

# Certaines Méthodes de Cryptage Asymétrique

Mr.Prof : MIHOUBI *DOUADI* et HALIMA SAADIA *BOUAZIZ*

23 juin 2018

---

## Remerciements

**L**A louange à dieu et la prière et la paix sur le Messagier d'Allah, et après.

D'abord, je remercie Allah Tout-Puissant, Qui nous aider pour cela et nous le demandons plus, puis je remercie beaucoup les parents, la famille et tous les camarades qui ont marché avec nous sur tout le chemin d'étude, et un grand merci à : mon directeur le professeur Mihoubi Douadi, le chef de département Ben Yatou Abdeet les professeurs . . . . , . . . . , . . . , . . . , et un merci spéciale à . . . . et à mes amis : . . . . . Finalement, je demande à Dieu la sincérité dans le dire et dans le travail.

---

**Notations :**

---

$Ord_g$	Ordre de l'élément $g$ .
$\mathbb{Z}/n\mathbb{Z}$	Groupe quotient.
$(\mathbb{Z}/n\mathbb{Z})^*$	Groupe inversible .
$\varphi$	Fonction d'indicatrice d'Euler .
$\sum$	Symbole de sommation .
$\prod$	Symbole de produit.
$\log_b n$	Logarithme en base $b$ de $n$ .

---

---

# TABLE DES MATIÈRES

<b>Introduction</b>	<b>1</b>
<b>1 Notions Mathématique de Base</b>	<b>3</b>
1.1 Notions sur la divisibilité . . . . .	3
1.1.1 La division euclidienne . . . . .	3
1.1.2 Plus grand commun diviseur ou PGCD . . . . .	4
1.1.3 Algorithme d'Euclide . . . . .	5
1.2 Structures algébriques . . . . .	5
1.2.1 Opérations . . . . .	5
1.2.2 Groupes . . . . .	6
1.2.3 Anneaux $Z/nZ$ . . . . .	8
1.2.4 Corps . . . . .	10
1.3 Préliminaires d'arithmétique . . . . .	11
1.3.1 L'indicatrice d'Euler . . . . .	11
1.3.2 Théorème de Fermat et d'Euler . . . . .	13
1.3.3 Système de congruence (Restes chinois) . . . . .	15
<b>2 Fondamental de cryptographie</b>	<b>17</b>
2.1 Cryptographie Symétrique . . . . .	21
2.1.1 Protocole . . . . .	21

2.2	Systèmes cryptographiques de clé secrète . . . . .	22
2.2.1	Chiffrement par décalage . . . . .	22
2.2.2	Chiffrement par substitution . . . . .	24
2.2.3	Chiffrement par permutation . . . . .	25
2.2.4	Chiffrement affine . . . . .	27
2.2.5	Chiffrement vigenère . . . . .	29
2.2.6	Chiffrement Hill . . . . .	31
<b>3</b>	<b>Cryptosystème asymétrique</b>	<b>36</b>
3.1	Protocole . . . . .	37
3.2	Principe des codes à clef publique. . . . .	37
3.2.1	Fonction sens unique . . . . .	37
3.3	Le cryptosystème Merkle-Hellman. . . . .	39
3.3.1	Problème sac à dos . . . . .	40
3.3.2	Description du cryptosystème Merkle-Hellman. . . . .	41
3.4	Échange de clés de Diffie-Hellman . . . . .	43
3.4.1	Présentation . . . . .	43
3.4.2	Logarithme Discret . . . . .	43
3.4.3	Description de l'algorithme . . . . .	44
3.5	L'algorithme à clé publique RSA . . . . .	46
3.5.1	Présentation . . . . .	46
3.5.2	Description de l'algorithme . . . . .	47
3.5.3	Sécurité de système RSA . . . . .	49
3.5.4	Avantages et Inconvénients . . . . .	49
3.6	L'algorithme à clé publique Al Gamel . . . . .	51
3.6.1	Présentation . . . . .	51
3.6.2	Description de l'algorithme . . . . .	52
3.6.3	Inconvénients et avantages du système El Gamal. . . . .	54
3.7	L'algorithme à clé publique Rabin . . . . .	54
3.7.1	Présentation . . . . .	54

3.7.2	Description de l'algorithme . . . . .	55
3.7.3	Efficacité système de Rabin . . . . .	56
<b>4</b>	<b>L'application des méthodes à clé publique</b>	<b>58</b>
4.1	Cartes à puce . . . . .	59
4.2	RSA est la méthode le plus utilisé . . . . .	60
	<b>Conclusion</b>	<b>63</b>

---

## BIBLIOGRAPHIE

- [1] A. Slinko , *Algebra for Application*, Springer , Auckland (2015).
- [2] B.M. Gilles , *Arithmétique et cryptologie*, ellipses , France (2012).
- [3] B. Magalie , *Cryptographie*, Travaux d'études et de Recherches(2005).
- [4] D .Barsky et G. Dartois , *Cryptographie Paris 13* , France (2010) pp. 99-100.
- [5] D. Mihoubi , *Cours 2<sup>ime</sup> Master Discrète " la Cryptographie "* , Université M'sila , 2017-2018.
- [6] D. Lakel , *Congruence et cryptographie à clé publique* , Université M'sila ,(2014).
- [7] J. Buchmann , *Introduction à la Cryptographie*, Dunod, France (2006).
- [8] J.C. Deneuville , *Contributions à la Cryptographie Post-Quantique* , Thèse de Doctorat de l'Université de Limoges (2016),8-13.
- [9] L. Ladjlat , *Cours 1<sup>re</sup> Master Discrète "courbe Algébrique"*, Université M'sila , 2016-2017.
- [10] M. Mickaël , *Projet de Mathématiques pour l'informatique*. 04-08.
- [11] M. Pierre , *Algèbre avec application à l'algorithmique et à la cryptographie*, ellipses, France (2009).
- [12] S . Douglas R. , *Cryptography theory and bractice*,Champan and Hall/CRC , london (2003).
- [13] W. Pierre , *Arithmétique codes correcteurs cryptographie*, vuibert , France (2009).

- [14] H. Jeffrey, P. Piper et S. Joseph *In introduction to mathematical cryptography* , Springer , San francisco (2008).
- [15] S . Douglas R. , *Introduction to Modern Cryptography* ,Champan and Hall/CRC , london (2008).



---

## INTRODUCTION

Les années 1990 ont été marquées par l'explosion des systèmes de communication, qui ont permis le développement des échanges électroniques, tant dans le domaine industriel et bancaire que dans celui du commerce en ligne et récemment celui des relations entre les citoyens et les administrations. Si, jusqu'à présent, l'ouverture des réseaux et systèmes, ainsi que leurs performances, ont été privilégiées aux dépens de la sécurité, on assiste maintenant à une prise de conscience des problèmes par les acteurs de ces nouveaux réseaux, qui ont engagé des réflexions sur la sécurité et sur la cryptographie qui en constitue une brique fondamentale.

Longtemps réservée au domaine diplomatique et militaire, s'appuyant alors sur des principes mathématiques élémentaires, la cryptographie a commencé à évoluer vers le milieu du siècle avec le début des télécommunications en intégrant essentiellement des techniques de codage de l'information ; mais il a fallu attendre les années 1970 pour qu'elle passe du secret des laboratoires militaires au domaine public, et s'institue comme une véritable science dans le domaine universitaire.

L'objectif principal de ce mémoire est d'étudier " **Certaines méthodes de cryptage asymétrique**". Parce que nous avons désespérément besoin de lui à notre époque. Le sujet du mémoire appartient au domaine de la cryptographie. Ce dernier est divisé en cryptage symétrique et asymétrique. Dans ce travail on s'intéresse au cas asymétrique qui dépend des problèmes difficiles en mathématique.

Dans cette optique notre travail vient selon le plan suivant

Le premier chapitre, présente les notions de base de mathématique, à savoir les structures

algébriques, notion sur la divisibilité, préliminaires d'arithmétique..., dans le deuxième on donne quelques notions fondamentales sur la cryptographie et précisons quelques notions sur la cryptographie symétrique. le troisième est un aperçu sur la cryptographie asymétrique et certaines méthodes essentielles. Enfin, on termine cette mémoire par le quatrième chapitre, ce qui illustre quelques applications sur la cryptographie asymétrique.

---

---

# Chapitre 1

---

## NOTIONS MATHÉMATIQUE DE BASE

L'objectif de ce chapitre est de donner quelques notions d'algèbre élémentaire nécessaires par la suite.

### 1.1 Notions sur la divisibilité

#### 1.1.1 La division euclidienne

**Théorème 1.1.** *Soit  $a$  un entier et  $b > 1$  un entier strictement positif, alors il existe un couple unique  $(q, r)$  vérifiant la double condition*

$$a = bq + r \quad \text{et} \quad 0 \leq r < b.$$

**Définition 1.1.** On dit qu'un entier  $p \geq 2$  est **premier** lorsqu'il possède pour seuls diviseurs positifs 1 et lui-même.

**Théorème 1.2.** *(théorème d'Euclide)*

*Il y a une infinité des nombres premiers.*

**Preuve 1.1.** *supposons que  $p_1, \dots, p_n$  l'ensemble fini de tout les nombres **premiers**. Considérons l'entier*

$$N = p_1 \cdots p_n + 1$$

$N > 1$ , il résulte que  $N$  est divisible par un certain nombre **premier**  $p$ . Si  $p = p_i$  pour  $i = 1, \dots, n$ , puis  $p$  divise  $N - p_1 \cdots p_n = 1$ , ce qui est absurde. Par conséquent,  $p \neq p_i$ . Cela signifie que, pour un ensemble fini des nombres **premiers**, il existe toujours **un premier** qui n'appartient pas à l'ensemble, et donc l'ensemble des nombres **premiers** est infinie. ■

**Théorème 1.3.** (théorème fondamental de l'arithmétique) Tout entier  $a > 1$  s'écrit de façon unique

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$$

Où  $\alpha_i$  sont des entiers positifs, et les entiers  $p_i$  sont **premiers** et vérifient

$$p_1 < p_2 < \cdots < p_n.$$

**Exemple 1.1.**

$$60 = 2^2 \cdot 3 \cdot 5.$$

### 1.1.2 Plus grand commun diviseur ou PGCD

Nous définissons le **plus grand commun diviseur** de deux entiers.

**Définition 1.2.** Soit  $a$  et  $b$  deux entiers naturels. Un **diviseur commun** de  $a$  et  $b$  est un entier qui divise à la fois  $a$  et  $b$ .

**Théorème 1.4.** parmi tous les **diviseurs communs** de deux entiers  $a$  et  $b$ , qui ne sont pas tous les deux nuls, il en existe un qui est **plus grand** que tous les autres. On le note  $\text{pgcd}(a, b)$  où  $(a, b)$  et on l'appelle le **plus grand commun diviseur** de  $a$  et  $b$ .

**Exemple 1.2.** le plus grand commun diviseur de 18 et 30 est 6, on écrit

$$\text{pgcd}(30, 18) = (30, 18) = 6.$$

**Corollaire 1.1.** pour tous  $a, b, n$  l'équation  $ax + by = n$  possède des solution entières  $x$  et  $y$  si seulement si  $\text{pgcd}(a, b)$  divise  $n$ .

**Exemple 1.3.** le corolaire dit que l'équation

$$3x + 4y = 123$$

a un solution, parce que  $\text{pgcd}(4, 3) = 1$  et évidemment 1 divise 123.

### 1.1.3 Algorithme d'Euclide

Soient  $a$  et  $b$  deux entiers tels que  $a > b \geq 0$ .

1. Si  $b = 0$  alors  $\text{pgcd}(a, b) = \text{pgcd}(a, 0) = a$
2. Si  $b \neq 0$  alors  $\text{pgcd}(a, b) = \text{pgcd}(b, r)$ , où  $r$  est le reste de la division euclidienne de  $a$  par  $b$ .

L'algorithme d'Euclide consiste à réitérer la 2<sup>ème</sup> formule jusqu'à ce que l'on tombe sur un reste nul. Dans ce cas, on applique la 1<sup>ère</sup> formule.

**Exemple 1.4.**  $\text{pgcd}(96, 81) = ?$

$$96 = 81 \cdot 1 + 15 \text{ donc } \text{pgcd}(96, 81) = \text{pgcd}(81, 15)$$

$$81 = 15 \cdot 5 + 6 \text{ donc } \text{pgcd}(81, 15) = \text{pgcd}(15, 6)$$

$$15 = 6 \cdot 2 + 3 \text{ donc } \text{pgcd}(15, 6) = \text{pgcd}(6, 3)$$

$$6 = 3 \cdot 2 + 0 \text{ donc } \text{pgcd}(6, 3) = \text{pgcd}(3, 0) = 3$$

$$\text{pgcd}(96, 81) = 3.$$

## 1.2 Structures algébriques

### 1.2.1 Opérations

Une opération, ou loi de composition interne sur un ensemble  $E$  est tout simplement une application du produit cartésien  $E \times E$  dans  $E$ , notée

$$(x, y) \longmapsto x * y.$$

**Définition 1.3.** Une opération " $*$ " sur un ensemble  $E$  est dite

1. Associative, si

$$\forall (x, y, z) \in E \times E \times E, (x * y) * z = x * (y * z).$$

2. Possède un élément neutre, s'il existe un élément  $e \in E$  vérifiant

$$\forall x \in E, e * x = x * e = x.$$

3. Commutative, si

$$\forall (x, y) \in E \times E, x * y = y * x.$$

4. Tout élément admet un symétrique unique, ou est inversible (en notation multiplicative) ou possède un opposé (en notation additive), s'il existe un élément  $y \in E$  vérifiant

$$x * y = y * x = e.$$

En notation multiplicative, on dit alors que  $y$  est l'inverse de  $x$  et on note  $y = x^{-1}$ .

En notation additive, on dit que  $y$  est l'opposé de  $x$ , on note  $y = -x$ .

### 1.2.2 Groupes

**Définition 1.4.** Un groupe est la donnée d'un ensemble  $G$  muni d'une opération interne possédant les propriétés suivantes.

1. L'opération est associative.
2. Elle possède un élément neutre noté  $e$ .
3. Tout élément  $x$  de  $G$  admet un symétrique unique  $y$ .

*Notation 1.1.* On note en général l'élément neutre d'un groupe  $G$  par  $1_G$ .

Si de plus l'opération est commutative on dit que le groupe est commutatif ou abélien.

**Exemple 1.5.** On a

1.  $(\mathbb{Z}, +)$  est un groupe commutatif.
2.  $(\mathbb{Z}, \times)$  n'est pas un groupe car, par exemple  $0$  n'est pas inversible.

**Proposition 1.1.** Soit  $x$  et  $y$  deux éléments d'un groupe. On a

$$(xy)^{-1} = y^{-1}x^{-1}.$$

**Preuve 1.2.** On a

$$\blacklozenge (xy)(y^{-1}x^{-1}) = x(yy^{-1})x^{-1} = x1_Gx^{-1} = xx^{-1} = 1_G.$$

$$\blacklozenge (y^{-1}x^{-1})(xy) = y^{-1}(x^{-1}x)y = y^{-1}1_Gy = y^{-1}y = 1_G.$$

**Définition 1.5.** Une groupe  $G$  est fini si l'ensemble  $G$  est fini. Le nombre d'éléments de  $G$  est alors appelé l'ordre du groupe  $G$ .

**Exemple 1.6.** Le groupe  $S_n$  des permutations  $\{1, 2, \dots, n\}$  est une groupe fini d'ordre  $n!$ .

**Définition 1.6.** Soit  $G$  un groupe. Une partie  $H$  non vide de  $G$  est un sous-groupe de  $G$  si les conditions suivants sont réalisées :

1.  $\forall (x, y) \in H \times H, xy \in H.$
2.  $1_G \in H.$
3.  $\forall x \in H, x^{-1} \in H.$

**Exemple 1.7.** On a

1.  $\mathbb{Z}$  est un sous-groupe de  $\mathbb{Q}$ , qui est un sous-groupe de  $\mathbb{R}$ , lequel est un sous groupe de  $\mathbb{C}.$

**Proposition 1.2.**  $H$  est un sous-groupe de  $G$  si et seulement si

1.  $H \neq \emptyset.$
2.  $\forall (x, y) \in H \times H, xy^{-1} \in H.$

**Preuve 1.3.** Il existe  $x \in H$  d'après (1), il en résulte alors de (2) que  $xx^{-1} = 1_G \in H.$

On en déduit que pour tout  $y \in H, 1_G \cdot y^{-1} = y^{-1} \in H.$

Il en résulte que si  $\forall (x, y) \in H \times H$ , donc  $x(y^{-1})^{-1} = xy \in H.$  ■

**Définition 1.7.** Soit  $(G, \times)$  un groupe fini,  $G$  est **dit cyclique** s'il existe un élément  $g$  de  $G$  tel que  $G = \langle g \rangle$ , c'est-à-dire tel que  $\text{ord}(g) = |G|.$

Dans ce cas, on dit que  $g$  est dit **un générateur** de  $G$  ou encore que  $g$  est **un élément primitif** de  $G.$

**Définition 1.8.** Soit  $g$  élément d'un groupe  $G$ . S'il existe un entier strictement positif  $n$  tel que  $g^n = e$  ( $e$  est élément neutre), alors on peut choisir  $n$  minimal avec cette propriété. On dit alors que  $g$  est un élément d'ordre  $n$ , et on note  $n = \text{ord}(g)$ . S'il n'existe pas d'entier strictement positif  $n$  tel que  $g^n = e$ , on dit que  $g$  est un élément d'ordre infini.

**Théorème 1.5.** (Lagrange) Si  $G$  est un groupe fini et  $H$  est un sous-groupe de  $G$ , alors l'ordre de  $H$  divise l'ordre de  $G$ .

Pour une preuve voir [13]

**Définition 1.9.** Un groupe  $G$  est cyclique s'il existe un élément  $g \in G$ , appelé générateur de  $G$ , tel que  $G = \langle g \rangle$ , ce qui équivaut à l'égalité

$$\text{ord}(g) = \text{ord}(G).$$

On a évidemment tout groupe cyclique est commutatif.

### 1.2.3 Anneaux $\mathbb{Z}/n\mathbb{Z}$

*Remarque 1.1.* Un anneau est la donnée d'un triplet  $(A, +, \cdot)$  où  $A$  est un ensemble non vide et  $+$ ,  $\cdot$  sont deux lois de composition interne sur  $A$  tels que

$A_1$  :  $(A, +)$  est un groupe commutatif.

$A_2$  : La multiplication dans  $A$ , c'est à dire l'application

$$(x, y) \in A^2 \longrightarrow x \cdot y \in A$$

vérifie

1.  $x \cdot (y \cdot z) = (x \cdot y) \cdot z$  (associativité) pour  $x, y, z \in A$ .
2. 
$$\begin{cases} x \cdot (y + z) = x \cdot y + x \cdot z \\ (x + y) \cdot z = x \cdot z + y \cdot z \end{cases} \quad \text{pour tous } x, y, z \in A.$$

S'il existe  $e \in A$  tel que  $e \cdot x = x \cdot e = x$  pour tout  $x \in A$ , l'anneau est dit unitaire. Si de plus, la multiplication est commutative, on dit que l'anneau  $A$  est commutatif.



**Exemple 1.8.**  $(\mathbb{Z}, +, \cdot), (\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot), (\mathbb{C}, +, \cdot)$  sont des anneaux commutatifs unitaires.

**Définition 1.10. (Congruence)** Soit  $n$  un entier positif. On dit que deux entiers  $a$  et  $b$  sont congrus modulo  $n$  si leur différence  $(b - a)$  est multiple de  $n$ , c'est à dire si  $(b - a) \in n\mathbb{Z}$ . Cette relation est notée

$$a \equiv b \text{ mod } n \text{ ou bien } a \equiv b[n].$$

La notation de congruence modulo  $n$  a été introduite par Gauss.

**Exemple 1.9.**

$$2018 \equiv 2 \text{ mod } 12$$

**Proposition 1.3.** Si  $a, b, c, d, m$ , et  $n$  sont des entiers relatifs,

- ◆  $a \equiv a \text{ mod } n$
- ◆ si  $a \equiv b \text{ mod } n$ , alors  $b \equiv a \text{ mod } n$ ,
- ◆ si  $a \equiv b \text{ mod } n$  et  $b \equiv c \text{ mod } n$ , alors  $a \equiv c \text{ mod } n$ ,
- ◆ si  $a \equiv b \text{ mod } n$  et  $c \equiv d \text{ mod } n$ , alors  $a + c \equiv b + d \text{ mod } n$ ,
- ◆  $a \equiv b \text{ mod } n$  et  $c \equiv d \text{ mod } n$ , alors  $ac \equiv bd \text{ mod } n$ ,
- ◆  $a \equiv b \text{ mod } n$  et si  $m$  entier positif, alors  $a^m \equiv b^m \text{ mod } n$ . On vérifie que la relation  $\equiv$  est une relation d'équivalence sur  $\mathbb{Z}$  compatible avec l'addition et la multiplication, c'est-à-dire que si  $a \equiv a' \text{ mod } n$  et si  $b \equiv b' \text{ mod } n$  alors

$$a + b \equiv a' + b' \text{ mod } n \text{ et } ab \equiv a'b' \text{ mod } n.$$

Pour tout entier  $a$ , on not  $a \text{ mod } n$  la classe de congruence (ou la classe résiduelle) de  $a$  modulo  $n$ , et s'il n'y a pas d'ambiguïté, on utilisera aussi la notion  $\bar{a}$ . Autrement dit,

$$a \text{ mod } n = \bar{a} = \{x \in \mathbb{Z} : x \equiv a \text{ mod } n\}.$$

On note  $\mathbb{Z}/n\mathbb{Z}$  le quotient de  $\mathbb{Z}$  avec cette relation d'équivalence. Pour  $\bar{a}, \bar{b} \in \mathbb{Z}/n\mathbb{Z}$ , on pose  $\bar{a} + \bar{b} = \overline{a + b}$  et  $\bar{a}\bar{b} = \overline{ab}$ .

On vérifie alors que  $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$  est un anneau commutatif, dite l'anneau des classes

de congruence (des classe résiduelles). De plus, le groupe  $(\mathbb{Z}/n\mathbb{Z}, +)$  est l'unique groupe cyclique à  $n$  éléments, il engendré par  $\bar{1}$ , à savoir

$$\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \dots, \overline{(n-1)}\}.$$

**Définition 1.11.** Soit  $\bar{x}$  un élément de  $\mathbb{Z}/n\mathbb{Z}$ , on dit que  $\bar{x}$  est inversible si et seulement si il existe  $\bar{y} \in \mathbb{Z}/n\mathbb{Z}$  tel que  $\bar{x}\bar{y} = \bar{1}$ . Alors cet élément  $\bar{y}$  est unique et s'appelle l'inverse de  $\bar{x}$  et on not  $\bar{x}^{-1}$ .

### 1.2.4 Corps

**Définition 1.12.** Un corps  $\mathbb{K}$  est un anneau commutatif dans lequel tout élément non nul admet un inverse pour la multiplication, c'est-à-dire  $\mathbb{K}^* = (\mathbb{K} \setminus \{0\})$ . tel que

$$(\mathbb{K}, +, \cdot) : \begin{cases} \blacklozenge & (\mathbb{K}, +) \text{ est un groupe commutatif.} \\ \blacklozenge & (\mathbb{K}^*, \cdot) \text{ est un groupe.} \end{cases}$$

Un corps est dit commutatif s'il est commutatif en tant qu'anneau, c'est-à-dire si sa multiplication est commutative.

**Définition 1.13.** (Corps finis)

On appelle corps fini tout corps possédant un nombre fini d'éléments un corps fini est dit aussi un corps de Galois (Galois field).

*Remarque 1.2.* Le plus petit corps de Galois est  $F_2 = \{\bar{0}, \bar{1}\}$  muni de l'addition (+) et de la multiplications ( $\times$ ) modulo 2.

Avec  $\bar{0}$  est l'élément neutre de l'addition (+) et  $\bar{1}$  est élément neutre de multiplication ( $\times$ ).

**Exemple 1.10.** On a

1. Soit  $F_2 = \mathbb{Z}/2\mathbb{Z} = (\{\bar{0}, \bar{1}\}, +, \times)$ , la table d'addition et de multiplication de  $\mathbb{Z}/2\mathbb{Z}$  sont

+	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$
$\bar{1}$	$\bar{1}$	$\bar{0}$

$\times$	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{1}$	$\bar{0}$

2. Soit  $F_3 = \mathbb{Z}/3\mathbb{Z} = (\{\bar{0}, \bar{1}, \bar{2}\}, +, \times)$  la table d'addition et multiplication de  $\mathbb{Z}/3\mathbb{Z}$  sont

+	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{1}$

+	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{1}$

## 1.3 Préliminaires d'arithmétique

### 1.3.1 L'indicatrice d'Euler

**Définition 1.14.** Soit  $n$  un entier positif, l'indicatrice d'Euler de  $n$ , notée  $\varphi(n)$ , est définie comme étant égale au nombre des entiers  $k$  vérifiant

$$\varphi(n) = |\{1 \leq k \leq n \text{ et } \text{pgcd}(k, n) = 1\}|. \quad (1.1)$$

Notons que pour tout entier positif  $n$ , on a  $\text{pgcd}(1, n) = 1$ , ce qui fait que  $\varphi(n) \geq 1$ .

**Exemple 1.11.** On trouvera quelques valeurs de  $\varphi(n)$  dans le tableau suivant

$n$	1	2	3	4	5	6	7	8	9	10	...
$\varphi(n)$	1	1	2	2	4	2	6	4	6	4	...

**Théorème 1.6.** Soit  $m$  et  $n$  entiers premiers positifs. Pour chaque entier  $c$  il existe des entiers uniques  $a$  et  $b$  tels que

$$0 \leq a \leq n - 1,$$

$$0 \leq b \leq m - 1,$$

et

$$c \equiv ma + nb \pmod{mn}. \quad (1.2)$$

De plus,  $(c, mn) = 1$  si et seulement si  $(a, n) = (b, m) = 1$  dans la représentation (1.2).

**Définition 1.15.** Une fonction arithmétique  $f$  est dite multiplicative si pour toutes les paires premiers positifs  $m$  et  $n$

$$f(mn) = f(m) \cdot f(n)$$

**Théorème 1.7.** *La fonction d'Euler est multiplicatif. De plus*

$$\varphi(m) = m \prod_{(p|m)} (p - 1/p)$$

**Preuve 1.4.** *Soit  $(m, n) = 1$ . Il y a  $\varphi(mn)$  classes de congruence dans l'anneau  $Z/mnZ$  qui sont relativement premier avec  $mn$ .*

*D'après le théorème (1.6) pag 11, tous les classes des congruences modulo  $mn$  peut être écrit de manière unique sous la forme  $ma + nb + mnZ$ , où  $a$  et  $b$  sont des entiers tels que*

$$0 \leq a \leq n - 1 \text{ et } 0 \leq b \leq m - 1$$

*En outre, la classe de congruence  $ma + nb + mnZ$  est premier avec  $mn$  si et seulement si  $(b, m) = (a, n) = 1$ . Alors il existe  $\varphi(n)$  entiers  $a \in [0, n - 1]$ , qui sont relativement premier avec  $n$ , et  $\varphi(m)$  entiers  $b \in [0, m - 1]$  relativement premier à  $m$ , il se en suit que*

$$\varphi(mn) = \varphi(m) \cdot \varphi(n)$$

*Donc la fonction d'Euler  $\varphi$  est multiplicative. Si  $m_1, \dots, m_K$  sont deux à deux premiers positifs, alors*

$$\varphi(m_1 \cdots m_K) = \varphi(m_1) \cdots \varphi(m_K)$$

*En particulier, si  $m = p_1^{r_1} \cdots p_k^{r_k}$  la factorisation de  $m$ , où  $p_1, \dots, p_k$  sont des premiers distincts, et  $r_1, \dots, r_k$  sont des entier positifs, alors*

$$\varphi(m) = \prod_{i=1}^k \varphi(p_i^{r_i}) = \prod_{i=1}^k p_i^{r_i} \left(1 - \frac{1}{p_i}\right) = m \prod_{(p|m)} \left(1 - \frac{1}{p}\right).$$

■

**Exemple 1.12.** On a  $7875 = 3^2 \cdot 5^3 \cdot 7$  et

$$\varphi(7875) = \varphi(3^2) \cdot \varphi(5^3) \cdot \varphi(7) = (9 - 3)(125 - 25)(7 - 1) = 3600$$

**Théorème 1.8.** *Pour tout entier positif  $m$ , on a*

$$\sum_{(d|m)} \varphi(d) = m$$

**Exemple 1.13.**

$$\begin{aligned}\sum_{(d/10)} \varphi(d) &= \varphi(1) + \varphi(2) + \varphi(5) + \varphi(10) \\ &= 1 + 1 + 4 + 4 \\ &= 10.\end{aligned}$$

**Corollaire 1.2.** *Le groupe multiplicatif de résidus mod  $p$  est cyclique d'ordre  $p - 1$ . Il a exactement  $\varphi(p - 1)$  générateurs.*

**Définition 1.16.** Un entier  $a$  dont la classe résiduelle  $a + pZ$  engendre le groupe multiplicatif  $(Z/pZ)^*$  s'appelle une racine primitive mod  $p$ .

**Exemple 1.14.** Pour  $p = 13$ , nous avons  $p - 1 = 12$ . Le théorème 1.3 donne  $\varphi(12) = 4$ . Il existe donc racine primitives mod 13, ce sont 2, 6, 7 et 11.

### 1.3.2 Théorème de Fermat et d'Euler

Le résultat suivant a été proposé par le mathématicien et magistrat français Pierre de Fermat, (1601-1665), en 1640. Il a été démontré par Leonhard Euler près de cent ans plus tard. On l'appelle " petit théorème de Fermat " par opposition au célèbre théorème de Fermat, aussi appelé " dernier théorème de Fermat ", que Fermat avait cru démontrer, et dont la démonstration n'a en réalité été établie qu'en 1994 par le mathématicien britannique Andrew Wiles [13]. Nous allons nous intéresser aux puissances successives d'un entier  $a(mod\ m)$  lorsque  $(a, m) = 1$ . Commençons par un exemple.

**Exemple 1.15.** Prenons  $m = 7$  et considérons  $Z/7Z$ . Les unités dans cet anneau sont toutes les classes non nulles. Si l'on calcule les puissances de 2, on trouve que

$$2^2 = 4 \equiv 4 \mod 7 \qquad 2^3 = 8 \equiv 1 \mod 7$$

Ce qui donne, en d'autre termes que  $\bar{2}^3 = \bar{1}$  dans  $Z/7Z$ .

On trouve encore que

$$\begin{aligned}3^2 &= 9 \equiv 2 \mod 7 & 3^3 &= 27 \equiv -1 \mod 7 \\ 3^4 &= -1 \cdot 3 \equiv 4 \mod 7 & 3^5 &= 4 \cdot 3 \equiv 5 \mod 7\end{aligned}$$

$$3^6 = 15 \equiv 1 \pmod{7}.$$

Ce qui montre que  $\bar{3}^6 = \bar{1}$  dans  $Z/7Z$  et 6 est le plus petit entier positif  $n$  tel que  $\bar{3}^n = \bar{1}$ .

On peut montrer qu'il existe toujours un entier  $n$  tel que

$$a^n \equiv 1 \pmod{m}.$$

**Proposition 1.4.** *Soient  $a$  et  $m$  des entiers tel que  $(a, m) = 1$  et  $m \geq 1$ . Alors il existe un entier  $n$  tel que*

$$a^n \equiv 1 \pmod{m}.$$

**Définition 1.17.** (Ordre d'un entier mod  $m$ ) Soit  $m$  un entier  $> 1$  et  $a$  un entier tel que  $(a, m) = 1$ . Le plus petit entier positif  $n$  tel que

$$a^n \equiv 1 \pmod{m},$$

est appelé l'ordre de  $a$  modulo  $m$ .

**Théorème 1.9.** (Théorème Euler) Soit  $a$  et  $m$  deux entiers tels que  $m > 1$ , et  $(a, m) = 1$ .

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

Pour la preuve voir [6]

**Proposition 1.5.** Soit  $a$  un entier  $\geq 2$  et soit  $m \in \mathbb{N}$ . Si

$$(a, m) = (a - 1, m) = 1$$

Alors

$$1 + a + a^2 + \dots + a^{\varphi(m)-1} \equiv 0 \pmod{m}$$

**Preuve 1.5.** Puisque  $(a, m) = 1$ , alors d'après le théorème d'Euler, on a

$$a^{\varphi(m)-1} \equiv 0 \pmod{m}$$

alors

$$a^{\varphi(m)-1} = (a - 1)(a^{\varphi(m)-1} + a^{\varphi(m)-2} + \dots + a + 1)$$

et puisque  $(a - 1, m) = 1$ , donc

$$1 + a + a^2 + \dots + a^{\varphi(m)-1} \equiv 0 \pmod{m}$$

■

**Théorème 1.10.** (*petit théorème de Fermat*) Soit  $a$  un entier et  $p$  un premier ne divisant pas  $a$ . Alors

$$a^{p-1} \equiv 1 \pmod{p}.$$

Pas ailleurs,  $a^p \equiv a \pmod{p}$ .

**Preuve 1.6.** C'est une conséquence immédiate du théorème d'Euler en sachant que

$$\varphi(p) = p - 1$$

lorsque  $p$  est premier. ■

### 1.3.3 Système de congruence (Restes chinois)

**Théorème 1.11.** (*théorème des restes chinois*)

Soit  $m_1, m_2, \dots, m_k$  une suite d'entiers positifs deux à deux premiers entre eux. Alors le système de congruence

$$\begin{cases} x \equiv a_1 [m_1] \\ x \equiv a_2 [m_2] \\ \dots \\ x \equiv a_k [m_k] \end{cases}$$

a une solution unique  $x \pmod{M}$  ( $M = m_1 \cdot m_2 \cdot \dots \cdot m_k$ ),

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 + \dots + a_k M_k y_k$$

avec  $M_i = M / m_i$  et  $y_i M_i \equiv 1 [m_i]$

pour le prouver voir [9]

**Exemple 1.16.** Soit le système des congruences suivant

$$\begin{cases} x \equiv 1 [3] & (1) \\ x \equiv 2 [5] & (2) \\ x \equiv 3 [7] & (3) \end{cases}$$

On a  $(3, 5) = (5, 7) = (3, 7) = 1$ , donc le système précédent admet une seule solution modulo  $(3 \times 5 \times 7 = 105)$  d'après le théorème des restes chinois (1.11) pag 15, et pour trouver la solution On pose  $M = 3 \times 5 \times 7 = 105$ ,

$$M_1 = 105/3 = 35 \quad y_1 \times 35 \equiv 1[3] \quad y_1 = 2$$

$$M_2 = 105/5 = 21 \quad y_2 \times 21 \equiv 1[5] \quad y_2 = 1$$

$$M_3 = 105/7 = 15 \quad y_3 \times 15 \equiv 1[7] \quad y_3 = 1$$

$$x \equiv 1 \times 35 \times 2 + 2 \times 21 \times 1 + 3 \times 15 \times 1 = 1157[105]$$

$$x \equiv 52[105].$$

## Entiers de Blum

**Définition 1.18.** Un entier de Blum est un produit de deux nombres premiers distincts et tous deux congrus à 3 modulo 4.

Comme nous allons le voir, si  $n$  est un entier de Blum, alors nous pouvons facilement calculer les racines carrées dans  $(\mathbb{Z}/n\mathbb{Z})^\times$ . Sur cette propriété repose un algorithme de chiffrement à clé publique célèbre que nous étudierons plus tard : le chiffrement de Rabin (voir [2]).

**Proposition 1.6.** Soit  $n = pq$  un entier de Blum et soit  $x$  un carré de  $(\mathbb{Z}/n\mathbb{Z})^\times$ , alors  $x$  possède quatre racines dont une (et une seule) est elle-même un carré de  $(\mathbb{Z}/n\mathbb{Z})^\times$ . Cette racine est appelée **racine principale** de  $x$  et nous la noterons  $\sqrt{x}$ . pour la preuve voir [2]

**Proposition 1.7.** Soit  $n = pq$  un entier de Blum et soit  $x$  un carré de  $(\mathbb{Z}/n\mathbb{Z})$  non inversible.

- ◆ Si  $x = 0$ , son unique racine carrée est 0.
- ◆ Si  $x$  est multiple de  $p$ , alors ses deux racines carrées sont  $\pm x^{\frac{q+1}{4}}$ ,
- ◆ Si  $x$  est multiple de  $q$ , alors ses deux racines carrées sont  $\pm x^{\frac{p+1}{4}}$ .



---

---

# Chapitre 2

---

## FONDAMENTAL DE CRYPTOGRAPHIE

L'objectif fondamental de la cryptographie est de permettre à deux personnes, communément appelées Alice et Bob, de communiquer sur un canal non sécurisé de manière à ce qu'un adversaire, Oscar, ne puisse pas comprendre ce qui est dit. Ce canal pourrait être une ligne téléphonique ou un réseau informatique, par exemple. L'information qu'Alice envoie à Bob, que nous appelons « texte clair », peut être du texte anglais, des données numériques, ou quoi que ce soit, sa structure est complètement arbitraire. Alice crypte le texte en clair en utilisant une clé prédéterminée et envoie le texte chiffré résultant sur le canal. Oscar, en voyant le texte chiffré dans le canal, ne peut pas déterminer le texte en clair, mais Bob, qui connaît la clé de chiffrement, peut déchiffrer le texte chiffré et reconstruire le texte en clair. Dans toute méthode de cryptage on a besoin d'un algorithme de chiffrement  $E$  et un algorithme de déchiffrement  $D$ . Dans les systèmes de cryptage classique les deux algorithmes dépendent d'une même clé de cryptage  $k$  pour ce la ces méthodes de cryptage sont dits symétriques.[5][4]

On a  $D(k, E(k, m)) = m$

- ◆  $E$  : Encryptage ou bien, chiffrement.
- ◆  $D$  : Décryptage ou bien, déchiffrement.
- ◆  $k$  : clé.

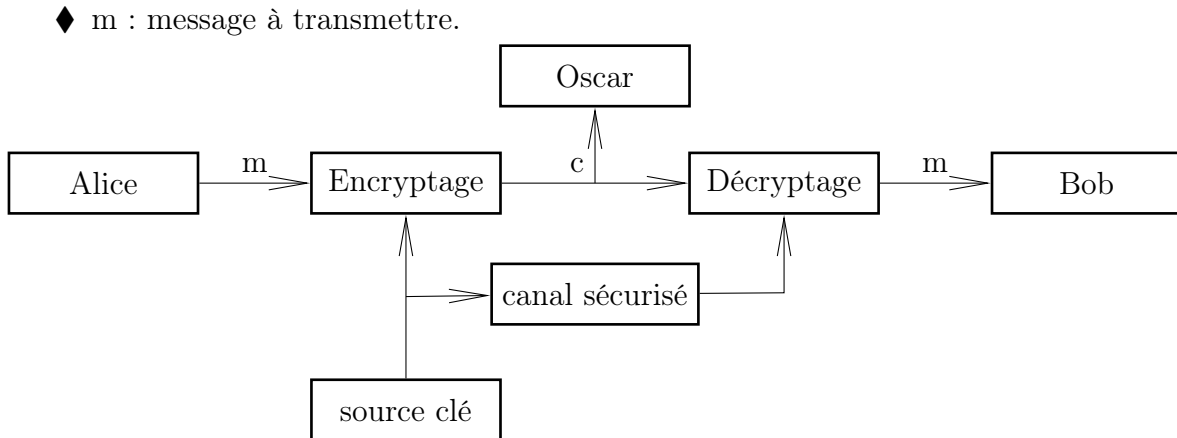


FIGURE 2.1 – Le canal de communication

## Quelques notions sur la cryptographie

- ◆ **Cryptographie** : est un mot grec signifiant (crypto - graphie = caché écriture ).
- ◆ **Cryptanalyse** : science analysant les cryptogrammes en vue de les décrypter .
- ◆ **Cryptologie** : science regroupant la cryptographie et la cryptanalyse.
- ◆ **Chiffre** : Un ensemble de règles permettant d'écrire et de lire dans un langage secret.
- ◆ **Cryptogramme** : Message chiffré.
- ◆ **Cryptosystème** : Algorithme de chiffrement.
- ◆ **Décrypter** : Retrouve le message clair correspondant à un message chiffré sans posséder la clé de déchiffrement.

**Définition 2.1.** Un système de chiffrement est un quintuplet  $(P, C, K, E, D)$  (voir [12]) où on a :

- ◆ Un ensemble fini  $P$  appelée l'espace des textes clairs (Plain texts).
- ◆ Un ensemble fini  $C$  appelée l'espace des textes chiffrés (cipher texts).
- ◆ Un ensemble fini  $K$  appelée l'espace des clés (keys).
- ◆ Pour chaque clé  $k \in K$ , une fonction de chiffrement (encryption)  $e_k : P \mapsto C$  et une fonction de déchiffrement (decryption)  $d_k : C \mapsto P$  telles que  $d_k \circ e_k = Id_P$

On suppose que le message qui suit va être transis  $m = x_1x_2...x_n$ ,  $n \geq 1$  où  $\forall i \in 1..n, x_i \in P$ .  $x_i$  est chiffré au utilisant la règle (règle = méthode de cryptage ),  $e_k$  spécifies par un clés  $k \in K$  donc

Alice calcule  $y_i = e_k(x_i)$  ,  $1 \leq i \leq n$ . Ce qui donne le texte chiffré  $y = y_1y_2...y_n$  qui va être envoyer à travers le canal.

Lorsque Bob reçoit le message  $y_1y_2...y_k$ , il le décrypte en utilisant la fonction  $d_k$  pour obtenir le message original  $x_1x_2...x_n$

- Il faut que la fonction  $e_k$  soit injective sinon le déchiffrement ne sera pas accomplit correctement. En effet,

$y = e_k(x_1) = e_k(x_2)$  avec  $x_1 \neq x_2$   $d_k(y) = d_k(e_{x_1})$ .

On sait pas par quoi décrypter y par  $x_1$  ou bien  $x_2$ .

## Principe de Auguste Kerckhoffs (1883)

En 1883 dans un article paru dans le Journal des sciences militaires, [4]. Auguste Kerckhoffs (1835-1903) posa le principe de la cryptographie moderne. Ce principe et en particulier le second stipulent entre autre que **la sécurité d'un cryptosystème ne doit pas reposer sur le secret de l'algorithme de codage mais qu'elle doit uniquement reposer sur la clef secrète du cryptosystème** qui est un paramètre facile à changer, de taille réduite (actuellement de 64 à 2048 bits suivant le type de code et la sécurité demandée) et donc assez facile à transmettre secrètement.



FIGURE 2.2 – Auguste Kerckhoffs

### Objectifs des codes actuels.

Rappelons les qualités attendues d'un cryptosystème. Tout d'abord les qualités fonctionnelles

1. **Confidentialité des données** : Les messages ne peuvent être déchiffrés que par le destinataire.
2. **Intégrité des données** : Ils ne peuvent être modifiés par un tiers non autorisé.
3. **Authentification** : L'identité des différents participants peut être vérifiée.
4. **Non-répudiation** : L'expéditeur ne peut nier avoir émis le message et le destinataire ne peut nier l'avoir reçu (voir [4] ).

Ensuite les qualités pratiques

1. Il doit résister aux attaques connues et si possible avoir une sécurité prouvée.
2. Il doit permettre de coder et décoder rapidement (en temps réel pour certaines applications).

Il n'existe pas de codes qui réunissent toutes ces qualités simultanément. Il faut donc un compromis adapté à chaque situation.

### Les familles de codes modernes.

Les principales familles de codes modernes sont

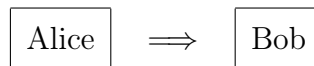
- ◆ Les codes par flot (registres à décalage).
- ◆ Les codes par blocs
  1. Les codes symétriques (ou à clé secrète).
  2. Les codes asymétriques (ou à clé publique).

Les codes à clef publique sont basés sur la notion de fonction à sens unique qui sera définie au chapitre (3.2.1) pag 37.

## 2.1 Cryptographie Symétrique

Dans la cryptographie symétrique avant d'émettre un message les deux communicants (émetteur - récepteur ) se mettent d'accord sur une même clé  $k \in K$  (l'espace des clés )**[5]**. Il existe deux grandes familles de systèmes modernes à clé secrète : les chiffrements à flots (chiffre le message bit à bit), en particulier ceux basés sur des registres à décalage, et les chiffrements par blocs (le message est découpé en blocs de taille fixe et chiffré bloc par bloc). Il existe essentiellement deux structures de chiffrement itératif par blocs

- ◆ Réseau de substitution-permutation ou réseau SP, par exemple AES (Advanced Encryption Standard).
- ◆ Schéma de Feistel, par exemple DES (Data Encryption Standard).



### 2.1.1 Protocole

Le protocole d'échange de communication (série d'étapes pour accomplir l'échange de message d'un manière sûre )

Alice et Bob veulent communiquer un message  $m$ .

1. Alice et Bob se mettent d'accord sur une règle pour chiffrer le message  $m$  (règle = méthode de cryptage ).
2. Alice chiffre le message  $m$ , avec la méthode de cryptage c'est à dire  $E_k(m) = c$ .
3. Alice envoie le message crypté  $c$  vers Bob.
4. Bob décrypte le message reçu  $c$  avec la règle de déchiffrement  $D_k$  , c'est à dire  $D_k(c) = D_k(E_k(m)) = m$ .

Avant d'émettre un message Alice et Bob se mettent d'accord sur une même clé  $k \in K$ . Voir la fig (2.3) suivant

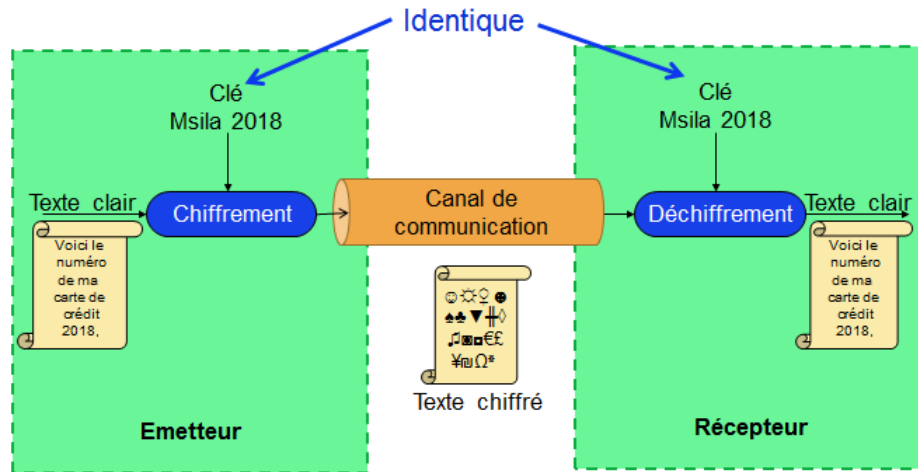


FIGURE 2.3 – Cryptage symétrique

## 2.2 Systèmes cryptographiques de clé secrète

### 2.2.1 Chiffrement par décalage

Identifions l'alphabet usuel avec  $Z_{26}$ , c'est à dire

A	B	C	D	E	F	..	..	..	Y	Z
0	1	2	3	4	5	..	..	..	24	25

On a :  $m = a_1a_2...a_n$ . On remplace chaque lettre  $a_i \in \{a, b, ..., y, z\}$  par le nombre correspondant  $m_i \in \{0, 1, ..., 24, 25\}$  et  $m' = m_1, m_2, ..., m_n$ .

On chiffre chaque nombre  $m_i$  par la règle de chiffrement .

$c = c_1, c_2, ..., c_n$  , telle que  $c_i = e_k(m_i)$  [5].

**Cryptosystème :** Chiffrement par décalage

Soit  $P = C = K = Z_{26}$ , pour une clé  $k$ ,  $0 \leq k \leq 25$  et soit  $k \in Z_{26}$ , nous définissons chiffrement par décalage

$$e_k(x) = (x + k) \bmod 26,$$

et déchiffrement par décalage

$$d_k(x) = (y - k) \bmod 26.$$

$$\forall x, y \in Z_{26}.$$

**Exemple**

Supposant que la clé pour le chiffrement par décalage est  $k = 11$

$$e_{11}(x) = x + 11 \bmod 26$$

$$d_{11}(y) = y - 11 \bmod 26.$$

Soit le texte clair suivant

<b>Texte clair</b>	<i>We wille meet at mid night</i>
--------------------	-----------------------------------

En premier lieu on transforme le texte en 11 nombre

w	e	w	i	l	l	e	m	e	e	t	a	t	m	i	d	n	i	g	h	t
22	4	22	8	11	11	4	12	4	4	19	0	19	12	8	3	13	8	6	7	19

Après on ajoute 11 à chaque nombre et on réduisant modulo 26, on obtient

7	15	7	19	22	22	15	23	15	15	14	11	4	23	19	14	24	19	17	18	4
h	p	h	t	w	w	p	x	p	p	e	l	e	x	t	o	y	t	r	e	s

Finalement on convertit l'ensemble sous forme de texte

<b>Texte chiffré</b>	<i>hp htwpp xppe le xto ytrse</i>
----------------------	-----------------------------------

### 2.2.2 Chiffrement par substitution

Un autre cryptosystème bien connu est le chiffrement par substitution que nous définissons maintenant. Ce système de cryptographie a été utilisé pendant des centaines d'années. Les Puzzle dans les journaux sont des exemples de chiffrement par substitution [12].

**Cryptosystème :** Chiffrement par substitution

Soit  $P = C = Z_{26}^m$ . L'ensemble des clés  $K$  est constitué de toutes les permutations possibles des 26 symboles  $1, \dots, 25$ . Pour chaque permutation  $\pi \in k$ , nous définissons

$$e_{\pi}(x) = \pi(x),$$

et

$$d_{\pi} = \pi^{-1}(y).$$

Où  $\pi^{-1}$  est la permutation inverse de  $\pi$ .

En fait, dans le cas du substitut, nous pourrions tout aussi bien prendre l'alphabet anglais de 26 lettres. Nous avons utilisé le chiffre de chiffrement car le chiffrement et le décryptage étaient des opérations algébriques. Mais dans le chapitre substitution, il est plus commode de considérer le cryptage et le décryptage comme des permutations de caractères alphabétiques. Voici un exemple de permutation "aléatoire", m, qui pourrait comprendre une fonction de cryptage. (Comme précédemment, les caractères en texte brut sont écrits en majuscules.)

a	b	c	d	e	f	g	h	i	j	k	l	m
X	N	Y	A	H	P	O	G	Z	Q	W	B	T

n	o	p	q	r	s	t	u	v	w	x	y	z
S	F	L	R	C	V	M	U	E	K	J	D	I

Ainsi,  $e_{\pi}(a) = X$ ,  $e_{\pi}(b) = N$ ,... etc. La fonction de décryptage est la permutation inverse. Ceci est formé en écrivant d'abord les deuxièmes lignes, puis en les triant par ordre alphabétique. Ce qui suit est obtenu :

A	B	C	D	E	F	G	H	I	J	K	L	M
d	l	r	y	v	o	h	e	z	x	w	p	t



N	O	P	Q	R	S	T	U	V	W	X	Y	Z
b	g	f	j	q	n	m	u	s	k	a	c	i

D'où,  $d_\pi(A) = d$ ,  $d_\pi(B) = l, \dots$  etc.

Une clé pour le chiffrement de substitution consiste simplement en une permutation de l'alphabet 26 caractères. Le nombre de permutations possibles est  $26! \approx 4.0 \times 10^{26}$ . Ainsi, la recherche exhaustive de clé est très difficile même avec un ordinateur. Cependant, nous verrons plus tard qu'un cryptogramme de substitution peut être cryptanalyse facilement par d'autres méthodes.

### 2.2.3 Chiffrement par permutation

Tous les cryptosystèmes dont nous avons parlé jusqu'ici impliquent une substitution : les caractères en clair sont remplacés par des caractères de texte chiffré différents. L'idée d'un chiffrement par permutation est de garder les caractères en clair, mais les positions en les réarrangeant en utilisant une permutation.

Une permutation d'un ensemble fini  $X$  est une fonction bijective  $\pi : X \mapsto X$ . En d'autres termes, la fonction  $\pi$  est un-à-un (injective) et (surjective). Il s'ensuit que, pour tout  $x \in X$  il y a un unique élément  $x' \in X$  tel que  $\pi(x') = x$ . Ceci nous permet de définir la permutation inverse,  $\pi^{-1} : X \mapsto X$  par la règle

$$\pi^{-1}(x) = x' \text{ si et seulement si } \pi(x') = x.$$

Alors  $\pi^{-1}$  est aussi une permutation de  $X$ .

Le chiffrement de permutation également connu sous le nom de transposition défini formellement sous le nom de cryptosystème suivant. Ce cryptosystème a été utilisé pendant des centaines d'années, en particulier en 1563 par Giovanni Porta.

Comme pour le chiffrement par substitution, il est plus pratique d'utiliser des caractères alphabétiques plutôt que des résidus modulo 26, car il n'y a pas d'opérations algébriques en cryptage ou décryptage ( voir [12][5]).

**Cryptosystème :** Chiffrement par permutation

Soit  $m$  est un entier positive. Soit  $P = C = Z_{26}^m$  et soit  $k$  constitué de toutes les permutations de  $\{1, \dots, m\}$ . Pour une clé (c'est-à-dire une permutation  $\pi$ ), nous définissons

$$e_{\pi}(x_1, \dots, x_m) = (x_{\pi(1)}, \dots, x_{\pi(m)}),$$

et

$$d_{\pi}(y_1, \dots, y_m) = (y_{\pi^{-1}(1)}, \dots, y_{\pi^{-1}(m)}).$$

Où  $\pi^{-1}$  est la permutation inverse de  $\pi$ .

Voici un exemple d'illustration

**Exemple**

Supposons que  $m = 6$  et la clé est la permutation suivant  $\pi$

x	1	2	3	4	5	6
$\pi(x)$	3	5	1	6	4	2

Notez que la première rangée du diagramme ci-dessus liste les valeurs de  $x$ ,  $1 \leq x \leq 6$ , et la deuxième ligne liste les valeurs correspondants de  $\pi(x)$ . Alors la permutation inverse  $\pi^{-1}$  peut être construit en inter changeant les deux rangs, et réarrangeant les colonnes de sorte que la première rangée soit dans un ordre croissant. En effectuant ces opérations, nous voyons que la permutation suivant

x	1	2	3	4	5	6
$\pi^{-1}(x)$	3	6	1	5	2	4

Maintenant, supposons qu'on nous donne le texte clair

*shesellsseashellsbytheseashore.*

Nous partitionnons d'abord le texte en groupes de six lettres

*shesel | lsseas | hellsb | ythese | ashore.*

Maintenant, chaque groupe de six lettres est réarrangé selon la permutation  $\pi$ , ce qui donne ce qui suit

$$EESLSH \mid SALSES \mid LSHBEL \mid HSYEET \mid HRAEOS.$$

Ainsi, le texte chiffré est

$$EESLSHSALSESLSHBELHSYEETHRAEOS.$$

Le texte chiffré peut être déchiffré de la même manière, en utilisant la permutation inverse  $\pi^{-1}$ .

### 2.2.4 Chiffrement affine

Le chiffrement par décalage est un cas particulier du chiffrement par substitution dans lequel on utilise une translation comme substitution. Un autre cas particulier du chiffrement par substitution est le chiffrement affine. Dans ce procédé, on limite les fonctions de chiffrement à certaines fonctions de la forme

$$E_{(a,b)}(x) = ax + b \mod 26, \quad (2.1)$$

où  $a, b \in \mathbb{Z}_{26}$ . Ces fonctions sont appelées des fonctions affines, d'où l'on a tiré le nom du procédé. On remarque que l'on retrouve le chiffrement par décalage pour  $a = 1$ .

Pour que l'opération de déchiffrement soit possible, il est nécessaire que la fonction affine soit bijective. Autrement dit, pour tout  $y \in \mathbb{Z}_{26}$ , l'équation

$$ax + b = y \mod 26 \quad (2.2)$$

doit avoir une, et une seule, solution  $x$ . L'équation (2.2) est équivalente à

$$ax = y - b \mod 26. \quad (2.3)$$

Lorsque  $y$  parcourt l'ensemble  $\mathbb{Z}_{26}$ ,  $y - b$  décrit également ce même ensemble. Donc, il suffit d'étudier l'équation  $ax = z \mod 26$  pour tout  $x \in \mathbb{Z}_{26}$ . On démontre que cette équation admet une unique solution pour tout  $z$  fixé, si et seulement si,  $\text{pgcd}(a, 26) = 1$  (où  $\text{pgcd}$  est le plus grand diviseur commun de ses arguments), au passage on dit que  $a$  et  $26$  sont premiers entre eux. En effet si  $a$  et  $26$  sont premiers entre eux (et seulement dans ce cas), alors  $a$  admet un inverse  $a^{-1} \in \mathbb{Z}_{26}$  (c'est à dire  $aa^{-1} = a^{-1}a = 1 \mod 26$ ), et l'unique solution de l'équation  $ax = z \mod 26$  est  $x = a^{-1}z \mod 26$ . En particulier,  $x = a^{-1}(y - b) \mod 26$  est

l'unique solution a l'équation (2.2) .

Supposons donc que  $a$  et  $26$  sont premiers entre eux. On vient de voir que, dans ce cas, l'application  $E_{(a,b)}$  est inversible. Sa bijection réciproque est donnée par

$$D_{(a,b)} = a^{-1}(y - b) \bmod 26. \text{ (Voir [1][12])}$$

Les ensembles de textes clairs  $P$  et chiffrés  $C$  sont tous les deux égaux à  $Z_{26}$ . L'espace des clefs secrètes  $K$  est quant à lui donné comme le cryptosystème suivant

**Cryptosystème : Chiffrement Affin.**

Soit  $P = C = Z_{26}$ , et soit

$$K = \{(a, b) \in Z_{26} \times Z_{26} : \text{pgcd}(a, 26) = 1\}. \quad (2.4)$$

Pour tout  $(a, b) \in K$ , on définit

$$E_{(a,b)}(x) = ax + b \bmod 26, \quad (2.5)$$

et

$$D_{(a,b)}(x) = a^{-1}(y - b) \bmod 26. \quad (2.6)$$

### Exemple

Supposons que  $k = (7, 3)$ . Comme noté ci-dessus,  $7^{-1} \bmod 26 = 15$ . La fonction de chiffrement est

$$e_k(x) = 7x + 3,$$

et la fonction de décryptage correspondant est

$$d_k(y) = 15(y - 3) = 15y - 19,$$

où toutes les opérations sont effectuées dans  $Z_{26}$ . C'est une bonne vérification pour vérifier  $d_k(e_k(x)) = x$ , pour tout  $x \in Z_{26}$ . Calcul en  $Z_{26}$ , nous obtenir

$$\begin{aligned}
 d_k(e_k(x)) &= d_k(7x + 3) \\
 &= 15(7x + 3) - 19 \\
 &= x + 49 - 19 \\
 &= x.
 \end{aligned}$$

Pour illustrer, chiffons le texte clair *hot*. Nous convertissons d'abord les lettres h, o, t, en résidus modulo 26. Ce sont respectivement 7, 14 et 19. Maintenant, nous cryptons

$$(7 \times 7 + 3) \bmod 26 = 52 \bmod 26 = 0$$

$$(7 \times 14 + 3) \bmod 26 = 101 \bmod 26 = 23$$

$$(7 \times 19 + 3) \bmod 26 = 136 \bmod 26 = 6.$$

Donc, les trois caractères chiffrés sont 0, 23 et 6, ce qui correspond à la chaîne alphabétique *AXG*.

### 2.2.5 Chiffrement vigenère

Dans le chiffre de décalage et le chiffre de substitution, une fois qu'une clé est choisie, chaque caractère alphabétique est associé à un caractère alphabétique unique. Pour cette raison, ces cryptosystèmes sont appelés cryptosystèmes monoalphabétiques. Nous présentons maintenant un cryptosystème qui n'est pas monoalphabétique, le fameux chiffrement de Vigenère comme cryptosystème suivant. Ce chiffre est nommé d'après Blaise de Vigenère, qui a vécu au XVI<sup>e</sup> siècle. En utilisant la correspondance  $A \longleftrightarrow 0$ ,  $B \longleftrightarrow 1, \dots, Z \longleftrightarrow 25$  décrite précédemment, on peut associer chaque clé  $K$  à une chaîne alphabétique de longueur  $m$ , appelé un mot-clé. Le chiffrement Vigenère crypte  $m$  caractères alphabétiques à la fois : chaque élément en clair est équivalent à  $m$  caractères alphabétiques [1][12][5]).

**Le cryptosystème : Chiffrement Vigenère**

Soit  $m$  un entier positif. On définissons par  $P = C = K = (Z_{26})^m$   
pour

$$K = (k_1, k_2, \dots, k_m) = (Z_{26})^m,$$

alors

$$e_k = (x_1, x_2, \dots, x_m) = (x_1 + k_1, x_2 + k_2, \dots, x_m + k_m),$$

et

$$d_k(y_1, y_2, \dots, y_m) = (x_1 - k_1, x_2 - k_2, \dots, x_m - k_m).$$

Où toutes les opération sont effectuées modulo  $Z_{26}$ .

**Exemple**

Supposons que  $m = 6$  et la clé est " CIPHER "

tel que  $K = (2, 8, 15, 7, 4, 17)$

et soit le texte clair :

**THIS CRYPTO SYSTEM IS NOT SECURE.**

Nous convertissons les élément en texte brut en résidus modulo 26, les écrivons en groupes de six puis " ajoutons " la clé modulo 26, comme suit

19	7	8	18	2	17	24	15	19	14	18	24
2	8	15	7	4	17	2	8	15	7	4	17
21	15	23	25	6	8	0	23	8	21	22	15
18	19	4	12	8	18	13	14	19	18	4	2
2	8	15	7	4	17	2	8	15	7	4	17
20	1	19	19	12	9	15	22	8	25	8	19
20	17	4									
2	8	15									
22	25	19									

L'équivalent alphabétique de texte chiffré

*VPXZGIA XIVWPUBTTMJPWIZITWZT.*

Pour déchiffrer, nous pouvons utiliser le même clé, mais nous le soustrairions au modulo 26 du texte chiffré, au lieu de l'ajouter.

Observons que le nombre de clés possibles de longueur  $m$  dans un chiffre de **Vigenère** est  $26^m$ . Donc même pour des valeurs relativement faibles de  $m$ . Une recherche de clé exhaustive demanderait beaucoup de temps. Par exemple, si nous prenons  $m = 5$ , l'espace de clé a une taille supérieure à  $1.1 \times 10^7$ . Ceci est déjà suffisamment important pour empêcher exhaustive de la clé à la main ( mais pas par ordinateur).

Dans un chiffrement Vigenère ayant une longueur de clé  $m$ , un caractère alphabétique peut être mappé à l'un des  $m$  caractères alphabétiques possibles (en supposant que la clé contient  $m$  caractères distincts). Un système de cryptographie est appelé un système cryptographique polyalphabétique. En général, la cryptanalyse est plus difficile pour les cryptosystèmes polyalphabétiques que pour les cryptosystèmes monoalphabétiques [14].

### 2.2.6 Chiffrement Hill

Dans cette section, nous décrivons un autre système de cryptage polyalphabétique appelé **chiffrement de Hill**. Ce chiffre a été inventé en 1929 par Lester S. Hill. Soit  $m$  un entier positif, et définissons  $P = C = (\mathbb{Z}_{26})^m$ . L'idée est de prendre  $m$  combinaisons linéaires des  $m$  caractère alphabétique dans un élément de texte clair, produisant ainsi les  $m$  caractères alphabétiques dans un élément de texte chiffré (Voir [1][12][5]).

**Cryptosystème : Chiffrement Hill**

Soit  $m \geq 2$  un entier. Soit  $P = C = (Z_{26})^m$  et soit

$$K = \{m \times m \text{ matrice inversibles sur } Z_{26}\}.$$

Pour une clé  $K$  on définit

$$e_K(x) = xK,$$

et

$$d_K(y) = yK^{-1}.$$

Où toutes les opérations sont effectuées dans  $Z_{26}$ .

Par exemple,  $m = 2$ , nous pourrions écrire un élément en texte clair comme  $x = (x_1, x_2)$  et l'élément de texte chiffré comme  $y = (y_1, y_2)$ . Ici,  $y_1$  serait une combinaison linéaire de  $x_1$  et  $x_2$ , tout comme  $y_2$ . Nous pourrions prendre :

$$y_1 = (11x_1 + 3x_2) \text{ mod } 26$$

$$y_2 = (8x_1 + 7x_2) \text{ mod } 26.$$

Bien sûr, ceci peut être écrit plus succinctement comme suit

$$(y_1, y_2) = (x_1, x_2) \begin{pmatrix} 11 & 3 \\ 8 & 7 \end{pmatrix}.$$

Où toutes les opérations sont effectuées en  $Z_{26}$ . En général, nous prendrons  $m \times m$  une matrice  $K$  comme notre clé. Si l'entrée dans la rangée  $i$  et la colonne  $j$  de  $k$  est  $k_{i,j}$ , alors nous écrivons  $K = k_{i,j}$ . Pour  $x = (x_1, x_2, \dots, x_m) \in P$  et  $k \in K$ , nous calculons  $y = e_k(x) = (y_1, y_2, \dots, y_m)$  comme suit :

$$(y_1, y_2, \dots, y_m) = (x_1, x_2, \dots, x_m) \begin{pmatrix} k_{1,1} & k_{1,2} & \dots & k_{1,m} \\ k_{2,1} & k_{2,2} & \dots & k_{2,m} \\ \vdots & \vdots & & \vdots \\ k_{m,1} & k_{m,2} & \dots & k_{m,m} \end{pmatrix}.$$

Autrement dit, en utilisant la notation matricielle,  $y = xk$ .

Nous disons que le texte chiffré est obtenu à partir du texte clair au moyen d'un transforma-



tion linéaire. Nous devons considérer comment le décryptage fonctionnera, c'est-à-dire, comment peut-on calculer à partir de  $y$ . Les lecteurs familiers avec l'algèbre linéaire se rendront compte que nous utiliserons la matrice inverse  $k^{-1}$  pour déchiffrer. Le texte chiffré est décrypté à l'aide de l'équation matricielle  $x = yk^{-1}$ .

Voici les définitions des concepts nécessaires à partir de l'algèbre linéaire. Si  $A = (a_{i,j})$  est une matrice  $l \times n$  et  $B = (b_{i,k})$  est une matrice  $m \times n$ , alors nous définissons le produit matriciel  $AB = (c_{i,k})$  par la formule

$$c_{i,k} = \sum_{j=1}^m a_{i,j}b_{j,k}$$

Pour  $1 \leq i \leq l$  et  $1 \leq k \leq n$ . C'est-à-dire que l'entrée dans la rangée  $i$  et la colonne  $k$  de  $AB$  est formée en prenant la  $i$ ème rangée de  $A$  et la  $k$ ème colonne de  $B$ , en multipliant les entrées correspondantes ensemble, et en sommant. Notez que  $AB$  est une matrice  $l \times n$ . La multiplication matricielle est associative (c'est-à-dire  $(AB)C = A(BC)$ ) mais pas, en général, commutative (ce n'est pas toujours le cas  $AB = BA$ , même pour les matrices carrées  $A$  et  $B$ ).

La matrice d'identité de  $m \times m$ , notée  $I_m$ , est la matrice de  $m \times m$  avec les 1 sur la diagonale principale et des 0 ailleurs. Ainsi,  $2 \times 2$  la matrice d'identité est

$$I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

$I_m$  est appelée matrice d'identité puisque  $AI_m = A$  pour toute matrice  $A$ ,  $l \times m$  et  $I_m B = B$  pour toute matrice  $B$ ,  $m \times n$ . Maintenant, la matrice inverse d'une matrice  $m \times m$   $A$  (si elle existe) est la matrice  $A^{-1}$  telle que  $AA^{-1} = A^{-1}A = I_m$ . Toutes les matrices n'ont pas d'inverses, mais si un inverse existe, il est unique. Avec ces faits à portée de main, il est facile de déduire la formule de déchiffrement donnée ci-dessus, en supposant que  $K$  a une matrice inverse  $K^{-1}$ . puisque  $y = xK$ . nous pouvons multiplier les deux côtés de la formule par  $K^{-1}$ , en obtenant

$$yK^{-1} = (xK)K^{-1} = x(KK^{-1}) = xI_m = x.$$

(Notez l'utilisation de la propriété d'associativité).

Nous pouvons vérifier que l'exemple de matrice de chiffrement défini ci-dessus a un inverse

dans  $Z_{26}$

$$\begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}^{-1} = \begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix}$$

puisque

$$\begin{aligned} \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix} \begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix} &= \begin{pmatrix} 11 \times 7 + 8 \times 23 & 11 \times 18 + 8 \times 11 \\ 3 \times 7 + 7 \times 23 & 3 \times 18 + 7 \times 11 \end{pmatrix} \\ &= \begin{pmatrix} 261 & 286 \\ 182 & 131 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \end{aligned}$$

(Rappelons-vous que toutes les opérations arithmétiques sont effectuées modulo 26).

Faisons maintenant un exemple pour illustrer le cryptage et décryptage dans le code de Hill.

### Exemple

Supposons que la clé est

$$K = \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}$$

à partir des calculs ci-dessus, nous avons cela

$$K^{-1} = \begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix}.$$

Supposons que nous voulons crypter le texte clair `july`. Nous deux élément de texte clair à chiffrer : (9,20)(correspondant à `ju`) et (11,24)(correspondant à `ly`). Nous calculons comme suit

$$(9, 20) \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix} = (99 + 60, 72 + 140) = (3, 4),$$

et

$$(11, 24) \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix} = (121 + 72, 88 + 168) = (11, 22).$$

Par conséquent, le cryptage de `"july"` est `"DELW"`. Pour décrypter, Bob calculerait

$$(3, 4) \begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix} = (9, 20).$$

et

$$(11, 22) \begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix} = (11, 24).$$

Par conséquent, le texte clair correct est obtenu ensuite, les codes symétriques ou à clefs secrètes aussi les types suivant

type DES (**D**ata **E**ncryption **V**standard), IDEA (**I**nternational **D**igital **E**ncryption **A**lgorithm), AES ( **A**dvanced **E**ncryption **S**tandard) ont été créés pour couvrir ces besoins.

---

---

## Chapitre 3

---

### CRYPTOSYSTÈME ASYMÉTRIQUE

Diffie et Hellman ont dégagé vers **1976** la notion de **code à clef publique** ou code asymétrique fondé sur la notion de fonction à sens unique.

Les codes asymétriques les plus utilisés

- **RSA** basé sur la difficulté calculatoire de la factorisation des grands entiers.
- **El Gamal** basé sur la difficulté calculatoire de calculer le logarithme discret dans un corps fini.
- **Menezes-Vanstone** basés sur le logarithme associé au groupe des points d'une courbe elliptique sur un corps fini. C'est une modification d'autres cryptosystèmes, comme El Gamal. Sa sureté peut être mieux analysée. La longueur de sa clé est bien inférieure à celle des systèmes RSA et El Gamal pour une sureté équivalente. Ils offrent des fonctionnalités supplémentaires comme la possibilité de monter un cryptosystème basée sur l'identité.

Il existe d'autres codes asymétriques peu utilisés en pratique comme

- **McEliece** basé sur la théorie algébrique des codes correcteurs d'erreurs. Il repose sur la difficulté calculatoire du décodage d'un code linéaire (problème NP complet).

Considéré comme sûr il nécessite des clefs extrêmement longues 1019 bits.

— **Chor-Rivest** basé sur une instance du problème du sac-à-dos.

## 3.1 Protocole

Le protocole est simple

1. Alice chiffre le document d'une part avec sa clé privée, signant ainsi le document, et d'autre part avec la clé publique de Bob.
2. Alice envoie les deux documents à Bob.
3. Bob déchiffre le premier document avec la clé publique d'Alice et le second avec sa clé privée. Si les deux sont identiques il est sûr qu'Alice est l'expéditeur ( voir fig(3.1)).

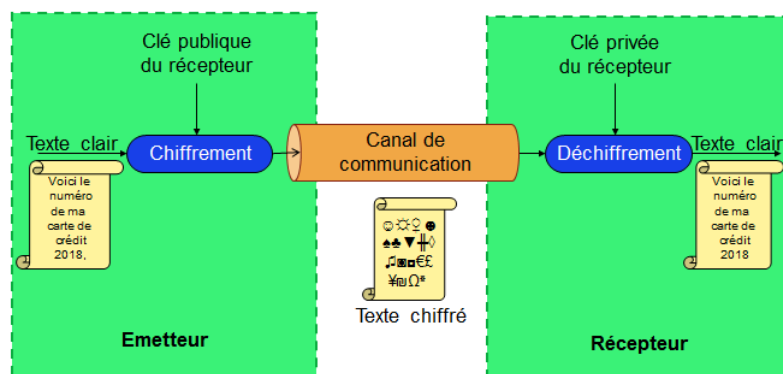


FIGURE 3.1 – Cryptage asymétrique

## 3.2 Principe des codes à clef publique.

### 3.2.1 Fonction sens unique

On cherche une fonction  $f$  entre des ensembles  $P$  et  $E$  telle que

Il existe bien d'autres situations mathématiques asymétriques : les fonctions à sens unique.

En d'autres termes, étant donnée une fonction  $f$ , il est possible connaissant  $x \in P$  de calculer « facilement »  $y = f(x)$  pour  $y \in E$  ; mais connaissant un élément de l'ensemble image de  $f$ ,

il est « difficile » ou impossible de trouver son antécédent. Dans le cadre de la cryptographie, posséder une fonction à sens unique qui joue le rôle de chiffrement n'a que peu de sens. En effet, il est indispensable de trouver un moyen efficace afin de pouvoir déchiffrer les messages chiffrés. On parle alors de fonction à sens unique avec trappe secrète.

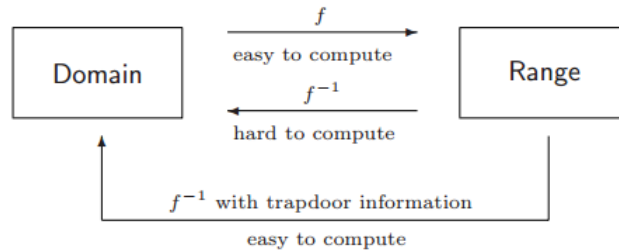


FIGURE 3.2 – Fonction sens unique

Autrement dit on cherche des fonction  $f : P \mapsto E$  appartenant à la classe des problèmes **P** (calculables en temps polynomial en fonction de la taille des données) et telle que la fonction réciproque (ou l'image réciproque si ne suppose pas  $f$  bijective)  $f^{-1}$  appartienne à la classe des problèmes **NP**, (non calculables en temps polynomial en fonction de la taille des données, mais vérifiables en temps polynomial).

Prenons par exemple le cas de la fonction  $f$  suivante

$$f : x \mapsto x^3 \bmod 100$$

- ◆ Connaissant  $x$ , trouver  $y = f(x)$  est facile, cela nécessite deux multiplications et deux divisions.
- ◆ Connaissant  $y$  image par  $f$  d'un élément  $x(y = f(x))$ , retrouver  $x$  est difficile.  
Tentons de résoudre le problème suivant : trouver  $x$  tel que  $x^3 \equiv 11 \pmod{100}$ .  
On peut pour cela
- ◆ Soit faire une recherche exhaustive, c'est-à-dire essayer successivement  $1, 2, 3, \dots, 99$ , on trouve alors

$$71^3 = 357911 \equiv 11 \pmod{100},$$

◆ Soit utiliser la trappe secrète :  $y \mapsto y^7 \pmod{100}$  qui fournit directement le résultat !

$$11^7 = 19487171 \equiv 71 \pmod{100}.$$

La morale est la suivante : le problème est dur à résoudre, sauf pour ceux qui connaissent la trappe secrète. (Attention, dans le cas de cet exemple, la fonction  $f$  n'est pas bijective).

La mise au point de telles fonctions a révolutionné la cryptographie et élargi son champ d'application (voir [4]).

### 3.3 Le cryptosystème Merkle-Hellman.

Ce cryptosystème qui fut historiquement un des premiers proposés (il a été publié en 1978) repose sur le problème du sac-à-dos. Génériquement il a une sécurité prouvée, car le problème du sac-à-dos est génériquement dans la classe NP (fig (3.3)). Malheureusement comme l'a montré Shamir sa sécurité ne repose pas sur un problème de sac-à-dos générique mais sur une instance particulière de ce problème qui elle peut ne pas être dans la classe NP [4][14].

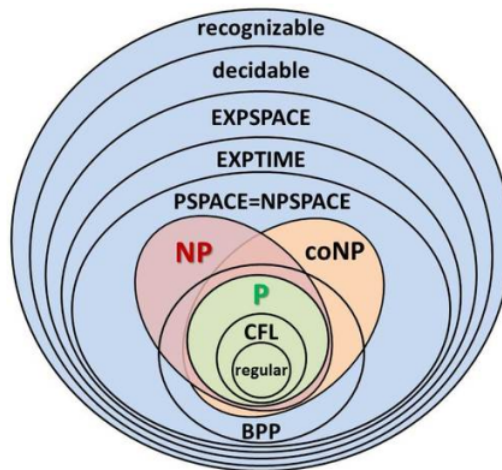


FIGURE 3.3 – La classe NP

### 3.3.1 Problème sac à dos

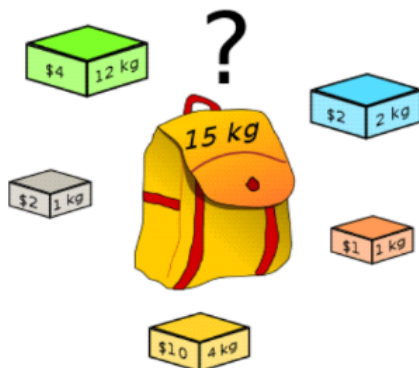


FIGURE 3.4 – Le problème du sac à dos : quelles boites choisir afin de maximiser la somme emportée tout en ne dépassant pas les 15 kg autorisés ?

Le problème du **sac-à-dos** s'énonce de la manière suivante

1. Soit  $a$  un ensemble d'entiers  $\{a_1, a_2, \dots, a_n; t\}$ .
2. Existe-t-il un sous-ensemble de  $\{a_1, a_2, \dots, a_n\}$  dont la somme soit  $t$

Intuitivement on peut considérer que les  $a_i$  représentent la taille de paquets que l'on veut mettre dans un **sac-à-dos** de taille  $t$ , ou encore qu'ils représentent des billets et des pièces monnaies destinées à payer un objet dont le prix est  $t$ .

L'intérêt de ce problème du **sac-à-dos** pour la cryptographie tient au théorème suivant

**Théorème 3.1.** (Karp 1972). *Le problème du calcul de la solution, supposée exister, du **sac-à-dos** est un problème génériquement NP-complet [4].*

Pour la définition de NP-complet ( voir [4]).

De manière un peu approximative ce théorème signifie que génériquement trouver une solution, que l'on sait exister, au problème du **sac-à-dos** est difficile c'est à dire que le calcul de la solution nécessite un temps exponentiel en fonction de la taille des données. Le mot générique signifie qu'il existe au moins un ensemble  $a$  ayant une solution tel que le calcul de la solution ne se fasse pas en temps polynomial en fonction de la taille des données.

Le problème est de cacher une clef secrète, une porte dérobée, ou trapdoor qui permette au



destinataire du message de le décoder.

On choisit un entier  $M$  on dira que  $a = \{a_1, a_2, \dots, a_n; t\}$  est un problème de sac-à-dos modulo  $M$  s'il existe

$$\{a_{k_1}, a_{k_2}, \dots, a_{k_m}\} \subset \{a_1, a_2, \dots, a_n; t\}.$$

tel que

$$a_{k_1}, a_{k_2}, \dots, a_{k_m} \equiv t \text{ mod } M$$

[4].

### 3.3.2 Description du cryptosystème Merkle-Hellman.

L'idée principale de Merkle et Hellman consiste à choisir un **sac-à-dos** particulier dont la solution est triviale et à cacher cette forme particulière du **sac-à-dos** par une transformation secrète connue du seul destinataire du message.

La forme retenue par Merkle et Hellman est le **sac-à-dos** super-croissant (super-increasing knapsack). Une suite d'entier  $\{b_1, b_2, \dots, b_n, b_{n+1}\}$  est dite super-croissante si l'on a

$$b_i > \sum_{j=1}^{i-1} b_j, \text{ pour } 1 \leq i \leq n+1$$

On remarque que si la suite  $\{b_1, b_2, \dots, b_n, b_{n+1}\}$  est super-croissante et si  $M = b_{n+1}$  alors tout problème de **sac-à-dos**  $\{b_1, b_2, \dots, b_n; t\}$  modulo  $M$  est équivalent au problème de **sac-à-dos**  $\{b_1, b_2, \dots, b_n; t\}$  sur les entiers naturels. Ce dernier est un problème facile. On remarque que  $b_n$  est dans le sous ensemble de la solution si et seulement si  $b_n \leq t$  et on peut alors ramener le problème initial au problème de **sac-à-dos**  $\{b_1, b_2, \dots, b_{n+1}, t'\}$  avec

$$t' = \begin{cases} t - b_n \\ \text{ou} \\ t \end{cases}.$$

La transformation secrète destinée à cacher le fait que l'on a un **sac-à-dos** super-croissant est simplement la multiplication par un nombre secret  $M$ . Le crypto-système de Merkle et Hellman est donc le suivant

1. Paramètre public  $n$ .

2. Fabrication de la clef : choisir une suite super croissante

$$\{b_1, b_2, \dots, b_{n+1} = M\}$$

choisir un nombre  $W \in \mathbb{Z}/M\mathbb{Z}$  et une permutation  $\Pi$  de  $\{1, \dots, n\}$ . Calculer  $a_i = Wb_{\Pi(i)} \pmod{M}$  pour  $1 \leq i \leq n$ .

3. Clef Publique :  $K_p = (a_1, a_2, \dots, a_n)$ .

4. Clé secrète :  $K_s = (b_1, b_2, \dots, b_n, M, W, \Pi)$ .

5. Message : une suite de zéros et de uns de longueur  $n, m = m_1 m_2 \dots m_n$ .

6. Codage :

$$c = \sum_{i=1}^n m_i a_i.$$

7. Décodage : calculer  $cW^{-1} \pmod{M}$ , résoudre le problème de **sac-à-dos** super-croissant  $x_1 b_1 + \dots + x_n b_n = cW^{-1} \pmod{M}$  et alors  $m_i = x_{\Pi(i)}$ .

Le cryptosystème **Merkle-Hellman** revient à trouver un vecteur dans un réseau. Un réseau (lattice) est l'ensemble des combinaisons à coefficients entiers relatifs de vecteurs de  $R_n$ . Trouver un petit vecteur au sens de la norme euclidienne est aussi un problème difficile. mais il y a des cas où ce problème devient facile. Plus précisément l'algorithme LLL peut être utilisé. En particulier il peut être utilisé pour casser des crypto-systèmes comme celui de **Merkle-Hellman**[4].

## 3.4 Échange de clés de Diffie-Hellman

### 3.4.1 Présentation

En cryptographie, l'échange de clés Diffie-Hellman, du nom de ses auteurs Whitfield Diffie et Martin Hellman (fig(3.5)), est une méthode, publiée en 1976, par laquelle deux agents, nommés par convention Alice et Bob, peuvent se mettre d'accord sur un nombre ( qu'ils peuvent utiliser comme clé pour chiffrer la conversation suivant ) sans qu'un troisième agent appelé Oscar puisse découvrir le nombre, même en ayant écouté tous leurs échanges[4].



FIGURE 3.5 – Whit Diffie et Martin E. Hellman

Dans cette section, nous décrivons le protocole de Diffie et Helman permettant d'échanger de clés secrètes sur des canaux qui ne sont pas sûrs. Par lui-même, ce protocole n'est pas un cryptosystème à clés publiques, mais il est à la base du système EL Gamal, qui sera décrit dans la prochaine section.

La sécurité du système d'échange de clés Diffie-Hellman ne pose pas sur le problème de la factorisation des entiers mais sur le problème du logarithme discret (le problème DL).

### 3.4.2 Logarithme Discret

Soit  $p$  un nombre premier. Nous savons que le groupe  $(\mathbb{Z}/p\mathbb{Z})^*$  est cyclique d'ordre  $p-1$  (voir corollaire (1.2) pag 13 ). Soit  $g$  une racine primitive mod  $p$  (définition (1.16) pag 13).

Alors pour tout entier  $A \in \{1, 2, \dots, p-1\}$  il existe un exposant  $a \in \{1, 2, \dots, p-1\}$  avec

$$A = g^a \bmod p.$$

Cet exposant s'appelle le logarithme discret de  $A$  dans la base  $g$ . Nous écrivons  $a = \log_g A$ . Le calcul du logarithme est considéré comme difficile parce qu'aucun algorithme efficace permettant de le retrouver n'est connu. À l'inverse, il n'existe pas de preuve que ce problème soit définitivement difficile [15].

### Exemple

Soit  $p = 13$ . Une racine primitive modulo 13 est 2. Le logarithme discret dans la base 2 de chaque entier de  $\{1, 2, \dots, 12\}$  est donné dans le tableau suivant

$A$	1	2	3	4	5	6	7	8	9	10	11	12
$\log_2 A$	0	1	4	2	9	5	11	3	8	10	7	6

#### 3.4.3 Description de l'algorithme

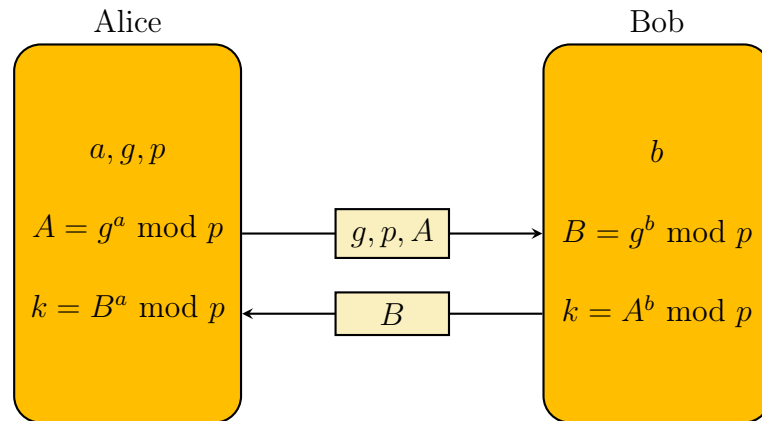


FIGURE 3.6 – Principe échange de clés Diffie-Hellman

Le protocole de Diffie-Hellman fonctionne de la façon suivante. Alice et Bob veulent se mettre d'accord sur une clé secrète commune, mais ils n'ont à disposition qu'un canal de communication qui n'est pas sûr. Pour commencer, ils se mettent d'accord sur un grand nombre premier  $p$  et un entier  $g$  avec  $2 \leq g \leq p-1$  choisi pour que l'ordre de  $g \bmod p$  soit suffisamment élevé.

Les nombre  $p$  et  $g$  peuvent être connus publiquement, ce qui fait que Bob et Alice peuvent utiliser leur canal de communication qui n'est pas sûr pour cet agrément.

- ◆ Maintenant Alice choisit un entier  $a \in \{0, 1, \dots, p-2\}$  au hasard, qu'elle garde secret. Elle calcule

$$A = g^a \text{ mod } p,$$

- ◆ et envoie le résultat  $A$  à Bob. Bob choisit un entier  $b \in \{0, 1, \dots, p-2\}$  au hasard. Il calcule

$$B = g^b \text{ mod } p$$

- ◆ et envoie le résultat à Alice. Il garde aussi son exposant  $b$  secret. Pour obtenir la clé secrète commune, Alice calcule

$$B^a \text{ mod } p = g^{ab} \text{ mod } p,$$

- ◆ et Bob calcule

$$A^b \text{ mod } p = g^{ab} \text{ mod } p.$$

- ◆ Leur clé commune est

$$k = g^{ab} \text{ mod } p.$$

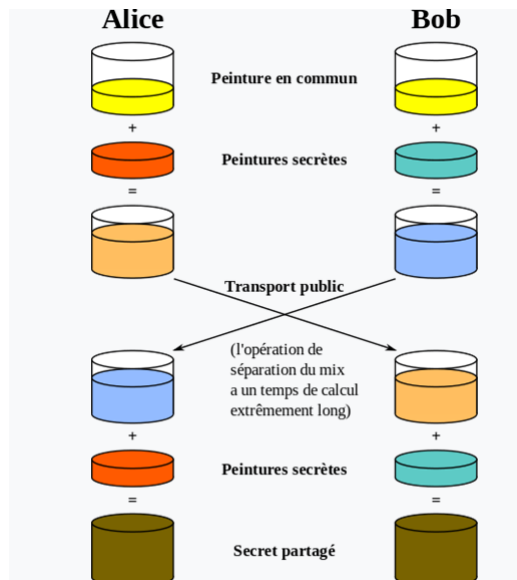


FIGURE 3.7 – Illustration conceptuelle d'un échange de clés Diffie-Hellman

## Exemple

1. Alice choisit un nombre premier  $p$  et une base  $g$ . Dans notre exemple,  $p = 23$  et  $g = 3$ .
2. Alice choisit un nombre secret  $a = 6$ .
3. Elle envoie à Bob la valeur  $A = g^a \bmod p = 36 \bmod 23 = 16$ .
4. Bob choisit à son tour un nombre secret  $b = 15$ .
5. Bob envoie à Alice la valeur  $B = g^b \bmod p = 315 \bmod 23 = 12$ .
6. Alice peut maintenant calculer la clé secrète :  $(B)^a \bmod p = 126 \bmod 23 = 9$ .
7. Bob fait de même et obtient la même clé qu'Alice :  $(A)^b \bmod p = 1615 \bmod 23 = 9$ .

Leur clé commune est 9.

## 3.5 L'algorithme à clé publique RSA

### 3.5.1 Présentation

Le système de cryptage RSA a été inventé en 1978 par Ronald Rivest, Adi Shamir, et Leonard Adleman. Ils avaient décidé de travailler ensemble pour établir qu'un nouveau système de codage révolutionnaire, dénommé " système à clé publique " que W.Diffie et M.Hellman venaient d'inventer, était une impossibilité logique (autrement dit, que tout système de cryptage de cette nature présentait des failles). Ils ne réussirent pas dans leur projet, mais, au contraire, découvrirent un nouveau système à clé publique qui supplanta vite celui de W.Diffie et M.Hellman. Il est fondé sur la difficulté de factoriser des grands nombres et **la fonction à sens unique** utilisée est la fonction puissance [4][3].

Il est basé sur la fonction à sens unique produit de deux entiers

$$f : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$$

$$(n, m) \longmapsto f(n, m) = n \times m$$

Le calcul du produit de deux nombres entiers est une opération " facile " et " rapide ", alors que la décomposition en facteurs premiers n'est pas " facile " et " lente ", En effet on montre que si les nombres entiers  $n$  et  $m$  s'écrivent avec  $k \leq \max\{\lceil \ln 2n \rceil, \lceil \ln 2m \rceil\}$  chiffres en base 2 alors le temps nécessaire pour calculer le produit  $m \times n$  est proportionnel à  $k^2$ [3][14]

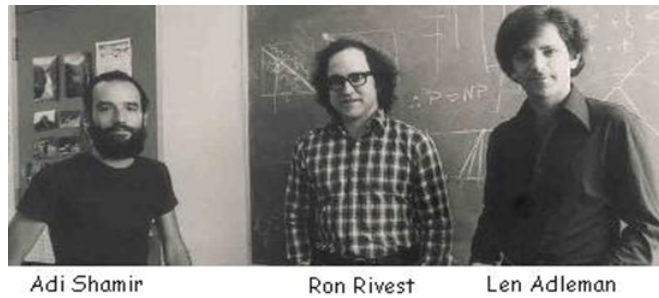


FIGURE 3.8 – Rivest, Shamir, Adleman - 1978

### 3.5.2 Description de l'algorithme

La clé secrète est constituée de deux grands nombres premiers  $p$  et  $q$ . La clé publique est constituée du produit  $n = pq$  et d'un entier  $e$  inversible modulo  $\varphi(n)$  (définition (1.14) pag 11).

Le chiffrement d'un message  $m$ , représenté par un entier  $c$  modulo  $n$ , se fait par la transformation suivante  $c \rightarrow m^e \bmod n$ .

Pour déchiffrer, il faut savoir calculer la fonction réciproque. voir le schéma suivant

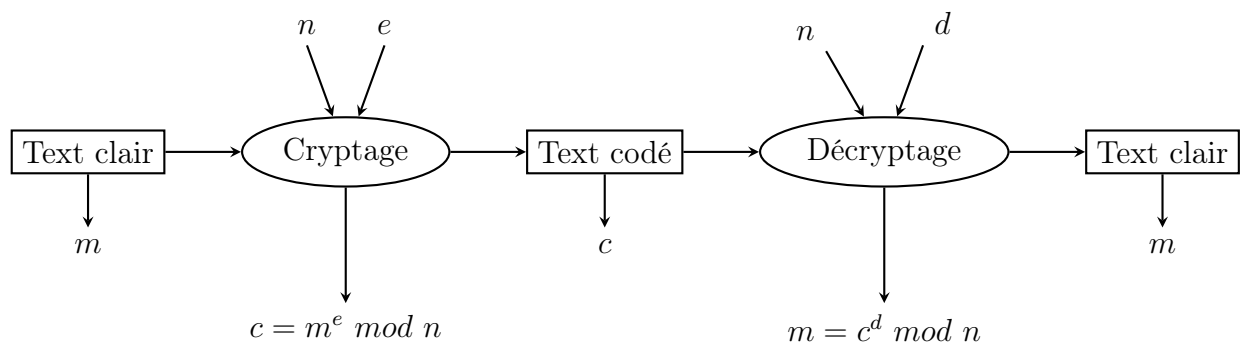


FIGURE 3.9 – Schéma de système RSA

### Génération des clés

Le RSA fonctionne à partir de deux nombres premiers, que l'on appellera  $p$  et  $q$ . Ces deux nombres doivent être très grand, car ils sont la clé de voûte de notre cryptage. Aujourd'hui, on utilise des clés de 128 à 1024 bits, ce qui représente des nombres décimaux allant de 38 à

308 chiffres (voir [10]). Les éléments d'information à transmettre, chiffres, lettres, etc., sont représentés par des entiers appartenant à un ensemble  $\{2, 3, \dots, C\}$ , où  $C$  est un entier positif (explication dans [13]).

Pour chaque utilisateur du cryptosystème RSA procède comme suit.

- ♦ Il choisit deux grands nombres premiers  $p$  et  $q$ . Il calcule le produit  $n = pq$  et l'indicatrice d'Euler  $\varphi(n) = (p-1)(q-1)$ .

Remarquons que l'on a toujours  $n > C$ .

- ♦ Il choisit un entier  $d > 1$  premier avec  $\varphi(n)$  et calcule son inverse  $e$  modulo  $\varphi(n)$ , que nous noterons  $d$ .

$$d \equiv e^{-1} \text{ mod } (p-1)(q-1).$$

- ♦ Il publie le couple  $(e, n)$  (**clé publique**), et conserve le couple  $(d, \varphi(n))$  (**clé secrète**).

## Cryptage

Si Alice veut crypter le message clair  $m$  et l'envoyer à Bob, elle prend connaissance de la clé publique  $(e, n)$  de ce dernier (dont la clé secrète est  $(d, \varphi(n))$ ), puis calcule l'entier. Pour crypter  $m$ , il suffit de le mettre à la puissance  $e$ .

$$c = m^e \text{ mod } n.$$

C'est le message crypté, qu'elle envoie à Bob.

## Décryptage

Pour décrypter, on utilise la même opération, mais en mettant à la puissance  $d$ .

$$m = c^d \text{ mod } n$$

et récupère  $m$  puisque

$$c^d = m^{ed} \text{ mod } n = m \text{ mod } n.$$

*Remarque 3.1.* Tout d'abord, il faut un message préalablement codé. On doit donc transformer en nombres le message d'origine, par exemple en utilisant la valeur ASCII (American Standard Code for Interchange) de chaque lettre ou en remplaçant chaque lettre par son rang dans l'alphabet.



### 3.5.3 Sécurité de système RSA

Une personne adverse Z a intercepté le message codé  $c$  et veut le décrypter. Elle sait aussi que le message est envoyé à B.

Elle essaie d'abord de calculer le nombre  $d$  de B (exposant de cryptage), connaissant le couple  $(n, e)$  de B.

Pour pouvoir déterminer  $d$  de B, on a besoin du résultat suivant

**Théorème 3.2.** *Les deux problèmes suivants*

1. *calculer le nombre  $d$ , connaissant le couple  $(n, e)$*
2. *factoriser  $n$  sont équivalents dans le sens où une solution de l'un conduit à une solution de l'autre (pour la preuve de théorème voir [3]).*

### 3.5.4 Avantages et Inconvénients

#### Avantages

Les cryptosystèmes à clé publique comme **RSA**, comparés à ceux à clé privée, peuvent être utilisés dans un mode signature. Pour cela, il suffit " d'inverser " le rôle des exposants  $e$  et  $d$ . Le détenteur de la clé secrète, c'est-à-dire de la factorisation de  $n$  ou de l'exposant secret  $d$ , peut signer un message  $m$  en prouvant qu'il détient  $d$ . Pour cela, il envoie en même temps que le message  $m$  la signature  $m^d$ . Pour vérifier l'authenticité de la signature, il suffit de l'élever à la puissance  $e$  (l'exposant public) et de vérifier que  $(m^d)^e = m$ .

#### Inconvénients

**RSA** et les schémas de chiffrement à clé publique en général étant significativement plus lents que les schémas symétriques, c'est-à-dire de chiffrement à clé privée, on ne les utilisera en pratique que pour le transport de clés secrètes ou pour le chiffrement de données de petite taille.

## Exemple

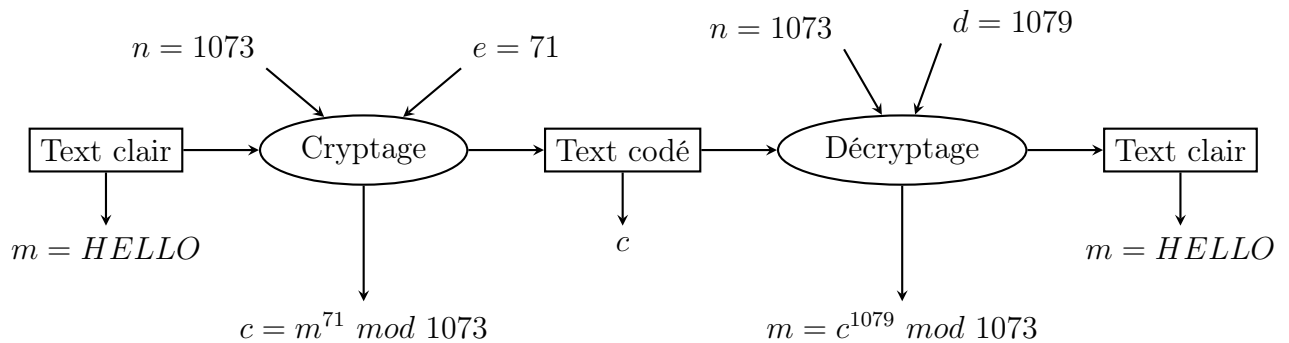


FIGURE 3.10 – Exemple sur utilisation de RSA

### Création de la paire de clés :

- ◆ Soient deux nombres premiers au hasard :  $p = 29$ ,  $q = 37$ , on calcule  $n = pq = 29 * 37 = 1073$ .
- ◆ On doit choisir  $e$  au hasard tel que  $e$  n'ai aucun facteur en commun avec  $(p-1)(q-1)$  :

$$(p-1)(q-1) = (29-1)(37-1) = 1008$$

- ◆ On prend  $e = 71$
- ◆ On choisit  $d$  tel que  $71 * d \bmod 1008 = 1$ , on trouve  $d = 1079$ .
- ◆ L'instruction  $d = \text{PowerMod}[e, -1, (p-1)(q-1)]$  de Mathematica permet de calculer  $d$  facilement.
- ◆ On a maintenant les clés

1. la clé publique est  $(e, n) = (71, 1073)$  (=clé de chiffrement),
2. la clé privée est  $(d, n) = (1079, 1073)$  (=clé de déchiffrement).

### Chiffrement du message " HELLO ".

code ASCII	72	69	76	79	
chiffres	H	E	L	L	O

- ◆ On prend le code ASCII de chaque caractère et on les met bout à bout :

$$m = 7269767679$$

- ♦ Il faut découper le message en blocs qui comportent moins de chiffres que  $n$ .  $n$  comporte 4 chiffres, on découpe notre message en blocs de 3 chiffres :

$726976767900$  (on compte avec des zéros)

- ♦ On chiffre chacun de ces blocs :

$$726^{71} \bmod 1073 = 436$$

$$976^{71} \bmod 1073 = 822$$

$$767^{71} \bmod 1073 = 825$$

$$900^{71} \bmod 1073 = 552$$

- ♦ Le message chiffré est 436 822 825 552.

**Déchiffrement du message chiffré " 436 822 825 552 ".**

- ♦ On chiffre chacun de ces blocs

$$436^{1079} \bmod 1073 = 726$$

$$822^{1079} \bmod 1073 = 976$$

$$825^{1079} \bmod 1073 = 767$$

$$552^{1079} \bmod 1073 = 900$$

- ♦ Le message déchiffré est 726 976 767 900  $\Rightarrow$  " HELLO ".

code ASCII	72	69	76	76	79
chiffres	H	E	L	L	O

## 3.6 L'algorithme à clé publique Al Gamel

### 3.6.1 Présentation

Le cryptosystème d'ElGamal, ou chiffrement El Gamal (ou encore système d'El Gamal) est un protocole de cryptographie asymétrique inventé par Taher El Gamal en 1984 et construit

à partir du problème du logarithme discret. Le cryptosystème El Gamal est basé sur la fonction à sens unique logarithme discret. On considère un groupe cyclique fini  $G$ , de cardinal  $n$  engendré par un générateur  $g$ . Donc

$$G = \{g^i | 0 \leq i \leq n - 1\}$$

On suppose que le calcul de  $g^i$  est " facile " et " rapide " mais que le calcul de  $i$  connaissant  $g^i$  n'est " pas facile " et " lent ". Si  $a = g^i$ ,  $i$  est appelé le logarithme discret de  $a$  [14].



FIGURE 3.11 – Tahre AlGamal

### 3.6.2 Description de l'algorithme

La première étape du schéma de chiffrement consiste à produire une paire de clefs : la clef publique, et la clef secrète. La première servira à chiffrer les messages et la deuxième à les déchiffrer.

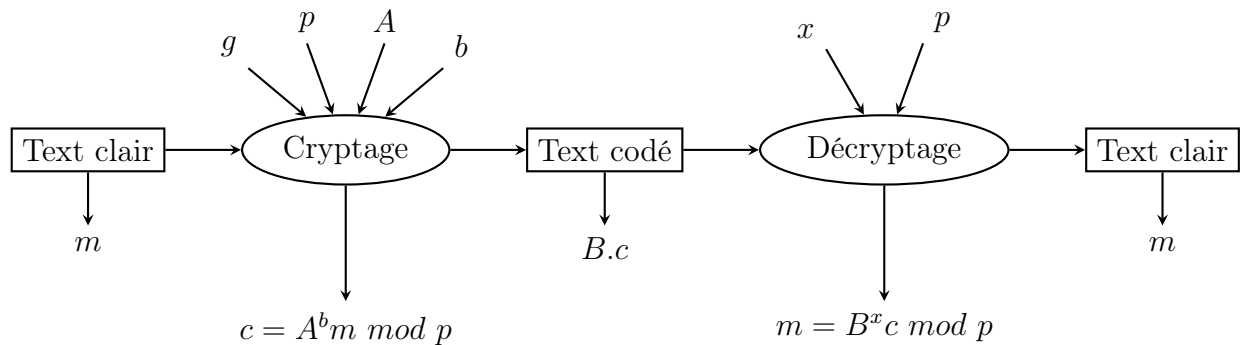


FIGURE 3.12 – Schéma de système El Gamal

## Génération des clés

Pour générer sa paire de clefs, Alice va commencer par prendre un groupe cyclique  $G$  d'ordre  $q$  dans lequel le problème décision de Diffie-Hellman (DDH) est difficile, ainsi qu'un générateur  $g$  de ce groupe.

Alice choisit un nombre premier  $p$  et une racine primitive  $g \bmod p$ . Ensuite, elle choisit un exposant au hasard  $a \in \{0, 1, \dots, p-2\}$  et calcule

$$A = g^a \bmod p.$$

La clé publique d'Alice est  $(p, g, A)$ , sa clé secrète est exposant  $a$ . L'entier  $A$  était la partie de clé venant d'Alice dans le protocole de Diffie-Hellman. Cette partie de la clé est fixée dans le cryptosystème El Gamal.

## Cryptage

L'espace des message clair est l'ensemble  $\{0, 1, \dots, p-1\}$ . Pour chiffrer un message clair  $m$ , Bob se procure la clé publique authentique d'Alice.

Il choisit un entier au hasard  $b \in \{0, 1, \dots, p-1\}$  et calcule

$$B = g^b \bmod p$$

Le nombre  $B$  était la partie de clé du protocole de Diffie-Hillman venant de Bob.

Bob détermine

$$c = A^b m \bmod p$$

En d'autre terme, Bob chiffre le message  $m$  en multipliant par la clé de Diffie-Hellman. Le cryptogramme ElGamal complet est  $(B, c)$ .

## Décryptage

Alice reçoit le cryptogramme  $(B, c)$ . Elle connaît sa clé secrète  $a$ . Pour reconstituer le message clair  $m$ , elle divise  $c$  par la clé de Diffie-Hillman  $B^a \bmod p$ . Afin d'éviter les inversion  $\bmod p$ , elle détermine d'abord l'exposant  $x = p - a$ . Puisque  $1 \leq a \leq p-2$ , on a  $1 \leq x \leq p-2$ . Puis elle calcule

$$m = B^x c \bmod p$$

C'est bien le message clair, comme montre le calcul suivant

$$B^x c \equiv g^{b(p-1-a)} A^b m \equiv (g^{p-1})^b (g^a)^{-b} A^b m \equiv A^{-b} A^b m \equiv m \pmod{p}$$

### 3.6.3 Inconvénients et avantages du système El Gamal.

1. **Inconvénient** : le message chiffré est deux fois plus long que le message original.
2. **Avantage** : l'introduction de l'aléa  $k$  permet au même message  $m$  chiffré deux fois à des moments différents de se traduire par des cryptogrammes différents.

### Exemple

Alice choisit  $p = 23, g = 7, a = 6$ , et calcule

$$A = g^a[p] = 7^6[23] = 4$$

Sa clé publique est  $(p, g, A) = (23, 7, 4)$ . Sa clé secrète est  $a = 6$ .

Bob chiffre  $m = 7$ . Il choisit  $b = 3$ , et calcule

$$B = g^b[p] = 7^3[23] = 21$$

et

$$c = A^b m[p] = 4^3 7[23] = 11.$$

Le cryptogramme est  $(B, c) = (21, 11)$ . Alice retrouve  $m$  en calculant

$$\begin{aligned} B^{p-1-6} c[p] &= 21^{16}[23] = 7. \\ &= m. \end{aligned}$$

## 3.7 L'algorithme à clé publique Rabin

### 3.7.1 Présentation

Cet algorithme fut publié en 1979 par Michael Rabin (voir [3][15]). La sécurité du système de Rabin, qui est présenté dans cette section, est aussi basé sur la difficulté de factoriser les entiers. Mais contrairement à RSA, on peut montrer que celui qui peut casser le système de Rabin efficacement peut tout aussi efficacement factoriser les entiers.

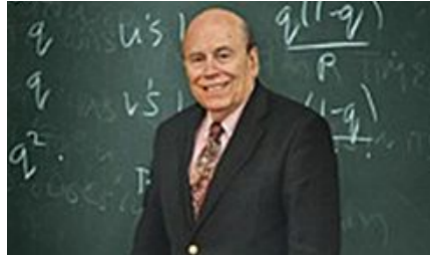


FIGURE 3.13 – Michael Rabin

### 3.7.2 Description de l'algorithme

#### Génération des clés

Il repose sur d'applications suivant

$$f : \mathbb{Z}/n\mathbb{Z} \mapsto \mathbb{Z}/n\mathbb{Z}$$

$$x \mapsto x(x + B)$$

Où  $n = p \cdot q$  est un entier de Blum (c'est-à-dire  $p$  et  $q$  sont congrus à 3 modulo 4, voir la définition (1.3) pag 16 ) et  $B$  est un entier positif inférieur ou égal à  $n - 1$ .

Alice choisit au hasard deux un entier de Blum  $p$  et  $q$  avec

$$p \equiv q \equiv 3 \text{ mod } 4.$$

Alice calcule

$$n = p \cdot q$$

Les données  $n$  et  $B$  sont publiques (  $p$  et  $q$  sont secret).

#### Cryptage

Nous supposons à nouveau que le message clair  $m$  est un entier positif inférieur à  $n$ . Pour crypter le message clair  $m$ , Bob calcule

$$c = m(m + B) \text{ dans } \mathbb{Z}/n\mathbb{Z}$$

et envoie  $c$  à Alice (avec  $c \leq n - 1$ ).

## Décryptage

Alice doit résoudre dans  $Z/nZ$  l'équation

$$x^2 + Bx = c,$$

elle procède comme pour l'équation du second degré classique.

Comme  $n$  est impair, 2 et 4 sont inversibles modulo  $n$ , notons leur inverse  $2^{-1}$  et  $4^{-1}$  et nous pouvons récrire l'équation sous forme canonique

$$(x + 2^{-1}B)^2 - 4^{-1}B^2 = c$$

ou

$$(x + 2^{-1}B)^2 = c - 4^{-1}B^2$$

Comme l'équation a forcément une solution (le message clair),  $c - 4^{-1}B^2$  est un carré dans  $Z/nZ$ .

Comme le montre les proposition (1.6) et (1.7), si nous connaissons  $p$  et  $q$ , il est facile de déterminer les racines carrées dans  $Z/nZ$ . Notons  $\pm x_1$  et  $\pm x_2$  les racines carrées de  $c - 4^{-1}B^2$ , nous obtenons

$$x = \begin{cases} -2^{-1}B \pm x_1 \\ ou \\ -2^{-1}B \pm x_2 \end{cases}$$

et  $m$  est une de ces solutions (Voir [2]).

### 3.7.3 Efficacité système de Rabin

Dans le système de Rabin, le chiffrement ne demande qu'une élévation au carré, c'est pourquoi ce chiffrement est plus efficace que le chiffrement RSA, même avec le plus petit possible exposant de chiffrement 3. Le déchiffrement dans le système de Rabin est aussi coûteux que le déchiffrement RSA amélioré par le théorème des restes chinois ( (1.11) pag 15 ). Il demande une exponentiation  $mod\ q$ , une autre  $mod\ q$ , et une application du théorème des restes chinois (voir [7])



### Exemple

Supposons que le clé publique  $(n, B) = (77, 9)$ . Alice reçoit le message  $c = 22$  de Bob. Dans  $Z/77Z$  l'inverse de 2 est 39 et l'inverse de 4 est 58. Donc

$$c - 4^{-1}B^2 = 22 + 58 \times 81 = 23$$

dans  $Z/77Z$ . Alice va donc résoudre

$$\begin{cases} x^2 = 2[7] \\ x^2 = 1[11] \end{cases},$$

et elle trouve

$$\begin{cases} x = \pm 4[7] \\ x = \pm 1[11] \end{cases}.$$

Alors, le théorème des restes chinois nous donne

$$\begin{aligned} x &\equiv \pm 4 \times 11 \times 2 + 1 \times 3 \times 7[77] \\ &\equiv \pm 88 \pm 21[77], \end{aligned}$$

donc les racine carrées de  $c - 4^{-1}B^2$  dans  $Z/77Z$  sont  $\pm 10$  et  $\pm 32$ , comme  $-2^{-1}B = -39 \times 9 = 34$  les différents valeurs possibles pour  $m$  sont

$$-34 - 32 = 2$$

$$-34 + 32 = 66$$

$$-34 - 10 = 24$$

$$-34 + 10 = 44.$$

Nous pouvons aisément vérifier que pour toutes ces valeurs nous avons

$$m(m + 9) = 22.$$

---

---

## Chapitre 4

---

### L'APPLICATION DES MÉTHODES À CLÉ PUBLIQUE

Jusqu'au 20-ième siècle la cryptographie (légale) était essentiellement réservée aux militaires et aux diplomates et accessoirement aux industriels et banquiers.

Le développement des moyens de communications électromagnétiques facile à intercepter, des stockages de données confidentielles dans des sites assez faciles à pénétrer et sur des supports (bandes ou disques, magnétiques optiques) faciles à dupliquer ont généré une demande de cryptosystèmes sûrs, faciles d'emploi et rapides pour des usages civils et commerciaux. Les codes symétriques ou à clefs secrètes, type DES et AES ont été créés pour couvrir ces besoins. L'application première de la cryptographie reste encore la transmission sécurisée de données sensibles mais d'autres applications commencent à se développer.

Le commerce en ligne (e-commerce : paiement par carte bancaire...), les transactions bancaires et boursière (e-banking : la consultation des données bancaires, ordres de bourse, virements de compte à compte,...), l'administration en ligne (e-administration : déclaration d'impôts, paiement de la TVA pour les entreprise,...), la télévision payante (chaîne payante, pay per view,...), la protection des télécommunications (internet, WIFI, Bluetooth, GSM, téléphonie mobile,...), l'identification automatique (avions, camions suivi par GPS,...), le tatouage ou watermarking des données numériques ainsi que la gestion des droits numériques (digital right management), etc. ont entraîné une explosion de l'utilisation de la cryptographie mais

aussi une extension de son champ d'applications.

Cette extension a été facilitée par la mise au point des procédés de transferts de clefs de Diffie et Hellman et des codes asymétriques ou à clefs publiques de type RSA ou El Gamal. Les codes à clef publique permettent de résoudre avec des protocoles légers les questions de transfert de clefs, d'identification, d'authentification, de signature entre correspondants.

Aujourd'hui les plus gros utilisateurs de cryptosystèmes sont les institutions financières (banques, bourses,...), les télécommunications (téléphonie mobile, WIFI, Internet, télévision payante,...), les sites d'achats en ligne, ...

Il est probable que le tatouage ou watermarking des données numériques ainsi que la gestion des droits numériques (digital right management ou DRM ) vont entraîner une demande accrue de cryptographie. Le mariage de la cryptographie et de la théorie de la complexité aboutit à des extensions spectaculaires du champ de la cryptographie classique voir ([4]).

### 4.1 Cartes à puce



FIGURE 4.1 – Cartes à puce

La carte à puce a été inventée par deux ingénieurs français, Roland Moreno (1974) et Michel Ugon (1977)

La sécurité des cartes à puces fait intervenir trois processus différents; le code PIN, le protocole RSA et le code DES.,

## Secret d'une carte bancaire

Vous devez vous identifier auprès de la banque. Vous avez deux clés : une publique que tout le monde connaît, une secrète (le code PIN) que personne d'autre que vous ne connaît.

Les messages que vous envoyez ou que vous recevez ne doivent pas révéler votre code



FIGURE 4.2 – Carte bancaire

secret. Tout le monde (y compris la banque) ayant accès aux messages échangés peut vérifier que vous connaissez ce code secret, mais cela ne leur permet pas de le connaître.

La banque vous envoie un message aléatoire. Votre réponse dépend de ce message et de votre code secret.

## Exemple

message aléatoire	Code Pin	Clé Publique
631	67	3
	$631^{67} \equiv 111$	$111^3 \equiv 631$

Connaissant la **clé publique** 3 et le message 631 envoyé par la banque, on vérifie que la réponse 111 est correcte, mais cela ne permet pas de deviner le **code secret** 67.

## 4.2 RSA est la méthode le plus utilisé

L'algorithme **RSA** est largement utilisé pour de nombreuses applications pratiques. Typiquement, ces applications peuvent être classées en "**échange de clés**" et / ou "**signature**".

numérique".

**Par exemple**, lorsque vous visitez un site **Web** commençant par «**https** : //», il est fort probable que votre navigateur **Web** utilise **RSA** pour valider le certificat du serveur distant auquel vous vous êtes connecté. Une fois que votre navigateur a validé la chaîne de certificats (en utilisant la fonctionnalité de signature **RSA**), il utilisera probablement **RSA** pour effectuer un échange de clé sécurisé avec le serveur. Le résultat final : votre navigateur peut communiquer en toute sécurité avec un serveur distant et vous assurer que le serveur distant en question est bien le serveur que vous avez l'intention de contacter - pas un méchant exécutant une attaque de type man-in-the-middle pour voler vos informations privées.

**HTTPS** est utilisé avec d'innombrables sites **Web** où l'échange d'informations personnelles ou privées a lieu (mots de passe, e-commerce, etc.)

Les applications informatiques sont souvent signées numériquement afin que le consom-

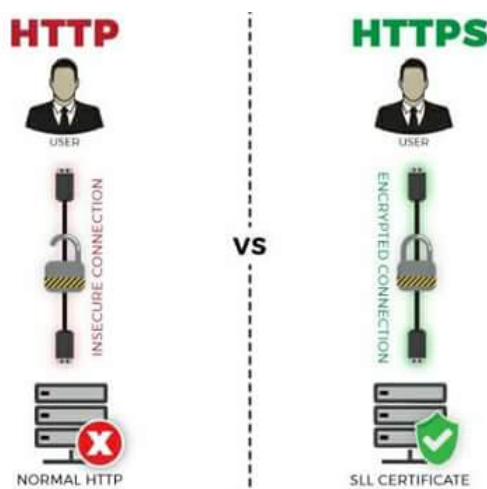


FIGURE 4.3 – https et http

mateur puisse vérifier que le logiciel n'a pas été modifié depuis que l'éditeur l'a publié. Si le logiciel est modifié après la signature (même d'un bit), la signature numérique échouera. Cela fournit un moyen d'empêcher l'exécution de code non approuvé.

Ensuite, il existe d'autres technologies comme **la radio commerciale** par satellite, **la**

**télévision** par satellite, etc. Si l'éditeur de contenu diffusait simplement les médias en clair, il aurait du mal à convaincre les gens de payer leur facture mensuelle. Au lieu de cela, ils ont besoin d'un moyen de distribuer les clés de décryptage à leurs abonnés payants, tout en gardant le public général - **RSA** est un candidat pour cela aussi.

RSA est utilisé pour de nombreuses autres applications de gestion des droits numériques (DRM).

Ce ne sont que quelques exemples.

**La sécurité de l'algorithme RSA** est basée sur la croyance que la factorisation de grands entiers est et continuera d'être coûteuse en termes de calcul. **RSA** est utilisé depuis plus de 30 ans et est encore considéré comme sécurisé à ce jour, à condition que des clés de longueur suffisante soient utilisées. Les clés créées aujourd'hui sont généralement au moins **2048** bits.

### Pourquoi RSA est-il si populaire par rapport aux autres méthodes ?

Il n'est pas régi par des brevets actifs. Tout le monde peut l'utiliser, libre de droits dans tout produit privé ou commercial. **RSA** peut faire le chiffrement, le décryptage, la signature et la vérification de signature - tous avec les mêmes deux fonctions. Il a été autour pendant plus de 30 ans et n'a pas été compromise.

---

## CONCLUSION

Ce mémoire dont l'objectif concerne à avoir l'étude des certaines méthodes de cryptage asymétrique.

Au début, nous expliquons les principes de codage, le chiffrement symétrique et certaines de ses méthodes. Il est clair d'étudier le cryptage de clé public et de mettre en évidence ses méthodes les plus utilisées comme RSA, Al Gamal et Rabin. Il utilisé dans le commerce en ligne, les transactions bancaires et boursière, l'administration en ligne, la télévision payante, la protection des télécommunications, l'identification automatique et site Web ...etc. RSA est caractérisé par être plus populaire que d'autres algorithmes. Quant à Al Gamal et Rabin sont peu utilisés aujourd'hui. Le but des algorithmes de cryptage sont d'assurés la sécurité.

L'intérêt du travail présenté dans ce mémoire est c'est que le principe de chiffrement et déchiffrement est presque le même, c'est-à-dire une fois que l'on a compris les méthodes exposées on pourra comprendre d'autre méthodes de cryptage.

finalement, Nous vous présenté les utilisations quotidiennes de ces méthodes et leur rôle dans la vie. La technologie d'aujourd'hui ouvre de larges horizons pour une telle science et est en progrès continu.