

Cryptographie et arithmétique – Feuille 7

Exercice 1. On cherche à calculer le logarithme discret de 173 en base 2 dans $(\mathbb{Z}/227\mathbb{Z})^*$.

1. Montrer que 2 engendre $(\mathbb{Z}/227\mathbb{Z})^*$, puis factoriser 2^{32} , 2^{40} , 2^{59} et $2^{156} \pmod{227}$.
2. En déduire la valeur de $\log_2(3)$, $\log_2(5)$, $\log_2(7)$ et $\log_2(11)$.
3. Factoriser $173 \cdot 2^{177} \pmod{227}$, et en déduire $\log_2(173)$.

Exercice 2. Soit p un nombre premier impair, s un diviseur de $p-1$ et g un générateur du sous-groupe G d'ordre s de $(\mathbb{Z}/p\mathbb{Z})^*$. On suppose que s se factorise de la manière suivante :

$s = \prod_{i=1}^r p_i^{e_i}$, où les p_i sont des nombres premiers distincts et pour tout $i \in \llbracket 1, r \rrbracket$, $e_i \geq 1$. Soit $h \in G$, on cherche le logarithme discret x de h en base g . L'algorithme de Pohlig-Hellman calcule $x \pmod{p_i^{e_i}}$ pour chaque i et retrouve ensuite x par le théorème des restes chinois.

1. Pour tout i , déterminer l'ordre de $\tilde{g}_i = g^{s/p_i}$.
2. On détermine maintenant la valeur de $x \pmod{p_i^{e_i}}$ pour chaque i . Pour alléger les notations, on fixe un indice i et on note $q = p_i$ et e le e_i correspondant. On note $x \pmod{q^e} = x_0 + x_1q + x_2q^2 + \dots + x_{e-1}q^{e-1}$ la décomposition en base q . On suppose x_0, x_1, \dots, x_k déterminés, avec $k < e-1$. Montrer comment déterminer x_{k+1} par le calcul d'un logarithme discret en base \tilde{g}_i .
3. Montrer que la complexité de cet algorithme est en $O\left(\sum_{i=1}^r e_i(\ln(s) + \sqrt{p_i})\right)$.
4. Application : 9 est d'ordre 63 dans $(\mathbb{Z}/127\mathbb{Z})^*$; calculer $\log_9(98)$.

Exercice 3. Soit G un groupe multiplicatif et $\alpha \in G$ un élément fixé d'ordre n . Soit β un élément de $\langle \alpha \rangle$ dont on veut calculer le logarithme discret en base α . L'idée de base de l'algorithme ρ de Pollard pour le logarithme discret est de calculer une suite $x_1, x_2, \dots, x_i, \dots$, d'éléments de G , de sorte qu'une collision $x_i = x_j$ pour $i < j$ permette de calculer $c = \log_\alpha(\beta)$. Plus précisément, chaque élément x de la suite fait partie d'un triplet (x, a, b) vérifiant $x = \alpha^a \beta^b$. Les triplets (x_i, a_i, b_i) définissent une « marche aléatoire ».

1. Montrer que si (x, a, b) vérifie $x = \alpha^a \beta^b$, alors les triplets $(\beta x, a, b+1)$, $(x^2, 2a, 2b)$ et $(\alpha x, a+1, b)$ vérifient la même relation.

On partitionne G en trois ensembles de même taille S_1, S_2 et S_3 , et on définit l'appli-

$$\text{cation } f : \begin{cases} \langle \alpha \rangle \times \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} & \rightarrow & \langle \alpha \rangle \times \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ (x, a, b) & \mapsto & \begin{cases} (\beta x, a, b+1) & \text{si } x \in S_1, \\ (x^2, 2a, 2b) & \text{si } x \in S_2, \\ (\alpha x, a+1, b) & \text{si } x \in S_3. \end{cases} \end{cases}$$

On pose $(x_0, a_0, b_0) = (1, 0, 0)$, et on définit la suite $((x_i, a_i, b_i))_{i \geq 0}$ par récurrence en posant $(x_{i+1}, a_{i+1}, b_{i+1}) = f((x_i, a_i, b_i))$ pour tout $i \geq 0$.

2. Montrer que pour tout $i \geq 0$, on a $x_i = \alpha^{a_i} \beta^{b_i}$.
3. Montrer que s'il existe $i < j$ tels que $x_i = x_j$, alors il existe $s < j$ tel que $x_s = x_{2s}$. Démontrer que si $\text{pgcd}(b_{2s} - b_s, n) = 1$, alors $\log_\alpha(\beta) \equiv (a_s - a_{2s})(b_{2s} - b_s)^{-1} \pmod{n}$.
4. Soit $G = (\mathbb{Z}/47\mathbb{Z})^*$. Vérifier que 2 est d'ordre 23. Calculer $\log_2(37)$; on prendra pour S_1 les entiers congrus à 2 mod 3, S_2 les multiples de 3 et S_3 les autres entiers.

Exercice 4. On présente le crible quadratique, qui est un raffinement de l'algorithme de Dixon. On commence par choisir une *base de facteurs* $\mathcal{B} = \{-1, p_1, \dots, p_k\}$, où p_i est un nombre premier pour tout $i \in \llbracket 1, k \rrbracket$. Ensuite, pour chaque entier relatif j , on calcule $x_j = \lfloor \sqrt{n} \rfloor + j$ et $y_j = x_j^2 - n$ jusqu'à avoir $k + 2$ entiers dont tous les facteurs premiers sont dans \mathcal{B} (on dit alors que y_j est *lisse* sur \mathcal{B}). Pour chaque y_j lisse, on a

$$y_j = \pm \prod_{i=1}^k p_i^{a_{i,j}}, \text{ et on pose } v_{0,j} = \begin{cases} 0 & \text{si } y_j > 0, \\ 1 & \text{si } y_j < 0, \end{cases} \text{ puis } v_{i,j} \equiv a_{i,j} \pmod{2} \text{ pour } i \geq 1.$$

1. On cherche un ensemble S d'entiers j tels que y_j est lisse et tels que pour tout $i \in \llbracket 0, k \rrbracket$, on ait $\sum_{j \in S} v_{i,j} \equiv 0 \pmod{2}$. Expliquer comment obtenir un facteur non trivial de n à partir de $x = \prod_{j \in S} x_j$ et $y^2 = \prod_{j \in S} y_j$, si $x \not\equiv \pm y \pmod{n}$.
2. Montrer que s'il n'existe pas d'entier s tel que $n \equiv s^2 \pmod{p}$ pour un certain nombre premier p , alors on doit exclure p de \mathcal{B} pour que la méthode fonctionne.
3. On pose $n = 30167$, et on choisit $\mathcal{B} = \{-1, 2, 7, 11, 17, 29, 31, 37, 41, 43, 53, 67\}$. Dédurre une factorisation de n du tableau obtenu :

j	0	-1	-5	5	-6	7	11
x_j	173	172	168	178	167	180	184
y_j	$-2 \cdot 7 \cdot 17$	$-11 \cdot 53$	$-29 \cdot 67$	$37 \cdot 41$	$-2 \cdot 17 \cdot 67$	$7 \cdot 11 \cdot 29$	$7 \cdot 17 \cdot 31$
j	14	-15	-17	18	-23	28	
x_j	187	158	156	191	150	201	
y_j	$2 \cdot 7^4$	$-11 \cdot 43$	$-7^3 \cdot 17$	$2 \cdot 7 \cdot 11 \cdot 41$	$-11 \cdot 17 \cdot 41$	$2 \cdot 7 \cdot 17 \cdot 43$	