe) On appelle *cardinalité* ou *ordre* d'un groupe G, et on le note $|G|$, le nombre d'éléments de l'ensemble G.

Exemple 2.4. $(\mathbb{Z}_n^*, \cdot)$: L'ordre de ce groupe est $|\mathbb{Z}_n^*| = \phi(n)$. Par exemple,

$$|\mathbb{Z}_8^*| = \phi(8) = 2^3 - 2^2 = 4.$$

Pour les applications cryptographiques on s'intéresse principalement aux groupes $(\mathbb{Z}_p^*, \cdot)$, ou p est un nombre premier. Dans ce cas,

$$|\mathbb{Z}_p^*| = \phi(p) = p - 1.$$

2.1 Groupes cycliques

On définit ici l'*ordre d'un élément dans un groupe*.

Définition 2.5. L'*ordre* $\text{ord}(a)$ d'un élément a d'un groupe $(G, \circ)$ est le plus petit entier positif k tel que

$$a^k = \underbrace{a \circ a \circ \cdots \circ a}_{k \text{ fois}} = 1,$$

où 1 est l'élément neutre de G.

Exemple 2.6. On cherche à déterminer l'ordre de $a = 3$ dans le groupe $\mathbb{Z}_{11}^*$. On calcule alors des puissances successives de a jusqu'à obtenir l'élément 1.

$$\begin{aligned} a^1 &= 3 \\ a^2 &= a \cdot a = 3 \cdot 3 = 9 \\ a^3 &= a^2 \cdot a = 9 \cdot 3 = 27 \equiv 5 \mod 11 \\ a^4 &= a^3 \cdot a = 5 \cdot 3 = 15 \equiv 4 \mod 11 \\ a^5 &= a^4 \cdot a = 4 \cdot 3 = 12 \equiv 1 \mod 11 \end{aligned}$$

On conclut alors que $\text{ord}(3) = 5$.

Regardons ce qui se passe si on continue à multiplier le résultat par a :

$$\begin{aligned} a^6 &= a^5 \cdot a = 1 \cdot a \equiv 3 \mod 11 \\ a^7 &= a^5 \cdot a^2 = 1 \cdot a^2 \equiv 9 \mod 11 \\ a^8 &= a^5 \cdot a^3 = 1 \cdot a^3 \equiv 5 \mod 11 \\ a^9 &= a^5 \cdot a^4 = 1 \cdot a^4 \equiv 4 \mod 11 \\ a^{10} &= a^5 \cdot a^5 = 1 \cdot 1 \equiv 1 \mod 11 \\ a^{11} &= a^{10} \cdot a = 1 \cdot a \equiv 3 \mod 11 \\ &\vdots \end{aligned}$$

On remarque que les puissances de a parcourent la suite $\{3, 9, 5, 4, 1\}$ indéfiniment. Ce comportement cyclique nous amène à la définition suivante :

Définition 2.7. (*Groupe cyclique*) Un groupe G contenant un élément a d'ordre maximal $\text{ord}(a) = |G|$ est dit *cyclique*. Les éléments d'ordre maximal sont appelés éléments *primitifs* (ou *générateurs*).

Exemple 2.8. $\mathbb{Z}_{11}^*$. Le groupe $\mathbb{Z}_{11}^*$ est cyclique. En effet, nous pouvons constater que l'ordre de l'élément $a = 2$ est $\text{ord}(a) = 10 = |\mathbb{Z}_{11}^*| = \phi(11)$:

$$\begin{aligned} a &= 2 \\ a^2 &= 4 \\ a^3 &= 8 \\ a^4 &\equiv 5 \mod 11 \\ a^5 &\equiv 10 \mod 11 \end{aligned} \qquad \begin{aligned} a^6 &\equiv 9 \mod 11 \\ a^7 &\equiv 7 \mod 11 \\ a^8 &\equiv 3 \mod 11 \\ a^9 &\equiv 6 \mod 11 \\ a^{10} &\equiv 1 \mod 11 \end{aligned}$$

En particulier nous voyons que les puissances de a génèrent tous les éléments du groupe $\mathbb{Z}_{11}^*$.

i	1	2	3	4	5	6	7	8	9	10
2^i	2	4	8	5	10	9	7	3	6	1

En observant la dernière ligne de ce tableau, on voit qu'il n'y a pas de relation évidente entre les exposants i et les éléments 2^i, or il semble que l'ordre de ces derniers est aléatoire. Cette relation aléatoire en apparence a une importance majeure pour des cryptosystèmes de type Diffie-Hellman.

Les groupes cycliques sont très importants pour la cryptographie. Nous introduirons ici les propriétés les plus importantes pour les applications cryptographiques.

Théorème 2.9. *Soit p un nombre premier. Alors, le groupe $(\mathbb{Z}_p^*, \times)$ est un groupe abélien cyclique fini.*

Ce théorème indique que le groupe multiplicatif de chaque corps premier est cyclique. Cette propriété fait de ces groupes le choix le plus populaire pour la construction de cryptosystèmes basés sur le logarithme discret.

Exemple 2.10. On note dans le tableau ci-dessous tous les éléments de $\mathbb{Z}_{11}^*$ avec leur ordre multiplicatif correspondant.

a	1	2	3	4	5	6	7	8	9	10
ord(a)	1	10	5	5	5	10	10	10	5	2

On remarque que l'ordre de tous les éléments de $\mathbb{Z}_{11}^*$, est une des valeurs $1, 2, 5$ ou 10. Ce comportement s'explique par le théorème suivant.

Théorème 2.11. *Soit G un groupe fini. Alors, pour tout $a \in G$ nous avons :*

1. $a^{|G|} = 1$
2. ord(a) *divise* $|G|$.

Le premier résultat est une généralisation du Petit Théorème de Fermat à tous les groupes cycliques. Le dernier résultat découle du Théorème de Lagrange et est très important dans la pratique. Il indique que dans un groupe fini, seulement des éléments d'ordre divisant la cardinalité du groupe existent.

3 Sécurité du protocole Diffie-Hellman

Dans le cadre du protocole Diffie-Hellman, une adversaire *passive* Ève écoutant le trafic entre Alice et Bob ne peut pas calculer facilement la clé secrète que les deux parties établissent. Plus précisément, Éve doit s'affronter au *problème Diffie-Hellman* qui consiste à calculer $\alpha^{ab} \mod p$, à partir de α, p, $\alpha^a \mod p$ et $\alpha^b \mod p$.

La solution à ce problème devient triviale si Ève sait résoudre un autre problème, celui du *logarithme discret* dans $\mathbb{Z}_p^*$.

Nous avons vu que le groupe $\mathbb{Z}_p^*$ est un groupe cyclique fini. Par conséquent, il existe (au moins un) générateur α de ce groupe de façon que tout élément β du groupe s'écrit d'une façon unique sous la forme

$$\beta = \alpha^x,$$

pour $x \in \{1, \ldots, p-1\}$. L'exposant x est appelé le *logarithme discret de l'élément β de G*. Le problème du logarithme discret consiste à retrouver x à partir de β.

Définition 3.1. Problème du Logarithme Discret dans $\mathbb{Z}_p^*$.

Soit le groupe $\mathbb{Z}_p^*$ d'ordre $p-1$. Soit α un élément primitif dans $\mathbb{Z}_p^*$ et β un élément $\mathbb{Z}_p^*$. Le *problème du logarithme discret* consiste à déterminer un entier $1 \leq x \leq p-1$ tel que :

$$\alpha^x = \beta \mod p.$$

Il existe trois conditions nécessaires pour que le problème du logarithme discret soit difficile :

1. Le nombre premier p doit être grand.
2. Le plus petit entier positif tel que $\alpha^m \equiv 1 \mod p$ doit être grand.
3. $p-1$ doit avoir au moins un grand facteur premier.

3.1 La taille de p

Exemple 3.2. Soit $p = 23423429$ $\alpha = 2$ et soit

$$\beta = \alpha^x = 19556038 \mod p.$$

Est-il difficile de trouver x ?

Dans cet exemple il est relativement facile de trouver x en simplement essayant une par une toutes les valeurs possibles pour x : On commence par $x = 0$, ensuite $x = 1$ etc. jusqu'à trouver x tel que $\alpha^x = \beta \mod p$. Les nombres dans cet exemple sont donc très petits, $p \approx 2^{25}$ et donc il y a au plus autant de nombres à tester afin de trouver une solution.

Pour cette raison il est recommandé de choisir des nombres premiers d'au moins 1024 bits, c'est-à-dire $p > 2^{1024}$.

3.2 L'ordre de α modulo p

Exemple 3.3. Soit le nombre premier $p = 589640540809904183368339807$.
Soient $\alpha = 151369338077029664651937484$ et

$$\beta = 438271202732874518716402322 \mod p.$$

Est-il difficile de trouver a tel que $\beta \equiv \alpha^a \mod p$?

Dans cet exemple, le problème du logarithme discret est facile puisque nous pouvons vérifier que $\alpha^3 \equiv 1 \mod p$. Par conséquent, $\alpha^a \equiv \alpha^{a \bmod 3} \mod p$ et le β de cet exemple est forcement une des trois valeurs $\alpha^0 \mod p, \alpha^1 \mod p$ ou $\alpha^2 \mod p$. En particulier, comme $\beta \not\equiv 1, \alpha \mod p$ on voit directement que $a = 2$.

Le problème de cet exemple est que la valeur $\mathrm{ord}(\alpha)$ est très petite. Si α était choisi en étant un élément primitif de $\mathbb{Z}_p^*$ ce problème aurait été évité.

3.2.1 Comment trouver un élément primitif α ?

Théorème 3.4. *Soit p un nombre premier impair et soit α un élément de $\mathbb{Z}_p^*$. Si pour tous les diviseurs premiers q de $p-1$*

$$\alpha^{(p-1)/q} \not\equiv 1 \mod p,$$

alors α est un élément primitif.

Ce résultat nous fournit une méthode permettant de trouver un élément primitif modulo p. On choisit un élément $\alpha \in \mathbb{Z}_p^*$ et on calcule $\alpha^{(p-1)/q} \not\equiv 1 \mod p$ pour tous les diviseurs q de $p-1$. Si aucun de ces calculs ne donne $1 \mod p$, alors α est un élément primitif. Si le test échoue, a n'est pas un élément primitif et on répète les calculs avec un α différent. Puisque, $\mathbb{Z}_p^*$ est un groupe cyclique, on est sûrs de réussir après quelques essais.

Corollaire 3.5. *Soit p et q des nombres premiers, tels que $p = 2q+1$. Un élément $\alpha \in \mathbb{Z}_p^*$ est un élément primitif si*

$$\alpha^2 \not\equiv 1 \mod p \text{ et } \alpha^q \not\equiv 1 \mod p.$$

Nous avons déjà vu que

$$\alpha^2 \equiv 1 \mod p \Rightarrow \alpha^2 - 1 \equiv 0 \mod p \Rightarrow (\alpha+1)(\alpha-1) \equiv 0 \mod p \Rightarrow \alpha \equiv \pm 1 \mod p,$$

donc si on est sûrs de choisir α différent de 1 et de $-1 \mod p$, nous n'avons qu'une seule exponentiation à faire.