Université Paris 8 J. Lavauzelle

Master 1 Mathématiques et applications — année 2025–26

Cryptographie à clé publique – Mini-projet

transmis le mercredi 25 mars 2026
à rendre pour le **samedi 25 avril 2026**, dernier délai

Documents à fournir. Vous devez rendre par email adressé à `julien.lavauzelle@univ-paris8.fr`, vos réponses sous la forme d'une archive contenant éventuellement

1. un fichier au format `.pdf` contenant vos réponses aux questions de nature théorique ;
2. si vous utilisez `python`, un fichier au format `.ipynb` ou `.py`, contenant vos réponses aux questions de nature pratique (implémentation).

Remarques. Lors de vos implantations, vous allez manier de grands entiers. Certains langages comme `python` les supportent nativement. Pour d'autres, comme `C`, il faut importer une bibliothèque externe (GMP pour `C`, par exemple). Veuillez prévenir l'enseignant au préalable si vous faites ce choix.

Ressources. Comme aide à la programmation, on trouvera notamment sur la page du cours

`https://www.lvzl.fr/teaching/2025-26/cp.html`

des fichiers auxiliaires contenant des listes de premiers p de taille particulière, ou des listes des nombres premiers p tels que $p+1$ est B-superfriable pour des bornes B particulières.

La méthode $p+1$ de Williams pour la factorisation d'entiers

Dans ce sujet, on considère la méthode de factorisation d'entiers dite « $p+1$ » de Williams. Cette méthode permet de trouver des facteurs p d'un grand entier N à factoriser, tels que $p+1$ a une forme particulière, dite *superfriable*, que l'on définira plus tard.

1) Partie théorique

On suppose dans cette partie de l'énoncé que p est un diviseur **premier et impair** de N, le nombre à factoriser. On note $\mathbb{Z}/N\mathbb{Z}$ l'anneau des entiers modulo N. Pour un certain $D \in \mathbb{Z}$, on définit

$$\mathcal{A}^D := \{(x,y) \in (\mathbb{Z}/N\mathbb{Z})^2 \mid x^2 - Dy^2 \equiv 1 \mod N\} \subseteq (\mathbb{Z}/N\mathbb{Z})^2 .$$

Puis, on note $\mathcal{A}_p^D$ la réduction de cet ensemble modulo p :

$$\mathcal{A}_p^D := \{(x \mod p, y \mod p) \mid (x,y) \in \mathcal{A}^D\} \subseteq (\mathbb{Z}/p\mathbb{Z})^2 .$$

Question 1.– Dans cette question uniquement, on fixe $p = 5$, $N = 15$ et $D = 2$. Calculez les ensembles $\mathcal{A}^D$ et $\mathcal{A}_p^D$, en précisant votre méthode.

Lorsque D est n'est pas un carré modulo p, on rappelle que $\mathbb{F}_p[X]/(X^2-D)$ est un corps que l'on note $\mathbb{F}_p(\sqrt{D})$, où $\sqrt{D}$ représente la classe de X dans $\mathbb{F}_p[X]/(X^2-D)$. On note enfin ψ l'isomorphisme d'espace vectoriel :

$$\begin{array}{rccc} \psi : & (\mathbb{Z}/p\mathbb{Z})^2 & \longrightarrow & \mathbb{F}_p(\sqrt{D}) \\ & (x,y) & \longmapsto & x+y\sqrt{D} \end{array}$$

Question 2.– Démontrez que $\psi(\mathcal{A}_p^D)$ est un sous-groupe multiplicatif de $\mathbb{F}_p(\sqrt{D})$, dont l'ordre est $p+1$.

On note dorénavant $\mathcal{U} \coloneqq \psi(\mathcal{A}_p^D)$. Tout $u \in \mathcal{U}$ s'écrit de manière unique comme $u = x + y\sqrt{D}$. On définit alors

$$x(u) \coloneqq x \in \mathbb{F}_p \quad \text{et } y(u) \coloneqq y \in \mathbb{F}_p\,.$$

Observons que les applications $x(\cdot)$ et $y(\cdot)$ dépendent *a priori* de D.

Question 3.– Soit $u \in \mathcal{U}$. Calculez u^2 puis exprimez $x(u^2)$ en fonction de $x(u)$.

Question 4.– Soit $u \in \mathcal{U}$. Démontrez que pour tout $n \geq 1$, on a :

$$\begin{aligned} x(u^{2n}) &\equiv 2 \cdot x(u^n)^2 - 1 \mod p, \\ x(u^{2n+1}) &\equiv 2 \cdot x(u^n) \cdot x(u^{n+1}) - x(u) \mod p. \end{aligned}$$

Pour ce faire, vous pourrez vous aider du calcul intermédiaire de $y(u^{2n})$.

Nous verrons dans la partie suivante comment exploiter ces relations pour calculer la valeur de $x(u^n)$ en temps polynomial en $\log(n)$, à la manière de l'exponentiation rapide.

Question 5.– Soit $u \in \mathcal{U}$. Démontrez que si $M \geq 1$ est un multiple de $p+1$, alors p divise $x(u^M) - 1$.

2) Partie implantation

De la partie précédente, on va pouvoir déduire un algorithme permettant de trouver un diviseur p de N, dans le cas où l'entier $p+1$ est *superfriable*. Voici une définition de cette notion.

Définition 0.1

*Soit $B \geq 2$. On dit qu'un entier $x \geq 2$ est B-*superfriable *si tout entier de la forme q^e qui divise x (avec q un nombre premier et $e \geq 1$) est inférieur ou égal à B.*

Exemple. L'entier $16 = 2^4$ n'est pas 9-superfriable, mais l'entier $72 = 2^3 \times 3^2$ l'est.

Question 6.– Implantez une fonction `est_superfriable(x, B)` qui prend en entrée deux entiers x et B, et qui teste si l'entier x est B-superfriable.

Question 7.– Implanter une fonction `calcule_borne(B)` qui calcule le plus efficacement possible la valeur $M = \text{ppcm}(2, \ldots, B)$. On pourra utiliser le fait que $\text{ppcm}(2, \ldots, B)$ est le produit de tous les entiers de la forme $p_i^{e_i}$, où p_i est un nombre premier $\leq B$ et e_i le plus grand entier tel que $p_i^{e_i} \leq B$.
Pour vous aider, et si besoin, vous pourrez aussi trouver dans le fichier annexe `liste_petits_premiers.txt` la liste de tous les nombres premiers plus petits que 10 000.

La méthode « $p+1$ » de Williams repose sur le calcul d'une suite $(x_n)_{n\geq 1}$ définie par les relations de récurrence vues dans la section précédente :

$$\begin{cases} x_{2n} &= 2x_n^2 - 1 \mod N \\ x_{2n+1} &= 2x_n x_{n+1} - x_1 \mod N \end{cases} \qquad \text{pour } n \geq 1$$

Ainsi, si z_n désigne le couple (x_n, x_{n+1}), on peut déduire (z_{2n}, z_{2n+1}) à partir de x_1 et z_n. Cela signifie qu'on peut **adapter la méthode d'exponentiation binaire** au calcul de x_n.

Exemple 0.2

Si $M = 18$, l'écriture de M en base de M est $(10010)_2$. Les troncations de cette écriture forment les entiers $1 = (1)_2$, $2 = (10)_2$, $4 = (100)_2$, $9 = (1001)_2$ et $18 = (10010)_2$. Donc, on va successivement calculer x_1, x_2, x_4, x_9 et x_{18}.
Il est facile de passer de x_1 à x_2 et de x_2 à x_4, par l'équation $x_{2n} = 2x_n^2 - 1 \mod N$ donnée plus haut. En revanche, pour calculer x_9, on a besoin à la fois de x_4 et de x_5. Dans l'algorithme de calcul de la suite (x_n), il faudra donc maintenir la connaissance de $z_n = (x_n, x_{n+1})$.
Pour $x_1 = 2$, on doit obtenir les valeurs suivantes

n	x_n	x_{n+1}
1	2	7
2	7	26
4	97	362
9	70226	262087
18	9863382151	–

Question 8.– Implanter une fonction `calcule_x(x1, M, N)` qui prend en entrée un élément $x_1 \in \{1, \ldots, N-1\}$ et qui calcule la valeur de $x_M \mod N$ par une méthode analogue à l'exponentiation binaire.

On s'intéresse maintenant à l'Algorithme 1, dit méthode de factorisation « $p+1$ » de Williams.

Algorithme 1 : Méthode $p+1$ de Williams

Entrée : un entier $B \geq 3$ et un entier composé impair $N \geq 15$ possédant un facteur premier impair p tel que $p+1$ est B-superfriable
Sortie : un diviseur d de N

Initialiser $d \leftarrow N$.
Tant que $d = N$ **faire**
  Calculer $M \leftarrow \text{ppcm}\{2, \ldots, B\}$.
  Tirer aléatoirement x_1 dans $\{1, \ldots, N-1\}$.
  Calculer $d \leftarrow \text{pgcd}(x_1, N)$.
  Si $d \neq 1$
    Retourner d
  Calculer $x_M \leftarrow \texttt{calcule\_x}(x_1, M, N)$.
  Calculer $d \leftarrow \text{pgcd}(x_M - 1, N)$.
Retourner d.

Question 9.– Implanter un algorithme qui calcule de pgcd de deux entiers. Cet algorithme devra supporter des entrées de taille importante (plusieurs centaines de chiffres).

Question 10.– Implanter l'Algorithme 1. Tester votre implantation avec certaines valeurs données en annexe.

3) Partie analyse

Dans cette dernière partie, on analyse la validité et la complexité de la méthode $p+1$ de Williams.

Question 11.– En utilisant la partie théorique, expliquez pourquoi l'Algorithme 1 calcule bien un diviseur p de N tel que $p+1$ est B-superfriable.

Question 12.– Donnez une estimation de la complexité de la méthode $p+1$ de Williams en fonction de B et N.

Question 13.– **[BONUS]** Calculez **expérimentalement** la complexité de la méthode $p+1$ de Williams. Commentez les résultats obtenus (même s'ils ne sont pas convaincants).
Pour cela, on tracera des graphes du temps de calcul (ou du nombre d'opérations comptées) en fonction de N et/ou de la borne de friabilité B choisie. On pourra également s'aider des entiers donnés dans les fichiers auxiliaires, ou implémenter son propre générateur d'entiers composés (de taille et forme particulière).
Rappelons enfin que :

- pour vérifier qu'une fonction $f(x)$ se comporte comme un polynôme en x, c'est-à-dire $\beta x^\alpha + o(x^\alpha)$, on trace $\log(f(x))$ en fonction de $\log(x)$,
- pour vérifier qu'une fonction $g(x)$ se comporte comme une exponentielle en x, c'est-à-dire $(\delta + o(1))\gamma^x$, on trace $\log(f(x))$ en fonction de x

Annexe

Pour vous aider à tester vos programmes, voici ci-dessous quelques valeurs de N, p et q qui doivent mener à une factorisation quasi-immédiate de N.

$N = pq$	facteurs p, q tels que $p+1$ est B-superfriable		B
8435923	2243	3761	20
433214017981	526679	822539	20
668877085585453	20540519	32563787	20
29601945037090540097	4302501839	6880170223	60
220293021228080219150428 7	1099511799979	2003553042653	150
1434606164092147949243688378019	1125899906956109	1274186235586991	400
16837394551147962923619919655269202 83	1152921504620379229	1460411180090875927	1000

TABLE 1 – Exemples de factorisations « faciles » effectuées par l'algorithme $p+1$ de Williams.

Quelques exemples de taille plus conséquente, mais que l'algorithme $p+1$ règle toujours très rapidement (< 1 seconde si l'implantation est bonne) :

- $N = 10562256276314677189367086699051860083179133005474255536770513713410152272327$
  $p = 80694878738093144866358575156611462449$
  $q = 13089128382726742425590053490410316402 3$
  où $p+1$ est 100-superfriable.

- $N = 62168737006042231928510814222178349101156309737965504752177410010962889443724567730 7...$
  $...16203710521739874848738315366444050483000922241076559240303096972312 29$
  $p = 67370446184902616587480990283695167230411304043318606176733774562163367914599$
  $q = 92278945036843081009237393938740885814972681387747472129904570310056540085371$
  où $p+1$ est 200-superfriable.

- $N = 75335665860992821169105470726766540912231610419365378084109059906708119860068536707...$
  $...23673944387751725757220297910047314599198514346142077537459486353899376688526034522045 70...$
  $...46051949701511230965455078708866820795617315314721680376760845 13$
  $p = 25859751346998904721315154541135445772069592027081540466915141922132646156251 8...$
  $...12286986260376922317805736767051853068 79$
  $q = 29132401487586512476354570916689568474194168376146508296871732993914796687724 5...$
  $...60484143488960272064176130757946206028 47$
  où $p+1$ est 300-superfriable.