ARITHMÉTIQUE ET INITIATION À LA CRYPTOGRAPHIE

Dr SORO Kolo Fousséni

ASSISTANT

Université Alassane Ouattara de Bouaké (Côte d'Ivoire)
UFR-SM
Département des Sciences et Techniques
Parcours : Mathématiques et Informatique
Niveau : Licence 1

koloetienne180@gmail.com

7 mai 2023

Table des matières

Introduction

L'arithmétique est un des secteurs scientifiques les plus anciens et les plus féconds. Fondée essentiellement par les pythagoriciens pour qui tout était nombre, elle connu de grands progrès sous l'impulsion de FERMAT, EULER, LAGRANGE, GAUSS, DIOPHANTE et LEGENDRE. Longtemps considérée comme la branche la plus abstraite et la moins utile des mathématiques, elle connaît aujourd'hui de nombreuses applications en informatique, en électronique et en cryptographie.

Chapitre 1

ARITHMETIQUE DANS $\mathbb{Z}$

1.1 Les nombres entiers

1.1.1 Un peu d'histoire des nombres

D'abord étaient connus les entiers $1, 2, 3, ...$ Ces entiers sont connus aussi dans les langues africaines. Puis furent créés 0 et ensuite -1, -2, -3, ...grâce aux paris faits dans des jeux (courses de chevaux, combats,...), par les arabes vers le $V^{ème}$ siècle après J-C.

Remarque : Au départ, bien avant le $V^{ème}$ siècle, zéro comme chiffre n'était pas toujours représenté. Par exemple :

305 était écrit $3 \quad 5$ pour ne pas être confondu à 35.

1.1.2 Les ensembles $\mathbb{N}$ et $\mathbb{Z}$

Définition 1.1.1.

$\mathbb{N} = \{0, 1, 2, 3, ...\}$ *est l'ensemble des entiers naturels.*

$\mathbb{Z} = \{\ldots, -4, -3, -2, -1, 0, 1, 2, 3, \ldots\}$ *est l'ensemble des entiers relatifs.*

Remarque 1.1.1. *Il y a deux types d'entiers : les pairs et les impairs. Les nombres pairs* $\ldots, -4, -2, 0, 2, \ldots$ *sont de la forme* $2n$. *Les nombres impairs* $\ldots, -3, -1, 1, 3, \ldots$ *sont de la forme* $2n + 1$.

Proposition 1.1.1. *On définit sur* $\mathbb{Z}$ *une relation, notée* $\leq$, *par :*

$$\forall a, b \in \mathbb{Z},\ a \leq b \iff \exists c \in \mathbb{N} : b = a + c.$$

C'est une ***relation d'ordre totale****. Sa restriction sur* $\mathbb{N}$ *fait également de* $\mathbb{N}$ *un ensemble totalement ordonné.*

Proposition 1.1.2.

1) *Toute partie non vide de* $\mathbb{N}$ *admet un plus petit élément.*
2) *Toute partie non vide et majorée de* $\mathbb{Z}$ *admet un plus grand élément.*
3) *Toute partie non vide et minorée de* $\mathbb{Z}$ *admet un plus petit élément.*

Proposition 1.1.3. *Soient* $a, b \in \mathbb{Z}$ *tels que* $b \neq 0$. *Il existe* $n \in \mathbb{Z}$ *tel que* $nb \geq a$.

On dit que $\mathbb{Z}$ est archimédien.

Preuve

1^{er} **Cas :** $b \geq 1$.

- Pour $a \geq 0$, il suffit de prendre $n \geq a$;
- Pour $a < 0$, il suffit de prendre n dans $\mathbb{N}$.

$2^{ème}$ **Cas :** $b \leq -1$. Alors $-b \geq 1$ et on retrouve le premier cas, cest-à-dire qu'il existe $m \in \mathbb{Z}$ $(m = -n)$ tel que $m(-b) \geq a$.

1.2 Diviseurs et multiples dans $\mathbb{Z}$

1.2.1 Aperçu historique

Euclide : Naissance inconnue, Actif vers 300 av J.C.

L'expression "**division euclidienne**" est un hommage rendu a **Euclide** qui en explique le principe par soustractions successives dans ses éléments. Faire une division euclidienne consiste à distribuer équitablement une quantité D entre plusieurs entités n. Par exemple, comment repartir 74 stylos sur 8 personnes ? L'application de la méthode de soustractions successives, appelée aussi la méthode naïve, consiste à commencer par donner un stylo à chacune de ces huit personnes, ainsi chacune aura un stylo, et il en reste 66 $(66 = 74 - 8)$. On itère jusqu'à ce qu'il ne soit plus possible de donner 8 stylos. A la dernière distribution, on se rend compte que chacune des huit personnes a eu 9 stylos et qu'il en reste un stock de 2. Ils sont impartageables. On dit que 2 est **le reste** et que 9 est **le quotient** : c'est la part de chacune des 8 personnes.

Ainsi aux deux entiers 74 et 8 de départ, on a associé deux autres entiers 9 et 2 $(2 < 8)$.

Conclusion : Une division euclidienne d'un entier naturel D par un entier naturel $d \neq 0$ est une condensation d'une répétition de q soustraction(s) du nombre d du nombre D :

$$\underbrace{\Big(\Big(\Big(D-d\Big)-d\Big)-d--\Big)}_{q \text{ fois } d}.$$

Une multiplication d'un entier naturel a par un entier naturel n était aussi vue comme étant une condensation d'une répétition de n addition(s) du nombre a :

$$\underbrace{\Big(\Big(\Big(a+a\Big)+a\Big)+a...\Big)}_{n \text{ fois } a}.$$

Ainsi nos quatre opérations actuelles se résumaient en deux seulement.

1.2.2 Division euclidienne dans $\mathbb{Z}$

Définition 1.2.1. *Soient a et b deux entiers. On dit que a divise b, ou que b est divisible par a, s'il existe un entier q tel que $b = aq$.*

*On dit encore que a est **un diviseur** de b, ou que b est **un multiple** de a. On note $a|b$.*

Propriétés 1. *Soient a, b et c des entiers relatifs.*

1) *Si $b \neq 0$, alors b divise a si et seulement si la fraction $\frac{a}{b}$ est un entier.*
2) *Si $b \neq 0$ et b divise a alors $|b| \leq |a|$. Cela montre en particulier que a n'a qu'un nombre fini de diviseurs.*
3) *Si a divise b et que b divise a, alors $|a| = |b|$.*
4) *Si a divise b et b divise c, alors a divise c.*
5) *Si a divise b et c, alors pour tous entiers n et m, a divise $nb + mc$.*
6) *Tous les entiers divisent 0 et sont divisibles par 1.*
7) *Un entier n est toujours divisible par 1, -1, n et $-n$.*

Exercice 1 : Soient x et y des entiers. Montrer que $2x+3y$ est divisible par 7 si et seulement si $5x + 4y$ l'est.

1.3 PGCD (Plus Grand Commun Diviseur)

1.3.1 Comment les anciennes civilisations interprétaient le PGCD de deux nombres ?

Dans la tradition grecque, un nombre entier est pris pour **une longueur** et un couple d'entiers comme **un rectangle** dont les dimensions sont les termes de ce couple. Leur PGCD est la longueur du côté du plus grand carré permettant de carreler entièrement ce rectangle. L'algorithme décompose ce rectangle en carrés, de plus en plus petits, par divisions euclidiennes successives, de la longueur par la largeur, puis de la largeur par le reste, jusqu'à un reste nul.

1.3.2 Définitions et propriétés

Définition 1.3.1. *Soient a et b deux entiers non tous deux nuls. L'ensemble des diviseurs communs de a et de b est fini et non vide, il possède donc un plus grand élément appelé* ***plus grand commun diviseur*** *(pgcd) de a et b et noté $pgcd(a, b)$ ou $a \wedge b$.*

Remarque 1.3.1. *Si a divise b, alors $pgcd(a, b) = a$.*

Propriétés 2. *Soit $(a, b) \in \mathbb{Z} \times \mathbb{Z}\backslash\{(0, 0)\}$.*

i) $0 \wedge 0 = 0$, $a \wedge 0 = a$ *et* $a \wedge 1 = 1$.
ii) $a \wedge b = |a| \wedge |b|$.
iii) $a \wedge b = b \wedge a$.
iv) $\forall k \in \mathbb{N}^*$, $(ka) \wedge (kb) = k(a \wedge b)$.
v) Si k divise a et b, alors $\frac{a}{k} \wedge \frac{b}{k} = \frac{a \wedge b}{k}$.

Lemme 1. (La division euclidienne dans $\mathbb{Z}$)
Soient $b \in \mathbb{Z}$ et $a \in \mathbb{N}^*$. Il existe un unique couple $(s, r) \in \mathbb{Z} \times \mathbb{N}$ tel que

- $0 \leq r < a$
- $b = sa + r$

Définition 1.3.2. *s et r sont appelés respectivement **quotient** et **reste** de la division euclidienne de b par a.*

Remarque 1.3.2. *a divise b si et seulement si $r = 0$.*

1.3.3 Algorithme d'Euclide

Lemme 2. (Lemme d'Euclide)
Soient a et b deux entiers non nuls. S'il existent un entier non nul r et un entier k tels que $a = kb + s$, alors les diviseurs communs à a et b sont exactement les diviseurs commun à b et s. En particulier on a :

$$pgcd(a, b) = pgcd(b, s)$$

Algorithme d'Euclide :
Soient a un entier non nul, b un entier naturel non nul. Comment trouver $d = pgcd(a, b)$?
On pose $r_0 = b$, et on effectue les divisions euclidiennes successives suivantes **tant que le reste n'est pas nul** :

$$a = s_1 r_0 + r_1,\ r_0 = s_2 r_1 + r_2,\ r_1 = s_3 r_2 + r_3,\ r_2 = s_4 r_3 + r_4,\ \ldots$$
$$r_{n-1} = s_{n+1} r_n + r_{n+1}, \forall n \in \mathbb{N}^*.$$

Théorème 1.1. *Le $pgcd(a, b)$ est le dernier reste non nul obtenu par l'algorithme d'Euclide.*

Exercice 2 : Calculer le pgcd des nombres suivants :

1) 1026, 612.
2) 5360, 4780, 3150.
3) 540, 9090, 2250.

1.3.4 Nombres premiers entre eux

Définition 1.3.3. *Deux entiers non nuls a et b sont dits premiers entre eux, si $pgcd(a, b) = 1$.*

Remarque 1.3.3. *Si $d = pgcd(a, b)$, alors $\frac{a}{d}$ et $\frac{b}{d}$ sont premiers entre eux.*

Exercice 3 : Soient a et b des nombres premiers entre eux. Montrer que ab et $a + b$ sont aussi premiers entre eux.

1.4 Théorèmes de Bézout et de Gauss

1.4.1 Sous-groupes de $(\mathbb{Z}, +)$

Théorème 1.2. *Soit H un sous-groupe de $(\mathbb{Z}, +)$. Alors il existe $a \in \mathbb{N}$ tel que $H = a\mathbb{Z}$*

Rappel. On a

$$a\mathbb{Z} + b\mathbb{Z} = pgcd(a,b)\mathbb{Z} \text{ et } a\mathbb{Z} \cap b\mathbb{Z} = ppcm(a,b)\mathbb{Z}.$$

$a\mathbb{Z} + b\mathbb{Z}$ et $a\mathbb{Z} \cap b\mathbb{Z}$ sont des sous-groupes de $(\mathbb{Z}, +)$.

1.4.2 Théorème de Bézout

Théorème 1.3. (Théorème de Bézout)

1) *Soient $a, b \in \mathbb{Z}$ et $d = pgcd(a,b)$. Alors*

$$\exists (u,v) \in \mathbb{Z}^2 \textit{ tel que } au + bv = d \quad (d > 0).$$

2) *a et b deux entiers sont premiers entre eux si et seulement si*

$$\exists (u,v) \in \mathbb{Z}^2 \textit{ telque } au + bv = 1$$

Preuve

1) On considère l'ensemble $\{am + bn, (m,n) \in \mathbb{Z}^2\}$ qu'on note $a\mathbb{Z} + b\mathbb{Z}$.
   Il est clair que $a\mathbb{Z} + b\mathbb{Z}$ est un sous-groupe de $(\mathbb{Z}, +)$, donc

   $$\exists c \in \mathbb{N} \text{ tel que } a\mathbb{Z} + b\mathbb{Z} = c\mathbb{Z}.$$

   Par ailleurs, $a\mathbb{Z} \subset d\mathbb{Z}$ et $b\mathbb{Z} \subset d\mathbb{Z}$ donc $c\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z} \subset d\mathbb{Z}$. En particulier c est un multiple de d et alors $c \geq d$.
   L'égalité $a\mathbb{Z} + b\mathbb{Z} = c\mathbb{Z}$ montre que c divise à la fois a et b, donc $pgcd(a,b) = d \geq c$.
   Finalement, on a $c = d$.

2) ($\Rightarrow$) est clair.
   ($\Leftarrow$) si $au + bv = 1$, alors tout diviseur de a et b divise $au + bv$, donc divise 1.

Comment trouver une relation de Bézout ?

Pour a et b donnés, on trouve une relation de Bézout $au + bv = pgcd(a,b)$ en utilisant encore l'algorithme d'Euclide.

1.4.3 Théorème de Gauss

Théorème 1.4. (Théorème de Gauss)
Soient a, b et c trois entiers non nuls.

1) *Si a divise le produit bc et que a est premier avec b, alors a divise c.*
2) *Si a et b sont premiers entre eux et chacun divise c, alors le produit ab divise c.*

Proposition 1.4.1. *Soit $(a,b,c) \in \mathbb{Z}^3$. Alors les assertions suivantes sont équivalentes.*

i) $a \wedge b = 1$ *et* $a \wedge c = 1$.

ii) $a \wedge bc = 1$.

Généralisation : Si $a_1, ..., a_n$ et $b_1, ..., b_m$ sont deux familles d'entiers relatifs, alors les assertions suivantes sont equivalentes.

i) Chacun des entiér $a_1, ..., a_n$ est premier avec chaque $b_1, ..., b_m$. Autrement dit,

$$a_i \wedge b_j = 1, \forall i \neq j,\ 1 \leq i \leq n \text{ et } 1 \leq j \leq m.$$

ii) $\prod_{i=1}^{n} a_i$ est premiéer avec $\prod_{j=1}^{m} b_j$. Autrement dit

$$pgcd\left(\prod_{i=1}^{n} a_i, \prod_{j=1}^{m} b_j\right) = 1.$$

Par conséquence, si $a \wedge b = 1$, alors

$$\forall m, n \in \mathbb{N}^*,\ a^n \wedge b^m = 1.$$

1.5 Equations diophantiennes du 1^{er} dégré

1.5.1 Présentation et ensemble des solutions

Définition 1.5.1. *Une équation diophantienne du 1^{er} dégré est une équation de la forme*

$$(E) : ax + by = c \text{ avec } a, b, c \in \mathbb{Z}.$$

Proposition 1.5.1. *Soit $(a, b) \in \mathbb{Z}^2$ avec $a \wedge b = 1$. Alors il existe une infinité de couples $(x, y) \in \mathbb{Z}^2$ tels que $ax + by = 1$.*

Si (x_0, y_0) est une solution, alors les autres solutions sont de la forme

$$\begin{cases} x = x_0 + kb \\ y = y_0 - ka \end{cases} \text{ avec } k \in \mathbb{Z}\ .$$

1.5.2 Méthode de résolution

Pour résoudre l'équation diophantienne du 1^{er} dégré $(E) : ax+by = c$, on procède comme suit :

$1^{ère}$ **étape :** Calcul de $pgcd(a, b)$.

- Si $pgcd(a, b)$ ne divise pas c, alors l'équation (E) n'a pas de solution.
- Si $pgcd(a, b) = d$ divise c, alors on consière la nouvelle équation

$$(E') : \frac{a}{d}x + \frac{b}{d}y = \frac{c}{d}.$$

$2^{ème}$ **étape :** Recherche d'une solution particulière avec l'algorithme d'Euclide.

$3^{ème}$ **étape :** Détermination de l'ensemble des solutions.

Exercice 4 : Résoudre dans $\mathbb{Z}^2$, l'équation $1176x + 198y = 6$.

1.6 PPCM (Plus Petit Commun Multiple)

Définition 1.6.1. *Soient a et b deux entiers non nuls. Le plus petit entier naturel non nul qui est multiple à la fois a et b est appelé* ***le plus petit commun diviseur*** *de a et b. On le note $ppcm(a,b)$ ou $a \vee b$.*

Propriétés 3. (Propriétés Remarquables)
Soient a, b deux entiers non nuls.

1) *Si $c \in \mathbb{Z}$ est un multiple de a et b, alors c est un multiple de $ppcm(a,b)$.*
2) *On a :*

$$pgcd(a,b) \cdot ppcm(a,b) = ab.$$

Exercice 5 : Résoudre dans $\mathbb{N}^2$ le système suivante.

$$\begin{cases} xy = 630 \\ x \vee y = 210 \end{cases}.$$

1.7 Nombres premiers

1.7.1 Définitions et propriétés

Définition 1.7.1. *Un entier $n \geq 2$ est dit premier si ses seuls diviveurs positifs sont 1 et n lui même.*

Un nombre qui n'est pas premier est appelé nombre composé.

Théorème 1.5. *Il y a une infinité de nombres premiers.*

Preuve Soit $\mathcal{P} = \{2, 3, 5, 7, \ldots\}$ l'ensemble des nombres premiers. Par l'absurde supposons que $\mathcal{P}$ soit fini, et p_n son plus grand élément. Alors l'entier naturel $q = 2 \cdot 3 \cdot 5 \cdot 7 \cdots p_n + 1$ n'est pas premier, et serait donc divisible par un élément de $\mathcal{P}$. Mais aucun nombre premier ne pourrait diviser q car il divise déjà le facteur produit de q, et donc diviserait 1. Cela est absurde, et donc $\mathcal{P}$ ne peut être fini. ■

1.7.2 Décomposition en produit de facteurs premiers

Théorème 1.6. (**Théorème fondamental de l'arithmétique**).
Tout entier $n \geq 2$ peut s'écrire de façon unique comme produit

$$n = p_1 \cdot p_2 \cdot p_3 \cdots p_r$$

où $r \in \mathbb{N}^\star$, les p_i sont des nombres premiers tels que $p_1 \leq p_2 \cdots \leq p_r$.

Preuve Soit $n \in \mathbb{N}^\star$ et $n \geq 2$.

Existence de la décomposition : Par récurrence sur n, on obtient facilement que soit n est lui-même premier, soit il est produit d'un nombre avec un autre entier n'. On alors $n = pn'$, et forcement $n' < n$ donc n' s'écrit comme produit de nombres premiers selons l'hypothèse de récurrence et par suite n aussi.

Unicité : Si pour un entier $n \geq 2$, on a

$$n = p_1 \cdot \cdot p_s = p'_1 \cdot \cdot p'_{s'} \ ,$$

grâce aux théorèmes de **Bézout** et **Gauss**, on aura

1) $s = s'$,

2) $p_i = p'_i$

Définition 1.7.2. *Soient p un nombre premier et n un entier naturel non nul.*

- *Si p divise n, on dit que p est un* ***facteur premier*** *de n.*
- *Le plus grand entier naturel k tel que p^k divise n s'appelle* ***l'exposant*** *de p dans n.*

Dans le théorème de la décomposition, en regroupant les nombres premiers identiques, on obtient :

Tout entier $n \geq 2$ peut s'écrire de façon unique comme produit

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_r^{\alpha_r}$$

où $r \in \mathbb{N}^\star$, les p_i sont des nombres premiers distincts tels que $p_1 < p_2 < \cdots < p_r$.

Remarque 1.7.1. *Si un nombre premier p n'apparaît pas dans la décomposition de n, son exposant dans n est* ***zéro****.*

Théorème 1.7. *Soient a et b deux entiers naturels non nuls. Pour tout nombre premier p, on note $\alpha(p)$ et $\beta(p)$ respectivement l'exposant de p dans a et l'exposant de p dans b. On a l'équivalence suivante :*

a divise b ***si et seulement si*** *pour tout nombre premier p, $\alpha(p) \leq \beta(p)$.*

Exercice 6 : Soit p un nombre premier. Montrer que

$$\forall i \in \mathbb{N},\ 0 < i < p, \text{ on a : } p \text{ divise } \binom{p}{i}.$$

1.8 Congruence modulo un entier

1.8.1 Définition et propriétés

Définition 1.8.1. *Soient $n \in \mathbb{N}^\star$ et $a, b \in \mathbb{Z}$. On dira que a est congru à b modulo n et on notera $a \equiv b[n]$, si $a - b \in n\mathbb{Z}$, c'est-à-dire $a - b$ est un multiple de n.*

La congruence modulo n définit une relation binaire sur $\mathbb{Z}$. Cette relation est clairement une relation d'équivalence.

Exercice 7 :

1. Calculer $37^3 + 100$ modulo 24.
2. Calculer 15×16 modulo 11.
3. Calculer 7^{2020} modulo 8, et 13^{20} modulo 17.
4. Trouver **l'inverse** de 101^2 modulo 39.
5. Trouver **l'inverse** de 101^2 modulo 3.
6. Dire si 13217 est inversible modulo 21. Si oui, donner son **inverse**.

1.8.2 Systèmes de congruences

On a le théorème suivant :

Théorème 1.8. Théorème des restes chinois
Si n_1, n_2,....,n_k sont des entiers positifs deux à deux premiers entre eux, alors pour tous a_1, a_2,.....,$a_k \in \mathbb{Z}$, le système suivant, appelé système de congruences,

$$\begin{cases} x & \equiv & a_1 & \mod (n_1) \\ x & \equiv & a_2 & \mod (n_2) \\ \cdot & \equiv & \cdot & \\ \cdot & \equiv & \cdot & \\ x & \equiv & a_k & \mod (n_k) \end{cases}$$

a des solutions et, si x_0 est une solution particulière, alors l'ensemble des solutions s'écrit :

$$\{x_0 + (n_1 \cdot n_2 \cdots n_k) \cdot a,\ a \in \mathbb{Z}\}.$$

Exercice 8 : (Systèmes de congruences dans $\mathbb{Z}$.)
Résoudre dans $\mathbb{Z}$ les systèmes de congruences suivants :

$$\begin{cases} x & \equiv & 11 & \mod (117) \\ x & \equiv & -6 & \mod (29) \end{cases}, \quad \begin{cases} x & \equiv & 1 & \mod (117) \\ 22x & \equiv & 1 & \mod (23) \\ x & \equiv & -1 & \mod (5) \end{cases}.$$

Chapitre 2

INITIATION À LA CRYPTOGRAPHIE

De plus en plus, la sécurité de communication est préoccupante pour des structures qui se veulent confidentielles. Alors on recherche perpétuellement des méthodes afin de transmettre ou de sauvegarder des données sur un support sans qu'elles ne soient perçues par des personnes non autorisées : c'est l'objet de la cryptographie. Nous allons étudier quelques-unes de ces méthodes.

2.1 Définitions et vocabulaire

2.1.1 Définitions

(1) La **cryptologie** est la science des messages secrets. Longtemps restreinte aux usages diplomatiques et militaires, elle est aujourd'hui une discipline scientifique à part entière, dont l'objet est l'étude des méthodes permettant d'assurer les services d'intégrité, d'authenticité et de confidentialité dans les systèmes d'information et de communication.

(2) Un service d'**intégrité** garantit que le contenu d'une communication ou d'un fichier n'a pas été modifié.

(3) Un service d'**authenticité** garantit l'identité d'une personne donnée ou l'origine d'une communication ou d'un fichier.

(4) Un service de **confidentialité** garantit que le contenu d'une communication ou d'un fichier n'est pas accessible aux tiers. Des services de confidentialité sont offerts dans de nombreux contextes (téléphonie mobile, communications aérienne, crypter pour réserver la réception des données aux abonnés (télévision), ...).

La cryptologie se divise en deux sous-disciplines :

- la **cryptographie** dont l'objet est de proposer des méthodes pour assurer les services définis plus haut ;
- la **cryptanalyse** qui recherche les failles dans les mécanismes proposés.

2.1.2 Vocabulaire de base

Chiffrement : Il consiste à transformer une donnée (texte clair) afin de la rendre incompréhensible pour une personne autre que celui qui a créé le message et celui qui en est le destinataire.

Texte chiffré : Appelé également cryptogramme, le texte chiffré est le résultat de l'application d'un chiffrement à un texte clair.

Déchiffrement : C'est l'opération permettant de retrouver le texte clair à partir du texte chiffré.

Clé : Il s'agit du paramètre impliqué permettant des opérations de chiffrement ou de déchiffrement.

Cryptanalyse : Elle est opposée à la cryptographie et a pour but de retrouver le texte clair à partir de textes chiffrés en déterminant les failles des algorithmes utilisés.

Cryptosystème : Il est défini comme l'ensemble des clés possibles (espace de clés), des textes clairs et des textes chiffrés possibles associés à un algorithme donné.

Notation 1. *On désigne par :*

. $\mathcal{M}$ *le texte clair,*

. $\mathcal{C}$ *le texte chiffré,*

. $\mathcal{E}_k$ *et* $\mathcal{D}_k$ *respectivement les clés de chiffrement et de déchiffrement,*

. $E(x)$ *la fonction de chiffrement,*

. $D(x)$ *la fonction de déchiffrement.*

Ainsi, en cryptographie la propriété de base est :

$$\mathcal{M} = D(\mathcal{C}) \iff \mathcal{C} = E(\mathcal{M}).$$

2.2 Algorithmes et gestion des clés

2.2.1 Algorithmes symétriques et asymétriques

En cryptographie, il y a deux grandes familles d'algorithmes : les algorithmes symétriques et les algorithmes asymétriques.

Dans le cas des systèmes symétriques, on utilise une même clé pour le chiffrement et le déchiffrement. Le problème repose dans la transmission de la clé : il faut une clé par destinataire. On parle alors de chiffrement à clé secrète. Ces algorithmes sont basés sur des opérations de transposition et de substitution des bits du texte clair en fonction de la clé. L'avantage principal de ce mode de chiffrement est sa rapidité. Le principal désavantage réside dans la distribution des clés : pour une meilleure sécurité, on préfèrera l'échange manuel.

Avec les algorithmes asymétriques, les clés de chiffrement et de déchiffrement sont distinctes et ne peuvent se déduire facilement l'une de l'autre. On peut donc rendre l'une des

deux publique tandis que l'autre reste privée (secrète). Chaque interlocuteur possède donc deux clés distinctes. On parle alors de chiffrement à clé publique. Dans ce cas, tout le monde peut chiffrer un message que seul le propriétaire de la clé privée pourra déchiffrer. On assure ainsi la confidentialité. Certains algorithmes permettent l'utilisation de la clé privée pour chiffrer. Dans ce cas, n'importe qui pourra déchiffrer mais seul le possesseur de la clé privée peut chiffrer. Cela permet donc la signature du message. Ici la distribution des clés est grandement facilitée car l'échange des clés secrètes n'est plus nécessaire.

Tous les algorithmes asymétriques présentent l'inconvénient d'être bien plus lents que les algorithmes à clé secrète. De ce fait, ils sont souvent utilisés, pas pour chiffrer directement des données, mais pour chiffrer une clé secrète.

En marge de ces deux systèmes cryptographiques, il existe également un système appelé "**hybride**", reposant sur les deux systèmes. Par l'intermédiaire du système à clé publique, on sécurise l'échange de la clé K. Ensuite, les deux parties ayant acquis de manière sécurisée cette clé de chiffrement K, on utilisera le système à clé symétrique pour chiffrer le message.

2.2.2 Protocole d'échange de clé

Vers 1978, Diffie, Hellman et Merkle résolvaient le problème de partage d'une clé secrète sans envoi physique de celle-ci. Leur protocole est le suivant :

- Alice et Bob choisissent d'un commun accord, sur une ligne non protégée, un grand nombre premier p et α un générateur de $\dfrac{\mathbb{Z}}{p\mathbb{Z}}$;
- Alice choisit un entier a et calcule $\alpha_a \equiv \alpha^a \mod p$;
- Bob choisit un entier b et calcule $\alpha_b \equiv \alpha^b \mod p$;
- Alice et Bob s'échangent α_a et α_b ;
- Alice calcule $\alpha_b^a mod p$ et Bob calcule $\alpha_a^b \mod p$.

On a :

$$\alpha_b^a \mod p \equiv \alpha_a^b \mod p \equiv \alpha^{ab} \mod p.$$

C'est la clé commune de Alice et Bob.

2.3 La cryptographie classique

2.3.1 Substitution monoalphabétique

Ici, chaque lettre du message est remplacée par une autre lettre ou symbole de l'alphabet choisi. Parmi les plus connus, on citera le chiffre de César, le chiffre affine, ou encore les chiffres désordonnés. De nos jours, ces chiffres sont utilisés pour le grand public, pour les énigmes de revues ou de journaux, etc.

a) Le chiffre de César (50 av. JC)

Soit Γ l'alphabet choisi et $N = card(\Gamma)$. A chaque lettre du message clair, on associe son rang dans l'alphabet Γ. On choisit un nombre entier k compris entre 1 et N : c'est la clé. Elle servira pour le chiffrement et pour le déchiffrement.

Pour le chiffrement, on applique la relation

$$message\_chiffré \equiv (message\_clair + k) \mod N.$$

Pour le déchiffrement, on applique la relation

$$message\_clair \equiv (message\_chiffré - k) \mod N.$$

Exercice 9 : En utilisant l'alphabet $\Gamma = \{A, B, ..., Z\}$ avec la correspondance

$$A = 00,\ B = 01,\ \ldots,\ Z = 25,$$

chiffrer le message suivant "**VENDREDI SOIR**" avec la clé $k = 7$.
Déchiffrer le message obtenu.

b) Le chiffre affine

Soit Γ l'alphabet choisi et $N = card(\Gamma)$. A chaque lettre du message clair, on associe son rang dans l'alphabet Γ. On utilise comme fonction de chiffrement la fonction affine f définie sur $\dfrac{\mathbb{Z}}{N\mathbb{Z}}$, par :

$$f(x) \equiv \overline{a}x + \overline{b},\ a, b \in \mathbb{Z}.$$

La clé c'est le couple $(\overline{a}, \overline{b})$ tel que $pgcd(N, a) = 1$. Le chiffrement est donné par :

$$c_i = f(m_i) \equiv (a \times m_i + b) \mod N$$

où m_i est le rang dans Γ, de la $i^{ème}$ lettre du texte à chiffrer et c_i le resultatdu chiffrement.

Pour le déchiffrement, il vient

$$m_i = f^{-1}(c_i) \equiv a^{-1} \times (c_i - b) \mod N.$$

Remarque 2.3.1.

- *Si $a = 1$, alors on retrouve le chiffre de César où b est le décalage ;*
- *Si $a = 1$ et $b = 0$, il n'y a pas de chiffrement.*
- *La condition $pgcd(N, a) = 1$ assure que a est bien inversible modulo N.*

On notera qu'il existe beaucoup d'autres types de chiffrements monoalphabétiques.

Exercice 10 : Soit $\Gamma = \{A, B, ..., Z, -, '\}$ et f définie sur $\dfrac{\mathbb{Z}}{28\mathbb{Z}}$, par :

$$f(x) \equiv (3x + 11)\,[28]\,.$$

1) Chiffrer le message "**PRATIQUE**" avec la fonction f.
On utilisera la correspondance $A = 00$, $B = 01$, ...

2.*a*) Déterminer f^{-1}.

b) Déchiffrer le message "**EPTFRG'AMZ**".

2.3.2 Chiffrement polygraphique

Il s'agit ici de chiffrer un groupe de symboles à la fois. Ce type de chiffrement porte également le nom de substitutions polygrammiques.

Le chiffre de Hill (1929)

Soit Γ l'alphabet choisi et $N = card(\Gamma)$. On choisit une matrice $A \in \mathcal{M}_n(\mathbb{N})$ inversible modulo N, c'est-à-dire dont le déterminant est premier avec N. Le texte clair $\mathcal{M}$ est subdivisé en blocs de n lettres, partant de la première lettre du texte, c'est-à-dire

$$\mathcal{M} = [m_1 m_2 \dots m_n][m_{n+1} \dots m_{2n}] \dots$$

Ensuite on remplace chaque lettre par son rang dans l'alphabet utilisé. On complètera éventuellement le dernier bloc avec une lettre de choix, qui influencérait moins le chiffrement. Chaque bloc $P = [p_k p_{k+1} \dots p_{k+n}]$ est chiffré de la façon suivante

$$C \equiv AP \mod N$$

où $C = \begin{pmatrix} c_k \\ \vdots \\ c_{k+n} \end{pmatrix}$ est le message chiffré et $P = \begin{pmatrix} p_k \\ \vdots \\ p_{k+n} \end{pmatrix}$. La clé c'est la matrice A.

Pour le déchiffrement on procède comme-ci :

$$P \equiv A^{-1}C \mod N.$$

Exercice 11 : On utilise l'alphabet $\Gamma = \{A, B, ..., Z\}$ avec la correspondance

$$A = 00,\ B = 01,\ \dots,\ Z = 25.$$

Alice choisit comme clé de chiffrement la matrice $A = \begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix}$ pour envoyer le message "**JE VOUS AIME**" à Bob.

1) Déterminer le message reçu par Bob.
2) Calculer A^{-1} l'inverse de la matrice A.
3) Déchiffrer le message reçu par Bob.

2.4 La cryptographie moderne

La cryptographie moderne repose sur les algorithmes à clé publique utilisés soit directement pour le chiffrement, soit pour chiffrer la clé dans un système classique. Le système le plus répandu est le R.S.A..

R.S.A. (Rivest, Shamir, Adleman : 1978**)**

La sécurité de ce système repose sur un problème calculatoire : la factorisation de grands entiers. Le principe est le suivant :

- Choisir p et q deux nombres premiers assez grands et calculer $n = pq$.
- Choisir un très grand entier "e", relativement premier avec $\varphi(n) = (p-1)(q-1)$. La clé publique est formée par le couple (e, n).
- Calculer ensuite l'entier "d" tel que

$$e \times d \equiv 1 \bmod \varphi(n),$$

  La clé privée est donnée par (d, n).

  Les entiers p et q doivent disparaître du processus. Le cryptanaliste devrant retrouver ces valeurs, il faut les effacer pour éviter les fuites.
- A chaque lettre du message clair, on associe son rang dans l'alphabet utilisé ($A = 01$, $B = 02$, ..., $Z = 26$). On procède par découpage du message en blocs de même taille (inferieur ou égal à celui de n) tel que chaque bloc soit inférieur à n, partant de la droite vers la gauche, en ajoutant éventuellement des zéros au début pour compléter le dernier bloc.
- Le chiffrement se fait selon la relation : $\mathcal{C} \equiv \mathcal{M}^e \bmod n$
  et le déchiffrement par : $\mathcal{M} \equiv \mathcal{C}^d \bmod n$.

Remarque 2.4.1. La condition $pgcd(e, \varphi(n)) = 1$ assure l'existence et l'unicité de d modulo $\varphi(n)$.

Exercice 12 : Soient $p = 463$ et $q = 71$.

1) Calculer N le modulus et $\varphi(N)$.

2) Avec $e = 47$ la clé de chiffrement, chiffrer le message suivant :

DEMAIN MATIN.

3) Calculer la clé privée d puis déchiffrer le message obtenu.

UAO Bouaké
Departement : Sciences et Techniques
Année académique : $2022-2023$
Parcours : Maths-Info
Niveau : Licence 1

FICHE DE TRAVAUX DIRIGES

Arithmétique et initiation à la cryptographie

Arithmétique.

Exercice 1 **:** Soit $n \in \mathbb{N}$. Démontrer que le nombre 7^n+1 est divisible par 8 si n est impair. Dans le cas n pair, donner le reste de sa division par 8.

Exercice 2 **:** Montrer que si n est un entier naturel somme de deux carrés d'entiers, alors le reste de la division euclidienne de n par 4 n'est jamais égal à 3.

Exercice 3 **:**

1) Déterminer tous les diviseurs de 7!
2) Déterminer le reste de la division euclidienne de 6^{2023} par 7.
3) Montrer que le reste de la division euclidienne par 8 du carré de tout nombre entier impair est 1.
4) Montrer de même que tout nombre entier pair vérifie $x^2 \equiv 0[8]$ ou $x^2 \equiv 4[8]$.

Exercice 4 **:** Résoudre dans $\mathbb{Z}^2$ les équations suivantes.

a) $170x + 340y = 510$.

b) $81x + 21y = 40$.

c) $174x + 84y = 18$.

Exercice 5 **:** Résoudre dans $\mathbb{N}^2$ le système : $\begin{cases} x \wedge y = 9 \\ x \vee y = 315 \end{cases}$.

Exercice 6 **:**

$$\begin{cases} x \equiv 1 \mod (117) \\ 22x \equiv 1 \mod (23) \\ x \equiv -1 \mod (5) \end{cases}$$

Exercice 7 **:**

1. Calculer modulo 122767 les nombres 41×31, 1271×17, 21607×125.
2. En déduire les inverses de 125 et de 41 modulo 122767.
3. Calculer 41×2978 et 42×2977 modulo 122056. En déduire l'inverse de 41 modulo 122056.

Cryptographie

On considère l'alphabet $\Gamma = \{A, B, ..., Z, -, '\}$ de cardinal 28 et la correspondance suivante :

$$A = 01,\ B = 02,\ ...,\ Z = 26,\ - = 27,\ ' = 28.$$

NB : $-$ *désigne l'espace.*

Exercice 8 **:** (Chiffre de César)

1) Chiffrer le message"**AH LES MATHS**" avec la clé $k = 19$.

2) Déchiffrer le message "**MKHITXABX**" sachant que la clé de chiffrement est $k = 21$.

Exercice 9 **:** (Chiffre affine)

On considère l'application f définie de $\dfrac{\mathbb{Z}}{28\mathbb{Z}}$ dans $\dfrac{\mathbb{Z}}{28\mathbb{Z}}$ par :

$$\forall \overline{x} \in \frac{\mathbb{Z}}{28\mathbb{Z}},\ f(\overline{x}) = \overline{3x - 7}.$$

Alice et Bob utilisent la fonction de chiffrement (affine) f afin de s'envoyer des messages.

1) Justifier que f est bien définie.

2) Montrer que f est une permutation et déterminer f^{-1} son inverse.

3) Pour informer Bob de son résultat pour la première session d'algèbre 1, Alice veut lui envoyer le message clair suivant : "**C'EST VALIDE**".
   a) Déterminer le cryptogramme reçu par Bob.
   b) Décrire comment Bob procède pour retrouver le message clair correspondant.

Exercice 10 **:** (Chiffrement de Hill)

Alice et Bob utilise la matrice $\mathcal{A} = \begin{pmatrix} 1 & 2 & -1 \\ 3 & 0 & 4 \\ 3 & 1 & 3 \end{pmatrix}$ comme clé, afin de s'envoyer des messages.

1) Justifier que $\mathcal{A}$ est inversible modulo 28 puis déterminer $\mathcal{A}^{-1}$ son inverse.

2) Alice reçoit le message

"**NYRMXAQUFFMDUHAMJJ**"

de son ami Bob. Déterminer le message clair correspondant.

Exercice 11 **:** (R.S.A.)

Eli reçoit le message "$\mathbf{001 - 305 - 266 - 352}$" de son ami Eugène. Sachant que la clé publique d'Eli est $(43 \times 17, 29)$, déterminer le message clair correspondant.

Exercice 12 **:** (R.S.A.)

Soient $p = 463$ et $q = 71$.

1) Calculer N le modulus et $\varphi(N)$.

2) Avec $e = 47$ la clé de chiffrement, chiffrer le message suivant :

RENDEZ VOUS AU LYCEE.

3) Calculer la clé privée d puis déchiffrer le message obtenu.