RAPPORT DE STAGE

L3 MATHÉMATIQUES

Introduction à la cryptologie : Chiffrement et Déchiffrement

---

06 JANVIER 2025 — 31 JANVIER 2025

Sujet traité par :

M. MATHIS JEANNE-LOUISE

Sous l'encadrement du:

DR. JAMES LARROUY

UNIVERSITÉ DES ANTILLES - PÔLE GUADELOUPE
U.F.R. SCIENCES EXACTES ET NATURELLES
DÉPARTEMENT DE MATHÉMATIQUES ET INFORMATIQUE

Sommaire

1 Introduction

D'après la Commission nationale de l'informatique et des libertés (CNIL), le terme cryptologie a pour étymologie "science du secret" en grec. Elle réunit la **cryptographie**, ou littéralement "l'écriture secrète", et la **cryptanalyse**, qui désigne l'étude des attaques contre les mécanismes de cryptographie.

Durant ce stage, nous avons fait le choix de nous focaliser sur le cas de la cryptographie, et plus précisément la cryptographie à clé publique (ou asymétrique) qui sera décrite à la Section 3. De façon générale, les principaux usages de la cryptographie sont synthétisés au sein de la figure ci-dessous.

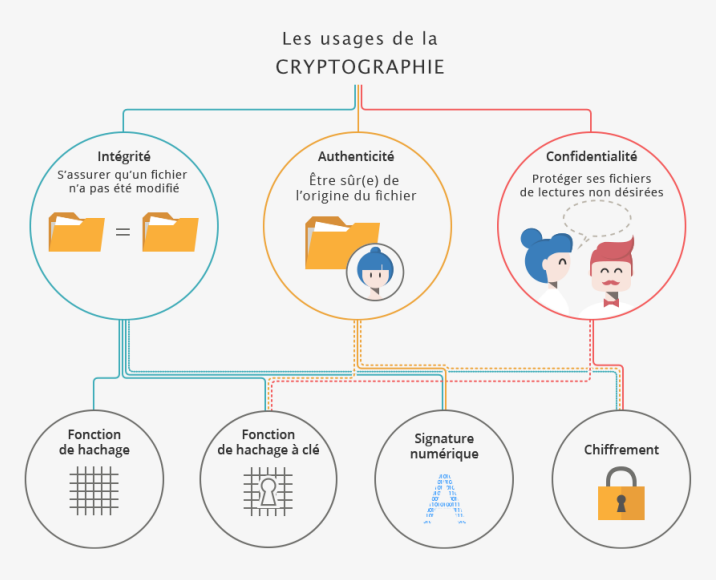

Figure 1: Usages de la cryptographie (Source: CNIL).

En fait, il existe deux types d'attaques qui motivent l'intérêt pour le développement d'outils robustes en cryptographie. D'abord, on parle d'**attaques passives**, c'est-à-dire que l'attaquant intercepte les messages transmis avec l'intention de lire et d'analyser les messages sans pour autant les modifier. Ensuite, on parle d'**attaque actives**, c'est-à-dire que l'attaquant intercepte les messages dans le but de modifier leur contenu. Dans le premier cas, on peut par exemple penser à un hacker qui souhaiterait récupérer les mots de passe ou les données personnelles de la personne attaquée ; dans le second cas, on peut par exemple penser à de l'usurpation d'identité. Ainsi, la cryptographie se scinde en deux pans distincts :

- la **cryptographie à clé publique** (ou asymétrique) ;
- la **cryptographie à clé secrète** (ou symétrique).

La cryptographie a clé publique date des années 1976 avec les travaux de Diffie & Hellman [3]. Elle permet d'assurer la confidentialité d'une communication, ou d'authentifier les participants, sans que cela repose sur une donnée secrète partagée entre ceux-ci, contrairement à la cryptographie symétrique, beaucoup plus ancienne (env. 2000 an av. J.-C.), qui nécessite ce secret partagé préalable. À noter qu'historiquement, la cryptographie avait pour objectif de sécuriser les communications. En guise d'illustration, deux personnes partagent un secret que l'on appelle **clé** et que l'on note souvent K. Ainsi, celui qui envoie le message, le *chiffre* avec K et celui qui reçoit le message le *déchiffre* à l'aide de K. En somme, la cryptographie repose sur l'utilisation de trois fonctions majeures :

(*a*) **Gen**$(\cdot)$, l'algorithme de génération des clés ;

(*b*) **Enc**$(\cdot)$, l'algorithme de chiffrement des clés ;

(*c*) **Dec**$(\cdot)$, l'algorithme de déchiffrement des clés.

Enfin, il convient de préciser que le principe fondamentale de la cryptographie à été énoncé en 1883 par le cryptologue militaire néerlandais Auguste Kerckhoffs van Nieuwenhoff [4]. Il s'énonce comme suit.

Définition 1.1 (Principe de Kerckhoffs)**.** *La méthode de chiffrement ne doit pas être secrète, et elle doit pouvoir tomber entre les mains de l'ennemi sans provoquer de problème.*

Le principe de Kerckhoffs précise essentiellement que le caractère secret de la clé K ne devrait pas être au centre de la sécurité d'un système donné.

Avant d'aller plus loin, nous disons quelques mots sur le déroulé du stage et ses objectifs.

Cadre de réalisation et objectifs du stage

J'ai effectué mon stage de 3^{eme} année de licence sous l'encadrement du Dr. James Larrouy au sein du laboratoire de Mathématiques Informatique et Applications (LAMIA) de l'Université des Antilles. J'ai souhaité découvrir le métier de chercheur en mathématiques à travers les domaines des mathématiques qui me passionnent : l'algèbre et l'arithmétique.
Durant mon stage, j'ai essentiellement eu à réaliser de la recherche bibliographie sur la cryptologie qui est une discipline nouvelle pour moi, mais qui prend ses racines dans les principes arithmétiques et, en particulier, en arithmétique modulaire. Après un lourd travail de synthèse en autonomie, j'ai eu à produire un rapport de stage en Latex qui respecte les standards académiques des articles scientifiques modernes. Ce travail se situe à la frontière entre mathématiques pures et applications des mathématiques.

Description de la structure d'acceuil

Comme indiqué sur son site web (cf. https://lamia.univ-antilles.fr/newsite/), le LAMIA est une unité de recherche (UR1 1) reconnue par le Ministère de l'enseignement supérieur et de la recherche. Il est la conséquence du regroupement de membres issus des laboratoires AOC-EA 3591 et GRIMAAG-EA 3590 de l'université des Antilles et de la Guyane (UAG).

Le laboratoire est dirigé par le Professeur Gisèle Mophou. Le LAMIA compte une soixantaine de membres répartis au sein de groupes de recherches ainsi que de projets. Chacun des Groupes de recherches est doté d'un responsable en charge de l'animation et de la coordination scientifiques. Les membres sont sous-catégorisés en plusieurs grade : Professeur des universités (PU), Maitre de conférence habilité à diriger des recherches (MCF -HDR), Maitre de conférence des universités (MCF), Docteurs (Dr) et doctorants.

Les groupes de recherches en mathématiques du LAMIA travaillent sur les thématiques suivantes : Optimisation, Contrôle, Modélisation, Imagerie.

Organisation du rapport

Tout au long de ce rapport nous nous focalisons sur les mathématiques de la cryptographie moderne ou en d'autres termes, la cryptographie à clé publique. Nous choisissons de nous centrer sur l'aspect mathématique du cryptosystème RSA, sans discuter de l'aspect computationnel de ce derniern. Nous fournirons tout de même les algorithmes qui sont au coeur de RSA.
À la Section 2, nous introduisons les outils mathématiques qui permettrons de comprendre le fonctionnement du cryptosystème RSA. Dans une première partie, nous rappelons certains concepts de base de l'arithmétique dans $\mathbb{Z}$ qui sont important pour la suite. Ensuite, nous présentons les notions et résultats d'arithmétique modulaire, c'est à dire sur l'anneau $\mathbb{Z}/n\mathbb{Z}$, qui sont à la base de la cryptographie. Enfin, nous présentons trois théorèmes d'arithmétique modulaire sur lesquels reposent le cryptosystème RSA.
La Section 3, est dédiée à la Cryptographie à clé publique. Compte tenu du nombre de pages imposé, nous nous restreignons à l'étude du protocole RSA. Dans une première partie, nous présentons RSA sous formes d'algorithme que nous commentons. Ensuite, nous prouvons que le cryptosystème RSA déchiffre réellement le message chiffré initial. Enfin, nous fournissons un résultat de cryptoanalyse lié à RSA.
Nous achevons ce travail avec une conclusion qui résume le travail réalisé durant le stage et une bibliographie écrite en respectant la norme APA utilisée dans les articles de recherches scientifique.

2 Éléments d'arithmétique modulaire

Cette section est consacrée à la présentation des outils mathématiques nécessaire à la bonne compréhension des mathématiques de le cryptosystème RSA (voir Section 3). Les définitions présentés ci-dessous et les preuves des résultats non démontrés peuvent être retrouvés dans Bourbaki [2, Chapitres 5 et 7].

2.1 Quelques notions élémentaires

Par soucis de complétude, nous commençons par rappeler certains concepts de base. On rappel qu'une relation binaire $\mathcal{R}$ sur un ensemble E est la donnée d'une partie $\mathcal{R} \subset E \times E$. Par ailleurs, on écrit en général $x\mathcal{R}y$ pour signifier que $(x, y) \in \mathcal{R}$. Ainsi, on a le concept suivant.

Définition 2.1 (Relation d'équivalence)**.** *Soit E un ensemble non vide. On dit qu'une relation binaire $\backsim$ sur E est une relation d'équivalence sur E si elle est*

- *réflexive : pour tout $x \in E$, $x \backsim x$;*
- *symétrique : pour tous $x, y \in E$, si $x \backsim y$ alors $y \backsim x$;*
- *transitive : pour tous $x, y, z \in E$, si $x \backsim y$ et $y \backsim z$ alors $x \backsim z$.*

À l'aide de la définition précédente, on peut définir la notion d'ensemble quotient.

Définition 2.2 (Classe d'équivalence)**.** *Soit E un ensemble non vide et $\backsim$ une relation d'équivalence sur E. On dit qu'une partie $A \subsetneq E$* ***est une classe d'équivalence*** *pour la relation $\backsim$ si :*

- *A est non vide ;*
- *pour tous $x, y \in A$, on a $x \backsim y$;*
- *pour tous $x \in A$ et $y \notin A$, on a $x \nsim y$.*

Définition 2.3 (Ensemble quotient)**.** *L'ensemble $E/\backsim$ constitué de toutes les classes d'équivalences de $\backsim$ est appelé* ***ensemble quotient de*** *E par la relation $\backsim$.*

Remarque 2.4. *On vérifie aisément que les classes d'équivalences forment une partition de E. Ainsi, tout élément de E appartient à une et une seule classe d'équivalence.*

On rappel que $\mathbb{N}$ et $\mathbb{Z}$ désignent l'ensemble des entiers naturels et l'ensemble des entiers relatifs, respectivement. Ainsi, on définit sur $\mathbb{Z}$ les concepts suivants.

Définition 2.5 (Divisibilité)**.** *Soient $a, b \in \mathbb{Z}$. On dit que a* ***divise*** *b s'il existe un entier c tel que $b = ac$. Dans ce cas, on note $a \mid b$.*

Définition 2.6 (Nombre premier)**.** *On dit qu'un entier $p \in \mathbb{N}$ est* ***premier*** *s'il n'est divisible que par 1 et lui-même.*

Définition 2.7 (PGCD)**.** *Soient $a, b \in \mathbb{Z}$. On appelle* ***plus grand commun diviseur de*** *a* ***et*** *b , et on note* $\operatorname{pgcd}(a, b)$*, le plus grand entier qui est à la fois diviseur de a et diviseur de b.*

Définition 2.8 (Nombre premiers entre eux)**.** *On dit que deux entiers a* ***et*** *b* ***sont premiers entre eux*** *si et seulement si* $\operatorname{pgcd}(a, b) = 1$.

Lemme 2.9. *Soient $a, b, c \in \mathbb{Z}$. Si $a \mid b$, $b \mid c$ et* $\operatorname{pgcd}(a, b) = 1$*, alors $ab \mid c$.*

Enfin, nous énonçons le théorème de Bézout.

Théorème 2.10 (Théorème de Bézout)**.** *Deux entiers a et b sont premiers entre eux si et seulement s'il existe $(u, v) \in \mathbb{Z}^2$ tels que $au + bv = 1$.*

Nous introduisons désormais la notions au centre de la sous-section qui succède.

Définition 2.11 (Congruence modulo n)**.** *Soient $n \in \mathbb{N}$ tel que $n \geq 2$ et $a, b \in \mathbb{Z}$. On dit que a* ***et*** *b* ***sont congrus modulo*** *n si $a - b$ divise n. Dans ce cas, on note $a \equiv b\ [n]$, ou plus simplement $a \equiv_{[n]} b$.*

Remarque 2.12. *On montre facilement que la relation binaire $\equiv_{[n]}$ est une relation d'équivalence.*

2.2 Généralités sur l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$

Nous nous discutons maintenant de l'aspect arithmétique de l'anneau $\mathbb{Z}/n\mathbb{Z}$. Sauf indication contraire, dans la suite, n désignera toujours un élément de $\mathbb{N}$ supérieur ou égale à 2 fixé.

Pour un entier $k \in \mathbb{Z}$, on note $\overline{k}$, la classe d'équivalence de k pour la relation d'équivalence $\equiv_{[n]}$, c'est-à-dire l'ensemble des entiers qui sont congrus à k modulo n. Pour tout $a, b \in \mathbb{Z}$, nous définissons la relation $\overset{n}{\backsim}$ donnée par

$$a \overset{n}{\backsim} b \quad \Longleftrightarrow \quad \overline{a} = \overline{b}. \tag{1}$$

Ainsi, on montre que l'on peut décrire $\mathbb{Z}/\overset{n}{\backsim}$ au moyen d'un ensemble fini de cardinal n. Pour ce faire, nous prouvons le résultat suivant.

Lemme 2.13. *Soient $a, b \in \mathbb{Z}$. Alors $\overline{a} = \overline{b}$ si et seulement si $a \equiv_{[n]} b$.*

Preuve. Supposons que $\overline{a} = \overline{b}$. Comme $a \in \overline{a}$, on a $a \in \overline{b}$ d'où $a \equiv_{[n]} b$. Supposons à l'inverse que $a \equiv_{[n]} b$. Alors, si $c \in \overline{a}$, on a $c \equiv_{[n]} a$. D'après la Remarque 2.12, on déduit que $c \equiv_{[n]} b$, ce qui veux dire que $c \in \overline{b}$. Ce qui prouve que $\overline{a} \subseteq \overline{b}$. En procédant de la même façon, on prouve aussi que $\overline{b} \subseteq \overline{a}$. □

Grâce à cela, nous pouvons prouver une caractérisation de $\mathbb{Z}/\overset{n}{\backsim}$.

Proposition 2.14. *Soit $n \in \mathbb{N}$ supérieur ou égal à 2. Alors, $\mathbb{Z}/\overset{n}{\backsim} = \left\{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\right\}$. De plus, $\mathbb{Z}/\overset{n}{\backsim}$ est de cardinal n.*

Preuve. Nous procédons en deux étapes. Il est clair que $\left\{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\right\} \subseteq \mathbb{Z}/\overset{n}{\backsim}$. Il nous reste donc à prouver l'inclusion inverse. Soit $\overline{a} \in \mathbb{Z}/\overset{n}{\backsim}$. Considérons un représentant $a \in \overline{a}$. On déduit de la division euclidienne de a par n, l'existence d'un couple $(q, r) \in \mathbb{Z} \times [[0, n-1]]$ tel que $a \equiv_{[n]} r$. Ainsi, d'après le Lemme 2.13, on a $\overline{a} = \overline{r}$. Donc, $\mathbb{Z}/\overset{n}{\backsim} \subseteq \left\{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\right\}$. Ce qui nous démontre l'égalité recherchée.
Nous montrons maintenant que $\mathbb{Z}/\overset{n}{\backsim}$ est de cardinal n. Supposons qu'il existe $k, l \in [[0, n-1]]$ tels que $l < k$ et $\overline{k} = \overline{l}$. Alors, d'après le Lemme 2.13, on a $k \equiv_{[n]} l$. Par conséquent, on a $k - l \equiv_{[n]} 0$, ou en d'autres termes, $n \mid k - l$ avec $0 < k - l < n$, ce qui est absurde. □

Dans l'ensemble du rapport, on écrira sans perte de généralité $\mathbb{Z}/n\mathbb{Z}$ plutôt que $\mathbb{Z}/\overset{n}{\backsim}$. Ainsi, d'après la Proposition 2.14, l'ensemble des classes d'équivalences pour la relation $\equiv_{[n]}$ est définie par

$$\mathbb{Z}/n\mathbb{Z} = \left\{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\right\}. \tag{2}$$

Considérant l'addition modulaire, notée $+$, et la multiplication modulaire, notée $\times$, on observe facilement que pour tout $\overline{a}, \overline{b} \in \mathbb{Z}/n\mathbb{Z}$, si a est un représentant de $\overline{a}$ et b un représentant de $\overline{b}$, alors les classes $\overline{a+b}$ et $\overline{a \times b}$ ne dépendent pas du choix des représentants a et b. En d'autres termes, on a :

$$\overline{a+b} = \overline{a} + \overline{b},$$
$$\overline{a \times b} = \overline{a} \times \overline{b}.$$

On déduit de ces deux égalités modulaires le résultat suivant.

Proposition 2.15. *$(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un anneau commutatif.*

Nous nous intéressons maintenant à la question de l'inversibilité dans $\mathbb{Z}/n\mathbb{Z}$.

Définition 2.16 (Éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$)**.** *Soit $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$. On dit que $\overline{a}$ est inversible s'il existe une classe $\overline{b} \in \mathbb{Z}/n\mathbb{Z}$ tel que $\overline{a} \times \overline{b} = \overline{1}$.*
L'ensemble des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$ est noté $(\mathbb{Z}/n\mathbb{Z})^\times$.

Nous prouvons une caractérisation des éléments de $(\mathbb{Z}/n\mathbb{Z})^\times$.

Proposition 2.17. *Soit $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$, et $a \in \overline{a}$. La classe $\overline{a}$ est inversible si et seulement si* $\operatorname{pgcd}(a, n) = 1$.

Preuve. Supposons que $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$. Alors, on peut trouver $\overline{u} \in \mathbb{Z}/n\mathbb{Z}$ vérifiant

$$\overline{a} \times \overline{u} = \overline{1}. \tag{3}$$

D'après le Lemme 2.13, l'égalité modulaire (3) équivaut à dire qu'il existe $a \in \overline{a}$ et $u \in \overline{u}$ tels que $au \equiv_{[n]} 1$, soit encore $au - 1 \equiv_{[n]} 0$. En d'autres termes, il existe $v \in \mathbb{N}^\star$ tel que $au - 1 = nv$ c'est-à-dire $au + n(-v) = 1$. Finalement, d'après le Théorème 2.10, on déduit que l'égalité modulaire (3) est vérifiée si et seulement si il existe $a \in \overline{a}$ tel que $\operatorname{pgcd}(a, n) = 1$. □

Comme nous l'illustrons avec l'exemple suivant, si $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$ alors on peut déterminer l'inverse de $\overline{a}$ à l'aide de la relation de Bézout.

Exemple 2.18. *Considérons l'anneau* $\mathbb{Z}/52\mathbb{Z}$. *Comme* $\text{pgcd}(17, 52) = 1$, *d'après la Proposition 2.17, on a* $\overline{17} \in (\mathbb{Z}/52\mathbb{Z})^\times$. *Après quelques calculs, on obtient que la relation de Bézout entre* 52 *et* 17 *est* $52 + 17(-3) = 1$. *Par conséquent, l'inverse de* $\overline{17}$ *dans* $\mathbb{Z}/52\mathbb{Z}$ *est* $\overline{-3} = \overline{49}$.

Enfin, nous prouvons que la structure de $\mathbb{Z}/n\mathbb{Z}$ est plus riche lorsque n est premier.

Théorème 2.19. $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ *est un corps si et seulement si* n *est premier.*

Preuve. Le cas $n = 2$ étant trivial, on fixe un entier $n > 2$. Si $\mathbb{Z}/n\mathbb{Z}$ est un corps, alors tout élément différent de $\overline{0}$ est inversible. Ainsi, puisque $i \in \overline{i}$ pour tout $i \in [[2, n-1]]$, on déduit de la Proposition 2.17 que n est premier avec tous les éléments de $[[2, n-1]]$ donc n est un nombre premier. Réciproquement, si n est premier, alors on déduit avec un raisonnement analogue que $\text{pgcd}(k, n) = 1$ pour tout $k \in [[1, n-1]]$. En appliquant la Proposition 2.17, on obtient que pour tout $\overline{k} \in \left\{\overline{1}, \overline{2}, \ldots, \overline{n-1}\right\}$, $\overline{k}$ est inversible. □

Un outils très important pour la cryptologie à clé publique (et en particulier pour RSA) est la **fonction indicatrice d'Euler**, communément notée φ, qui dénombre la quantité d'entier entre 1 et n qui sont premiers avec n. Ainsi, conformément à la Proposition 3, la fonction φ se définit comme suit.

Définition 2.20 (Indicatrice d'Euler)**.** *On appelle* ***indicatrice d'Euler*** *l'application* $\varphi : \mathbb{N}^\star \to \mathbb{N}$ *telle que* $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$, *pour tout* $n \in \mathbb{N}^\star$.

Remarque 2.21. *L'importance de l'indicatrice d'Euler provient essentiellement du fait qu'il n'existe pour l'heure pas de méthode générale et efficace de calcul de l'indicatrice d'Euler, ce qui assure la sécurité du cryptosystème RSA.*

Nous montrons que la fonction indicatrice d'Euler se calcul facilement pour les nombres premiers et leurs puissances.

Proposition 2.22. *Soit* $p \in \mathbb{N}$ *un nombre premier et* $k \in \mathbb{N}^\star$. *Alors :*

(*i*) $\varphi(p) = p - 1$;

(*ii*) $\varphi(p^k) = p^{k-1}(p - 1)$.

Preuve. (*i*) Si p est premier, alors p est premier avec pour les éléments de $[[1, p-1]]$. Donc $\varphi(p) = p - 1$. (*ii*) Considérons un entier $q \in \mathbb{N}^\star$. Il est clair que q n'est pas premier avec p^k si et seulement si p divise q. Ainsi, les entiers non premiers avec p et inférieurs à p^k sont de la forme qp où $q \in [[1, p^{k-1}]]$. On déduit donc qu'il y a $p^k - p^{k-1}$ entiers inférieurs à p^k qui sont premiers avec p^k. Par conséquent, on a $\varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p - 1)$. □

Au sein de la sous-section suivante nous prouverons un résultat qui permet d'étudier le cas du calcul de $\varphi(n)$ quand n est composé, c'est-à-dire quand n n'est pas un nombre premier.

2.3 Théorèmes modulaires fondamentaux

Dans cette section, nous présentons quelques résultats importants de l'arithmétique modulaire pour la cryptographie asymétrique.

Soit $k \in \mathbb{N}^\star$. Désormais, considérant $n_1, n_2, \ldots, n_k \in \mathcal{N}^\star$, on définit la structure d'anneau

$$(\mathbb{N}/n_1\mathbb{Z} \times \mathbb{N}/n_2\mathbb{Z} \times \ldots \mathbb{N}/n_k\mathbb{Z}, +_M, \times_M), \tag{4}$$

muni d'une addition modulaire $+_M$ sommant terme à terme les composantes et d'une multiplication modulaire $\times_M$ en multipliant termes à termes les composantes. On notera dans la suite pour $a \in \mathbb{Z}$, $\overline{a}^k$ sa classe d'équivalence pour la relation d'équivalence $\equiv_{[k]}$.

Exemple 2.23. *Dans l'anneau* $\mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, *les opérations* $+_M$ *et* $\times_M$ *se décrivent comme suit :*

$$(\overline{1}^7, \overline{2}^4) +_M (\overline{5}^7, \overline{3}^4) = (\overline{6}^7, \overline{1}^4),$$
$$(\overline{1}^7, \overline{2}^4) \times_M (\overline{5}^7, \overline{3}^4) = (\overline{5}^7, \overline{2}^4).$$

Nous prouvons une version du théorème des restes chinois.

Théorème 2.24 (Théorème des restes chinois)**.** *Soient $p, q \in \mathbb{N}^\star$. Si* $\text{pgcd}(p,q) = 1$*, alors l'application*

$$\begin{aligned} \pi \,:\, \mathbb{Z}/(pq)\mathbb{Z} &\to \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \\ \overline{x}^{pq} &\mapsto \pi(\overline{x}^{pq}) = (\overline{x}^{p}, \overline{x}^{q}), \end{aligned}$$

est un isomorphisme d'anneaux, c'est-à-dire une application bijective vérifiant pour tout $a, b \in \mathbb{Z}/(pq)\mathbb{Z}$:

(i) $\pi(\overline{1}^{pq}) = \left(\overline{1}^{p}, \overline{1}^{q}\right)$;

(ii) $\pi(\overline{a}^{pq} + \overline{b}^{pq}) = \pi(\overline{a}^{pq}) +_M \pi(\overline{b}^{pq})$;

(iii) $\pi(\overline{a}^{pq} \times \overline{b}^{pq}) = \pi(\overline{a}^{pq}) \times_M \pi(\overline{b}^{pq})$.

Remarque 2.25. *On peut observer que l'application π est bien définie, i.e. π ne dépend pas du représentant x choisi. En fait, si a et b sont deux représentants de $\overline{x}^{pq} \in \mathbb{Z}/(pq)\mathbb{Z}$, on montre que $\pi(\overline{a}^{pq}) = \pi(\overline{b}^{pq})$. Notons que l'on a $\pi(\overline{a}^{pq}) = (\overline{a}^{p}, \overline{a}^{q})$. Pour conclure, il suffit donc de montrer que $a \equiv_{[p]} b$ et $a \equiv_{[q]} b$. Puisque $\overline{a}^{pq} = \overline{b}^{pq}$, on déduit du Lemme 2.13 que $a \equiv_{[pq]} b$. Ainsi, on a $pq \mid a - b$. En d'autres termes, on peut trouver $k \in \mathbb{Z}^\star$ tel que $a - b = k(pq)$. Comme* $\text{pgcd}(p,q) = 1$*, on a $a - b \equiv_{[p]} 0$ et $a - b \equiv_{[q]} 0$, d'où $a \equiv_{[p]} b$ et $a \equiv_{[q]} b$.*

Preuve du Théorème 2.24. Les propriétés (i), (ii) et (iii) se vérifiant aisément, nous omméttons volontairement cette partie de la preuve. Montrons que π est bijective. D'après la Proposition 2.14, π est un morphisme entre cardinaux égaux. Ainsi, pour conclure, il suffit de montrer que π est injective. Soient $\overline{a}^{pq}, \overline{b}^{pq} \in \mathbb{Z}/(pq)\mathbb{Z}$ tels que $\pi(\overline{a}^{pq}) = \pi(\overline{b}^{pq})$. Posons $\overline{y}^{pq} = \overline{a}^{pq} - \overline{b}^{pq}$. Alors, d'après (ii), on a $\pi(\overline{y}^{pq}) = \left(\overline{0}^{p}, \overline{0}^{q}\right)$. D'où :

$$\overline{y}^{p} = \overline{0}^{p} \quad \text{et} \quad \overline{y}^{q} = \overline{0}^{q}. \tag{5}$$

Ainsi, si $\overline{a}^{pq}, \overline{a}^{p}$ et $\overline{a}^{q}$ désignent les classes de a dans $\mathbb{Z}/(pq)\mathbb{Z}, \mathbb{Z}/p\mathbb{Z}$ et $\mathbb{Z}/q\mathbb{Z}$, respectivement, et que $\overline{b}^{pq}, \overline{b}^{p}$ et $\overline{b}^{q}$ désignent les classes de b, en combinant le Lemme 2.13 à (5), on déduit que :

$$a - b \equiv_{[p]} 0 \quad \text{et} \quad a - b \equiv_{[q]} 0,$$

d'où $p \mid a - b$ et $q \mid a - b$. Comme $\text{pgcd}(p,q) = 1$, on déduit du Lemme 2.9 que $pq \mid a - b$. Enfin, d'après le Lemme 2.13, on obtient finalement que $\overline{a}^{pq} = \overline{b}^{pq}$. □

Grâce au théorème précédent, on prouve que **l'indicatrice d'Euler est multiplicative**. Comme nous le verrons plus tard, cette propriété est essentielle pour le cryptosystème RSA.

Théorème 2.26. *Soient $a, b \in \mathbb{N}^\star$ tels que* $\text{pgcd}(a,b) = 1$*. Alors, $\varphi(ab) = \varphi(a)\varphi(b)$.*

Preuve. D'après le Théorème 2.24, $\mathbb{Z}/(ab)\mathbb{Z}$ est isomorphe à $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$. Or, on sait qu'un élément $(\overline{x}^{a}, \overline{x}^{b}) \in \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ est inversible si et seulement si $\overline{x}^{a}$ est inversible et $\overline{x}^{b}$ est inversible. On déduit donc que

$$|\,[(\mathbb{Z}/a\mathbb{Z}) \times (\mathbb{Z}/b\mathbb{Z})]^\times\,| = |(\mathbb{Z}/a\mathbb{Z})^\times| \times |(\mathbb{Z}/a\mathbb{Z})^\times|.$$

En d'autres termes, on a $|(\mathbb{Z}/(ab)\mathbb{Z})^\times| = |(\mathbb{Z}/a\mathbb{Z})^\times| \times |(\mathbb{Z}/a\mathbb{Z})^\times|$, soit encore $\varphi(ab) = \varphi(a)\varphi(b)$. □

Enfin, nous achevons cette section en montrant une version arithmétique du Théorème de Lagrange.

Théorème 2.27 (Théorème de Lagrange)**.** *Soient $a, n \in \mathbb{N}^\star$ tels que* $\text{pgcd}(a,n) = 1$*. Alors l'application*

$$\begin{aligned} \sigma \,:\, (\mathbb{Z}/n\mathbb{Z})^\times &\to (\mathbb{Z}/n\mathbb{Z})^\times \\ \overline{x} &\mapsto \sigma(\overline{x}) = \overline{ax}, \end{aligned}$$

est une bijection.

Preuve. Notons que puisque $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$ est inversible, il existe $\overline{a}^{-1} \in (\mathbb{Z}/n\mathbb{Z})^\times$ tel que $\overline{a}^{-1}\overline{a} = \overline{1}$. Comme l'ensemble de départ et l'ensemble d'arrivé de σ coincident, il suffit de montrer que σ est injective. Soient $\overline{x}, \overline{y} \in (\mathbb{Z}/n\mathbb{Z})^\times$ et x et y leur représentants respectifs. Supposons que $\sigma(\overline{x}) = \sigma(\overline{y})$. Ainsi, on a : $a(x - y) \equiv_{[n]} 0$. Il vient alors que :

$$a^{-1}a(x - y) \equiv_{[n]} 0 \quad \text{ce qui implique que } x \equiv_{[n]} y. \tag{6}$$

Finalement, en combinant (6) au Lemme 2.13, on déduit que $\overline{x} = \overline{y}$. □

Remarque 2.28. *En théorie des groupes, le Théorème 2.27 est appelé Théorème de Lagrange pour les groupes et s'énonce comme suit : Pour tout groupe fini G et tout sous-groupe H de G, l'ordre de H divise celui de G : $|H|$ divise $|G|$.*

3 Cryptologie contemporaine : cas de la cryptographie à clé publique via RSA

La cryptographie moderne est basée sur les mathématiques pour sécuriser l'information. Comme nous l'avons précisé en introduction (voir page 3) il existe deux types de protocoles cryptographiques : la cryptographie à clé privé et la cryptographie à clé publique.

Dans cette section, nous présentons la cryptographie à clé publique introduite par Diffie & Hellman [3]. Ce protocole cryptographique repose sur deux types de clés : une **clé publique** et une **clé privée**. Le principes de l'usage de ces clés est le suivant : pour chiffrer un message, on utilise la clé publique de son destinataire et dans ce cas, seul le destinataire peut déchiffrer le message reçu à l'aide de sa propre clé privée. Le premier cryptosystème à clé publique à été proposé dans les années 1978 par Ronald **R**ivest, Adi **S**hamir et Leonard **A**delman [5]. Il s'agit du cryptosystème **RSA**, qui est le plus répandu au monde car il est facile à réaliser mais très difficile à casser. En fait, sa sécurité repose sur l'un des problèmes les plus difficiles en arithmétique (et en mathématiques), celui de la factorisation des grands nombre.

3.1 Vu d'ensemble du cryptosystème RSA

Nous présentons le principe de RSA. Désormais nous notons $\mathcal{P}$ l'ensemble des nombres premiers.

Soient $p_1, p_2 \in \mathcal{P}$ deux nombres premiers supposés très grands. On appelle **module RSA**, et on note $\mathcal{N}$, le produit $\mathcal{N} = p_1 p_2$. Ainsi, le principe de RSA est le suivant : supposons que deux personnes A et B souhaitent communiquer de façon sûre et font le choix d'utiliser le protocole RSA. Nous listons dans ce qui suit les étapes qui constituent le protocole

Étape 1 - Création de $\mathcal{N}$ (à faire par A et B)

La première étape consiste en la création de deux modules RSA $\mathcal{N}_A$ pour l'individu A et $\mathcal{N}_B$ pour l'individu B. Pour ce faire A et B peuvent chacun utiliser l'algorithme ci-dessous.

Algorithme 1 Création d'un module RSA $\mathcal{N}$

Entrées : Taille T (en bits).
Sorties : Un module RSA $\mathcal{N}$ à T-bits.
1: Choisir aléatoirement un nombre premier $p_1 \in \left[2^{\frac{T}{2}}, 2^{\frac{T+1}{2}}\right]$.
2: Choisir aléatoirement un nombre premier $p_2 \in \left[2^{\frac{T}{2}}, 2^{\frac{T+1}{2}}\right]$.
3: **si** $p_1 = p_2$ **alors**
4: Aller à l'étape 2.
5: **sinon**
6: $\mathcal{N} = p_1 * p_2$.
7: **Fin si**

Étape 2 - Préparation des clés publiques et privées (à faire par A et B)

Une fois que chaque individu est en possession de son propre module RSA, chacun doit préparer une clé secrète d et une clé publique $(\mathcal{N}, e)$. À ce moment, l'indicatrice d'Euler φ (voir Définition 2.20) entre en jeu. Un algorithme permettant de fabriquer ces clés est donné ci-dessous.

Algorithme 2 Création des clés secrètes et publiques

Entrées : $p_1, p_2 \in \mathcal{P}$.
Sorties : Une clé secrète d et un exposant e pour la clé publique .
1: Calculer $\varphi(\mathcal{N}) = (p_1 - 1)(p_2 - 1)$.
2: Choisir aléatoirement un nombre $e \in [[1, \varphi(\mathcal{N})]]$.
3: **si** $\text{pgcd}(e, \varphi(\mathcal{N})) = 1$ **alors**
4: Aller à l'étape 2.
5: **sinon**
6: Calculer $d \equiv_{[\varphi(\mathcal{N})]} e^{-1}$.
7: **Fin si**

Avant de passer à l'étape suivante, nous justifions mathématiquement l'étape 1 de l'algorithme 2. En fait, nous justifions une telle caractérisation de $\varphi(\mathcal{N})$ au moyen de résultat suivant.

Lemme 3.1. *Soient $p_1, p_2 \in \mathcal{P}$. Si $n = p_1 \times p_2$, alors $\varphi(n) = (p_1 - 1)(p_2 - 1)$.*

Preuve. Comme $\text{pgcd}(p_1, p_2) = 1$, on a déduit du Théorème 2.26, que l'on a :

$$\varphi(n) = \varphi(p_1 p_2) = \varphi(p_1) \times \varphi(p_2). \tag{7}$$

En combinant l'estimation (7) à la Proposition 2.22 (i), on obtient le résultat souhaité. □

Étape 3 - Chiffrement du message envoyé par A

On suppose désormais que A et B ont réalisés chacun les étapes 1 et 2. Notons d_B la clé secrète de B et $(\mathcal{N}_B, e_B)$ la clé publique de B. Si A veux envoyer un message à B, il peut procéder comme dans l'algorithme suivant.

Algorithme 3 Chiffrement d'un message envoyé par A à destination de B.

Entrées : Un message clair et la clé publique $(\mathcal{N}_B, e_B)$ de B.
Sorties : Un message chiffré C.
1: Transformer le message en un nombre entier $M \in [2, \mathcal{N}_B]$.
2: Calculer $C \equiv_{[\mathcal{N}_B]} M^{e_B}$.
3: Envoyer le message chiffré C.

Étape 4 - Déchiffrement du message reçu par B

À ce stade, on suppose que B a reçu le message chiffré C envoyé par A. Alors, en utilisant sa propre clé secrète d_B, B est en mesure de déchiffrer le message en procédant comme dans l'algorithme ci-dessous.

Algorithme 4 Déchiffrement d'un message reçu par B.

Entrées : Un message chiffré C et la clé privée d_B de B.
Sorties : Un message déchiffré M.
1: Transformer le message en un nombre entier $M \in [2, \mathcal{N}_B]$.
2: Calculer $M \equiv_{[\mathcal{N}_B]} C^{d_B}$.
3: Transformer le nombre M en un message clair.

Remarque 3.2. *Dans le cadre de ce stage, nous nous limitons au déchiffrement. Toutefois, nous précisons que RSA permet également de vérifier que le message reçu par B provient bien de A. C'est ce que l'on appelle la* ***signature d'un message*** *qui peut être déterminée et faire l'objet d'une vérification.*

3.2 Preuve mathématique du bien fondé du déchiffrement pour RSA

Au sein de cette sous-section, nous prouvons que le crytposystème RSA respecte ses engagement. En d'autres termes, nous montrons que le déchiffrement (en étape 4) d'un message M chiffré à l'étape 3 redonne effectivement le message d'origine M. Cela est une conséquence du Théorème d'Euler que nous montrons ci-dessous.

Théorème 3.3 (Théorème d'Euler)**.** *Soit $n \in \mathbb{N}^\star$. Si $a \in \mathbb{N}^\star$ est tel que $\text{pgcd}(a, n) = 1$, alors $a^{\varphi(n)} \equiv_{[n]} 1$.*

Preuve. Considérons deux entiers $a, n \in \mathbb{N}^\star$ tels que $\text{pgcd}(a, n) = 1$. Notons $\overline{a}$ la classe d'équivalence de a dans $\mathbb{Z}/n\mathbb{Z}$. D'après le Théorème 2.27, on a :

$$\varphi(n) = \left| \left\{ \overline{x} \in \mathbb{Z}/n\mathbb{Z} \;\middle|\; \overline{x} \in (\mathbb{Z}/n\mathbb{Z})^\times \right\} \right| = \left| \left\{ \overline{ax} \in \mathbb{Z}/n\mathbb{Z} \;\middle|\; \overline{x} \in (\mathbb{Z}/n\mathbb{Z})^\times \right\} \right|. \tag{8}$$

Ainsi, on déduit des identités précisées en (8) que l'on a :

$$\prod_{\overline{x} \in (\mathbb{Z}/n\mathbb{Z})^\times} \overline{x} = \prod_{\overline{x} \in (\mathbb{Z}/n\mathbb{Z})^\times} \overline{ax} = \prod_{\overline{x} \in (\mathbb{Z}/n\mathbb{Z})^\times} [\overline{a} \times \overline{x}] = \overline{a}^{\varphi(n)} \left(\prod_{\overline{x} \in (\mathbb{Z}/n\mathbb{Z})^\times} \overline{x} \right). \tag{9}$$

En multipliant la première et la dernière égalité de (9) par le produit de tous les inverses $\overline{x}^{-1} \in (\mathbb{Z}/n\mathbb{Z})^\times$ possibles, on obtient $\overline{1} = \overline{a}^{\varphi(n)}$. □

Grâce au Théorème d'Euler, nous prouvons un Lemme de déchiffrement qui prouve que le message chiffré M par A est bien celui déchiffré par B.

Lemme 3.4 (Lemme de déchiffrement)**.** *Soient $d, e \in \mathbb{N}^\star$ tels que $d \equiv_{[\varphi(\mathcal{N})]} e^{-1}$ avec $\mathcal{N} = p_1 p_2$ où $p_1, p_2 \in \mathcal{P}$. Considérons un entier $M \in \mathbb{N}^\star$. Si $C \equiv_{[\mathcal{N}]} M^e$ alors $M \equiv_{[\mathcal{N}]} C^d$.*

Preuve. D'après le Lemme 3.1, on a $\mathcal{N} = (p_1 - 1)(p_2 - 1)$. Supposons que $\text{pgcd}(M, \mathcal{N}) = 1$. Alors, d'après le Théorème 3.3, on a :

$$M^{\varphi(\mathcal{N})} \equiv_{[\mathcal{N}]} 1. \tag{10}$$

Notons que puisque $d \equiv_{[\varphi(\mathcal{N})]} e^{-1}$, on peut trouver un entier $k \in \mathbb{Z}^\star$ tel que

$$de = 1 + k\varphi(\mathcal{N}). \tag{11}$$

Ainsi, si $C \equiv_{[\mathcal{N}]} M^e$ on obtient, en combinant (10) à (11), que :

$$C^d \equiv_{[\mathcal{N}]} (M^e)^d \equiv_{[\mathcal{N}]} M^{1+k\varphi(\mathcal{N})} \equiv_{[\mathcal{N}]} M \times \left(M^{\varphi(\mathcal{N})}\right)^k \equiv_{[\mathcal{N}]} M.$$

Supposons maintenant que $\text{pgcd}(M, \mathcal{N}) \neq 1$. Alors, comme $p_1, p_2 \in \mathcal{P}$, on a soit $\text{pgcd}(M, \mathcal{N}) = p_1$ et $\text{pgcd}(M, p_2) = 1$ ou bien $\text{pgcd}(M, \mathcal{N}) = p_2$ et $\text{pgcd}(M, p_1) = 1$. Il suffit donc de traiter l'un des deux cas pour conclure. Supposons que $\text{pgcd}(M, \mathcal{N}) = p_1$ et $\text{pgcd}(M, p_2) = 1$. Ainsi, on a $M \equiv_{[p_1]} 0$, d'où $(M^e)^d \equiv_{[p_1]} 0$. Ainsi, on déduit que

$$(M^e)^d \equiv_{[p_1]} M. \tag{12}$$

Puisque $p_2 \in \mathcal{P}$, on déduit de la Proposition 2.22 que $\varphi(p_2) = p_2 - 1$. Ainsi, comme $\text{pgcd}(M, p_2) = 1$, on déduit du Théorème 3.3 que

$$M^{p_2 - 1} \equiv_{[p_2]} 1. \tag{13}$$

Notons que d'après le Théorème 2.26, on a $\varphi(\mathcal{N}) = \varphi(p_1)(p_2 - 1)$. Par conséquent, en utilisant, (11) et (13), on obtient :

$$(M^e)^d \equiv_{[p_2]} M \times \left(M^{\varphi(\mathcal{N})}\right)^k \equiv_{[p_2]} M \times \left(M^{p_2-1}\right)^{k\varphi(p_1)} \equiv_{[p_2]} M \times 1^k \equiv_{[p_2]} M. \tag{14}$$

Enfin, en faisant le produit de (12) et de (14), on obtient $(M^e)^d \equiv_{[\mathcal{N}]} M$. Donc, si $C \equiv_{[\mathcal{N}]} M^e$ on a bien $M \equiv_{[\mathcal{N}]} C^d$. □

3.3 Un résultat de cryptanalyse pour RSA

Au sein de cette ultime sous-section, nous présentons une attaque élémentaire sur le cryptosystème RSA. On discutera essentiellement ici d'un résultat sur la factorisation du module RSA $\mathcal{N}$.

On montre que si l'on connait les valeurs du module RSA $\mathcal{N}$ d'un message chiffré et de son indicatrice d'Euler, alors on peut très simplement retrouver les entiers $p_1, p_2 \in \mathcal{P}$ tels que $\mathcal{N} = p_1 \times p_2$.

Proposition 3.5. *Considérons un module RSA $\mathcal{N}$ dont on connait la valeur. Si $\varphi(\mathcal{N})$ est également connu, alors on peut trouver la factorisation de $\mathcal{N}$.*

Preuve. Si $\mathcal{N}$ et $\varphi(\mathcal{N})$ sont connus, alors d'après le Lemme 3.1, il existe deux entiers $p_1, p_2 \in \mathcal{P}$ tels que :

$$(\mathcal{S}_{p_1,p_2}) : \begin{cases} \mathcal{N} &= p_1 p_2, \\ \varphi(\mathcal{N}) &= p_1 p_2 - p_1 - p_2 + 1, \end{cases}$$

ce qui équivaut à :

$$(\mathcal{S}_{p_1,p_2}) : \begin{cases} \mathcal{N} &= p_1 p_2, \\ -\varphi(\mathcal{N}) + \mathcal{N} + 1 - p_1 &= p_2. \end{cases}$$

Comme $\mathcal{N} \in \mathbb{N}$, alors en injectant la valeur de la deuxième ligne de $(\mathcal{S}_{p_1,p_2})$ dans la première ligne, on déduit que p_1 est solution de l'équation :

$$x^2 - (\mathcal{N} + 1 - \varphi(\mathcal{N}))\, x + \mathcal{N} = 0. \tag{15}$$

Observons que d'après $(\mathcal{S}_{p_1,p_2})$, puisque $\varphi(\mathcal{N})$ est connue, l'équation (15) possède au moins une solution. De plus, si on suppose que (15) possède une unique solution, alors on aurait :

$$p_1 = \frac{\mathcal{N} + 1 - \varphi(\mathcal{N})}{2},$$

ce qui impliquerait, en se référant à la deuxième ligne de $(\mathcal{S}_{p_1,p_2})$, que l'on a $p_1 = p_2$, ce qui est absurde car $p_1, p_2 \in \mathcal{P}$. On déduit donc que l'équation (15) possède exactement deux solutions. Ainsi, en utilisant la deuxième ligne de $(\mathcal{S}_{p_1,p_2})$, on observe que si

$$p_1 = \frac{\mathcal{N}+1-\varphi(\mathcal{N})-\sqrt{(\mathcal{N}+1-\varphi(\mathcal{N}))^2-4\mathcal{N}}}{2}, \text{ alors } p_2 = \frac{\mathcal{N}+1-\varphi(\mathcal{N})+\sqrt{(\mathcal{N}+1-\varphi(\mathcal{N}))^2-4\mathcal{N}}}{2},$$

et a contrario, si

$$p_1 = \frac{\mathcal{N}+1-\varphi(\mathcal{N})+\sqrt{(\mathcal{N}+1-\varphi(\mathcal{N}))^2-4\mathcal{N}}}{2}, \text{ alors } p_2 = \frac{\mathcal{N}+1-\varphi(\mathcal{N})-\sqrt{(\mathcal{N}+1-\varphi(\mathcal{N}))^2-4\mathcal{N}}}{2}.$$

On obtient finalement que le module RSA $\mathcal{N}$ admet la factorisation suivante :

$$\mathcal{N} = \left(\frac{\mathcal{N}+1-\varphi(\mathcal{N})-\sqrt{(\mathcal{N}+1-\varphi(\mathcal{N}))^2-4\mathcal{N}}}{2}\right)\left(\frac{\mathcal{N}+1-\varphi(\mathcal{N})+\sqrt{(\mathcal{N}+1-\varphi(\mathcal{N}))^2-4\mathcal{N}}}{2}\right).$$

La preuve est donc complète. □

4 Conclusion

Nous achevons ce rapport avec quelques mots sur le déroulé du stage. Durant ce stage, j'ai pour mission principale de respecter le formalisme de la rédaction académique qui est fondamentale pour le métier de chercheur. J'ai d'abord eu à me documenter sur la thématique du mémoire, puis j'ai du apprendre à synthétiser les connaissances que je découvrais sur le sujet. Ce stage fut une expérience enrichissante tant sur le plan professionnel que personnel. Il me subjugua par la rigueur nécessaire à la carrière de chercheur que j'ai pu expérimenter. Ce fut la première fois que je considérais les mathématiques comme une fin en soi. Il fit de moi un passionné dévoué à cette discipline.

References

[1] Bailly-Maitre, G. (2021). Arithmétique et cryptologie, 2Ed, Editions Ellipses.

[2] Bourbaki, N. (2007). Algèbre commutative: Chapitres 4 à 7. Springer Science & Business Media.

[3] Diffie, W., & Hellman, M. (1976). New Directions in cryptography. https://caislab.kaist.ac.kr/lecture/2010/spring/cs548/basic/B08.pdf

[4] Kerckhoffs, A. (1883). La cryptographie militaire. J. des Sci. Militaires, 9, 161-191.

[5] Rivest, R., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems, Communications of the ACM, Vol. 21 (2), 120—126.