Congrès Dédra-MATH-isons

Modulus VS Cryptographix

L'arithmétique modulaire au service du chiffrement affine.

Par

BOREUX Romain
DELVAUX Frédérique
GEORGIN Maxime
MAUDOUX Jérôme
PIETTE Cyril
POELVOORDE Nora
STONE Ethan
SWERTVAEGHER Maxime
TENG Feida

Enseignant : *Mme Sabine DE BLIECK*

Introduction

Dès l'aube de l'histoire, les hommes ont utilisé diverses méthodes pour transmettre des secrets, essentiellement à des fins militaires et diplomatiques. La **cryptographie** est l'étude des messages codés de telle sorte que seul le destinataire puisse les décoder.

Aujourd'hui, la cryptographie s'applique dans des domaines aussi variés que la sécurité des transactions bancaires, des transmissions de fichiers et de bases de données sous forme électronique.

Dans le jargon de la cryptographie :

- Le message à transmettre est le **texte clair** ;
- Le message codé est le **cryptogramme** ;
- L'action de coder un texte clair est le **chiffrement** ;
- L'action de décoder un cryptogramme est le **déchiffrement**.

Pour rendre inintelligible un message à des lecteurs indésirables, plusieurs méthodes existent. Nous nous sommes intéressés à celle qui consiste à substituer un nombre à chaque lettre de l'alphabet ou à un symbole. C'est d'ailleurs se qui justifie le terme « chiffrement ».

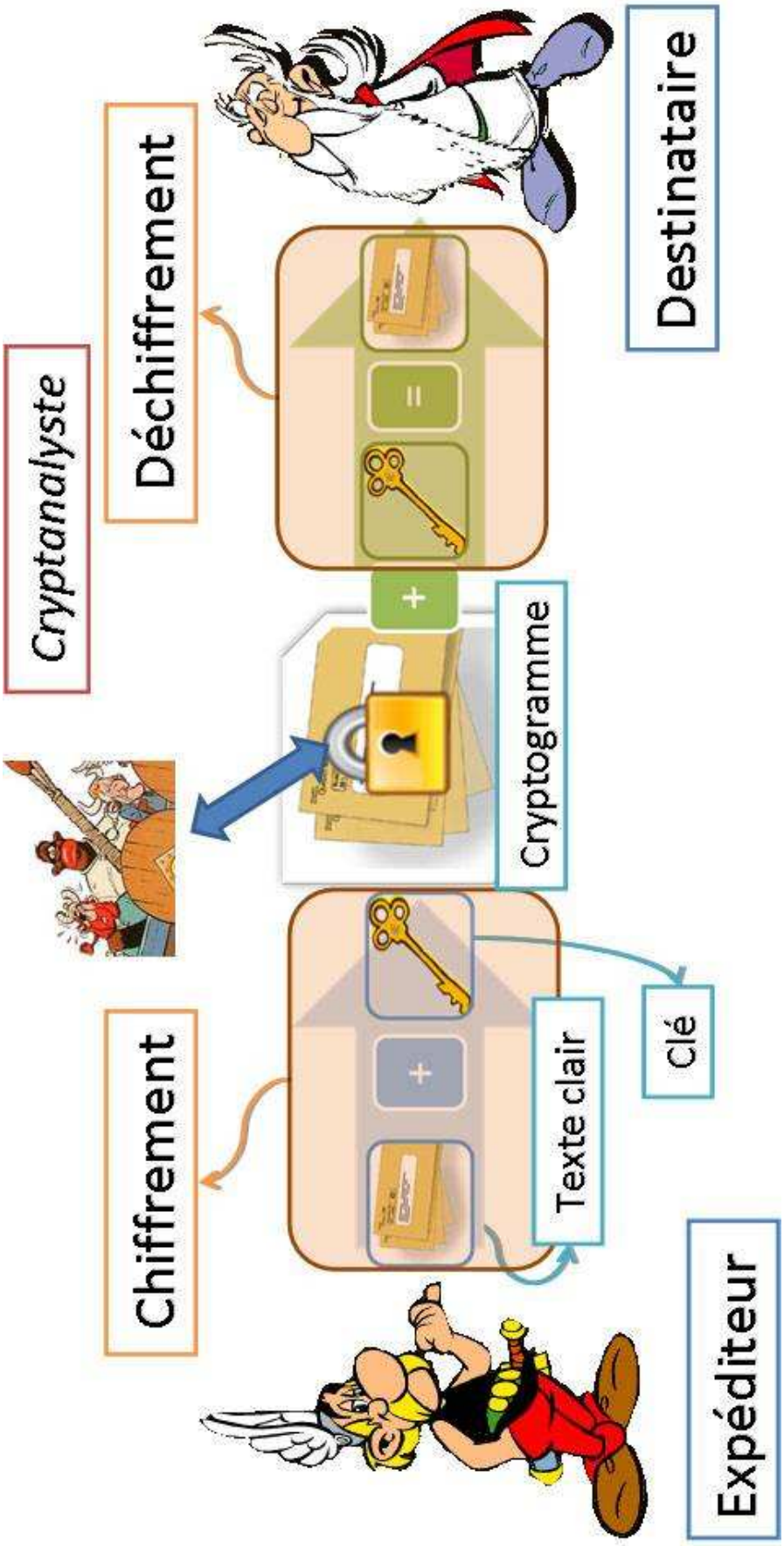
Pour effectuer un chiffrement, on utilise une **clé** de codage (mot, nombre ou tableau de nombres) que le destinataire utilisera pour retrouver le texte d'origine.

Qui dit messages codés dit messages importants, secrets. Le destinataire n'est donc pas le seul à vouloir le décrypter. Des personnes peuvent donc essayer de le décoder mais en ne possédant pas la clé de chiffrement. Ils vont alors tenter plusieurs sortes d'attaques, ils vont essayer de « casser » le code : trouver le sens du message secret et la clé de chiffrement. Ces attaques relèvent de la **cryptanalyse**.

Un bon chiffrement est alors un chiffrement qui permet de coder facilement un message, c'est-à- dire avec une clé assez courte, sans pour autant la rendre trop vulnérable face aux attaques externes. Compte tenu des moyens techniques (aujourd'hui, les ordinateurs puissants sont des alliés essentiels de la cryptographie), il faut réussir à trouver un compromis entre sécurité et facilité d'utilisation. Si le temps et le coût de cryptanalyse dépassent la valeur de l'information, on peut considérer le chiffrement comme efficace.

Nous présenterons dans ce travail des modes de chiffrement basés sur des principes de **congruence arithmétique** et de **transformations affines**. Nous avons choisi de les classer en deux catégories : le chiffrement par **substitution monoalphabétique** (un même caractère du texte initial est toujours codé de la même façon) et le chiffrement par **substitution polyalphabétique** (le texte initial est découpé en blocs codés séparément). Au départ des formules générales présentées, nous effectuerons un bref tour d'horizon des systèmes cryptographiques classiques utilisés jusqu'à la deuxième guerre mondiale. S'ils sont caducs à l'heure actuelle, ils n'en restent pas moins des exemples importants de l'histoire de la cryptographie.

Le Vocabulaire du Cryptologue



Première partie

Notions élémentaires de congruence arithmétique

I. La congruence et les modulos

1. *Définition :*

Soit a et $b \in \mathbb{Z}$ et $m \in \mathbb{N}_0$

On dit que a est **congru à *b* modulo *m*** si et seulement si $a-b$ est divisible par m.

On écrit $a \equiv b(\mathrm{mod}\, m) \iff a = km+b \iff a-b = km \iff m|(a-b)$

Dans le cas contraire, nous disons que "a est non congru à b modulo m".

Exemples :

$4 \equiv 9$ mod 5 car 4-9=-1.5

$-5 \equiv 3$mod 4 car -5-3=-2.4

$37 \equiv 25$ mod 12 car 37-25=1.12

$\forall\, a \in \mathbb{Z}$ et $m \in \mathbb{N}_0$, $k \in \mathbb{Z}$ et $b \in N$

$$a = km+b \text{ et } 0 \le b < |m| \Rightarrow a \equiv b(\mathrm{mod}\, m)$$

En effet, il suffit d'écrire $a = km+b \Leftrightarrow (a-b) = km$.

Par contre, inversement :

Si $a \equiv b(\mathrm{mod}\, m)$, b n'est le reste de la division de a par m que si $0 \le b < |m|$.

Nous avons donc :

$$\forall\, a \in \mathbb{Z}, \exists\, !\, b \in \mathbb{Z} : 0 \le b < |m| \text{ et } a \equiv b(\mathrm{mod}\, m)$$

b n'est rien d'autre que le reste de la division de a par m. On l'appelle « **résidu de a modulo m** ». Dans l'arithmétique des congruences, on ne s'intéresse qu'aux restes, pas à la valeur du k (quotient).

L'opération qui à a et m fait correspondre b sera notée : b = a (mod m).

Exemples :

47 mod 15 = 2,

–20 mod 7 = 1.

Remarque :

Il ne faudra donc pas confondre les deux notions qu'on a introduites :

- la relation «≡» : $a \equiv b(\mathrm{mod}\, m) \iff a = km+b$
- l'opération « mod » : $b = a(\mathrm{mod}\, m) \iff a = km+b$ et $0 \le b < |m|$

Donc $b = a$ mod $m \Rightarrow a \equiv b$ mod m mais $a \equiv$bmod m n'implique pas $b = a$mod m

Exemple :

2 = 37 mod 35 mais 37 ≠ 2 mod 35,

Par contre, 37 ≡2 mod 35.

Traduction

- $a \equiv km + b$: a divisé par m a pour reste b ssi $0 < b < |m|$
- $a - b = k \times m$: a-b est divisible par/multiple de m
- $a \equiv b(\mathrm{mod}\, m)$: a et b sont congrus modulo m ou a est congru à b modulo m

Explication facile du sens de deux petits mots :

-modulo m : diviser par m

-résidu b : le reste de cette division

2. *Quelques propriétés*

1.

$$a \equiv 0(\mathrm{mod}\, m) \Leftrightarrow m / a$$

Démonstration

$\Rightarrow a \equiv 0 \bmod m \Rightarrow m / a$ par définition $a \equiv 0 \bmod m \Leftrightarrow m / (a - 0)$

$\Leftarrow m / a \Rightarrow a = km$ (le reste est nul) $\Leftrightarrow 0 = a \bmod m \Rightarrow a \equiv 0 \bmod m$

2. **Réflexivité de la relation de congruence**

$$a \equiv a(\mathrm{mod}\, m) \quad \forall a \in \mathbb{Z}$$

Démonstration

$a \equiv a(\mathrm{mod}\, m) \Leftrightarrow m/(a\text{-}a) \Leftrightarrow m/0$

3. **Symétrie de la relation de congruence**

$$a \equiv b \bmod m \Leftrightarrow b \equiv a \bmod m$$

Démonstration

$a \equiv b(\mathrm{mod}\, m) \Leftrightarrow m|(a - b) \Leftrightarrow m|(b - a) \Leftrightarrow b \equiv a \bmod m$

4. **Transitivité de la relation de congruence**

si $a \equiv b(\mathrm{mod}\, m)$ et $a \equiv c(\mathrm{mod}\, m)$ alors $b \equiv c(\mathrm{mod}\, m)$

Démonstration

$a \equiv b(\mathrm{mod}\, m) \Leftrightarrow$ m|(a-b)

$a \equiv c(\mathrm{mod}\, m) \Leftrightarrow$ m|(a-c)

(m|(a-b)) $\wedge$ (m|(a-c)) $\Rightarrow$ m| ((a-c)-(a-b)) $\Leftrightarrow$ m|(b-c) $\Leftrightarrow b \equiv c(\mathrm{mod}\, m)$

La relation de congruence $\equiv$ est donc une relation d'équivalence.

5. **Multiples**

si m' est multiple de m
$a \equiv b(\mathrm{mod}\, m') \Rightarrow a \equiv b(\mathrm{mod}\, m)$

Démonstration

m' est multiple de m . $\exists$ q $\in \mathbb{Z}_0$: $m' = mq$.

$$a \equiv b(\mathrm{mod}\, m') \Leftrightarrow a = km' + b \quad \Leftrightarrow a \equiv kqm + b \Rightarrow a = k'm + b \quad \Leftrightarrow a \equiv b(\mathrm{mod}\, m)$$

II. Les classes de résidus

1. *Notion de classe*

Prenons les entiers 35, 38, 41, 44. On s'aperçoit que:

- Leur résidu par la division euclidienne par 3 vaut 2;

2 = 35 mod 3 = 38 mod 3 = 41 mod 3 = 44 mod 3.

- Ils sont tous congrus modulo 3.

35 ≡ 38 mod 3 ≡ 41 mod 3 ≡ 44 mod 3.

Prenons les entiers 16, 19, 22, 25. On s'aperçoit que :

- - Leur résidu par la division euclidienne par 3 vaut 1;

1 = 16 mod 3 = 19 mod 3 = 22 mod 3 = 25 mod 3.

- Ils sont aussi tous congrus modulo 3.

16 ≡19 mod 3 ≡ 22 mod 3 ≡ 25 mod 3.

Ces entiers appartiennent donc à un même ensemble qu'on appelle **classe**.

En modulo 3, 35, 38, 41, 44 appartiennent à la classe de résidu égal à 2.

En modulo 3, 16, 19, 22, 25 appartiennent à la classe de résidu égal à 1.

De la même manière, on peut rassembler tous les entiers en différentes classes. Nous appellerons la classe de a modulo m, notée $\bar{a}_m$ [1], l'ensemble des entiers congrus à a modulo m: $\bar{a}_m = \{a+k.m \mid k \in \mathbb{Z}\}$

[1] Cette écriture n'est sans doute pas conventionnelle, mais nous la trouvons plus commode que la notation officielle ā, car elle fait apparaître le m.

2. Représentant d'une classe

On sait que le résidu r est le reste de la division euclidienne de a par m:

$$\mathbf{r = a \bmod m}$$

Or, par la définition de classe, on peut dire que tous les éléments d'une même classe ont le même résidu modulo m.

On peut donc choisir le résidu r comme représentant de cette classe, et l'utiliser de préférence pour désigner la classe à laquelle il correspond.

Nous désignerons comme **représentant de classe $\bar{a}_m$** modulo m le reste par la division euclidienne par m de tous les nombres de la classe $\bar{a}_m=\{a+k.m \mid k\in\mathbb{Z}\}$. Le symbole $\bar{a}_m$ désignera donc à la fois la classe (ensemble de nombre) et son représentant (le reste/résidu).

3. Nombre de classes en fonction de m

Soit m = 3

a	…	-3	-2	-1	0	1	2	3	4	5	6	…	3k-1	3k	3k+1	3k+2	3(k+1)	…
r	…	0	1	2	0	1	2	0	1	2	0	…	2	0	1	2	0	…
classe	…	$\bar{0}_3$	$\bar{1}_3$	$\bar{2}_3$	$\bar{0}_3$	$\bar{1}_3$	$\bar{2}_3$	$\bar{0}_3$	$\bar{1}_3$	$\bar{2}_3$	$\bar{0}_3$	…	$\bar{2}_3$	$\bar{0}_3$	$\bar{1}_3$	$\bar{2}_3$	$\bar{0}_3$	…

Il existe trois classes en modulo 3 : $\bar{0}_3, \bar{1}_3, \bar{2}_3$

Soit m = 4

a	…	-4	-3	-2	-1	0	1	2	3	4	5	6	…	4k-1	4k	4k+1	4k+2	4k+3	4(k+1)	…
r	…	0	1	2	3	0	1	2	3	0	1	2	…	3	0	1	2	3	0	…
classe	…	$\bar{0}_3$	$\bar{1}_4$	$\bar{2}_4$	$\bar{3}_4$	$\bar{0}_4$	$\bar{1}_4$	$\bar{2}_4$	$\bar{3}_4$	$\bar{0}_4$	$\bar{1}_4$	$\bar{2}_4$	…	$\bar{3}_4$	$\bar{0}_4$	$\bar{1}_4$	$\bar{2}_4$	$\bar{3}_4$	$\bar{0}_4$	…

Il existe quatre classes en modulo 4 : $\bar{0}_4, \bar{1}_4, \bar{2}_4, \bar{3}_4$

Soit m = 5

a	…	-1	0	1	2	3	4	5	6	…	5k-1	5k	5k+1	5k+2	5k+3	5k+4	5(k+1)	…
r	…	4	0	1	2	3	4	0	1	…	4	0	1	2	3	4	0	…
classe	…	$\bar{4}_5$	$\bar{0}_5$	$\bar{1}_5$	$\bar{2}_5$	$\bar{3}_5$	$\bar{4}_5$	$\bar{0}_5$	$\bar{1}_5$	…	$\bar{4}_5$	$\bar{0}_5$	$\bar{1}_5$	$\bar{2}_5$	$\bar{3}_5$	$\bar{4}_5$	$\bar{0}_5$	…

Il existe 5 classes en modulo 5 : $\bar{0}_5, \bar{1}_5, \bar{2}_5, \bar{3}_5, \bar{4}_5$

Soit m = m

a	1	2	3	…	m-1	m	m+1	…	2m-1	2m	2m+1	…	km-1	km	km+1	…	(k+1)m	…
r	1	2	3	…	m-1	0	1	…	m-1	0	1	…	m-1	0	1	…	0	…
Classe	$\bar{1}_m$	$\bar{2}_m$	$\bar{3}_m$	…	$\overline{m-1}_m$	$\bar{0}_m$	$\bar{1}_m$		$\overline{m-1}_m$	$\bar{0}_m$	$\bar{1}_m$	…	$\overline{m-1}_m$	$\bar{0}_m$	$\bar{1}_m$		$\bar{0}_m$	

Il existe m classes en modulo m : $\bar{0}_m$, $\bar{1}_m$, $\bar{2}_m$, $\bar{3}_m$, … $\overline{m-1}_m$

4. Présentation de l'ensemble $\mathbb{Z}_m$

On vient de voir que, pour un m donné, il existe m classes de modulo m.

Or chaque classe de modulo m contient un et un seul représentant.

Par conséquent, pour un m donné, il existe m représentants des classes de modulo m.

On peut donc rassembler les représentants de toutes les classes modulo dans un ensemble que l'on peut appeler $\mathbb{Z}_m$.

Nous appellerons $\mathbb{Z}_m$ l'ensemble des entiers représentant les classes de modulo m:

$\mathbb{Z}_m = \{r \in \mathbb{N} \mid a=r+km,\ r<m,\ a\in\mathbb{Z},\ k\in\mathbb{Z}\}$

Concrètement, l'ensemble $\mathbb{Z}_m$, c'est:

$\mathbb{Z}_m = \{0, 1, 2, \ldots, m-1\}$ car $r \in \mathbb{N}$ et $r<m$.

III. Les propriétés des opérations dans $\mathbb{Z}_m$

1. Compatibilité de la loi d'addition + avec la congruence ≡

$$(a+b) \bmod m \equiv a \bmod m + b \bmod m \quad (1)$$

Démonstration

On pose : $a' \equiv a \bmod m$ et $b' \equiv b \bmod m$

(1) de vient $(a+b) \bmod m \equiv a'+b'$

Il nous faut donc démontrer que : $m \mid [(a'+b')-(a+b)] \Leftrightarrow m \mid [(a'-a)+(b'-b)]$

et comme : $m|(a'-a)$ et $m|(b'-b)$, m divise donc bien $[(a'-a)+(b'-b)]$.

De cette compatibilité de la congruence $\equiv$ avec la loi d'addition + dans $\mathbb{Z}$, nous tirons la définition de l'addition dans $\mathbb{Z}_m$:

$$+ : \mathbb{Z}_m X \mathbb{Z}_m \to \mathbb{Z}_m : (\bar{a},\bar{b}) \to \bar{a}+\bar{b} = \overline{a+b}$$

Ce qui nous permet de démontrer les propriétés de l'addition dans $\mathbb{Z}_m$.

I. + est **Interne et partout définie** dans $\mathbb{Z}_m$:

par sa définition même.

II. + est **commutative** dans $\mathbb{Z}_m$:

$$\forall\ \bar{a}, \bar{b} \in \mathbb{Z}_m : \bar{a}+\bar{b} = \bar{b}+\bar{a}$$

Démonstration : Par définition de + dans $\mathbb{Z}_m$ et la commutativité de + dans $\mathbb{Z}$, on obtient :

$$\bar{a}+\bar{b} = \overline{a+b} = \overline{b+a} = \bar{b}+\bar{a}$$

III. + est **associative** dans $\mathbb{Z}_m$:

$$\forall\ \bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_m : (\bar{a}+\bar{b})+\bar{c} = \bar{a}+(\bar{b}+\bar{c})$$

Démonstration : Par définition de + dans $\mathbb{Z}_m$ on obtient :

$$(\bar{a}+\bar{b})+\bar{c} = \overline{a+b}+\bar{c} = \overline{a+b+c} \quad et \quad \bar{a}+(\bar{b}+\bar{c}) = \bar{a}+\overline{b+c} = \overline{a+b+c}$$

IV. + possède un **élément neutre** ($\bar{0}$) dans $\mathbb{Z}_m$:

$$\forall\ \bar{a} \in \mathbb{Z}_m\ \ \bar{a} + \bar{0} = \bar{0} + \bar{a} = \bar{a}$$

Démonstration : Par définition de + dans $\mathbb{Z}_m$ on obtient :

$$\bar{a} + \bar{0} = \overline{a+0} = \bar{a}$$

V. + a pour tout élément un **inverse** :

$$\forall\ \bar{a} \in \mathbb{Z}_m\ \ \bar{a} + \overline{m-a} = \bar{0}$$

Démonstration : Par définition de + dans $\mathbb{Z}_m$ on obtient :

$$\bar{a} + \overline{m-a} = \overline{a+m-a} = \overline{m} = \bar{0}$$

Nous pouvons donc affirmer que ($\mathbb{Z}_m$,+) est un groupe commutatif.

Application

Ces propriétés nous permettent par exemple de calculer mentalement le reste d'un entier très grand dans une division euclidienne.

Quel est le reste de 1459 dans la division par 7 ? Il suffit de décomposer 1459 en une somme de nombres plus simples.

1459= 1400 + 59.

1400 mod7=0 et 59 mod7= 3. Donc, 1459mod7=3

2. Compatibilité de la loi de multiplication . avec la congruence ≡

$$(a.b) \bmod m \equiv (a \bmod m) . (b \bmod m) \quad (1)$$

On pose : $\bar{a} = a \bmod m \Leftrightarrow \exists\ k_a \in \mathbb{Z}: a = km + \bar{a}$ et $\exists\ k_b \in \mathbb{Z}: \bar{b} = b \bmod m \Leftrightarrow b = k_b m + \bar{b}$

$\overline{a.b} = (ab) \bmod m \Leftrightarrow \exists\ k \in \mathbb{Z} : ab = km + \overline{a.b} \Leftrightarrow \overline{a.b} = ab - km$

On obtient : $\overline{a.b} - \bar{a}\bar{b} = ab - km - ((a-k_a m)(b-k_b m)) = ab - km - (ab - k_b am - k_a bm + k_a k_b m^2)$

$\overline{a.b} - \bar{a}\bar{b} = -km + k_b am + k_a bm - k_a k_b m^2 = m.(-k + k_b a + k_a b - k_a k_b m).$

Or $-k + k_b a + k_a b - k_a k_b m \in \mathbb{Z}$. Soit $K=-k + k_b a + k_a b - k_a k_b m$;

$\overline{a.b} - \bar{a}\bar{b} = Km \Leftrightarrow m | (\overline{a.b} - \bar{a}\bar{b}) \Leftrightarrow \overline{a.b} \equiv \bar{a}\bar{b} \bmod m.$

Remarque : En raison de (1), nous pouvons écrire : $(a^p) \bmod m \equiv (a \bmod m)^p$

De cette compatibilité de ≡ avec la loi de multiplication, on peut dire que :

$$. : \mathbb{Z}_m X \mathbb{Z}_m \to \mathbb{Z}_m : (\bar{a},\bar{b}) \to \bar{a}.\bar{b} = \overline{a.b}$$

Ce qui nous permet de démontrer que la multiplication

I. . est **Interne et partout définie** dans $\mathbb{Z}_m$:

par sa définition même.

II. . est **commutative** dans $\mathbb{Z}_m$:

$$\forall\ \bar{a}, \bar{b} \in \mathbb{Z}_m : \bar{a}.\bar{b} = \bar{b}.\bar{a}$$

Démonstration : Par définition de . dans $\mathbb{Z}_m$ et la commutativité de . dans $\mathbb{Z}$, on obtient :

$\bar{a}.\bar{b} = \overline{a.b} = \overline{b.a} = \bar{b}.\bar{a}$

III. . est **associative** dans $\mathbb{Z}_m$:

$$\forall\ \bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_m : (\bar{a}.\bar{b}).\bar{c} = \bar{a}.(\bar{b}.\bar{c})$$

Démonstration : Par définition de . dans $\mathbb{Z}_m$ on obtient :

$(\bar{a}.\bar{b}).\bar{c} = \overline{a.b}\ .\ \bar{c} = \overline{a.b.c}$ *et* $\bar{a}.(\bar{b}.\bar{c}) = \bar{a}.\overline{b.c} = \overline{a.b.c}$

IV. . possède un **élément neutre** ($\bar{1}$) dans $\mathbb{Z}_m$:

$$\forall\ \bar{a} \in \mathbb{Z}_m\ \ \bar{a}\ .\bar{1} = \bar{1}.\ \bar{a} = \bar{a}$$

Démonstration : Par définition de . dans $\mathbb{Z}_m$ on obtient :

$\bar{a}\ .\bar{1} = \overline{a.1} = \bar{a}$

V. Mais . n' a pas toujours un **inverse** pour tout élément!

L'inverse modulo m de b est le nombre entier b^{-1} tel que $(b \cdot b^{-1}) \bmod m = 1$. On peut le calculer avec l'algorithme d'Euclide étendu. (cfr. paragraphe IV).

Ainsi, par exemple, 3 est son propre inverse modulo 4 : (3.3)mod 4= 1 mais 2 n'a pas d'inverse modulo 4. En effet, aucun réel x ne permet de résoudre 2x=4k+1 si $k \in \mathbb{Z}$.
Cet aspect sera traité en détail dans le paragraphe IV : « Eléments inversibles dans $\mathbb{Z}_m$. »

VI. . est **distributive par rapport à +** :

$$\forall\ \bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_m : (\bar{a}+\bar{b}).\bar{c} = \bar{a}.\bar{c}+\bar{b}.\bar{c}$$

Démonstration : Par définition de + et de . dans $\mathbb{Z}_m$, et de la distributivité de . par rapport à + dans $\mathbb{Z}$,on obtient :

$(\bar{a}+\bar{b}).\bar{c} = \overline{a+b}\ .\bar{c} = \overline{(a+b).c} = \overline{a.c+b.c} = \overline{a.c} + \overline{b.c} = \bar{a}.\bar{c}+\bar{b}.\bar{c}$

Application

Ceci nous permet de résoudre facilement : $(3^{343}.17^{71})$mod4.

En effet, $3 \equiv -1$ mod4 et 17=1 mod4. Donc $(3^{343}.17^{71})$mod4=$(-1)^{343}$mod4.1mod4=-1mod4=3.

Ceci est également à la base de nombreux critères de divisibilité.

IV. Eléments inversibles dans $\mathbb{Z}_m$

1. *Conditions d'inversibilité*

Théorème :

> $\bar{x}$ est inversible dans $\mathbb{Z}_m \Leftrightarrow$ x et m sont **premiers**[2] entre eux.

Démonstration :

$\Rightarrow$ $\bar{x}$ est inversible dans $\mathbb{Z}_m \Leftrightarrow \exists\ \bar{y} \in \mathbb{Z}_m$; $\bar{x}.\bar{y}=\bar{1} \Leftrightarrow \overline{x.y}=1 \Leftrightarrow$ (x.y)modm=1 $\Leftrightarrow$

$\exists k \in \mathbb{Z}$: xy=km+1$\Leftrightarrow$ xy-km=1. $\Leftrightarrow$ x et m sont premiers entre eux.

$\Leftarrow$ Supposons que x et m soient premiers entre eux. D'après le théorème de Bézout[3], $\exists$ (a, b) $\in \mathbb{Z}^2$:ax+bm=1$\Rightarrow \overline{ax+bm}=\bar{1} \Leftrightarrow \overline{ax}+\overline{bm}=\bar{1} \Leftrightarrow \bar{a}.\bar{x}+\bar{b}.\bar{m}=\bar{1}$.

Or, $\bar{m}=\bar{0}$, donc, $\bar{a}.\bar{x}=\bar{1}$. Par définition, $\bar{x}$ est inversible dans $\mathbb{Z}_m$ et $\bar{a}$ est son inverse.

Exemple : Cherchons l'inverse mod299 de 367.

1) 367 est-il inversible mod299 ? Cherchons le PGCD (367,299)

$367 = 1.299 + 68$
$299 = 4.68 + 27$
$68 = 2.27 + 14$
$27 = 1.14 + 13$
$14 = 1.13 + 1$ => **dernier reste non nul = 1 = PGCD(367,299)**
$13 = 1.13 + 0$

⇨ Ces deux nombres (367 et 299) sont donc premiers entre eux. 367 est inversible mod299.

2) Cherchons l'inverse de 367 mod299. Calculons les coefficients de Bézout.

On reprend les équations de l'étape précédente dans l'ordre inverse…

(1) $14 = 1.13 + 1$
(2) $27 = 1.14 + 13$
(3) $68 = 2.27 + 14$
(4) $299 = 4.68 + 27$
(5) $367 = 1.299 + 68$

[2] Deux nombres a et b sont premiers entre eux ssi il existe u et v $\in \mathbb{Z}$ tels que au + bv = 1, soit PGCD(a,b)=1.

[3] Théorème de Bézout : « Si pgcd(a, b) = d, il existe deux entiers u et v $\in \mathbb{Z}$ tels que ua + vb = d. »

… et on élimine tous les restes des divisions ci-dessus en gardant 367 et 299.

(1) $14 = 1.13 + 1$ $(1) - (2)$ pour éliminer les 13.

(2) $27 = 1.14 + 13$

⇨ $(1')\ 14 - 27 = 1 - 1.14 \leftrightarrow -27 = 1 - 2.14$

(3) $68 = 2.27 + 14$ $(1') + 2.(3)$ pour éliminer les **14**

⇨ $(1'') - 27 + 2.68 = 1 + 4.27 \leftrightarrow 2.68 = 1 + 5.27$

(4) $299 = 4.68 + 27$ $(1'') - 5.(4)$ pour éliminer les **27**

⇨ $(1''')\ 2.68 - 5.299 = 1 - 20.68 \leftrightarrow -5.299 = 1 - 22.68$

(5) $367 = 1.299 + 68$ $(1''') + 22.(5)$ pour éliminer les **68**

⇨ $-5.299 + 22.367 = 1 + 22.299 \leftrightarrow$

$$22.367 - 27.299 = 1$$

En gras, les coefficients de Bézout (22 et -27) de 367 et 299. 22 est donc l'inverse de 367 mod299.

Nous pourrions aussi affirmer que -27 ≡ 299^{-1}mod367. 340 est donc l'inverse de 299 mod367.

2. Cas où m est premier

> Si m est un nombre premier, tous les éléments de $\mathbb{Z}_m$ ont un inverse pour la multiplication dans $\mathbb{Z}_m$.

Démonstration :

Sachant que m est un nombre premier, nous devons démontrer que $\forall\ \bar{x} \in \mathbb{Z}_m \backslash \{\bar{0}\}$, soit $\forall\ \bar{x} \in \{\bar{1}, \bar{2}, \ldots, \overline{m-1}\}$, $\bar{x}$ est inversible.

Or, si m est premier, $\bar{x}$ et m sont premiers entre eux. En effet, m étant premier, les seuls diviseurs de m sont m et 1. Or 0<$\bar{x}$<m. Donc le seul diviseur commun à $\bar{x}$ et m est 1.

Ayant préalablement démontré les propriétés de + et . dans $\mathbb{Z}_m$, nous pouvons affirmer que si m est premier, ($\mathbb{Z}_m$,+,.) est un champ.

3. Application utile en cryptographie

Nous utiliserons le modulo 29 ($\mathbb{Z}_{29}$) pour crypter. 29 (m) étant un nombre premier. Nous ajouterons donc les « , », «_» , « . » aux 26 lettres l'alphabet.

Dans les exemples présentés, nous utiliserons la table de codage suivante :

Table 1 : table de chiffrement

Lettre	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
Code	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Lettre	p	q	r	s	t	u	v	w	x	y	z	_	,	.	
Code	15	16	17	18	19	20	21	22	23	24	25	26	27	28	

Deuxième partie

Chiffrement par substitution monoalphabétique

I. Formule générale de codage

Dans ce système, chaque lettre de l'alphabet est transformée en une autre par substitution. Donc, une lettre du message clair correspond toujours à la même lettre (nombre), souvent différente, dans le message codé.

La substitution peut être décrite en termes de congruence au moyen d'une transformation affine.

Soit x, l'équivalent numérique d'une lettre de l'alphabet et c, l'équivalent numérique de la lettre codée correspondante.

Appelons $\sigma(x)$ la relation entre le message clair et le message codé. Nous pouvons écrire :

$$\sigma(x)=(ax+b) \bmod m.$$

où m=29 correspond au nombre de caractères de l'alphabet choisi. (cfr. *IV. Eléments inversibles dans $\mathbb{Z}_m$*).

Pour des raisons évidentes :

- $a, b \in \mathbb{N}$
- $a \neq 0$ (la valeur a=0 coderait toutes les lettres de la même façon)
- $0 \leq a, b < 29$ (nous travaillons en mod29)

Ayant choisi de travailler dans un alphabet de 29 caractères, il n'y a pas d'autres conditions[4] restrictives sur a et b. Nous avons donc dans l'absolu $29^2-29-1=$**811** possibilités de chiffrement (=B_{29}^2-*« cas où a=0 »- la transformation identique*). Cependant, nous pourrions imposer des conditions supplémentaires : que le chiffrement soit un dérangement : à chaque lettre correspondrait une lettre qui lui serait différente. Dans ce cas, toutes les valeurs de a et b ne pourraient pas convenir.

II. Cas particulier

Les valeurs particulières de (a,b)=(1,3) nous amène au chiffrement historique de César.

$$\sigma(x)=(x+3) \bmod m.$$

Jules César, qui à l'époque ne connaissait pas l'arithmétique modulaire, utilisait un système simple : chaque lettre de l'alphabet était remplacée par une lettre située trois rangs plus loin dans l'alphabet (A→D, B→E …). Aux dernières lettres de l'alphabet X, Y, Z correspondaient respectivement A, B, C.

Illustrons par un exemple simple en passant par les équivalents numériques pour notre alphabet (m=29).

Texte clair : **AVE CESAR**

[4] Pour un autre alphabet de m caractères, les conditions d'inversibilité dans $\mathbb{Z}_m$ imposeraient a premier avec m.

Texte clair	A	V	E		C	E	S	A	R
Equivalent num.	0	21	4	26	2	4	18	0	17
(x+3)mod29	3	24	7	0	5	7	21	3	20
Message codé	D	Y	H	A	F	H	V	D	U

Cryptogramme : **DYHAFHVDU**

Bien entendu, ce type de codage est suffisamment simple pour ne pas devoir passer par les équivalents numériques des lettres de l'alphabet.

III. Exemple de chiffrement

Soit le texte clair à crypter :

« ***Je ne suis pas intelligent, je suis incroyablement curieux.*** » (Einstein)

Pour cet exemple, nous avons choisi les valeurs a=2 et b=3. Par conséquent :

$\sigma(x)=c=(2x+3) \bmod 29$.

Message clair	Equivalent numérique	2x+3	(2x+3)mod 29	Cryptogramme
j	9	21	21	v
e	4	11	11	l
_	26	55	26	_
n	13	29	0	a
e	4	11	11	l
_	26	55	26	_
s	18	39	10	k
u	20	43	14	o
i	8	19	19	t
s	18	39	10	k
_	26	55	26	_
p	15	33	4	e
a	0	3	3	d
s	18	39	10	k
_	26	55	26	_
i	8	19	19	t
n	13	29	0	a
t	19	41	12	m
e	4	11	11	l
l	11	25	25	z
l	11	25	25	z

i	8	19	19	t
g	6	15	15	p
e	4	11	11	l
n	13	29	0	a
t	19	41	12	m
,	27	57	28	.
_	26	55	26	_
j	9	21	21	v
e	4	11	11	l
_	26	55	26	_
s	18	39	10	k
u	20	43	14	o
i	8	19	19	t
s	18	39	10	k
_	26	55	26	_
i	8	19	19	t
n	13	29	0	a
c	2	7	7	h
r	17	37	8	i
o	14	31	2	c
y	24	51	22	w
a	0	3	3	d
b	1	5	5	f
l	11	25	25	z
e	4	11	11	l
m	12	27	27	,
e	4	11	11	l
n	13	29	0	a
t	19	41	12	m
_	26	55	26	_
c	2	7	7	h
u	20	43	14	o
r	17	37	8	i
i	8	19	19	u
e	4	11	11	l
u	20	43	14	o
x	23	49	20	u

Cryptogramme :

vl_al_kotk_edk_tamlzztplam._vl_kotk_tahicwdfzl,lam_hoiulou

Nous constatons que la transformation affine opérée ne constitue pas un dérangement puisque l'espacement est son propre « transformé ». Cela peut constituer une faiblesse du système de cryptage : en effet, le découpage des mots a été conservé.

IV. Déchiffrement

Nous recevons le cryptogramme suivant :

zd_hoitcktml_lkm_oa_qtzdta_jlndom

Et avec ce message codé, nous avons la clé de codage a=2 et b=3.

Il suffit de retrouver la transformation affine réciproque.

Si $c=\sigma(x)= (a.x+b) \bmod 29$ alors $x=\sigma^{-1}(c)= a^{-1} (c-b) \bmod 29$

Il faut retrouver l'inverse de a en mod29. Ce qui est possible car a et 29 sont premiers.

Appliquons la recherche de σ^{-1} à notre exemple. **a=2**

Cherchons d'abord les coefficients de Bezout de 2 et 29 au moyen de l'algorithme d'Euclide :

$29=14.2+1$

$29-\mathbf{14}.2=1$ -14 => coefficient de Bézout

$2^{-1} \bmod 29 \equiv (-14) \bmod 29$ => $\mathbf{a^{-1}=15 mod 29}$

La transformation affine réciproque qui nous permettra de déchiffrer le cryptogramme est :

$\sigma^{-1}(c)= 15 (c-3) \bmod 29$

Cela donne :

Cryptogramme	Equivalent num.	15(c-3)	15 (c-3) mod 29	Texte clair
z	25	330	11	l
d	3	0	0	a
_	26	345	26	_
h	7	60	2	c
o	14	165	20	u
i	8	75	17	r
t	19	240	8	i
c	2	-15	14	o
k	10	105	18	s
t	19	240	8	i
m	12	135	19	t
l	11	120	4	e
_	26	345	26	_
l	11	120	4	e
k	10	105	18	s
m	12	135	19	t
_	26	345	26	_
o	14	165	20	u
a	0	-45	13	n

_	26	345	26	_
q	16	195	21	v
t	19	240	8	i
z	25	330	11	l
d	3	0	0	a
t	19	240	8	i
a	0	-45	13	n
_	26	345	26	_
j	9	90	3	d
l	11	120	4	e
n	13	150	5	f
d	3	0	0	a
o	14	165	20	u
m	12	135	19	t

Message clair déchiffré :

La curiosité est un vilain défaut

V. Cryptanalyse du chiffrement monoalphabétique

La cryptanalyse désigne l'ensemble des procédés pouvant être mis en œuvre pour percer à jour un texte codé, sans connaître à priori, la ou les clés de chiffrement et de déchiffrement.

Faisons l'hypothèse que le cryptanalyste sait que le mode de codage est une substitution monoalphabétique par transformation affine réalisée en mod29. Il lui suffit de découvrir les paramètres a et b ayant servi à composer la transformation.

En théorie, nous avons vu qu'il existait 811 transformations affines potentielles. Avec les moyens informatiques dont nous disposons aujourd'hui, il est théoriquement possible d'envisager chacune de ces transformations jusqu'à découvrir un texte à la syntaxe compréhensible. Néanmoins, ce travail reste fastidieux et il existe dans le cas des substitutions monoalphabétiques des techniques beaucoup plus rapides.

Nous avons choisi d'en présenter une parmi d'autres : l'analyse fréquentielle.

Admettons que nous ayons à décrypter le message suivant :

_e,ipjudlunm,mln,pb,ru_eub,kmoepn

Nous savons que les lettres de l'alphabet n'apparaissent pas avec la même fréquence dans une langue donnée. Certaines sont rares, d'autres plus fréquentes, en témoigne le jeu de Scrabble. C'est ainsi qu'en français, la lettre la plus fréquente est le E, suivi du S et du A. Et si on prend en compte l'espacement _, il précède en fréquence le E.

Avec un peu de chance, et si le message est suffisamment long, cet ordre « fréquentiel » va être suivi dans le cryptogramme.

Dans notre exemple, le caractère le plus fréquent est la virgule « , » qui apparaît cinq fois, suivie par le « m » et le « e » (3 fois). Remplaçons-les par des espaces « _ », des « e » et des« a ».

_e,ipjudlunm,mln,pb,ru_eub,kmoepn

_a ipjudlune eln pb ru_aub keoapn

Avec un minimum de connaissance de la langue française et de bon sens, on retrouve aisément le texte clair initial.

la ipjudlune eln pb rulaub keoapn

la ipjudsute est pb rulaub keoapt

la iujidsite est un vilain keoaut

la curiosité est un vilain défaut

Avec ce système, on peut retrouver également la transformation affine du chiffrement, c'est-à-dire le couple (a,b). Nous avons deux inconnues à trouver, il nous faut donc deux équations : deux correspondances.

Pour cela, passons aux équivalents numériques :

Cryptogramme	Equivalent numérique c	Texte clair	Equivalent numérique x
,	27	-	26
m	12	e	4

Les paramètres de codage a et b doivent vérifier les équations suivantes :

- $27=(a.26+b) \bmod 29$ (1)
- $12=(a.4+b) \bmod 29$ (2)

En utilisant les propriétés dans $\mathbb{Z}_{29}$, ces équations deviennent :

- $27=(a.26) \bmod 29 + b \bmod 29$ (1)
- $12=(a.4) \bmod 29 + b \bmod 29$ (2)

En soustrayant (2) de (1) :

- $15=(22a) \bmod 29$

Donc :

- $a=(22^{-1}.15) \bmod 29$

Cherchons l'inverse de 22 en mod29

$29=22.1+7$ (i)

$22=3.7+1$ (ii)

$22-3.29=-3.22+1$ (ii)-3.(i)

$\mathbf{4}.22-3.292=1$

$22^{-1} \bmod 29=4$

- $a=(4.15) \bmod 29 = \mathbf{2}$
- $b=(12-4.a) \bmod 29 = \mathbf{4}$

La transformation affine utilisée était donc $\sigma(x)= \mathbf{(2.x+4) \bmod 29}$

Cet exemple montre la fragilité du chiffrement monoalphabétique qui remplace toujours une lettre par la même lettre correspondante : une simple analyse statistique des fréquences permet de briser un cryptogramme quand on sait que celui-ci est le fruit d'une transformation affine monoalphabétique dans une langue connue. Pourtant, en raison de sa grande simplicité, ce type de chiffrement fut la technique de chiffrement la plus fréquemment utilisée durant le premier millénaire et fut encore employée par les officiers sudistes durant la guerre de Sécession et même par l'armée russe en 1915.

Troisième partie
Chiffrement par substitution polyalphabétique

La partie précédente a révélé que les codages monoalphabétiques résistent mal aux cryptanalystes, lesquels peuvent disposer de données sur les fréquences d'apparition des lettres d'une langue donnée. Pour pallier à cette faiblesse, d'autres systèmes de codage ont été développés, notamment pour éviter qu'une même lettre de l'alphabet soit toujours codée de la même façon. C'est le cas de la substitution polyalphabétique qui substitue à un bloc de lettres, un autre bloc de lettres de même longueur. Pour modéliser ce type de « codage par bloc », outre l'arithmétique modulaire, nous utiliserons le calcul matriciel.

La formule générale de la transformation affine appliquée sera alors

$$\mathcal{C} = (\mathcal{A}.\mathcal{M} + \mathcal{B}) \bmod 29, \quad \text{où}$$

- $\mathcal{C}$ est la matrice du message codé de genre [l x m]
- $\mathcal{A}$ est une matrice clé de genre [m x m]
- $\mathcal{B}$ est une matrice clé de genre [l x m]
- $\mathcal{M}$ est la matrice du message clair de genre [l x m]

Les dimensions des matrices dépendent de la longueur des blocs de textes traités. Par ailleurs, les opérations matricielles nous imposent des conditions sur le genre des matrices à utiliser pour les clés.

Ce mode de chiffrement nous étant apparu plus complexe, nous avons choisi de le présenter en deux parties pour mieux l'appréhender.

I. Chiffrement avec l'addition matricielle

Prenons un message clair à coder :

« IL_FAUT_DETRUIRE_CARTHAGE. »

Nous utilisons uniquement l'addition matricielle pour coder ce message. Ce qui revient à choisir

$$\mathcal{A} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$ la matrice identité,

et

$$\mathcal{C} = (\mathcal{M} + \mathcal{B}) \bmod 29, \quad \text{où}$$

Choisissons de travailler avec des blocs de 3 lettres. **Soit l = 3.**

Comment former la matrice du message clair, sachant qu'elle est composée de 3 lignes ?

Pour cela, nous allons découper le texte clair en blocs de 3 caractères :

« IL_/FAU/T_D/ETR/UIR/E_C/ART/HAG/E. »

Le dernier bloc contient moins de 3 lettres ; on lui ajoute donc des lettres qui ne sont pas susceptibles de brouiller le message comme X, A …

Nous choisissons « A » car il correspond à 0 et cela simplifiera les calculs :

« IL_/FAU/T_D/ETR/UIR/E_C/ART/HAG/E.A »

Nous avons donc la matrice du message clair : il suffit de transformer chaque lettre en son équivalent numérique et de remettre chaque chiffre dans la matrice du message clair à la bonne place : a_{11} est la première lettre du premier bloc, a_{12} la deuxième lettre du premier bloc, a_{13} …, a_{21} la première lettre du second bloc, … :

$$\mathcal{M} = \begin{pmatrix} 8 & 5 & 19 & 4 & 20 & 4 & 0 & 7 & 4 \\ 11 & 0 & 26 & 19 & 8 & 26 & 17 & 0 & 28 \\ 26 & 20 & 3 & 17 & 17 & 2 & 19 & 6 & 0 \end{pmatrix}$$

Nous obtenons une matrice 3x9.

Maintenant, occupons nous de la matrice clé :

Deux choix s'offrent à nous :

- Soit $\mathcal{B}$ est obtenue en dupliquant m fois une matrice de genre [3 x 1], appelée matrice clé, représentée par un mot de 3 lettres. C'est le principe de Vigenère[5]
- Soit $\mathcal{B}$: matrice de genre [3 x m] représentée par une phrase clé de même longueur que le message. Ce principe est celui découvert par Vernam[6]: c'est la technique du masque jetable.

Nous choisissons la méthode du chiffre de Vigenère avec comme clé le mot « KEY », soit une matrice [3x1] qu'on dupliquera 9 fois pour qu'elle soit du même genre que la matrice du message clair.

$$\mathcal{B} = \begin{pmatrix} 10 \\ 4 \\ 24 \end{pmatrix}$$ dupliqué 9 fois.

Pour trouver la matrice du message codé, il suffit maintenant d'appliquer l'addition matricielle :

$$\mathcal{C} = (\mathcal{M} + \mathcal{B}) \bmod 29$$

$$\mathcal{C} = \left(\begin{pmatrix} 8 & 5 & 19 & 4 & 20 & 4 & 0 & 7 & 4 \\ 11 & 0 & 26 & 19 & 8 & 26 & 17 & 0 & 28 \\ 26 & 20 & 3 & 17 & 17 & 2 & 19 & 6 & 0 \end{pmatrix} + \begin{pmatrix} 10 & 10 & 10 & 10 & 10 & 10 & 10 & 10 & 10 \\ 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 \\ 24 & 24 & 24 & 24 & 24 & 24 & 24 & 24 & 24 \end{pmatrix} \right) \bmod 29$$

Voici donc la matrice du message codé :

$$\mathcal{C} = \begin{pmatrix} 18 & 15 & 0 & 14 & 1 & 14 & 10 & 17 & 14 \\ 15 & 4 & 1 & 23 & 12 & 1 & 21 & 4 & 3 \\ 21 & 15 & 27 & 12 & 12 & 26 & 14 & 1 & 24 \end{pmatrix}$$

En le remettant en lettres, cela donne le cryptogramme :

« SPVPEPAB,OXMBMMOB_KVOREBODY »

[5] Au XVI^{ème} siècle, le diplomate français Blaise de Vigenère met au point un système de chiffrement qu'il qualifie d'indéchiffrable en changeant l'alphabet de substitution à chaque chiffrement de lettres. Ce système cryptographique permit de déjouer les attaques des cryptanalystes pendant près de trois siècles.

[6] Mis au point par Gilbert Vernam en 1917, ce chiffrement suppose de disposer d'une clé aussi longue que le texte à chiffrer, à usage unique, d'où le nom de « masque jetable ».

On constate que ce type de chiffrement est plus efficace puisque, par exemple, la lettre A est codée de différentes façons : d'abord, elle est transformée en E, puis en K, de nouveau en E et enfin en Y.

II. Déchiffrement par la soustraction matricielle :

Prenons un message crypté à décoder :

« MEMALYQIVOWOHH.AVPSX.JEY »

Pour cela, il suffit d'appliquer la soustraction matricielle :

$$\mathcal{M} = (\mathcal{C} - \mathcal{B}) \bmod 29$$

En supposant que nous soyons un destinataire « autorisé », nous disposons de la matrice clé de codage $\mathcal{B}$.

Construisons la matrice $\mathcal{C}$ du cryptogramme en recherchant les équivalents numériques des lettres employées :

$$\mathcal{C} = \begin{pmatrix} 12 & 0 & 16 & 14 & 7 & 0 & 18 & 9 \\ 4 & 11 & 8 & 22 & 7 & 21 & 23 & 4 \\ 12 & 24 & 21 & 14 & 28 & 15 & 28 & 24 \end{pmatrix}$$

La matrice clé est la même que celle utilisée plus tôt :

$$\mathcal{B} = \begin{pmatrix} 10 \\ 4 \\ 24 \end{pmatrix}$$ dupliqué 8 fois.

Pour trouver la matrice du message clair, il faut non pas additionner mais, cette fois, soustraire ces deux matrices :

$$\mathcal{M} = \left(\begin{pmatrix} 12 & 0 & 16 & 14 & 7 & 0 & 18 & 9 \\ 4 & 11 & 8 & 22 & 7 & 21 & 23 & 4 \\ 12 & 24 & 21 & 14 & 28 & 15 & 28 & 24 \end{pmatrix} - \begin{pmatrix} 10 & 10 & 10 & 10 & 10 & 10 & 10 & 10 \\ 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 \\ 24 & 24 & 24 & 24 & 24 & 24 & 24 & 24 \end{pmatrix} \right) \bmod 29$$

$$\mathcal{M} = \begin{pmatrix} 2 & 19 & 6 & 4 & 26 & 19 & 8 & 28 \\ 0 & 7 & 4 & 18 & 3 & 17 & 19 & 0 \\ 17 & 0 & 26 & 19 & 4 & 20 & 4 & 0 \end{pmatrix}$$

Remis en lettres, le message clair donne :

« CARTHAGE_EST_DETRUITE.AA »

Soit en langage normal :

« Carthage est *détruite*. »

III. Le codage par multiplication matricielle :

L'utilisation du produit matriciel pour coder un message est apparentée au chiffrement de Hill[7].

Nous allons coder la même phrase, avec le même découpage en blocs de 3 lettres :

« IL_FAUT_DETRUIRE_CARTHAGE. »

Mais cette fois, nous utilisons la multiplication matricielle pour chiffrer ce message :

$$\mathcal{C} = (\mathcal{A}.\mathcal{M}) \text{ mod29}$$

Considérons $\mathcal{A}$, matrice clé de genre [3 x 3] et $\mathcal{M}$ matrice du message clair de genre [3 x m] (ici m=9) obtenue en faisant correspondre chaque lettre de notre alphabet à son équivalent numérique (éventuellement complétée pour parvenir à 3x9 caractères).

$$\mathcal{M} = \begin{pmatrix} 8 & 5 & 19 & 4 & 20 & 4 & 0 & 7 & 4 \\ 11 & 0 & 26 & 19 & 8 & 26 & 17 & 0 & 28 \\ 26 & 20 & 3 & 17 & 17 & 2 & 19 & 6 & 0 \end{pmatrix}$$

Fixons pour $\mathcal{A}$, la matrice carrée suivante :

$$\mathcal{A} = \begin{pmatrix} 3 & 5 & 1 \\ 1 & 0 & 0 \\ 2 & 3 & 1 \end{pmatrix}$$

La matrice du message clair comporte de grands nombres, et puisque nous utilisons la multiplication matricielle, des grands nombres peuvent considérablement allonger les calculs.

Pour faciliter ces calculs, nous avons convenu de substituer à chaque nombre supérieur à 14 la valeur négative qui lui est congrue mod29.

Ex. : 20 => -9 car -9 est congru à 20mod29

Nous obtenons donc deux matrices formées de l'ensemble des entiers {-14, …, 14}, ou de l'ensemble $\mathbb{Z}_{29}$ transformé en {-14, -13,….14}

$$\mathcal{M} \text{ devient : } \begin{pmatrix} 8 & 5 & -10 & 4 & -9 & 4 & 0 & 7 & 4 \\ 11 & 0 & -3 & -10 & 8 & -3 & -12 & 0 & -1 \\ -3 & -9 & 3 & -12 & -12 & 2 & -10 & 6 & 0 \end{pmatrix}$$

Effectuons maintenant le produit matriciel :

$$\mathcal{A}.\mathcal{M} = \begin{pmatrix} 76 & 6 & -42 & -50 & 1 & -1 & -70 & 27 & 7 \\ 8 & 5 & -10 & 4 & -9 & 4 & 0 & 7 & 4 \\ 46 & 1 & -26 & -34 & -6 & 1 & -46 & 20 & 5 \end{pmatrix}$$

Il faut maintenant appliquer le mod29 à chaque élément et ainsi repasser de $\mathbb{Z}$ à $\mathbb{Z}_{29}$:

$$\mathcal{C} = \begin{pmatrix} 18 & 6 & 16 & 8 & 1 & 28 & 17 & 27 & 7 \\ 8 & 5 & 19 & 4 & 20 & 4 & 0 & 7 & 4 \\ 17 & 1 & 3 & 24 & 23 & 1 & 12 & 20 & 5 \end{pmatrix}$$

[7] Mis au point par Lester S. Hill en 1929.

Et enfin, remettre cette matrice en lettres :

« SIRGFBQTDIEYBUX.EBRAM,HUHEF »

IV. Déchiffrement par inversion matricielle :

Nous allons déchiffrer la phrase :

« XCVFTBGGVFEXK_HRTWHIT_.,»

En tant que destinataire autorisé, nous savons que

$$\mathcal{C} = (\mathcal{A}.\mathcal{M}) \text{ mod29}$$

et que

$$\mathcal{A} = \begin{pmatrix} 3 & 5 & 1 \\ 1 & 0 & 0 \\ 2 & 3 & 1 \end{pmatrix}$$

Pour retrouver le message clair d'origine, nous devrons effectuer la transformation réciproque suivante :

$$\mathcal{M} = (\mathcal{A}^{-1}.\mathcal{C}) \text{ mod29}$$

Commençons par construire $\mathcal{C}$, matrice du message codé, en utilisant les conventions précédentes :

$$\mathcal{C} = \begin{pmatrix} 23 & 5 & 6 & 5 & 10 & 17 & 7 & 26 \\ 2 & 19 & 6 & 4 & 26 & 19 & 8 & 28 \\ 21 & 1 & 21 & 23 & 7 & 22 & 19 & 27 \end{pmatrix}$$

devient par facilité

$$\mathcal{C} = \begin{pmatrix} -6 & 5 & 6 & 5 & 10 & -12 & 7 & -3 \\ 2 & -10 & 6 & 4 & -3 & -10 & 8 & -1 \\ -8 & 1 & -8 & -6 & 7 & -7 & -10 & -2 \end{pmatrix}$$

Recherchons l'inverse de la matrice $\mathcal{A}$, $\mathcal{A}^{-1}$. Nous devons pour cela nous assurer que $\mathcal{A}$ est de rang 3 ($dét A \neq 0$).

$$\mathcal{A} = \begin{pmatrix} 3 & 5 & 1 \\ 1 & 0 & 0 \\ 2 & 3 & 1 \end{pmatrix}$$

$$dét\ \mathcal{A} = \begin{vmatrix} 3 & 5 & 1 \\ 1 & 0 & 0 \\ 2 & 3 & 1 \end{vmatrix} = - \begin{vmatrix} 1 & 0 & 0 \\ 3 & 5 & 1 \\ 2 & 3 & 1 \end{vmatrix} = - \begin{vmatrix} 1 & 0 & 0 \\ 1 & 2 & 0 \\ 2 & 3 & 1 \end{vmatrix} = -2$$

$$\mathcal{A}^{-1} = \begin{pmatrix} 0 & -2 & 0 \\ -1 & 1 & 1 \\ 3 & 1 & -5 \end{pmatrix} .[(-2)^{-1}] \text{ mod29}$$

Or $[(-2)^{-1}]$ mod29 = $[(-2) \text{ mod29 }]^{-1}$ mod29 = (27^{-1}) mod29 = 14

$$\mathcal{A}^{-1} = \begin{pmatrix} 0 & -28 & 0 \\ -14 & 14 & 14 \\ 42 & 14 & -70 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 \\ -14 & 14 & 14 \\ 13 & 14 & -12 \end{pmatrix}$$

Nous sommes prêts à effectuer la transformation qui nous permettra de retrouver la matrice du message clair :

$$\mathcal{M} = (\mathcal{A}^{-1}.\mathcal{C}) \text{ mod29}$$

Effectuons d'abord le produit matriciel de $\mathcal{A}^{-1}.\mathcal{C}$:

$$\mathcal{A}^{-1}.\mathcal{C} = \begin{pmatrix} 2 & -10 & 6 & 4 & -3 & -10 & 8 & -1 \\ 0 & -196 & -112 & -98 & -84 & -70 & -126 & 0 \\ 46 & -87 & 258 & 193 & 4 & -212 & 323 & -29 \end{pmatrix}$$

On arrive à la matrice $\mathcal{M}$ remise dans l'ensemble $\mathbb{Z}_{29}$:

$$\mathcal{M} = \begin{pmatrix} 2 & 19 & 6 & 4 & 26 & 19 & 8 & 28 \\ 0 & 7 & 4 & 18 & 3 & 17 & 19 & 0 \\ 17 & 0 & 26 & 19 & 4 & 20 & 4 & 0 \end{pmatrix}$$

Lorsqu'on remet cette matrice dans l'alphabet usuel, cela donne le message :

« CARTHAGE_EST_DETRUITE.AA »

Soit en langage normal :

« Carthage est détruite. »

V. Quelques remarques sur les chiffrements polyalphabétiques

On peut, tout d'abord, tout chiffrer : en effet, tous les messages peuvent se présenter sous forme de matrice. Toutes les matrices de même genre peuvent être additionnées et on peut multiplier une matrice de chiffrement par n'importe qu'elle autre qui soit inversible.

Quant au déchiffrement, cela dépend de la méthode utilisée (3 possibles : addition seule (Vigenère ou Vernam), multiplication seule (Hill) ou encore la méthode Affine, c'est-à-dire les deux à la fois.)

Avec l'addition matricielle, la connaissance de la clé suffit pour pouvoir déchiffrer tout message codé. La soustraction matricielle ne requiert en effet aucune condition, de même que l'addition matricielle.

Avec la multiplication matricielle, par contre, quelques problèmes peuvent se poser si la clé n'est pas inversible. Deux cas de figure mènent à une clé non inversible :

-Soit le déterminant est congru à 0, et dans ce cas peu importe la classe dans laquelle on opère, la clé ne sera jamais inversible.

-Soit le déterminant n'est pas premier avec la classe dans laquelle on travaille Ainsi par exemple en travaillant avec l'alphabet usuel (26 caractères), un déterminant multiple de 2 ou de 13 ne serait pas inversible car non premier avec26. Par conséquent, l'inverse du déterminant de la matrice clé n'existant pas , la matrice clé n'est pas inversible. Mais en ce qui nous concerne, le problème ne se pose pas puisque nous travaillons avec 29 caractères, et que 29 est un nombre premier.

Avec la méthode Affine, les conditions restent les mêmes.

Parlons aussi du nombre de transformations possibles que présente le chiffrement polyalphabétique : il est en effet beaucoup plus élevé que pour le chiffrement mono alphabétique.

Par exemple, pour le chiffrement de Vigenère, ce nombre dépend de la longueur de la clé choisie. Dans notre cas, nous avons choisi une clé de longueur 3. Pour la première lettre, 29 choix s'offrent à nous. 29 autres pour la seconde lettre, et encore 29 pour la troisième lettre.

Cela nous donne : 29 x 29 x 29, soit 29^3 ou encore 24 389 transformations possibles auxquelles nous devons retirer la transformation identique (0,0,0).

Si nous souhaitons coder sur une base de 3 alphabets de substitution différents, avec obligation de transformation (0 non permis dans le triplet), il nous resterait encore 28x27x26= 19656 transformations possibles.

Dans le cas d'une clé plus longue, les possibilités se multiplient : 29^m-1, jusqu'au cas de Vernam ou la clé étant aussi longue que le message codé !

VI. Cryptanalyse du chiffrement polyalphabétique

Une méthode couramment utilisée dans les attaques des chiffrements poly-alphabétiques est l'attaque à texte clair connu. Son principe est assez simple : on suppose la présence dans le message clair d'un mot ou une partie de texte assez longue pour pouvoir en déduire son contenu et la clé. Bien entendu, il faut que ce texte clair soit plus long que le nombre de caractères composant la clé. On en alors tire des équations qui permettent d'abord de trouver la clé, puis de décoder le message de la manière classique.

Par exemple :

On suppose que ce message codé par un chiffrement de Hill avec une matrice clé de genre [2 x 2]

« AETEAOEYEGTGDDTHUHTP.F »

commence par le mot : ***« CARTHAGE »***.

On dispose donc du cryptogramme et une partie du message clair. Ainsi pouvons nous trouver la clé et l'appliquer ensuite au restant du message codé.

Ici, il ne s'agira pas d'inverser la clé trouvée puisque la clé que nous donneront les équations sera la clé de décodage, autrement dit l'inverse de la clé utilisée pour coder le message.

Dans l'équation :

$$\mathcal{M} = (\mathcal{A}.\mathcal{C}) \text{ mod29}$$

On connaît :

- Une partie de $\mathcal{M}$, matrice de genre [2 x 11] du message clair.
- $\mathcal{C}$, matrice de genre [2 x 11] du message codé.

On cherche :

- $\mathcal{A}$ matrice clé de genre [2 x 2]

On peut donc en déduire que :

$$\mathcal{A} = (\mathcal{M}.\mathcal{C}^{-1}) \text{ mod29}$$

Pour pouvoir inverser la matrice $\mathcal{C}$, il faut qu'elle soit carrée, autrement dit de genre [2 x 2] et qu'elle soit inversible (dét $\mathcal{C} \neq 0$).

Nous pouvons tenter l'opération en ne prenant que les 4 premiers caractères des messages codé et clair.

$$\mathcal{A} = (\mathcal{M}_{[2 \times 2]} . \mathcal{C}^{-1}_{[2 \times 2]}) \text{mod29}$$

Or en exprimant le texte clair connu et le cryptogramme en termes d'équivalents numériques dans $\mathbb{Z}_{29}$, nous obtenons:

$$\mathcal{M}_{[2 \times 2]} = \begin{pmatrix} 2 & 17 \\ 0 & 19 \end{pmatrix} \text{ et } \mathcal{C}_{[2 \times 2]} = \begin{pmatrix} 0 & 19 \\ 4 & 4 \end{pmatrix}$$

d'où, nous pouvons calculer $\mathcal{C}^{-1}_{[2 \times 2]}$.

$$\text{dét } \mathcal{C} = (-76) \text{ mod29} = 11$$

$$11^{-1} \text{ mod29} = 8$$

$$\mathcal{C}^{-1}_{[2 \times 2]} = \begin{pmatrix} 3 & -7 \\ -3 & 0 \end{pmatrix}$$

$$\mathcal{A} = \left[\begin{pmatrix} 2 & 17 \\ 0 & 19 \end{pmatrix} . \begin{pmatrix} 3 & -7 \\ -3 & 0 \end{pmatrix} \right] \text{mod29}$$

En écrivant la matrice recherchée avec des inconnues :

$$\mathcal{A} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

Nous en déduisons ces quatre équations :

- a = [2 . 3 + 17. (-3)]mod 29 = (6 – 51) mod 29 = (-45) mod29= **13**
- b = [2 . (-7) + 17 . 0]mod29 = (-14)mod29= **15**
- c = [0 . 3 + 19. (-3)]mod29 = (-57)mod29= **1**
- d = [0 . (-7) + 19. 0]mod29 = **0**

Voici donc la clé de déchiffrement :

$$\mathcal{A}' = \begin{pmatrix} 13 & 15 \\ 1 & 0 \end{pmatrix}$$

Ou, en utilisant la convention qui facilite nos calculs :

$$\mathcal{A}' = \begin{pmatrix} 13 & -14 \\ 1 & 0 \end{pmatrix}$$

Nous pouvons maintenant déchiffrer le message codé :

$$\mathcal{M} = (\mathcal{A}'.\mathcal{C}) \bmod 29$$

$$\mathcal{M} = \left[\begin{pmatrix} 13 & -14 \\ 1 & 0 \end{pmatrix}.\begin{pmatrix} 0 & -10 & 0 & 4 & 4 & -10 & 3 & -10 & -9 & -10 & -1 \\ 4 & 4 & 14 & -5 & 6 & 6 & 3 & 7 & 7 & -14 & 5 \end{pmatrix}\right]_{\bmod 29}$$

$$\mathcal{M} = \begin{pmatrix} -56 & -186 & -196 & 122 & -32 & -214 & -3 & -228 & -215 & 66 & -83 \\ 0 & -10 & 0 & 4 & 4 & -10 & 3 & -10 & -9 & -10 & -1 \end{pmatrix}$$

Ou encore, ramené dans l'ensemble $\mathbb{Z}_{29}$ de départ :

$$\mathcal{M} = \begin{pmatrix} 2 & 17 & 7 & 6 & 26 & 18 & 26 & 4 & 17 & 8 & 4 \\ 0 & 19 & 0 & 4 & 4 & 19 & 3 & 19 & 20 & 19 & 28 \end{pmatrix}$$

Voici donc le message clair décrypté grâce à l'attaque à texte clair :

« CARTHAGE_EST_DETRUITE. »

Ou en langage courant :

« Carthage est détruite. »

Si la matrice $\mathcal{C}_{[2 \times 2]}$ n'avait pas été inversible, nous aurions simplement décalé de quelques lettres le travail. C'est possible si le message clair connu est suffisamment long par rapport à la taille de la clé à découvrir.

La longueur de la clé peut donc sécuriser le message. En effet, plus celle-ci est longue, plus la partie du message clair connue doit être longue pour pouvoir trouver la clé. La difficulté est encore doublée si la transformation est affine : le nombre d'inconnues se multiplie !

La technique du masque jetable suit cette règle en proposant une clé aussi longue que le message en lui-même. Dans ce cas, seul la personne qui possède la clé de chiffrement peut déchiffrer le message. Mais c'est alors la transmission de la clé qui pose problème car sans la clé, le message est perdu !

Ainsi est souligné le grand dilemme de tous les cryptographes : trouver le bon équilibre entre longueur de la clé et sécurité face aux attaques.

Les différentes méthodes présentées dans ce travail donnent un aperçu de la cryptographie à clé secrète. Ce type de chiffrement connaît principalement deux faiblesses : la première est la relative facilité par laquelle l'attaque à texte clair connu permet de décrypter l'ensemble du code, la seconde réside dans l'échange de la clé, qui doit être connue par l'expéditeur et par le destinataire.

On utilise plutôt aujourd'hui la cryptographie à deux clés, dont l'une est publique et l'autre connue de l'expéditeur (ou destinataire) uniquement. Ce type de cryptographie utilise des transformations non linéaires plus complexes à décrypter.

Bibliographie

Noirfalise R. : *Arithmétique et Cryptographie*, Ed IREM de Clermont-Ferrand

Bergeron F. et Goupil A. : *(2006) La cryptographie de l'Antiquité à l'Internet,* Ed UQAM de Montréal

Dalang R et Chaabouni A. : *(2001) Algèbre linéaire, Aide-mémoire, exercices et applications,* Ed Presses polytechniques et universitaires romandes

Costantini G : *PGCD, PPCM dans ℤ. Théorème de Bezout. Applications.*

Cuaz M. : *Arithmétique,* Ed Lycée militaire de Saint-Cyr

Obaton V : *Mathématiques en Terminale S (Spécialité),* Site personnel de l'auteur. Page consultée en novembre 2008. http://vincent.obaton.free.fr/MathsLycee/TerminaleSpeS.htm#1

Müller D : *(dernière mise à jour le 21/01/09) Ars Cryptographica*, du Site Apprendre-en-ligne. Page consultée en octobre 2008. http://www.apprendre-en-ligne.net/crypto/menu/index.html