DLP, Diffie-Hellman

11 Mars 2021

Table des matières

1 Logarithmme Discret

$$\text{One-way function} \rightarrow \left.\begin{array}{ll} \boxed{f(x) = y} & \Rightarrow \text{facile} \\ \boxed{f^{-}1(y) = x} & \Rightarrow \text{difficile} \end{array}\right\} \text{RSA} \implies \text{factorisation}$$

→ Problème du logarithme discret (DLP)
(DHKE) : (Diffie-Hellman key exchange) 1976 → SSH/TLS/IPSec

$$\boxed{k = (\alpha^x)^y \equiv (\alpha^y)^x \mod p} \rightarrow \text{exponentiation commutative}$$

Exponentiation dans $\mathbb{Z}_p^*$ est une one-way function

2 étapes:

1. **Initialisation**
   (a) Choisir un grand nombre premier
   (b) Choisir un entier $\alpha \in \{2, 3, \ldots, p-2\}$
   (c) Publier p et α

2. **Echange de clef**

$$\boxed{p \text{ et } \alpha \text{ publiques}} \quad \alpha^x \mod p = A$$

ALICE		*BOB*
choisir $a = K_{pr_A} \in \{2, \dots, p-2\}$		*choisir* $b = K_{pr_B} \in \{2, \dots, p-2\}$
$A = K_{pub_A} = \alpha^a \mod p$	$\xrightarrow{A}$	
	$\xleftarrow{B}$	$B = K_{pub_B} = \alpha^b \mod p$
$K_{AB} = k_{pub_B}^{k_{pr_A}} = \boxed{B^a \mod p}$		$K_{AB} = k_{pub_A}^{k_{pr_B}} = \boxed{A^b \mod p}$

Preuve.

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

□

Exemple.

$$p = 29 \qquad \overbrace{\boxed{\alpha = 2}}^{\text{élément primitif (générateur)}}$$

ALICE		*BOB*
$a = K_{pr_A} = 5$		*choisir* $b = K_{pr_B} = 12$
$A = K_{pub_A} = 2^5 \mod 29 \equiv 3 \mod 29$	$\xrightarrow{A=3}$	
	$\xleftarrow{B=7}$	$B = K_{pub_B} = 2^{12} \equiv 7 \mod 29$
$K_{AB} = B^a \equiv 7^5 \equiv \boxed{16} \mod 29$		$K_{AB} = A^b \equiv 3^{12} \mod 29 \equiv \boxed{16} \mod 29$

2 Groupe

Un groupe est un ensemble d'éléments G munis d'une opération binaire $*, \circ$ tel que :

1. Le groupe est fermé sous l'opération $\circ$: $\forall a, b \in G,\ a \circ b \in G$
2. $\exists 1, e \in G$, **élément identité** tel que $a \circ 1 = 1 \circ a = a, \forall a \in G$
3. $\forall a \in G, \exists a^{-1} \in G$ tel que $a \circ a^{-1} = a^{-1} \circ a = 1$
4. $\forall a, b, c \in G,\ a \circ (b \circ c) = (a \circ b) \circ c$

$\Rightarrow$ Un groupe où l'opération est commutative est dit abélien.

Exemple.

$(\mathbb{Z}, +)$ est un groupe ($1✓, 2✓, 3✓\ a^{-1} = -a, 4✓$).
$(\mathbb{Z}, \textbf{sans zéro}, \times)$ n'est pas un groupe.

Théorème. L'ensemble $\mathbb{Z}_n^*$ qui consiste des entiers $i = 0, 1, \cdots, n-1$ tel que $pgcd(i, n) = 1$ forme un groupe abélien sous la multiplication modulo n. $e = 1$

$\mathbb{Z}_q^* = \{1, 2, 4, 5, 7, 8\}$
$\mathbb{Z}_q = \{0, \dots, 8\}$

×	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

3 Groupe fini

$(G, \circ)$ est fini s'il est composé d'un nombre fini d'éléments.
$|G| = \#$ d'éléments

$(\mathbb{Z}_n, +)$ $|\mathbb{Z}_n| = n$
$(\mathbb{Z}_n^*, \times)$ $|\mathbb{Z}_n^*| = \phi(n)$

Exemple. $\phi(9)$

$$n = p_0^{e_0} p_1^{e_1} \ldots p_l^{e_l}$$
$$\phi(n) = (p_0^{e_0} - p_0^{e_0-1})(p_1^{e_1} - p_1^{e_1-1}) \ldots (p_l^{e_l} - p_l^{e_l-1})$$
$$\phi(9) = (3^2 - 3^1) = 6 \qquad \boxed{\phi(p) = (p^1 - p^0) = p - 1}$$

Définition. L'ordre d'un élément $ord(a)$, $a \in G, (G, \circ)$ est l'entier k le plus petit possible tel que:

$$\left.\begin{aligned} a^k = \underbrace{a \circ a \circ \ldots \circ a}_{\text{k fois}} &= 1 \\ &= e \end{aligned}\right\} \text{élément identité de } G$$

Exemple. $\mathbb{Z}_{11}^*$ $a = 3$ $ord(3) = 5$

$a^1 = 3$	$a^6 = 1 \cdot 3 = 3$	Puissances de 3
$a^2 = 3 \cdot 3 = 9$	$a^7 = 3 \cdot 3 = 9$	$\{3, 9, 5, 4, 1\}$
$a^3 = 27 \equiv 5 \mod 11$	$a^8 = 27 \equiv 5 \mod 11$	
$a^4 = 15 \equiv 4 \mod 11$	$a^9 = 15 \equiv 4 \mod 11$	
$a^5 = 12 \equiv 1 \mod 11$	$a^{10} = 12 \equiv 1 \mod 11$	

4 Groupe cyclique

Un groupe G qui contient un élément α avec ordre maximal $ord(\alpha) = |G|$ est cyclique.
Les éléments α avec ordre maximal sont des éléments primitifs/générateurs. $a \in G$ $\alpha^i = a$

Exemple.

$\mathbb{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ $\alpha = 2$
$|\mathbb{Z}_{11}^*| = \phi(11) = 10$

$\alpha^1 = 2$	$\alpha^6 = 9 \mod 11$	$\Rightarrow \alpha$ est un élément générateur
$\alpha^2 = 4$	$\alpha^7 = 7 \mod 11$	$\Rightarrow (\mathbb{Z}_{11}^*, \times)$ cyclique
$\alpha^3 = 8$	$\alpha^8 = 3 \mod 11$	
$\alpha^4 = 16 \equiv 5 \mod 11$	$\alpha^9 = 6 \mod 11$	
$\alpha^5 = 10 \mod 11$	$\alpha^{10} = 1 \mod 11$	

Note. 2 n'est pas toujours un générateur dans $\mathbb{Z}_n^*$
$\Rightarrow \mathbb{Z}_7^*$, $ord(2) = 3$

Théorème. $\forall p$ premier, $(\mathbb{Z}_p^*, \times)$ abélien fini cyclique.

Théorème. Soit G un groupe fini. $\forall a \in G$:

1. $a^{|G|} = 1 \rightarrow$ généralisation du petit théorème de Fermat
2. $ord(a) \mid |G|$

Exemple. $\mathbb{Z}_{11}^*$ $\quad\phi(11) = 10 \quad |\mathbb{Z}_{11}^*| = 10 \quad \longrightarrow \quad \underbrace{1|10,\ 2|10,\ 5|10,\ 10|10}_{\text{Seules valeurs possibles des ordres des éléments du groupe}}$

$$\left.\begin{array}{r} ord(1) = 1 \\ ord(2) = 10 \\ ord(3) = 5 \\ ord(4) = 5 \\ ord(5) = 5 \\ ord(6) = 10 \\ ord(7) = 10 \\ ord(8) = 10 \\ ord(9) = 5 \\ ord(10) = 2 \end{array}\right\} \text{Seuls les ordres qui divisent 10 sont possibles}$$

Théorème. Soit G un groupe cyclique fini. Alors:

1. Le nombre de générateur de G est $\phi(|G|)$ $\qquad p = |G|$
2. Si $|G|$ est premier, $\forall a \neq 1 \in G$ sont des éléments primitifs et donc générateurs.

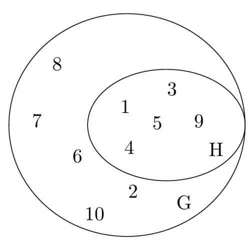
Exemple. $\mathbb{Z}_{11}^*$ $\quad \phi(11) = 10 \quad |\mathbb{Z}_{11}^*| = 10 \quad \phi(10) = (2^1 - 2^0)(5^1 - 5^0) = \overbrace{4}$

5 Sous-groupe cyclique

Soit $(G, \circ)$ un groupe cyclique.
$\forall a \in G,\ ord(a) = s$ est le générateur d'un sous-groupe cyclique avec s éléments.

Exemple. $G = (\mathbb{Z}_{11}^*, \times) \quad ord(3) = 5 \quad H = \{1, 3, 4, 5, 9\}$

$x \mod n$	1	3	4	5	9
1	1	3	4	5	9
3	3	9	1	4	5
4	4	1	5	9	3
5	5	4	9	3	1
9	9	5	3	1	4



- H est un sous-groupe cyclique d'ordre **premier** 5
- $3, 4, 5, 9$ sont des générateurs de H

Théorème (Théorème de Lagrange)**.** Soit H un sous-groupe de $G \implies |H| \mid |G|$

Exemple. $\mathbb{Z}_{11}^*$ $\quad |\mathbb{Z}_{11}^*| = 10 = 1 \cdot 2 \cdot 5 \longleftarrow 1|10, 2|10, 5|10, 10|10$

Sous-groupe	Eléments	Eléments-primitifs	
H_1	$\{1\}$	$\alpha = 1$	(trivial)
H_2	$\{1, 10\}$	$\alpha = 10$	
H_3	$\{1, 3, 4, 5, 9\}$	$\alpha = 3, 4, 5, 9$	

Théorème. Soit G un groupe cyclique d'ordre n et α un générateur de G.
$\forall k \in \mathbb{Z}$ tel que $k \mid n$, $\exists$ **exactement un sous-groupe cyclique** H de G.
Ce sous-groupe est généré par $\alpha^{n/k}$.
H consiste exactement des éléments $a \in G$ tel que $a^k = 1$.
Il n'y a pas d'autre sous-groupes.

Exemple. $\alpha = 8^{10/2} = 8^5 = 32768 \equiv 10 \mod 11$ $\qquad \phi(11) = 10 = n$

6 DLP

Etant donné un groupe fini cyclique $\mathbb{Z}_p^*$ d'ordre $p-1$ et un élément générateur $\alpha \in \mathbb{Z}_p^*$ et un autre élément $\beta \in \mathbb{Z}_p^*$, déterminer $1 \leq x \leq p-1$ tel que : $\alpha \Rightarrow$ est générateur $\Rightarrow \beta = \alpha^i$

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

x doit exister car chaque élément d'un groupe peut être exprimé comme une puissance d'un élément générateur.

$$x = \log_\alpha \beta \mod p$$

Exemple. $\mathbb{Z}_{47}^* \qquad \alpha = 5 \qquad \beta = 41$

$$\begin{aligned} 5^x &= 41 \mod 47 \\ x &= 15 \end{aligned}$$

Pour prévenir Pohlig-Hellman, on utilise des groupes de cardinalité premier, $|G| = p$
$\mathbb{Z}_p^* = p - 1 \leftarrow$ pair

$$\begin{aligned} \mathbb{Z}_{47}^* &= 46 = 2 \cdot \boxed{23} \\ \alpha &= 2 \in H \quad \updownarrow \\ 2^x &\equiv 36 \boxed{mod\ 47} \end{aligned}$$

7 Briser le DLP

$$\left.\begin{aligned} \alpha^1 &\stackrel{?}{=} \beta \mod p \\ \alpha^2 &\stackrel{?}{=} \beta \mod p \\ &\vdots \\ \alpha^x &= \beta \mod p \end{aligned}\right\} O(|G|)$$

Attaque de Pohlig-Hellman :

$$\begin{aligned} \alpha^x &= \beta \mod p \\ |G| &= p_0^{e^0} p_1^{e^1} \dots p_l^{e^l} \end{aligned}$$

$$x = \log_\alpha \beta \text{ dans } G \implies \underbrace{\boxed{x_i \equiv x \mod p_i^{e^i}}}_{\text{Chinese Remainder theorem (CRT)}}$$