Arithmétique & Éléments de cryptanalyse

David Hébert
hebert.iut@gmail.com

2021

Table des matières

1. Avant de commencer

1.1 Introduction

La cryptographie est une science et un peu plus. Quelque part entre l'art et la guerre. "Art" parce que cette science use et abuse de technique magnifique (mathématiques). "Guerre" parce tout message est attaqué, torturé, malmené pour révéler ses secrets.

Définition 1.1.1

La **stéganographie** est l'art qui vise à *dissimuler* l'existence d'un message.

Remarque 1.1.2 : En 484 av. J.-C., Xerxès Ier, roi des Perses, décide de préparer une armée gigantesque pour envahir la Grèce. Quatre ans plus tard, lorsqu'il lance l'offensive, les Grecs sont depuis longtemps au courant de ses intentions. C'est que Démarate, ancien roi de Sparte réfugié auprès de Xerxès, a appris l'existence de ce projet et décide de transmettre l'information à Sparte :

> il prit une tablette double, en gratta la cire, puis écrivit sur le bois même les projets de Xerxès ; ensuite il recouvrit de cire son message : ainsi le porteur d'une tablette vierge ne risquait pas d'ennuis.

Remarque 1.1.3 : Histiée incite son gendre Aristagoras, gouverneur de Milet, à se révolter contre son roi, Darius, et pour ce faire,

> il fit raser la tête de son esclave le plus fidèle, lui tatoua son message sur le crâne et attendit que les cheveux eussent repoussé ; quand la chevelure fut redevenue normale, il fit partir l'esclave pour Milet.

Aujourd'hui encore on peut utiliser la stéganographie pour transmettre une information en modifiant subtilement les pixels d'une image par exemple.

Néanmoins la stéganographie à ses limites et il est vite apparut nécessaire de dissimuler l'information tout en la rendant visible ! C'est la cryptographie.

Définition 1.1.4

La **cryptographie** vise à transformer un message clair en un message chiffré de sorte que le message originel soit complètement incompréhensible.

Le message chiffré est appelé un **cryptogramme**.

Définition 1.1.5

La **cryptanalyse** est une science qui consiste à tenter de déchiffrer un message ayant été chiffré.

Le processus par lequel on tente de comprendre un message chiffré est appelé une **attaque**.

Définition 1.1.6

La **cryptologie** englobe la cryptographie et la cryptanalyse.

Dans ce cours, la cryptologie est "une excuse pour faire des mathématiques".

A chaque chapitre on introduit une méthode de chiffrement qui nécessite pour son indentation, sa compréhension et le déploiement de techniques d'attaques, l'introduction d'outils mathématiques.

Pour être tout à fait rigoureux il faudrait d'abord définir les outils mathématiques offrant le meilleur formalisation des cryptosystème. Nous pensons que nous gagnerons en clarté en se permettant quelques liberté avec la "Rigueur".

1.2 Quelques outils

Définition 1.2.1

- Le **chiffrement** ou **cryptage** est le processus de transformation d'un message clair de façon à le rendre incompréhensible.
- Le **déchiffrement** ou **décryptage** est le processus de reconstitution du message clair à partir du message chiffré.

Dans la pratique les processus de transformation et de reconstitution sont paramétrés par des fonctions elles-mêmes paramétrées par des clefs.

Définition 1.2.2

Un **système cryptographique** ou **cryptosystème** est constitué de

1. un **espace de clefs** $\mathcal{K}$,
2. une **fonction de chiffrement** et une **fonction de déchiffrement** paramétrées par les éléments de $\mathcal{K}$.

Ces données devant satisfaire la **propriété de déchiffrement** :

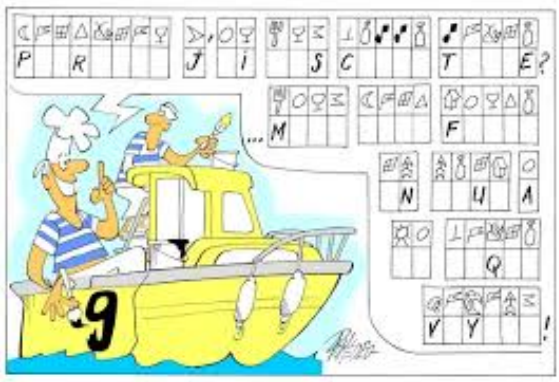
Pour $k \in \mathcal{K}$, notons C_k la fonction de chiffrement, D_k la fonction de déchiffrement (paramétrées par k) et M un message claire

$$\forall k \in \mathcal{K},\ \forall M,\ D_k\Big(C_k(M)\Big) = M$$

Remarque 1.2.3 : La propriété de déchiffrement se traduit par le fait que pour chaque "manière" de crypter il existe un moyen de décrypter pour retrouver le message original.

On prendra garde au vocabulaire. Nous parlerons majoritairement de (dé)cryptage ou (dé)chiffrement et en aucun cas de (dé)codage.

Pour faire simple, le codage est un dictionnaire d'échange : les lettres du message claire sont transformés en d'autre symbole comme ceux que l'on trouve dans les magazines pour enfants



Puisque nous voulons "*faire des opérations dans le texte*" nous utiliserons notre langage préféré : le nombre. Dans tout ce cours notre codage, c'est à dire notre langage de préférence, sera

A	B	C	D	E	F	G	H	I	J	K	L	M
00	01	02	03	04	05	06	07	08	09	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

2. La méthode de César

2.1 Principe

Nous voulons crypter le mot *BONJOUR*. La première étape, comme souvent avant de **crypter**, est de **coder** ce message. Dans notre cas, coder signifie transformer le message dans le langage des mathématiques par des associations triviales : A = 0, B = 1 etc.

B	O	N	J	O	U	R
1	14	13	9	14	20	17

Le mot *BONJOUR* est ainsi codé en *1-14-13-9-14-20-17*.

Le principe du codage de César consiste à modifier chaque caractère (du texte codé) en lui ajoutant un certain nombre ; par exemple 3.

B	O	N	J	O	U	R
1	14	13	9	14	20	17
4	17	16	12	17	23	20

Ainsi *BONJOUR* est crypté en *4-17-16-12-17-23-20*.

On peut ensuite **décoder** ce message par les associations inverses 0 = A, 1 = B etc.

B	O	N	J	O	U	R
1	14	13	9	14	20	17
4	17	16	12	17	23	20
E	R	Q	M	R	X	U

Le mot *BONJOUR* est crypté en *ERQMRXU*.

La clef de cryptage est le nombre utilisé pour le décalage ; dans notre exemple c'est le nombre 3.

Recommençons un exemple et cryptons le mot *ZAKARIA* avec 4 comme clef de cryptage.

Z	A	K	A	R	I	A
25	0	10	0	17	8	0
29	4	14	4	21	12	4
?	E	O	E	V	M	E

Problème : quelle est la lettre 29 ?

Solution : l'alphabet latin va de A = 0 à Z = 25, mais on peut revenir à A à partir de 26. Ainsi A = 26, B = 27, C = 28 et donc D = 29.

Ainsi le mot *ZAKARIA* est crypté en *DEOEVME*.

En fait $29 = 26 + 3$ et D = 3 donc D = 29. Puisque A = 0 et que A = 26, on aimerai dire que $26 = 0$ [1]. Nous allons donner un cadre à cette égalité : les congruences.

2.2 Le calcul modulaire

Théorème 2.2.1 (Division euclidienne)

$$\forall a \in \mathbb{Z},\ \forall b \in \mathbb{N}_{>0},\ \exists! q \in \mathbb{Z},\ \exists! r \in \mathbb{N},\quad \begin{cases} a = bq + r \\ 0 \leqslant r < b \end{cases}$$

On nomme a le **dividende**, b le **diviseur**, q le **quotient** et r le **reste**.

Démonstration.

Existence. Posons $q = E\left(\frac{a}{b}\right)$ la partie entière de la division réelle de a par b et $r = a - bq$. Par construction $a = bq + r$. De plus, par définition de la fonction partie entière, $q \leqslant \frac{a}{b} < q + 1$ soit en multipliant par b (que nous avons supposé positif) $bq \leqslant a < bq + b$ et en soustrayant finalement par bq on obtient $0 \leqslant a - bq < b$ et donc $0 \leqslant r < b$.

Unicité. Supposons que $a = bq + r$ et $a = bq' + r'$ avec $0 \leqslant r < b$ et $0 \leqslant r' < b$. Alors $bq + r = bq' + r'$ soit encore $b(q - q') = r' - r$ or $-b < r' - r < b$ soit $-b < b(q - q') < b$. En simplifiant par b : $-1 < q - q' < 1$. Or $q - q'$ est un nombre entier et le seul nombre entier strictement compris entre -1 et 1 est 0 d'où $q - q' = 0$ et donc $q = q'$. Pour finir $r = a - bq = a - bq' = r'$.

1. Oui ! Ca fait mal aux yeux.

□

Remarque 2.2.2 :

- $522 = 7 \times 74 + 4$ est la division euclidienne de 522 par 7 ; le quotient est 74 et le reste 4.
- $2015 = 7 \times 286 + 13$ n'est pas la division euclidienne de 2015 par 7 car ce qui jouerai le rôle du reste, à savoir 13 ne satisfait pas $0 \leqslant 13 < 7$.
- $2015 = 286 \times 7 + 13$ est la division euclidienne de 2015 par 286 ; le quotient est 7 et le reste 13.

Définition 2.2.3

Soient a et b des entiers, b étant non nul. On dira que

- b **divise** a
- a est **un multiple** de b
- b est **un diviseur** de a

noté $b \mid a$, si le reste de la division euclidienne de a par b est nul.

- Le nombre 666 divise 1998.
- Le nombre 522 est un multiple de 3.
- Le nombre 2 est un diviseur de 6.

Proposition 2.2.4

Soient a et b des entiers, b étant non nul. Le nombre b divise a si et seulement si il existe un entier k tel que $a = bk$.

Démonstration. D'après le théorème de la division euclidienne, il existe k et r tel que $a = bk + r$. Par définition de "a divise b", le reste est nul donc, $a = bk + 0 = bk$. □

Définition 2.2.5

Soient a, b et n des entiers relatifs tels que $n \geqslant 2$. On dira que a **est congru à** b **modulo** n si a et b ont le même reste dans leur division euclidienne par n. On note

$$a \equiv_n b$$

Proposition 2.2.6

Soient a, b et n des entiers relatifs tels que $n \geqslant 2$ tels que $a \equiv_n b$. Alors n divise $a - b$.

Démonstration. Par définition, puisque $a \equiv_n b$, il existe q, q' et r tel que $a = nq + r$ et $b = nq' + r$. En effectuant la différence de ces deux égalités, on obtient $a - b = nq - nq'$ soit encore en factorisant $a - b = n(q - q')$ ce qui prouve que $a - b$ est un multiple de n. □

Autrement dit : $a \equiv_n b$ si et seulement si il existe un $k \in \mathbb{Z}$ tel que $a - b = kn$.
Par exemple :

- $500 \equiv_{11} 5$ car $500 - 5 = 495 = 11 \times 45$.
- $6 \equiv_{123456} 6$ car $6 - 6 = 0 = 123456 \times 0$.
- $253 \equiv_7 1$ car $253 - 1 = 252 = 7 \times 36$.
- $-1 \equiv_2 1$ car $-1 - 1 = -2 = 2 \times (-1)$.

Théorème 2.2.7 (Opérations)

Soient a, b, α, β et n des entiers relatifs tels que $n \geqslant 2$.

$$(a \equiv_n \alpha) \wedge (b \equiv_n \beta) \Longrightarrow \begin{cases} \text{(i)} & a+b \equiv_n \alpha+\beta \\ \text{(ii)} & ab \equiv_n \alpha\beta \end{cases}$$

Démonstration. Par définition, il existe des entiers relatifs k_a et k_b tels que $a = \alpha + nk_a$ et $b = \beta + nk_b$

(i) $a+b = (\alpha+nk_a)+(\beta+nk_b) = \alpha+\beta+nk_a+nk_b = (\alpha+\beta)+n(k_a+k_b)$ ce qui traduit que $a+b \equiv_n \alpha+\beta$.

(ii) $a+b = (\alpha+nk_a)(\beta+nk_b) = \alpha\beta + nk_a\beta + nk_b\alpha + n^2k_ak_b = (\alpha\beta) + n(k_a\beta + k_b\alpha + nk_ak_b)$ ce qui traduit que $ab \equiv_n \alpha\beta$.

□

Corollaire 2.2.8

Soient a, b, n et k des entiers relatifs tels que $n \geqslant 2$ et $k \in \mathbb{N}$.

$$(a \equiv_n b) \Longrightarrow (a^k \equiv_n b^k)$$

Démonstration. On raisonne par récurrence sur $k \in \mathbb{N}$, la propriété étant triviale pour $k = 0$.

$$\begin{array}{lll} a^{k+1} & \equiv_n & a \times a^k \\ & \equiv_n & a \times b^k \qquad \text{par hypothèse de récurrence} \\ & \equiv_n & b \times b^k \qquad \text{car } a \equiv_n b \text{ ; en utilisant le théorème précédent} \\ & \equiv_n & b^{k+1} \end{array}$$

Ce qui achève la récurrence. □

- $25 \equiv_4 1$ et $10 \equiv_4 2$ donc $35 \equiv_4 3$
- $5 \equiv_3 2$ et $11 \equiv_3 -1$ donc $55 \equiv_3 -2$
- $10 \equiv_9 1$ donc $10^{2016} \equiv_9 1$

Corollaire 2.2.9

Soient a, b, c, α, β, γ et n des entiers relatifs tels que $n \geqslant 2$.

Commutativité. $a+b \equiv_n b+a$, $ab \equiv_n ba$

Associativité. $(a+b)+c \equiv_n a+(b+c)$, $(ab)c \equiv_n a(bc)$

Element neutre. $a+0 \equiv_n a$, $a1 \equiv_n a$

Symétrie. $a+(-a) \equiv_n 0$

Distributivité. $a(b+c) \equiv_n (ab)+(ac)$

Démonstration. Il suffit de revenir à la définition. □

Dans la pratique, lorsque l'on veut travailler modulo un entier n, on a tendance à choisir un représentant dans l'intervalle $[\![0; n-1]\!]$ [2] ce qui est toujours possible d'après le théorème de la division euclidienne.

2. L'intervalle noté $[\![a; b]\!]$ désigne l'ensemble des nombres entiers compris entre a et b

Proposition 2.2.10

Soient a et n des entiers relatifs tels que $n \geqslant 2$. Il existe un unique $\alpha \in [\![0; n-1]\!]$ tel que $a \equiv_n \alpha$.
On note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble $[\![0; n-1]\!]$ munis des opérations d'addition et de multiplication.

Démonstration. Ceci est une conséquence du théorème de la division euclidienne. □

Remarque 2.2.11 : Avec la "Rigueur" on peut construire $\mathbb{Z}/n\mathbb{Z}$ plus proprement comme le quotient de $\mathbb{Z}$ par une certaine relation d'équivalence. Nous n'approfondirons pas ce point de vue mais il faudra garder en tête que les "nombres" que l'on manipulent dans $\mathbb{Z}/n\mathbb{Z}$ sont en fait des ensembles. Par exemple dans $\mathbb{Z}/5\mathbb{Z}$, le nombre 1 cache en fait 1, 6, 11, 16 etc (de 5 en 5). C'est pour cela que l'on parle davantage de *représentant*.

Dans ce cas 6 existe dans $\mathbb{Z}/5\mathbb{Z}$, il est représenté par 1.

Remarque 2.2.12 : Lorsque l'on est amené a effectuer des opérations modulo n il peut être utile de dessiner les tables de multiplications et d'addition de $\mathbb{Z}/n\mathbb{Z}$. Par exemple si $n = 6$ on a

$+$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$\times$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

2.3 Cryptologie de César

Cryptosystème

Proposition 2.3.1

Soient n et k des entiers tels que $n \geqslant 2$.

$$\forall x \in \mathbb{Z},\ (x + k) - k \equiv_n x$$

Démonstration. Ceci est une conséquence triviale de l'associativité de la congruence. □

Définition 2.3.2

Les données suivantes définissent le cryptosystème de César.

Espace de clefs. $\mathcal{K} = \mathbb{Z}/26\mathbb{Z}$

Fonction de chiffrement. Quelque soit $k \in \mathcal{K}$ et $x \in \mathbb{Z}$, $C_k(x) \equiv_{26} x + k$

Fonction de déchiffrement. Quelque soit $k \in \mathcal{K}$ et $x \in \mathbb{Z}$, $D_k(x) \equiv_{26} x - k$

La proposition précédente justifie que la propriété de déchiffrement est satisfaite.

Remarque 2.3.3 : On aurait put définir l'espace de clefs par $\mathcal{K} = \mathbb{Z}$ mais, puisque les fonctions sont définies modulo 26, la clef 26 et la clef 0 donnent la même chose.

Si par exemple le message crypté est *RTTFIUVFE* avec 17 comme clef, on décrypte de la manière suivante.

R	T	T	F	I	U	V	F	E	
17	19	19	5	8	20	21	5	4	Codage (A = 0 , B = 1 , ...)
0	2	2	−12	−9	3	4	−12	−13	Fonction de déchiffrement $x - 17$
0	2	2	14	17	3	4	14	13	On se place dans $\mathbb{Z}/26\mathbb{Z}$
A	C	C	O	R	D	E	O	N	

Cryptanalyse

Une attaque **en force brute** permet en général de casser le cryptage par la méthode de César. Le principe d'une attaque en force brute consiste a essayer toutes les clefs.

Par exemple, nous savons qu'un message codé avec la méthode de César est *LEDVJJRXVUVTVJRI*. On teste toutes les clefs.

Clef	L	E	D	V	J	J	R	X	V	U	V	T	V	J	R	I
0	L	E	D	V	J	J	R	X	V	U	V	T	V	J	R	I
1	K	D	C	U	I	I	Q	W	U	T	U	S	U	I	Q	H
2	J	C	B	T	H	H	P	V	T	S	T	R	T	H	P	G
3	I	B	A	S	G	G	O	U	S	R	S	Q	S	G	O	F
4	H	A	Z	R	F	F	N	T	R	Q	R	P	R	F	N	E
5	G	Z	Y	Q	E	E	M	S	Q	P	Q	O	Q	E	M	D
6	F	Y	X	P	D	D	L	R	P	O	P	N	P	D	L	C
7	E	X	W	O	C	C	K	Q	O	N	O	M	O	C	K	B
8	D	W	V	N	B	B	J	P	N	M	N	L	N	B	J	A
9	C	V	U	M	A	A	I	O	M	L	M	K	M	A	I	Z
10	B	U	T	L	Z	Z	H	N	L	K	L	J	L	Z	H	Y
11	A	T	S	K	Y	Y	G	M	K	J	K	I	K	Y	G	X
12	Z	S	R	J	X	X	F	L	J	I	J	H	J	X	F	W

Clef	L	E	D	V	J	J	R	X	V	U	V	T	V	J	R	I
13	Y	R	Q	I	W	W	E	K	I	H	I	G	I	W	E	V
14	X	Q	P	H	V	V	D	J	H	G	H	F	H	V	D	U
15	W	P	O	G	U	U	C	I	G	F	G	E	G	U	C	T
16	V	O	N	F	T	T	B	H	F	E	F	D	F	T	B	S
17	U	N	M	E	S	S	A	G	E	D	E	C	E	S	A	R
18	T	M	L	D	R	R	Z	F	D	C	D	B	D	R	Z	Q
19	S	L	K	C	Q	Q	Y	E	C	B	C	A	C	Q	Y	P
20	R	K	J	B	P	P	X	D	B	A	B	Z	B	P	X	O
21	Q	J	I	A	O	O	W	C	A	Z	A	Y	A	O	W	N
22	P	I	H	Z	N	N	V	B	Z	Y	Z	X	Z	N	V	M
23	O	H	G	Y	M	M	U	A	Y	X	Y	W	Y	M	U	L
24	N	G	F	X	L	L	T	Z	X	W	X	V	X	L	T	K
25	M	F	E	W	K	K	S	Y	W	V	W	U	W	K	S	J

On voit apparaitre, pour la clef 17, un message de César.

Pour compliquer un peu

Au lieu de chiffrer lettre par lettre, on peut le faire par paquet de deux lettres. Supposons, par exemple, que nous souhaitons chiffrer *ONCOMPLIQUECESAR*.

On commence comme d'habitude par coder ce message.

O	N	C	O	M	P	L	I	Q	U	E	C	E	S	A	R
14	13	02	14	12	15	11	08	16	20	04	02	04	18	00	17

Attention, il est important de mettre les 0 devant les chiffres de 0 à 9 pour que l'on obtienne des nombres à 4 chiffres (avec éventuellement des 0 à gauche).

On forme des nombres à 4 chiffres.

O	N	C	O	M	P	L	I	Q	U	E	C	E	S	A	R
14	13	02	14	12	15	11	08	16	20	04	02	04	18	00	17
1413		214		1215		1108		1620		402		418		17	

Ainsi le codage de *ONCOMPLIQUECESAR* est 1413-214-1215-1108-1620-402-518-17 (on choisit de mettre des "-" entre les nombres).

On ajoute ensuite la clef. On prend 2016 comme clef.

O	N	C	O	M	P	L	I	Q	U	E	C	E	S	A	R
14	13	02	14	12	15	11	08	16	20	04	02	04	18	00	17
1413		214		1215		1108		1620		402		418		17	
3429		2230		3231		3124		3636		2418		2434		2033	

Ainsi le message chiffrer est 3429-2230-3231-3124-3636-2418-2434-2033. Bien sur on ne va pas (et surtout on ne peut pas) décoder ce message. Le message crypté est cette suite de nombre. On peut cependant simplifier cette expression. En effet, lorsque l'on chiffrait lettre par lettre on allait de $A = 0$ à $Z = 25$ c'est pour cette raison que l'on travaillait modulo 26. Dans cet exemple, on code par paquet de 2 ; c'est à dire que l'on va de $AA = 0000$ à $ZZ = 2525$. Certes il y a des nombres qui ne correspondent à aucune paire de lettre (comme 0999) mais le plus grand entier de ce système de chiffrement est 2525. On va donc travailler modulo 2526.

O	N	C	O	M	P	L	I	Q	U	E	C	E	S	A	R
14	13	02	14	12	15	11	08	16	20	04	02	04	18	00	17
1413		214		1215		1108		1620		402		418		17	
3429		2230		3231		3124		3636		2418		2434		2033	
903		2230		705		598		1110		2418		2434		2033	

Le chiffrement de César *ONCOMPLIQUECESAR* par paquet de 2 avec 2016 comme clef est 903-2230-705-598-1110-2418-2434-2033.

Ce que nous venons de faire par paquet de 2 peut aussi être fait par paquet de 3, 4 etc... Formalisons.

Définition 2.3.4

Soit $n \geqslant 1$ un entier. Posons $N = \left(\sum_{i=0}^{n-1} 25 \times 10^{2i}\right) + 1 = \underbrace{25...2525}_{n\times} + 1 = 25...2526$. Le **cryptosystème de César par paquet de n** est défini par les données suivantes.

Espace de clefs. $\mathcal{K} = \mathbb{Z}/N\mathbb{Z}$

Fonction de chiffrement. Quelque soit $k \in \mathcal{K}$ et $x \in \mathbb{Z}$, $C_k(x) \equiv_N x + k$

Fonction de déchiffrement. Quelque soit $k \in \mathcal{K}$ et $x \in \mathbb{Z}$, $D_k(x) \equiv_N x - k$

La propriété de déchiffrement est encore une conséquence de l'associativité.

Une attaque en force brute permet de casser la méthode de César par paquet de n. Par exemple le message suivant est codé avec la méthode de César : 212407-21819-132903-232903-31804-51801-82110-41002-41216-242518-42699. On va donc décrypter ce message pour toutes les clefs et nous afficherons le message claire lorsque nous reconnaitrons des lettres de l'alphabet (entre 0 et 25). Mais quel est le nombre de paquet ? Le message crypté contient des nombres tous plus petit que 242518. Ainsi l'entier N ne peut pas être 26 ou 2526. Le premier candidat est 252526^3 et donc le cryptage se fait par paquet de 3. Finalement 999 est la clef de cryptage.

212407			21819			132903			232903			31804			51801			82110			41002			41216			242518			42699		
211408			20820			131904			231904			30805			50802			81111			40003			40217			241519			41700		
21	14	08	02	08	20	13	19	04	23	19	04	03	08	05	05	08	02	08	11	11	04	00	03	04	02	17	24	15	19	04	17	00
V	O	I	C	I	U	N	T	E	X	T	E	D	I	F	F	I	C	I	L	L	E	A	D	E	C	R	Y	P	T	E	R	A

Et *VOICI UN TEXTE DIFFICILLE A DECRYPTER*[4]

3. "Premier candidat" car si nous n'arrivons pas à déchiffrer le message, on poursuivra avec le "second candidat" : 25252526. S'il ne fonctionne pas on essayera avec 2525252526 etc.

4. Avec une belle faute d'orthographe ! A noter qu'il manquait un caractère pour faire 11 paquets de 3. On a rajouté un caractère (en l'occurrence *A*) à la fin du texte.

3. La méthode affine

3.1 Principe

La fonction de chiffrement par la méthode affine est une généralisation de la méthode de César. Au lieu de prendre comme fonction de chiffrement une fonction *linéaire* de la forme $C(x) \equiv_{26} x + k$ on va considérer une fonction *affine* comme par exemple $C(x) \equiv_{26} 2x + 3$.

Chiffrons le message *BONJOUR*.

B	O	N	J	O	U	R
1	14	13	9	14	20	17
5	5	3	21	5	17	11
F	F	D	V	F	R	L

La première observation que nous pouvons faire est que la lettre B est cryptée en F et que la lettre O est également cryptée en F. Si nous recevons ce message comment pourrons-nous faire la différence entre le F qui est le cryptogramme de la lettre B et celui qui est le cryptogramme de la lettre O ?

Quelle est la fonction de déchiffrement ? Si nous travaillions avec nombres réels (on "oublie" le modulo 26), on vérifierai rapidement que la fonction $D(x) = \frac{1}{2}(x-3)$ satisfait la propriété de déchiffrement $D(C(x)) = x$. Quel est l'équivalent du $\frac{1}{2}$ modulo 26 ? Pour répondre à cette question nous allons avoir besoin de définir l'inverse modulaire.

3.2 L'inverse modulaire

Définition 3.2.1

Soit $a \in \mathbb{Z}$. On note $D(a)$ l'ensemble des diviseurs positifs de a.

$$D(a) = \left\{ x \in \mathbb{N} \middle| \; x \mid a \right\}$$

Par exemple $D(132) = \{1, 2, 3, 4, 6, 12, 11, 22, 33, 44, 66, 132\}$.

Proposition 3.2.2

Soient a et b deux diviseurs positifs d'un entier n tel que $n = ab$.

$$(a \leqslant \sqrt{n}) \; \vee \; (b \leqslant \sqrt{n})$$

Démonstration. Raisonnons par l'absurde. S'il existe deux diviseurs a et b de n tel que $a > \sqrt{n}$ et $b > \sqrt{n}$ alors $ab > \sqrt{n}^2 = n$ et $n > n$ ce qui est impossible. □

Dans la pratique, pour la recherche des diviseurs d'un entiers, on va chercher à le factoriser par des entiers allant de 1 jusqu'à sa racine carré (sa partie entière précisement).

Par exemple déterminons $D(108)$. Puisque $\sqrt{108} \simeq 10.3923$. On va chercher à factoriser 108 par des entiers entre 1 et 10.

$$\begin{aligned} 108 &= 1 \times 108 \\ &= 2 \times 54 \\ &= 3 \times 36 \\ &= 4 \times 27 \\ &= 6 \times 18 \\ &= 9 \times 12 \end{aligned}$$

Ainsi $D(108) = \{1, 2, 3, 4, 6, 9, 12, 18, 27, 36, 54, 108\}$.

Définition 3.2.3

Le **plus grand commun diviseur** entre deux entiers a et b, noté $\mathrm{PGCD}(a,b)$, est le plus grand entier de l'ensemble $D(a) \cap D(b)$.

Par exemple $\mathrm{PGCD}(132,108) = 12$ car $D(132) \cap D(108) = \{1,2,3,4,6,12\}$.

Lemme 3.2.4 : Soient a et b des entiers non nuls.

$$D\big(\mathrm{PGCD}(a,b)\big) = D(a) \cap D(b)$$

Démonstration. Ceci est une conséquence de la construction du PGCD. □

Théorème 3.2.5 Caractérisation du PGCD

Soient a, b et d des entiers non nuls.

$$\Big((d \mid a) \wedge (d \mid b)\Big) \iff \Big(d \mid \mathrm{PGCD}(a,b)\Big)$$

Démonstration. Il s'agit d'une reformulation du lemme précédent. □

Corollaire 3.2.6 Algorithme d'Euclide

Soit $a = bq + r$ une division euclidienne de deux entiers a et b.

$$\mathrm{PGCD}(a,b) = \mathrm{PGCD}(b,r)$$

Démonstration. Notons $d = \mathrm{PGCD}(a,b)$ et $d' = \mathrm{PGCD}(b,r)$.

Puisque d est un diviseur de a et b, il est nécessairement un diviseur de $r = a - bq$. Ainsi d est un diviseur de b et de r donc de leur PGCD à savoir d'.

De la même manière, puisque d' est un diviseur de b et r, c'est aussi un diviseur de $a = bq + r$. Ainsi d' est un diviseur de b et de a donc de leur PGCD à savoir d.

Nous venons de montrer que d est un diviseur de d' qui est lui même un diviseur de d. Nécessairement $d = d'$. □

Remarque 3.2.7 :

Dans la pratique, lorsque l'on veut déterminer le PGCD entre deux entiers, on va réaliser des divisions euclidiennes successives en remplaçant à chaque fois, dividende et diviseur par diviseur et reste jusqu'à obtenir un reste nul, ce qui sera toujours possible par la construction de $\mathbb{N}$ (toute partie non vide de $\mathbb{N}$ admet un plus petit élément). Le PGCD est le dernier reste non nul.

Pour ordonner les idées, on place ces données dans un tableau, chaque ligne représentant une division euclidienne $a = bq + r$.

a	b	r	q
132	108	24	1
108	24	$\boxed{12}$	4
24	12	0	2

Ainsi le PGCD est 12.

Définition 3.2.8

Soient a, b et n des entiers tels que $n \geqslant 2$. On dira que b **est l'inverse de** a **modulo** n si $ab \equiv_n 1$

Par exemple 3 est l'inverse de 7 modulo 20 car $7 \times 3 = 21 \equiv_{20} 1$.

La question naturelle est de savoir si tous les nombres modulaires ont un inverse et accessoirement comment le trouver.

Définition 3.2.9

On dira que deux entiers a et b sont **premiers entre eux** si $\mathrm{PGCD}(a, b) = 1$.

Par exemple 24 et 25 sont premiers entre eux.

Théorème 3.2.10 Identité de Bachet-Bézout

Deux entiers a et b sont premiers entre eux si et seulement si il existe $u \in \mathbb{Z}$ et $v \in \mathbb{Z}$ tel que $au + bv = 1$.

Démonstration. Si d est le PGCD de a et b alors puisque $au + bv = 1$, on en déduit que d est un diviseur de 1 et le seul diviseur positif de 1 est 1 et donc a et b sont premiers entre eux.

La réciproque se déduit de *l'algorithme d'Euclide étendue* que nous détaillerons par la suite. □

Corollaire 3.2.11

Soient a et n des entiers tels que $n \geqslant 2$. L'entier a admet un inverse modulo n si et seulement si a et n sont premiers entre eux.

Démonstration. D'après l'identité de Bachet-Bézout, les entiers a et n sont premiers entre eux si et seulement s'il existe $u \in \mathbb{Z}$ et $v \in \mathbb{Z}$ tel que $au + nv = 1$, ce qui équivaut à dire que $au \equiv_n 1$ (puisque $n \equiv_n 0$) et u est l'inverse modulaire de a. □

§3.2.12 :

Pour déterminer l'inverse modulaire d'un entier, on applique l'algorithme d'Euclide étendue. Détaillons un exemple et cherchons l'inverse de 382 modulo 2365. Pour que cela soit au moins possible, nous devons déterminer le PGCD de ces deux entiers. Appliquons l'algorithme d'Euclide.

a	b	r	q
2365	382	73	6
382	73	17	5
73	17	5	4
17	5	2	3
5	2	1	2
2	1	0	2

Puisque le dernier reste non nul est 1, on en déduit que 2365 et 382 sont premiers entre eux. D'après le corollaire précédent, il existe un inverse modulaire. Pour le trouver, il faut déterminer u et v tels que $2365u + 382v = 1$. Pur cela nous allons rajouter au tableau de l'algorithme d'Euclide deux colonnes u et v.

On va remplir ce tableau par le bas en initialisant u et v par des valeurs évidentes 0 et 1 respectivement. On peut vérifier, qu'à cette dernière ligne, on a bien $au + bv = 1$ ($2 \times 0 + 1 \times 1 = 1$).

a	b	r	q	u	v
2365	382	73	6		
382	73	17	5		
73	17	5	4		
17	5	2	3		
5	2	1	2		
2	1	0	2	0	1

On va remplir la ligne du dessus. On va mettre la valeur de v dans la nouvelle case de u.

a	b	r	q	u	v
2365	382	73	6		
382	73	17	5		
73	17	5	4		
17	5	2	3		
5	2	1	2	1	-2
2	1	0	2	0	1

Pour la nouvelle valeur de v on va mettre $-q \times \underset{\text{NEW}}{u} + \underset{\text{OLD}}{u}$ où $\underset{\text{NEW}}{u}$ représente le nouveau u (ici 1) et $\underset{\text{OLD}}{u}$ l'ancienne valeur (ici 0).

On recommence : à la ligne de dessus, on place l'ancienne valeur de v comme nouvelle valeur de u et pour la nouvelle valeur de u le résultat de $-q \times \underset{\text{NEW}}{u} + \underset{\text{OLD}}{u}$. Ici $\underset{\text{NEW}}{u} = -2$ et $\underset{\text{OLD}}{u} = 1$.

a	b	r	q	u	v
2365	382	73	6		
382	73	17	5		
73	17	5	4		
17	5	2	3	-2	7
5	2	1	2	1	-2
2	1	0	2	0	1

On peut vérifier qu'à chaque ligne $au + bv = 1$ (par exemple, notre dernier calcul permet d'aboutir à $17 \times (-2) + 5 \times 7 = 1$).

On réitère pour aboutir à :

a	b	r	q	u	v
2365	382	73	6	157	-972
382	73	17	5	-30	157
73	17	5	4	7	-30
17	5	2	3	-2	7
5	2	1	2	1	-2
2	1	0	2	0	1

Nous avons donc trouvé : $2365 \times 157 + 382 \times (-972) = 1$.

Pour finir (la question de départ était de trouver l'inverse de 382 modulo 2365), regardons cette égalité modulo 2365 (on rappel que $2365 \equiv_{2365} 0$) : $382 \times (-972) \equiv_{2365} 1$ et -972 est l'inverse modulaire de 382. On peut choisir un représentant positif : $-972 \equiv_{2365} -972 + 2365 = 1393$ et on peut donc conclure que l'inverse de 382 modulo 2365 est 1393.

Définition 3.2.13

Soit n un entier supérieur ou égal à 2. On note $(\mathbb{Z}/n\mathbb{Z})^\times$ l'ensemble des éléments de $\mathbb{Z}/n\mathbb{Z}$ qui admette un inverse modulaire.

De manière équivalente (d'après l'identité de Bachet-Bézout), les éléments inversibles de $(\mathbb{Z}/n\mathbb{Z})^\times$ sont les éléments de $\mathbb{Z}/n\mathbb{Z}$ premiers avec n.

On peut repérer les inverses modulaires dans la table de multiplication[5]. Prenons par exemple $n = 6$.

$\times$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

En détectant les 1, on identifie les éléments inversibles. $1 \times 1 \equiv_6 1$ et $5 \times 5 \equiv_6 1$. Les seuls éléments inversibles modulo 6 sont 1 et 5 qui sont par le même occasion, les seuls éléments de $\mathbb{Z}/6\mathbb{Z}$ premiers avec 6.

On peut alors grossièrement écrire $(\mathbb{Z}/n\mathbb{Z})^\times = \{1, 5\}$.

5. Si l'entier n n'est pas trop grand ! A ne pas faire pour $n = 2365$!

3.3 Digression : équations modulaires

Équations diophantiennes

Définition 3.3.1

Une **équation diophantienne** est une équation polynomiale à une ou plusieurs inconnues dont les solutions sont cherchées parmi les nombres entiers.

Nous nous intéressons aux équations linéaire de degrés 1, c'est à dire de la forme $ax+by=c$. L'identité de Bachet-Bézout, l'algorithme d'Euclide étendu et le lemme de Gauss sont les ingrédients de sa résolution.

Lemme 3.3.2 : (Gauss) Soient a, b et c des entiers.

$$\Big(a|bc \wedge \text{PGCD}(a,b)=1\Big) \Rightarrow a|c$$

Démonstration. Par définition $a|bc$ se traduit par l'existence d'un entier k tel que $bc=ak$. L'identité de Bachet-Bézout permet de trouver u et v tel que $au+bv=1$ ce qui donne en multipliant par c, $acu+bcv=c$ soit encore $acu+akv=c$. Le terme de gauche est multiple de a donc c est multiple de a. □

Théorème 3.3.3 Résolution des équations diophantiennes linéaire d'ordre 1

Considérons l'équation diophantienne d'inconnues x et y

$$ax+by=c$$

Notons $d=\text{PGCD}(a,b)$, $a'=\dfrac{a}{d}$, $b'=\dfrac{b}{d}$ et $(u,v)\in\mathbb{Z}^2$ tel que $a'u+b'v=1$, ce qui est possible puisque a' et b' sont premiers entre eux.

- Si c ne divise pas d alors il n'existe aucune solution entière.
- Si $d|c$, notons $c'=\dfrac{c}{d}$. Toutes les solutions entières sont de la forme

$$\begin{aligned} x &= c'u-b'k \\ y &= c'v+a'k \end{aligned}$$

pour $k\in\mathbb{Z}$.

Démonstration. Vérifions tout d'abord que les données sont solutions.

$$\begin{aligned} ax+by &= da'(c'u-b'k)+db'(c'v+a'k) \\ &= da'c'u-da'b'k+db'c'v+db'a'k \\ &= da'c'u+db'c'v \\ &= dc'(a'u+b'v) \\ &= c \end{aligned}$$

Réciproquement. En simplifiant par d, l'équation donne $a'x+b'y=c'$ où a' et b' sont premiers entre eux. L'identité de Bachet-Bézout permet de trouver u et v tel que $a'u+b'v=1$. En multipliant cette égalité par c' on arrive à $a'(c'u)+b'(c'v)=c'$ ce qui implique que $a'(x-c'u)+b'(y-c'v)=0$. Cette égalité nous informe qu $a'|b'(y-c'v)$ mais puisque a' et b' sont premier entre eux, le lemme de Gauss permet d'affirmer que $a'|(y-c'v)$. C'est à dire qu'il existe $k\in\mathbb{Z}$ tel que $y-c'v=a'k$ c'est à dire $y=c'v+a'k$. En substituant cette valeur de y dans $a'(x-c'u)+b'(y-c'v)=0$ on trouve que $x=c'u-b'k$. □

Par exemple $6x+4y=19$ n'admet pas de solution entière.
Autre exemple, $6x+4y=18$ admet des solutions entières de la forme

$$\begin{aligned} x &= 9 + 2k \\ y &= -9 - 3k \end{aligned}$$

pour $k \in \mathbb{Z}$.

Lemme chinois

On s'intéresse à résoudre des systèmes d'équations modulaires de la forme

$$\begin{cases} x \equiv_n a \\ x \equiv_m b \end{cases}$$

L'outil fondamentale est le lemme chinois.

Théorème 3.3.4 Lemme chinois

Soient n et m deux entiers premiers entre eux.

$$\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} = \mathbb{Z}/nm\mathbb{Z}$$

Démonstration. Considérons l'application bien définie suivante

$$\begin{aligned} \varphi : \mathbb{Z}/nm\mathbb{Z} &\longrightarrow \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \\ x &\longmapsto (x_n, x_m) \end{aligned}$$

où x_n représente x modulo n et x_m modulo m.

Pour prouver le théorème il faut prouver que ce morphisme est une bijection, ce qui se résume à trouver l'application inverse. Si on se donne $(a, b) \in \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ on cherche un $x \in \mathbb{Z}/nm\mathbb{Z}$ tel que $x_n \equiv_n a$ et $x_m \equiv_m b$.

D'après l'identité de Bachet-Bézout, puisque n et m sont premiers entre eux, il existe u et v dans $\mathbb{Z}$ tel que $nu + mv = 1$. En particulier $mv \equiv_n 1$ et $nu \equiv_m 1$. On pose alors $x \equiv_{nm} nub + mva$. On observe alors que $x \equiv_n \underbrace{nub}_{\equiv_n 0} + \underbrace{mv}_{\equiv_n 1} a \equiv_n a$. De même $x \equiv_m \underbrace{nu}_{\equiv_m 1} b + \underbrace{mva}_{\equiv_m 0} \equiv_m b$. □

Corollaire 3.3.5

Soient n et m des entiers premiers entre eux et a et b dans $\mathbb{Z}$. Soient $(u, v) \in \mathbb{Z}^2$ une solution de l'équation diophantienne $nx + my = 1$.

$$\begin{cases} x \equiv_n a \\ x \equiv_m b \end{cases} \iff x \equiv_{nm} nub + mva$$

Considérons par exemple le système $\begin{cases} x \equiv_3 1 \\ x \equiv_4 2 \end{cases}$ Sans besoin d'appliquer l'algorithme d'Euclide étendu, on observe que 3 et 4 sont premiers entre eux et $3 \times (-1) + 4 \times (1) = 1$. Alors les solutions de ce système sont de la forme $x \equiv_{12} 3 \times (-1) \times 2 + 4 \times (1) \times 1 \equiv_{12} -2 \equiv_{12} 10$.

Ainsi toutes les solutions sont de la forme $x = 10 + 12k$ pour $k \in \mathbb{Z}$.

3.4 Cryptologie affine

Cryptosystème

Proposition 3.4.1

Soit a, b et n des entiers tel que $n \geqslant 2$ et $\mathrm{PGCD}(a,n) = 1$. Notons a^{-1} l'inverse de a modulo n

$$\forall x \in \mathbb{Z},\ a^{-1}\big((ax+b)-b\big) \equiv_n x$$

Démonstration. Cela est une conséquence de la distributivité. □

Définition 3.4.2

Les données suivantes définissent le **cryptosystème affine**.

Espace des clefs. $\mathcal{K} = (\mathbb{Z}/26\mathbb{Z})^\times \times (\mathbb{Z}/26\mathbb{Z})$

Fonction de chiffrement. Quelque soit $(a,b) \in \mathcal{K}$ et $x \in \mathbb{Z}$, $C_{(a,b)}(x) \equiv_{26} ax+b$.

Fonction de déchiffrement. Quelque soit $(a,b) \in \mathcal{K}$ et $x \in \mathbb{Z}$, $D_{(a,b)}(x) \equiv_{26} a^{-1}(x-b)$ où a^{-1} désigne l'inverse de a modulo 26.

La proposition précédente justifie que la propriété de déchiffrement est satisfaite.

Dans l'exemple d'introduction de ce chapitre nous avions crypté le message *BONJOUR* avec $2x+3$ comme fonction de chiffrement. Nous avions obtenue le message *FFDVFRL* et nous avions d'ailleurs remarqué qu'il allait être difficile de distinguer le *F* qui est un *B* du *F* qui est un *O*. En fait la méthode de chiffrement utilisée n'est pas bonne car 2 n'est pas inversible modulo 26 (car $\mathrm{PGCD}(26,2) = 2$).

Le message suivant est chiffré par la méthode affine avec $(3,2)$ comme clef (cette clef est valide puisque 3 est premier avec 26 et admet donc un inverse modulaire) : *NSAIAKPMOEECUOCRRAPO*.

Pour déchiffrer ce message, déterminons l'inverse modulaire de 3.

a	b	r	q	u	v
26	3	2	8	−1	9
3	2	1	1	1	−1
2	1	0	2	0	1

Ainsi, $26 \times (-1) + 3 \times 9 = 1$. En regardant cette égalité modulo 26, on arrive à $3 \times 9 \equiv_{26} 1$ et 9 est l'inverse modulaire de 3. La fonction de déchiffrement est alors $D_{(3,2)}(x) \equiv_{26} 9(x-2)$. Déchiffrons le message.

	N	S	A	I	A	K	P	M	O	E	E	C	U	O	C	R	R	A	P	O
	13	18	0	8	0	10	15	12	14	4	4	2	20	14	2	17	17	0	15	14
−2	11	16	−2	6	−2	8	13	10	12	2	2	0	18	12	0	15	15	−2	13	12
×9	99	144	−18	54	−18	72	117	90	108	18	18	0	162	108	0	135	135	−18	117	108
$\equiv_{26}$	21	14	8	2	8	20	13	12	4	18	18	0	6	4	0	5	5	8	13	4
	V	O	I	C	I	U	N	M	E	S	S	A	G	E	A	F	F	I	N	E

Et *VOICI UN MESSAGE AFFINE*

Cryptanalyse

Dans le cas de la méthode affine, une attaque en force brute permet en général de casser le message crypté. On peut montrer qu'il y a 12 éléments de $\mathbb{Z}/26\mathbb{Z}$ qui sont inversibles. La cardinalité de l'espace des clefs pour la méthode affine est donc de $12 \times 26 = 312$. C'est un nombre important sur le papier mais dérisoire du point de vu de l'informatique.

Voici un exemple (nous ne présentons pas les 312 clefs possibles). Le message reçu est *TNCYGA*.

(a,b)	a^{-1}						
$(17,0)$	23	V	N	U	G	I	A
$(17,1)$	23	Y	Q	X	J	L	D
$(17,2)$	23	B	T	A	M	O	G
$(17,3)$	23	E	W	D	P	R	J
$(17,4)$	23	H	Z	G	S	U	M
$(17,5)$	23	K	C	J	V	X	P
$(17,6)$	23	N	F	M	Y	A	S
$(17,7)$	23	Q	I	P	B	D	V
$(17,8)$	23	T	L	S	E	G	Y
$(17,9)$	23	W	O	V	H	J	B
$(17,10)$	23	Z	R	Y	K	M	E
$(17,11)$	23	C	U	B	N	P	H
$(17,12)$	23	F	X	E	Q	S	K
$(17,13)$	23	I	A	H	T	V	N
$(17,14)$	23	L	D	K	W	Y	Q
$(17,15)$	23	O	G	N	Z	B	T
$(17,16)$	23	R	J	Q	C	E	W
$(17,17)$	23	U	M	T	F	H	Z
$(17,18)$	23	X	P	W	I	K	C
$(17,19)$	23	A	S	Z	L	N	F
$(17,20)$	23	D	V	C	O	Q	I
$(17,21)$	23	G	Y	F	R	T	L
$(17,22)$	23	J	B	I	U	W	O
$(17,23)$	23	M	E	L	X	Z	R
$(17,24)$	23	P	H	O	A	C	U
$(17,25)$	23	S	K	R	D	F	X

(a,b)	a^{-1}						
$(19,0)$	11	B	N	W	E	O	A
$(19,1)$	11	Q	C	L	T	D	P
$(19,2)$	11	F	R	A	I	S	E
$(19,3)$	11	U	G	P	X	H	T
$(19,4)$	11	J	V	E	M	W	I
$(19,5)$	11	Y	K	T	B	L	X
$(19,6)$	11	N	Z	I	Q	A	M
$(19,7)$	11	C	O	X	F	P	B
$(19,8)$	11	R	D	M	U	E	Q
$(19,9)$	11	G	S	B	J	T	F
$(19,10)$	11	V	H	Q	Y	I	U
$(19,11)$	11	K	W	F	N	X	J
$(19,12)$	11	Z	L	U	C	M	Y
$(19,13)$	11	O	A	J	R	B	N
$(19,14)$	11	D	P	Y	G	Q	C
$(19,15)$	11	S	E	N	V	F	R
$(19,16)$	11	H	T	C	K	U	G
$(19,17)$	11	W	I	R	Z	J	V
$(19,18)$	11	L	X	G	O	Y	K
$(19,19)$	11	A	M	V	D	N	Z
$(19,20)$	11	P	B	K	S	C	O
$(19,21)$	11	E	Q	Z	H	R	D
$(19,22)$	11	T	F	O	W	G	S
$(19,23)$	11	I	U	D	L	V	H
$(19,24)$	11	X	J	S	A	K	W
$(19,25)$	11	M	Y	H	P	Z	L

Et on gagne une bonne chose avec la fonction de chiffrement $19x+2$ qui admet $11(x-2)$ comme fonction de déchiffrement.

Pour compliquer un peu

Exactement de la même manière que pour la méthode de César, on peut raisonner en paquet.

Définition 3.4.3

Soit $n \geqslant 1$ un entier. Posons $N = \left(\sum_{i=0}^{n-1} 25 \times 10^{2i}\right) + 1 = \underbrace{25\ldots2525}_{n\times} + 1 = 25\ldots2526$. Le **cryptosystème affine par paquet de n** est défini par les données suivantes.

Espace de clefs. $\mathcal{K} = \left(\mathbb{Z}/N\mathbb{Z}\right)^{\times} \times \left(\mathbb{Z}/N\mathbb{Z}\right)$

Fonction de chiffrement. Quelque soit $(a,b) \in \mathcal{K}$ et $x \in \mathbb{Z}$, $C_{(a,b)}(x) \equiv_N ax+b$

Fonction de déchiffrement. Quelque soit $(a,b) \in \mathcal{K}$ et $x \in \mathbb{Z}$, $D_{(a,b)}(x) \equiv_N a^{-1}(x-b)$ où a^{-1} désigne l'inverse de a modulo N.

Considérons par exemple, la clef $(2017, 123)$. Il faut d'abord s'assurer que 2017 est bien inversible modulo 2526. Pour ce faire, on applique l'algorithme d'Euclide étendu.

a	b	r	q	u	v
2526	2017	509	1	531	−665
2017	509	490	3	−134	531
509	490	19	1	129	−134
490	19	15	25	−5	129
19	15	4	1	4	−5
15	4	3	3	−1	4
4	3	1	1	1	−1
3	1	0	3	0	1

Ainsi $2526 \times 531 + 2017 \times (-665) = 1$. En regardant cette égalité modulo 2526, on arrive à $2017 \times (-665) \equiv_{2526} 1$ et $-665 \equiv_{2526} 1861$ est l'inverse de 2017 modulo 2526.

Ceci prouve que $(2017, 123)$ est bien une clef du cryptosystème affine. On obtient de plus que la fonction de déchiffrement est $D_{(2017,123)}(x) \equiv_{2526} 1861(x - 123)$.

Déchiffrons le message *701-211-1485-2369-1306-1215-852-816-861* obtenu en appliquant la méthode affine par paquet de 2 avec $(2017, 123)$ comme clef.

Message chiffré	701		211		1485		2369		1306		1215		852		816		861	
Déchiffrement	2108		2104		1104		1802		1417		1308		207		1413		1800	
Paquettage	21	08	21	04	11	04	18	02	14	17	13	08	02	07	14	13	18	00
Décodage	V	I	V	E	L	E	S	C	O	R	N	I	C	H	O	N	S	A

4. La substitution

4.1 Principe

Comme nous l'avons vu le principe la méthode affine est un cas particulier de la méthode de César (en effet une clef affine de la forme $(1, k)$ donne le même cryptogramme qu'un message chiffré obtenu par la méthode de César de clef k). Il existe un moyen de généraliser davantage ces méthodes. Considérons par exemple un chiffrement affine de taille 1 de clef $(3, 2)$. Alors

La lettre	A	B	C	D	E	F	G	H	I	J	K	L	M
est transformée en	C	F	I	L	O	R	U	X	A	D	G	J	M

La lettre	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
est transformée en	P	S	V	Y	B	E	H	K	N	Q	T	W	Z

On observe que chaque lettre est remplacée par une autre (cela ne pouvait pas être autrement par construction du cryptosystème affine). On pourrait prendre le problème à l'envers et proposer un melange, comme par exemple

La lettre	A	B	C	D	E	F	G	H	I	J	K	L	M
est transformée en	A	Z	E	R	T	Y	U	I	O	P	Q	S	D

La lettre	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
est transformée en	F	G	H	J	K	L	M	W	X	C	V	B	N

Ce mélange provient-il d'une fonction affine $C(x) \equiv_{26} ax + b$?

Si c'était le cas, le fait que le A reste identique nous indique que $C(0) \equiv_{26} 0$ soit $a \times 0 + b \equiv_{26} 0$. Ainsi, on a $b \equiv_{26} 0$. En observant la transformation du B en Z, on arrive à l'équation $a \times 1 \equiv_{26} 25$ et donc $a \equiv_{26} 25$. Finalement, la fonction affine correspondant à ce mélange ne peut-être que $C(x) \equiv_{26} 25x$.

Mais $C(2) \equiv_{26} 25 \times 2 \equiv_{26} 50 \equiv_{26} 24$ et normalement la lettre C devrait être cryptée en Y ce qui n'est pas le cas.

En conclusion, ce mélange ne correspond pas à un cryptosystème affine. Nous pouvons tout de même lui donner un cadre : celui des substitutions.

4.2 Le groupe symétrique

Définition 4.2.1

Soit X, Y deux ensembles et $f : X \to Y$ une application. On dira que f est une **application bijective** où une **bijection de X sur Y** si

$$\forall y \in Y,\ \exists! x \in X,\ f(x) = y$$

Par exemple la fonction $f : [1;2] \to [2;3]$, $x \mapsto x + 1$ est une bijection de $[1;2]$ vers $[2;3]$.

Proposition 4.2.2

Soit X, Y deux ensembles et $f : X \to Y$ une application bijective. Il existe une application $g : Y \to X$ tel que

$$\Big(\forall x \in X,\ g\big(f(x)\big) = x\Big) \quad \wedge \quad \Big(\forall y \in Y,\ f\big(g(y)\big) = y\Big)$$

On dit que g est l'**application réciproque**, ou la **bijection inverse** et est notée f^{-1}.

Démonstration. Par définition d'application bijective, pour chaque élément $y \in Y$, il existe un unique $x \in X$ tel que $f(x) = y$. On considère l'application g qui associe à chaque y cet unique élément x : $g(y) = x$ où par construction $f(x) = y$. Ainsi $f(g(y)) = f(x) = y$ et $g(f(x)) = g(y) = x$. □

Par exemple la bijection inverse de $f : [1;2] \to [2;3]$, $x \mapsto x+1$ est $g : [2,3] \to [1;3]$, $y \mapsto y-1$.

Remarque 4.2.3 : Il faut faire attention à la notation. En général $f^{-1}(y) \neq \dfrac{1}{f(y)}$. La notation f^{-1} fait cependant bien référence à un inverse mais il s'agit de l'inverse pour la composition des fonctions (le $\circ$).

Définition 4.2.4

Soit $n \in \mathbb{N}$. Le **groupe symétrique d'ordre** n est l'ensemble formé des bijections de l'ensemble $[\![1;n]\!]$ sur lui-même. On le note $\mathfrak{S}_n$. Les éléments de $\mathfrak{S}_n$ sont appelés des **permutations**.

Par exemple pour $n = 2$. L'ensemble $\mathfrak{S}_2$ est composé des bijections de l'ensemble $[\![1;2]\!] = \{1;2\}$. Il est facile de voir qu'il n'y a pas beaucoup de possibilités.

$$\begin{array}{rcl} \sigma_1 : [\![1;2]\!] & \longrightarrow & [\![1;2]\!] \\ 1 & \longmapsto & 1 \\ 2 & \longmapsto & 2 \end{array} \qquad \begin{array}{rcl} \sigma_2 : [\![1;2]\!] & \longrightarrow & [\![1;2]\!] \\ 1 & \longmapsto & 2 \\ 2 & \longmapsto & 1 \end{array}$$

Ainsi $\mathfrak{S}_2 = \{\sigma_1, \sigma_2\}$[6] est composé de deux éléments.
Détaillons l'exemple de $\mathfrak{S}_3$ formé des bijections de l'ensemble $[\![1;3]\!] = \{1;2;3\}$ sur lui-même.

$$\begin{array}{rcl} \sigma_1 : [\![1;3]\!] & \longrightarrow & [\![1;3]\!] \\ 1 & \longmapsto & 1 \\ 2 & \longmapsto & 2 \\ 3 & \longmapsto & 3 \end{array} \qquad \begin{array}{rcl} \sigma_4 : [\![1;3]\!] & \longrightarrow & [\![1;3]\!] \\ 1 & \longmapsto & 2 \\ 2 & \longmapsto & 3 \\ 3 & \longmapsto & 1 \end{array}$$

$$\begin{array}{rcl} \sigma_2 : [\![1;3]\!] & \longrightarrow & [\![1;3]\!] \\ 1 & \longmapsto & 1 \\ 2 & \longmapsto & 3 \\ 3 & \longmapsto & 2 \end{array} \qquad \begin{array}{rcl} \sigma_5 : [\![1;3]\!] & \longrightarrow & [\![1;3]\!] \\ 1 & \longmapsto & 3 \\ 2 & \longmapsto & 2 \\ 3 & \longmapsto & 1 \end{array}$$

$$\begin{array}{rcl} \sigma_3 : [\![1;3]\!] & \longrightarrow & [\![1;3]\!] \\ 1 & \longmapsto & 2 \\ 2 & \longmapsto & 1 \\ 3 & \longmapsto & 3 \end{array} \qquad \begin{array}{rcl} \sigma_6 : [\![1;3]\!] & \longrightarrow & [\![1;3]\!] \\ 1 & \longmapsto & 3 \\ 2 & \longmapsto & 1 \\ 3 & \longmapsto & 2 \end{array}$$

Ainsi $\mathfrak{S}_3 = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_6\}$ est composé de six éléments.

Remarque 4.2.5 : Dans la pratique, on ne décrit pas les éléments de $\mathfrak{S}_n$ de la manière ci-dessus. C'est bien trop fastidieux. Nous allons adopter une notation beaucoup plus élégante et adaptée aux manipulations.

Prenons l'exemple de la permutation σ_6 qui transforme le 1 en 3, le 2 en 1 et le 3 en 2. Nous allons la noter (1 3 2). Le 1 est envoyé vers le 3 qui est lui-même envoyé vers le 2. Lorsque l'on arrive à la parenthèse fermante on recommence depuis le début. C'est à dire que le 2 est envoyé vers le 1. Ce qui correspond bien à la permutation σ_6.

L'élément (1 3 2) est toujours une permutation, c'est à dire une application bijective. En tant qu'ap-

6. L'application σ_1 est appelé l'identité.

plication, on peut considérer son image par 3 par exemple. Avec la notation des fonctions il n'y a pas d'ambiguïté : on note $\sigma_6(3)$. Avec cette nouvelle notation, on va écrire exactement la même chose, à ceci prêt que l'on va substituer σ_6 par $(1\ 3\ 2)$. Ainsi *l'image de* 3 *par la permutation* $(1\ 3\ 2)$ *est* 2 est mathématiquement noté

$$(1\ 3\ 2)(3) = 2$$

De la même manière $\sigma_5 = (1\ 3)$. Par construction, on a $(1\ 3)(1) = 3$ et $(1\ 3)(3) = 1$. Que dire de $(1\ 3)(2)$? On ne le voit pas apparaitre dans la notation $(1\ 3)$, donc en fait il n'est pas transformé par cette permutation, il reste 2 :

$$(1\ 3)(2) = 2$$

Il est alors naturel de noter $\sigma_1 = (\ )$.

On peut donc simplement et élégamment décrire le groupe symétrique d'ordre 3 :

$$\mathfrak{S}_3 = \Big\{ \underbrace{()}_{\sigma_1}, \underbrace{(2\ 3)}_{\sigma_2}, \underbrace{(1\ 2)}_{\sigma_3}, \underbrace{(1\ 2\ 3)}_{\sigma_4}, \underbrace{(1\ 3)}_{\sigma_5}, \underbrace{(1\ 3\ 2)}_{\sigma_6} \Big\}$$

Prenons le problème a l'envers. Quelle est la permutation $\sigma = (3\ 2\ 1)$? Nous ne la voyons pas apparaitre dans la liste des permutations de $\mathfrak{S}_3$. Cependant $\sigma(1) = (3\ 2\ 1)(1) = 3$, $\sigma(2) = (3\ 2\ 1)(2) = 1$ et $\sigma(3) = (3\ 2\ 1)(3) = 2$ ce qui est exactement la définition de σ_6. Donc $\sigma = \sigma_6$ et $(1\ 3\ 2) = (3\ 2\ 1)$! En fait il faut lire une permutation de manière circulaire ; l'ordre des éléments compte mais pas le point de départ de la lecture.

$$\begin{array}{lcll} (\ ) & & & \\ (2\ 3) & = & (3\ 2) & \\ (1\ 2) & = & (2\ 1) & \\ (1\ 2\ 3) & = & (2\ 3\ 1) & = (3\ 1\ 2) \\ (1\ 3) & = & (3\ 1) & \\ (1\ 3\ 2) & = & (3\ 2\ 1) & = (2\ 1\ 3) \end{array}$$

Prenons un autre exemple et plaçons nous dans $\mathfrak{S}_5$. Considérons la permutation

$$\begin{array}{rcl} \sigma : [\![1;5]\!] & \longrightarrow & [\![1;5]\!] \\ 1 & \longmapsto & 3 \\ 2 & \longmapsto & 4 \\ 3 & \longmapsto & 5 \\ 4 & \longmapsto & 2 \\ 5 & \longmapsto & 1 \end{array}$$

Alors $\sigma = (1\ 3\ 5)(2\ 4)$. On observe en effet que

$$\begin{array}{lcl} \big((1\ 3\ 5)(2\ 4)\big)(1) & = & (1\ 3\ 5)\underbrace{(2\ 4)(1)}_{1} = (1\ 3\ 5)(1) = 3 \\ \big((1\ 3\ 5)(2\ 4)\big)(2) & = & (1\ 3\ 5)\underbrace{(2\ 4)(2)}_{4} = (1\ 3\ 5)(4) = 4 \\ \big((1\ 3\ 5)(2\ 4)\big)(3) & = & (1\ 3\ 5)\underbrace{(2\ 4)(3)}_{3} = (1\ 3\ 5)(3) = 5 \\ \big((1\ 3\ 5)(2\ 4)\big)(4) & = & (1\ 3\ 5)\underbrace{(2\ 4)(4)}_{2} = (1\ 3\ 5)(2) = 2 \\ \big((1\ 3\ 5)(2\ 4)\big)(5) & = & (1\ 3\ 5)\underbrace{(2\ 4)(5)}_{5} = (1\ 3\ 5)(5) = 1 \end{array}$$

Toujours dans $\mathfrak{S}_5$, considérons $\sigma = (1\ 3\ 5)(2\ 1)$. Pour déterminer l'image de 1 par sigma, il faut d'abord déterminer l'image de 1 par $(2\ 1)$. C'est 2. Ensuite on détermine l'image de 2 par $(1\ 3\ 5)$ qui reste 2. Ainsi la permutation σ commence par $(1\ 2$.

Déterminons ensuite l'image de 2 par σ et comme précédement commençons par $(1\ 2)$ qui envoie donc 2 sur 1. Cet élément est ensuite transformer par la permutation $(1\ 3\ 5)$ en 3. Au final 2 est transformer en 3. En poursuivant donc la simplification de σ on a $(1\ 2\ 3$.

On poursuit en cherchant l'image de 3 : $(1\ 3\ 5)(2\ 1)(3) = (1\ 3\ 5)(3) = 5$. Ainsi $\sigma = (1\ 2\ 3\ 5$.

Ensuite, $(1\ 3\ 5)(2\ 1)(5) = (1\ 3\ 5)(5) = 1$ et on peut clore la parenthèse : $\sigma = (1\ 2\ 3\ 5)$ (on voit que 4 reste bien fixe).

Proposition 4.2.6

Soit $n \in \mathbb{N}$. L'ensemble $\mathfrak{S}_n$ est composé de $n!$ éléments.

Démonstration. Déterminons tous les éléments de $\mathfrak{S}_n$. Il s'agit des bijections de l'ensemble $[\![1;n]\!]$ dans $[\![1;n]\!]$. Ainsi l'élément 1 peut-être associé à 1 ou 2 ou 3 ... ou n. Il y a n possibilités d'association pour le 1. Pour l'élément 2, c'est la même chose, il y a n possibilités d'association sauf que nous souhaitons obtenir une bijection, c'est à dire que l'image de 2 doit être différente de l'image de 1. Il n'y a donc pas n possibilités mais $n-1$ (les n moins celle de 1). C'est la même chose pour 3 qui a n possibilités d'image moins les deux images de 1 et 2. En poursuivant de la sorte on obtient qu'il y a $n \times (n-1) \times \cdots \times 2 \times 1$ associations différentes possible. C'est, par définition, $n!$. □

Par exemple $\mathfrak{S}_4$ est composé de 24 permutations :

$$\mathfrak{S}_4 = \left\{ \begin{array}{ccc} () & & \\ (1\ 2) & (1\ 3) & (1\ 4) \\ (2\ 3) & (2\ 4) & (3\ 4) \\ (1\ 2\ 3) & (1\ 3\ 2) & \\ (1\ 2\ 4) & (1\ 4\ 2) & \\ (1\ 3\ 4) & (1\ 4\ 3) & \\ (2\ 3\ 4) & (2\ 4\ 3) & \\ (1\ 2)(3\ 4) & (1\ 3)(2\ 4) & (1\ 4)(2\ 3) \\ (1\ 2\ 3\ 4) & (1\ 2\ 4\ 3) & \\ (1\ 3\ 2\ 4) & (1\ 3\ 4\ 2) & \\ (1\ 4\ 2\ 3) & (1\ 4\ 3\ 2) & \end{array} \right\}$$

4.3 Cryptologie de substitution

Cryptosystème

Nous avons défini $\mathfrak{S}_n$ comme le groupe des bijections de l'ensemble $[\![1;n]\!]$. En effectuant une soustraction par 1 on peut également convenir que $\mathfrak{S}_n$ est le groupe des bijection de l'ensemble $[\![0;n-1]\!]$. Puisque nous allons travailler avec des nombres entre 0 et 25 nous allons adopter cette convention.

Définition 4.3.1

Les données suivantes définissent le cryptosystème de **substitution**.

Espace de clefs. $\mathcal{K} = \mathfrak{S}_{26}$

Fonction de chiffrement. Quelque soit $\sigma \in \mathcal{K}$ et $x \in [\![0;25]\!]$, $C_\sigma(x) = \sigma(x)$.

Fonction de déchiffrement. Quelque soit $\sigma \in \mathcal{K}$ et $x \in [\![0;25]\!]$, $D_\sigma(x) = \sigma^{-1}(x)$.

La propriété de déchiffrement est une conséquence de la construction de la bijection inverse.

Cryptanalyse

Il est absolument impensable de tenter une attaque en force brute. L'espace des clefs est $\mathfrak{S}_{26}$ dont la cardinalité est $26! = 403291461126605635584000000 > 4 \times 10^{26}$. Imaginons que nous programmions une machine capable de tester un million de milliard (10^{15}) de clefs par seconde (c'est donc un algorithme très performant avec une machine extrêmement puissante [7]). Nous aurons donc besoin de $\frac{4 \times 10^{26}}{10^{15}}$ secondes pour tester toutes les clefs soit $\frac{4 \times 10^{26}}{10^{15} \times 60 \times 60 \times 24 \times 365} > 12683$ ans !

Une manière beaucoup plus intelligente est une **cryptanalyse fréquentielle**.

Cette analyse est basée sur le fait que lettre apparaissent toujours avec (à peu près) la même fréquence.

Caractère	a	b	c	d	e	f	g	h	i	j	k	l	m
Fréquence (%)	8.122	0.901	3.345	3.669	17.115	1.066	0.866	0.737	7.580	0.545	0.049	5.456	2.968

Caractère	n	o	p	q	r	s	t	u	v	w	x	y	z
Fréquence (%)	7.095	5.378	3.021	1.362	6.553	7.948	7.244	6.311	1.628	0.114	0.387	0.308	0.136

(valeurs obtenues par l'analyse d'un texte en français sans vocabulaire spécifique ; les caractères accentués étant ramenés aux caractères dont ils dérivent).

Bien évidement plus le texte est long plus cette méthode sera rapidement efficace. Si par exemple, le texte chiffré est *W ANNATLI*, nous ne disposons pas assez de donnée pour pouvoir entamer une analyse fréquentielle. Considérons par exemple le message suivant :

> *VWLP WI ZXYCRI GI EARAENIRI IPN QYVXRNAZN VWLP W ANNATLI KRITLIZN-QIWWI PIRA VIRK XRYAZNI*

En comptant les lettres on arrive à

Caractère	A	B	C	D	E	F	G	H	I	J	K	L	M
Nb apparition	7	0	1	0	2	0	1	0	14	0	2	4	0

Caractère	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Nb apparition	8	0	4	2	8	0	2	0	4	6	3	3	4

Il est donc fort probable que le *I* corresponde eu *E*

> *VWLP WE ZXYCRE GE EARAENERE EPN QYVXRNAZN VWLP W ANNATLE KRETLEZNQEWWE PERA VERK XRYAZNE*

En analysant de la sorte les caractères on peut déchiffrer le message. Dans cette exemple, le nombre de caractère est trop faible pour arriver à exploiter l'attaque fréquentielle. On peut néanmoins déduire que le *A* est soit le *A*, le *N* ou le *R*...

A noter que la méthode de l'analyse fréquentiel s'applique également pour les méthodes de César et Affine puisqu'il s'agit de cas particulier de la substitution.

7. Rien de tout ça n'existe pour l'instant.

5. Le chiffrement de Hill

Le principe du chiffrement de Hill est d'essayer de rendre l'analyse fréquentielle caduc (même avec un chiffrement mono alphabétique, c'est à dire par paquet de 1).

L'idée est qu'au leu de chiffrer caractère par caractère, on va réunir les caractères par bloc. Ainsi tous les caractères du bloc "influeront" sur le chiffrement des autres.

Pour y arriver nous avons besoin d'un outil mathématique : les matrices.

5.1 Les matrices

Dans la suite on fixe un entier $n \geqslant 2$.

Définition 5.1.1

Une **matrice 2×2 à coefficient dans** $\mathbb{Z}/n\mathbb{Z}$ est la donnée d'un tableau à deux lignes et deux colonnes. Chaque case du tableau étant remplie d'une valeur de $\mathbb{Z}/n\mathbb{Z}$.

Si a, b, c et d sont des éléments de $\mathbb{Z}/n\mathbb{Z}$, on note une matrice

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

On note $\mathcal{M}_2(\mathbb{Z}/n\mathbb{Z})$ l'ensemble des matrices 2×2 à coefficient dans $\mathbb{Z}/n\mathbb{Z}$.

Remarque 5.1.2 : On peut bien sur généraliser cette définition à des matrices à n lignes et m colonnes et changer également l'ensemble des coefficients pour définir $\mathcal{M}_{n,m}(\mathbb{K})$. Cela ne sera pas nécessaire pour la suite.

Par exemple $\begin{pmatrix} 2 & 3 \\ -8 & 7 \end{pmatrix} \in \mathcal{M}_2(\mathbb{Z}/26\mathbb{Z})$

L'ensemble des matrices porte une structure algébrique dit d'anneau. Cela signifie que l'on peut additionner et multiplier des matrices entre elles de manière cohérente.

Définition 5.1.3 Opérations

Soient $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ et $B = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ des matrices de $\mathcal{M}_2(\mathbb{Z}/n\mathbb{Z})$ et $\lambda \in \mathbb{Z}/n\mathbb{Z}$

Addition. On pose :

$$A + B \equiv_n \begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \equiv_n \begin{pmatrix} a+\alpha & b+\beta \\ c+\gamma & d+\delta \end{pmatrix}$$

Multiplication matricielle. On pose

$$A.B \equiv_n \begin{pmatrix} a & b \\ c & d \end{pmatrix} . \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \equiv_n \begin{pmatrix} a\alpha + b\gamma & a\beta + b\delta \\ c\alpha + d\gamma & c\beta + d\delta \end{pmatrix}$$

Multiplication scalaire. On pose

$$\lambda.A \equiv_n \lambda. \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv_n \begin{pmatrix} \lambda a & \lambda b \\ \lambda c & \lambda d \end{pmatrix}$$

Les "cohérences" de ces deux opérations sont résumés dans la proposition suivante

Proposition 5.1.4 Structure algébrique

Soient A, B et C des matrices de $M_2(\mathbb{Z}/n\mathbb{Z})$.

Commutativité $+$. $A+B \equiv_n B+A$

Associativité $+$. $(A+B)+C \equiv_n A+(B+C)$

Neutralité $+$. $A+0 \equiv_n 0+A \equiv_n A$ où $0 \equiv_n \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

Symétrie $+$. $A+(-A) \equiv_n (-A)+A \equiv_n 0$ où $-A$ est la matrice où tous les coefficients ont changé de signe.

Associativité $\times$. $(A.B).C \equiv_n A.(B.C)$

Neutralité $\times$ $A.Id \equiv_n Id.A \equiv_n A$ où $Id \equiv_n \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

Distributivité. $A(B+C) \equiv_n AB+AC$ et $(A+B)C \equiv_n AC+BC$

Démonstration. Pour démontrer toutes ces propriétés, on se ramène à la définition (`#longetfastidieux`). □

Remarque 5.1.5 : Il était nécessaire de donner la règle de la distributivité de la sorte (en précisant la distributivité à droite et a gauche) et cela pour la même raison qui fait que nous n'avons pas écrit la règle "Commutativité $\times$" : le produit des matrices n'est pas commutatif.

Pour le voir, il suffit de traiter un exemple. Plaçons nous dans $\mathbb{Z}/2\mathbb{Z}$ et considérons les matrices $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ et $B = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$ Alors $AB \equiv_2 \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ et $BA \equiv_2 \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$

Il faut donc prendre garde ! En général, le produit des matrices n'est pas commutatif !

Une autre règle n'est pas vérifiée : celle que nous aurions pu appeler "Symétrie $\times$" qui consisterai à écrire $A.A^{-1} \equiv_n Id \equiv_n A^{-1}.A$. Le problème est que la multiplication étant "étrange" par définition, la division va aussi l'être.

Définition 5.1.6

Soit $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{M}_2(\mathbb{Z}/n\mathbb{Z})$.

On note $\det(A)$ le nombre $ad-bc$ que l'on appelle **déterminant** de A.

Par exemple si $A \equiv_{26} \begin{pmatrix} -5 & 2 \\ 8 & 7 \end{pmatrix} \in \mathcal{M}_2(\mathbb{Z}/26\mathbb{Z})$, alors $\det(A) \equiv_{26} (-5)\times(7)-(8)\times(2) \equiv_{26} -35-16 = -51 \equiv_{26} 1$.

Proposition 5.1.7

Soient A, B des matrices de $\mathcal{M}_2(\mathbb{Z}/n\mathbb{Z})$.

$$\det(AB) \equiv_n \det(A)\det(B)$$

Démonstration. Écrivons $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ et $B = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$. Alors $A.B \equiv_n \begin{pmatrix} a\alpha+b\gamma & a\beta+b\delta \\ c\alpha+d\gamma & c\beta+d\delta \end{pmatrix}$. Par définition $\det(A) = ad-bc$ et $\det(B) = \alpha\delta-\beta\gamma$. En multipliant ces résultats et en développant on arrive à

$$\det(A)\det(B) = ad\alpha\delta - ad\beta\gamma - bc\alpha\delta + bc\beta\gamma$$

D'autre par le déterminant de A.B se calcul :

$$\begin{aligned}\det(A.B) &= (a\alpha+b\gamma)(c\beta+d\delta)-(c\alpha+d\gamma)(a\beta+b\delta)\\ &= (ac\alpha\beta+ad\alpha\delta+bc\beta\gamma+bd\gamma\delta)\\ &- (ac\alpha\beta+bc\alpha\delta+ad\beta\gamma+bd\gamma\delta)\\ &= ad\alpha\delta+bc\beta\gamma-bc\alpha\delta-ad\beta\gamma\end{aligned}$$

□

Théorème 5.1.8 Inverse matricielle modulaire

Soit $A=\begin{pmatrix} a & b\\ c & d\end{pmatrix}\in\mathcal{M}_2(\mathbb{Z}/n\mathbb{Z})$.

La matrice A est inversible si et seulement si $\det(A)=ad-bc\in(\mathbb{Z}/n\mathbb{Z})^\times$. Précisément, si on note A^{-1} cet inverse alors

$$A^{-1}\equiv_n \det(A)^{-1}\begin{pmatrix} d & -b\\ -c & a\end{pmatrix}$$

où $\det(A)^{-1}$ désigne l'inverse de $\det(A)$ modulo n.

Démonstration. Si $\det(A)$ est inversible modulo n, on vérifie très facilement que $A.A^{-1}\equiv_n A^{-1}.A\equiv_n \mathrm{Id}$ pour le A^{-1} donné dans l'énoncé du théorème. Inversement si A est inversible alors il existe A^{-1} tel que $A.A^{-1}=A^{-1}.A=\mathrm{Id}$. En passant au déterminant et en utilisant la proposition précédente, on arrive à $\det(A)\det(A^{-1})\equiv_n\det(A^{-1})\det(A)\equiv_n\det(\mathrm{Id})\equiv_n 1$. □

Par exemple $A\equiv_{26}\begin{pmatrix} 5 & 3\\ 4 & 2\end{pmatrix}\in\mathcal{M}_2(\mathbb{Z}/26\mathbb{Z})$. On a $\det(A)\equiv_{26}10-12\equiv_{26}-2$. Il faut voir si cet élément est inversible modulo 26. Il faut pour cela qu'il soit premier avec 26, ce qui n'est clairement pas le cas. Conclusion : la matrice A n'est pas inversible modulo 26.

Autre exemple avec $A\equiv_{26}\begin{pmatrix} 5 & 3\\ -7 & -2\end{pmatrix}\in\mathcal{M}_2(\mathbb{Z}/26\mathbb{Z})$. On a $\det(A)\equiv_{26}(-10)-(-21)\equiv_{26}11$.

En appliquant l'algorithme d'Euclide étendue, on détermine que $26(3)+(11)(-7)=1$ soit encore $11(-7)\equiv_{26}$ et $11^{-1}\equiv_{26}-7$.

a	b	r	q	u	v
26	11	4	2	3	−7
11	4	3	2	−1	3
4	3	1	1	1	−1
3	1	0	3	0	1

En appliquant la formule on arrive à

$$\begin{pmatrix} 5 & 3\\ -7 & -2\end{pmatrix}^{-1}\equiv_{26}-7\begin{pmatrix} -2 & -3\\ 7 & 5\end{pmatrix}\equiv_{26}\begin{pmatrix} 14 & 21\\ -49 & -35\end{pmatrix}\equiv_{26}\begin{pmatrix} 14 & 21\\ 3 & 17\end{pmatrix}$$

Définition 5.1.9

On note $GL_2(\mathbb{Z}/n\mathbb{Z})$ l'ensemble des matrices inversibles de $\mathcal{M}_2(\mathbb{Z}/n\mathbb{Z})$.

Proposition 5.1.10

$\sharp(GL_2(\mathbb{Z}/26\mathbb{Z}))=(2^2-1)(2^2-2)(13^2-1)(13^2-13)=157248$

Démonstration. On peut démontrer un énoncé plus général : si p et q deux nombres premiers distincts alors $\sharp(GL_2(\mathbb{Z}/pq\mathbb{Z})) = (p^2-1)(p^2-p)(q^2-1)(q^2-q)$.

On montre en adaptant la preuve du *lemme chinois* que l'application

$$\begin{array}{rcl} \varphi : GL_2(\mathbb{Z}/pq\mathbb{Z}) & \longrightarrow & GL_2(\mathbb{Z}/p\mathbb{Z}) \times GL_2(\mathbb{Z}/q\mathbb{Z}) \\ M & \longmapsto & (M_p, M_q) \end{array}$$

où $M_q \equiv_q M$ et $M_p \equiv_p M$ est une bijection.

Il y a donc autant d'élément dans $GL_2(\mathbb{Z}/pq\mathbb{Z})$ que dans $GL_2(\mathbb{Z}/p\mathbb{Z}) \times GL_2(\mathbb{Z}/q\mathbb{Z})$. Or la cardinalité de ce dernier ensemble est le produit des cardinalités de $GL_2(\mathbb{Z}/q\mathbb{Z})$ et $GL_2(\mathbb{Z}/p\mathbb{Z})$.

Pour conclure il suffit de montrer que la cardinalité de $GL_2(\mathbb{Z}/p\mathbb{Z})$ est $(p^2-1)(p^2-p)$. Les éléments de $GL_2(\mathbb{Z}/p\mathbb{Z})$ sont composés de 2 vecteurs qui doivent être linéairement indépendant (car le déterminant de la matrice est non nul). Ainsi la première colonne (le premier vecteur) est n'importe quoi sauf 0 : p^2-1 possibilités. Le second vecteur ne doit pas être colinéaire au premier donc p^2-p possibilités. □

Pour finir, définissons le produit matrice-vecteur.

Définition 5.1.11

On note $(\mathbb{Z}/n\mathbb{Z})^2$ l'ensemble des vecteurs en dimension 2 à coefficient dans $\mathbb{Z}/n\mathbb{Z}$.

$$(\mathbb{Z}/n\mathbb{Z})^2 = \left\{ \binom{a}{b} \middle| (a \in \mathbb{Z}/n\mathbb{Z}) \wedge (b \in \mathbb{Z}/n\mathbb{Z}) \right\}$$

Définition 5.1.12 Produit matrice-vecteur

Soient $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{M}_2(\mathbb{Z}/n\mathbb{Z})$ et $X = \begin{pmatrix} x \\ y \end{pmatrix} \in (\mathbb{Z}/n\mathbb{Z})^2$. On pose

$$A.X = \begin{pmatrix} ax+by \\ cx+dy \end{pmatrix}$$

Par exemple pour $A = \begin{pmatrix} 4 & 3 \\ 1 & -2 \end{pmatrix}$ et $X = \begin{pmatrix} 2 \\ -3 \end{pmatrix}$ alors $A.X = \begin{pmatrix} -1 \\ 8 \end{pmatrix}$

5.2 Principe du chiffrement

Cryptosystème

Définition 5.2.1

Les données suivantes définissent le **cryptosystème de Hill de dimension 2 par paquet de 1**.

Espace de clefs. $\mathcal{K} = GL_2(\mathbb{Z}/26\mathbb{Z})$

Fonction de chiffrement. Quelque soit $A \in \mathcal{K}$ et $X \in (\mathbb{Z}/26\mathbb{Z})^2$, $C_A(X) = A.X$.

Fonction de déchiffrement. Quelque soit $A \in \mathcal{K}$ et $X \in (\mathbb{Z}/26\mathbb{Z})^2$, $D_A(X) = A^{-1}.X$.

L'associativité du calcul matriciel justifie la propriété du déchiffrement.

Prenons comme exemple la matrice $A = \begin{pmatrix} 5 & 3 \\ -7 & -2 \end{pmatrix}$ qui est bien un élément de $GL_2(\mathbb{Z}/26\mathbb{Z})$ puisque $\texttt{det}(A) = 11$ est un nombre premier avec 26.

Chiffrons le message *CHIFFREMENTDEHILL*

Texte	C	H	I	F	F	R	E	M	E	N	T	D	E	H	I	L	L	
Codage	2	7	8	5	5	17	4	12	4	13	19	3	4	7	8	11	11	
Vecteur X	(2,7)		(8,5)		(5,17)		(4,12)		(4,13)		(19,3)		(4,7)		(8,11)		(11,0)	
A.X	(31,−28)		(55,−66)		(76,−69)		(56,−52)		(59,−54)		(104,−139)		(41,−42)		(73,−78)		(55,−77)	
$\equiv_{26}$	(5,24)		(3,12)		(24,9)		(4,0)		(7,24)		(0,17)		(15,10)		(21,0)		(3,1)	
Dépaquetage	5	24	3	12	24	9	4	0	7	24	0	17	15	10	21	0	3	1
Décodage	F	Y	D	M	Y	J	A	E	H	Y	A	R	P	K	V	A	D	B

Ainsi le message chiffré est *FYDMYJAEHYARPKVADB*.

Inversement : imaginons avoir reçu le *DTQUCTEQGDAA* obtenue par un chiffrement de Hill de matrice $A = \begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix}$. La première étape consiste à déterminer l'inverse de A et avant cela il faut calculer son déterminant et l'inverse de celui-ci.

Calcul du déterminant. $\det(A) = 9 \times 7 - 5 \times 4 = 63 - 20 = 43 \equiv_{26} 17$

Calcul de l'inverse du déterminant.

a	b	r	q	u	v
26	17	9	1	2	−3
17	9	8	1	−1	2
9	8	1	1	1	−1
8	1	0	8	0	1

Ainsi $17^{-1} \equiv_{26} -3 (\equiv_{26} 23)$

Calcul de l'inverse de la matrice. On applique la formule :

$$A^{-1} \equiv_{26} -3 \begin{pmatrix} 7 & -4 \\ -5 & 9 \end{pmatrix} \equiv_{26} \begin{pmatrix} -21 & 12 \\ 15 & -27 \end{pmatrix} \equiv_{26} \begin{pmatrix} 5 & 12 \\ 15 & -1 \end{pmatrix}$$

Ceci étant on peut déchiffrer le message.

	D	T	Q	U	C	T	E	Q	G	D	A	
Codage	3	19	16	20	2	19	4	16	6	3	0	
Vecteur X	(3,19)		(16,20)		(2.19)		(4,16)		(6,3)		(0,0)	
$A^{-1}.X$	(243,26)		(320,220)		(238,11)		(212,44)		(66,87)		(0,0)	
$\equiv_{26}$	(9,0)		(8,12)		(4,11)		(4,18)		(14,9)		(0,0)	
Dépaquetage	9	0	8	12	4	11	4	18	14	9	0	0
Décodage	J	A	I	M	E	L	E	S	O	J	A	A

Cryptanalyse

Dans la précédente section nous avons vu que la cardinalité de $GL_2(\mathbb{Z}/26\mathbb{Z})$ c'est à dire de l'espace des clefs du chiffrement de Hill par paquet de 1 en dimension 2 était de 157 248. Ce nombre reste "raisonnable" et une attaque en force brute est suffisante dans ce cas.

Il est également possible de raisonner par analyse fréquentielle mais de manière différente que celle que nous avons vu. En effet, comme nous pouvons l'observer dans l'exemple précédent, la lettre *E* avait été codée, une fois par un *C* et un autre fois par la même lettre *E*. Le chiffrement de Hill, ne permet aucune analyse fréquentielle mono alphabétique. Mais puisque nous travaillons par paquet de 2, on peut faire une analyse fréquentielle 2-alphabétique[8]. Dans un texte en français, les blocs de 2 lettres les plus fréquents sont

8. C'est à dire par paquet de 2

Lettres	ES	LE	EN	DE	RE	NT	ON	TE	ER	SE
Fréquences	3.15%	2.46%	2.42%	2.15%	2.09%	1.97%	1.64%	1.63%	1.63%	1.55%

Ainsi, lorsque le texte est suffisamment long, une analyse fréquentielle peut aboutir au déchiffrement.

Il existe une autre manière d'attaquer un problème de cryptographie, l'**attaque à clair connu**, que nous allons détailler dans le cas du chiffrement de Hill, mais qui s'applique pour tous les autres cryptosystèmes.

Le principe de l'attaque à clair connu réside dans le fait que l'on ne possède pas seulement le message chiffré. On possède également un partie du texte claire [9].

Imaginons que vous interceptiez un flux d'information entre enseignants qui ont pris la peine de chiffrer leurs communications et ne se sont pas retenus de dire à leurs étudiants *"De toute manière nous utilisons un chiffrement de Hill pour toute nos communications."*. Vous interceptez un document `Exam_crypto.txt`. En l'ouvrant, bien sur tout est codé : *YXYIEZLD...*. Vous savez, que comme tout examen qui se respecte, il est fort probable que les premiers mots soient *EXAMENDECRYPTO*. Sachant qu'il s'agit d'un chiffrement de Hill, la clef est une matrice $A \equiv_{26} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}/26\mathbb{Z})$. En comparant la chaine dans le document et la chaine supposé on en déduit que "A.*EX*=*YX*", "A.*AM*=*YI*", "A.*EN*=*EZ*" et "A.*DE*=*LD*". En replaçant par les valeurs numériques, on arrive à quatre équations :

1. $A \begin{pmatrix} E \\ X \end{pmatrix} = \begin{pmatrix} Y \\ X \end{pmatrix} \Leftrightarrow A \begin{pmatrix} 4 \\ 23 \end{pmatrix} \equiv_{26} \begin{pmatrix} 24 \\ 23 \end{pmatrix}$ **3.** $A \begin{pmatrix} E \\ N \end{pmatrix} = \begin{pmatrix} E \\ Z \end{pmatrix} \Leftrightarrow A \begin{pmatrix} 4 \\ 13 \end{pmatrix} \equiv_{26} \begin{pmatrix} 4 \\ 25 \end{pmatrix}$

2. $A \begin{pmatrix} A \\ M \end{pmatrix} = \begin{pmatrix} Y \\ I \end{pmatrix} \Leftrightarrow A \begin{pmatrix} 0 \\ 12 \end{pmatrix} \equiv_{26} \begin{pmatrix} 24 \\ 8 \end{pmatrix}$ **4.** $A \begin{pmatrix} D \\ E \end{pmatrix} = \begin{pmatrix} L \\ D \end{pmatrix} \Leftrightarrow A \begin{pmatrix} 3 \\ 4 \end{pmatrix} \equiv_{26} \begin{pmatrix} 11 \\ 3 \end{pmatrix}$

On peut, grâce aux définitions du calcul matricielle, "fusionner" deux équations. Par exemple l'équation 1 et l'équation 2 donnent l'équation 1.2 : $A \begin{pmatrix} 4 & 0 \\ 23 & 12 \end{pmatrix} = \begin{pmatrix} 24 & 24 \\ 23 & 8 \end{pmatrix}$ qui se résout simplement en inversant la matrice à droite de A. Précisément : $A = \begin{pmatrix} 24 & 24 \\ 23 & 8 \end{pmatrix} . \begin{pmatrix} 4 & 0 \\ 23 & 12 \end{pmatrix}^{-1}$. Pour pouvoir réaliser cette opération, il faut que la matrice soit inversible, c'est à dire que son déterminant, soit premier avec 26. Or $\det \begin{pmatrix} 4 & 0 \\ 23 & 12 \end{pmatrix} = 48$ et $\mathrm{PGCD}(26, 48) = 2$. La matrice n'est donc pas inversible. Il faut être capable de trouver une matrice inversible en combinant les équations. Plus on dispose de *clair connu*, plus on dispose d'équation et donc plus il va être facile de trouver une matrice inversible. Dans cet exemple, avec les 4 équations dont nous disposons, nous pouvons former six matrices :

Équation 1.2 : $A \begin{pmatrix} 4 & 0 \\ 23 & 12 \end{pmatrix} \equiv_{26} \begin{pmatrix} 24 & 24 \\ 23 & 8 \end{pmatrix}$ et $\det \begin{pmatrix} 4 & 0 \\ 23 & 12 \end{pmatrix} \equiv_{26} 48$ qui n'est pas premier avec 26.

Équation 1.3 : $A \begin{pmatrix} 4 & 4 \\ 23 & 13 \end{pmatrix} \equiv_{26} \begin{pmatrix} 24 & 4 \\ 23 & 25 \end{pmatrix}$ et $\det \begin{pmatrix} 4 & 4 \\ 23 & 13 \end{pmatrix} \equiv_{26} -40$ qui n'est pas premier avec 26

Équation 1.4 : $A \begin{pmatrix} 4 & 3 \\ 23 & 4 \end{pmatrix} \equiv_{26} \begin{pmatrix} 24 & 11 \\ 23 & 3 \end{pmatrix}$ et $\det \begin{pmatrix} 4 & 3 \\ 23 & 4 \end{pmatrix} \equiv_{26} -53 \equiv_{26} -1$ qui est premier avec 26.

Dans ce cas

$$A \equiv_{26} \begin{pmatrix} 24 & 11 \\ 23 & 3 \end{pmatrix} \cdot \begin{pmatrix} 4 & 3 \\ 23 & 4 \end{pmatrix}^{-1} \equiv_{26} \begin{pmatrix} 24 & 11 \\ 23 & 3 \end{pmatrix} \cdot \begin{pmatrix} -4 & 3 \\ 23 & -4 \end{pmatrix} \equiv_{26} \begin{pmatrix} 1 & 2 \\ 3 & 5 \end{pmatrix}$$

9. C'est par ce type d'attaque qu'Alan Türing a réussi à casser *ENIGMA*

Équation 2.3 : $A \begin{pmatrix} 0 & 4 \\ 12 & 13 \end{pmatrix} \equiv_{26} \begin{pmatrix} 24 & 4 \\ 8 & 25 \end{pmatrix}$ et $\det \begin{pmatrix} 0 & 4 \\ 12 & 13 \end{pmatrix} \equiv_{26} -48$ qui n'est pas premier avec 26

Équation 2.4 : $A \begin{pmatrix} 0 & 3 \\ 12 & 4 \end{pmatrix} \equiv_{26} \begin{pmatrix} 24 & 11 \\ 8 & 3 \end{pmatrix}$ et $\det \begin{pmatrix} 0 & 3 \\ 12 & 4 \end{pmatrix} \equiv_{26} -36$ qui n'est pas premier avec 26

Équation 3.4 : $A \begin{pmatrix} 4 & 3 \\ 13 & 4 \end{pmatrix} \equiv_{26} \begin{pmatrix} 4 & 11 \\ 25 & 3 \end{pmatrix}$ et $\det \begin{pmatrix} 4 & 3 \\ 13 & 4 \end{pmatrix} \equiv_{26} -23 \equiv_{26} 3$ qui est premier avec 26.

Dans ce cas

$$A \equiv_{26} \begin{pmatrix} 4 & 11 \\ 25 & 3 \end{pmatrix} \cdot \begin{pmatrix} 4 & 3 \\ 13 & 4 \end{pmatrix}^{-1} \equiv_{26} \begin{pmatrix} 4 & 11 \\ 25 & 3 \end{pmatrix} \cdot \begin{pmatrix} 10 & -1 \\ -13 & 10 \end{pmatrix} \equiv_{26} \begin{pmatrix} 1 & 2 \\ 3 & 5 \end{pmatrix}$$

A chaque fois qu'il est possible d'inverser la matrice on trouve $A \equiv_{26} \begin{pmatrix} 1 & 2 \\ 3 & 5 \end{pmatrix}$ qui est donc la clef de chiffrement.

Pour déchiffrer il faudra appliquer la matrice inverse $A^{-1} \equiv_{26} \begin{pmatrix} 1 & 2 \\ 3 & 5 \end{pmatrix}^{-1} \equiv_{26} \begin{pmatrix} -5 & 2 \\ 3 & -1 \end{pmatrix}$

Lemme 5.2.2 : Supposons que le *clair connu* d'un message obtenu par un chiffrement de Hill, soit composé de $2n$ caractères pour un certain entier $n \in \mathbb{N}_{>0}$. Alors il existe $\frac{n(n-1)}{2}$ équations matricielles différentes permettant de déterminer la clef de chiffrement.

Démonstration. Se donner $2n$ caractères connus donne n équations matrices-vecteurs. Il y a $\binom{n}{2} = \frac{n!}{2!(n-2)!} = \frac{n(n-1)}{2}$ façon de coupler des équations matrice-vecteur pour obtenir des équations matrice-matrice (par définition du combinatoire). □

Complication

Le chiffrement de Hill est déjà un principe de paquetage, mais rien n'empêche de compiler les paquetages. On sera dans ce cas amener à travailler avec des matrice de $GL_2(\mathbb{Z}/2526\mathbb{Z})$ ou $GL_2(\mathbb{Z}/252526\mathbb{Z})$ qui sont de cardinalités respective $(2^2-1)(2^2-2)(3^2-1)(3^2-3)(421^2-1)(421^2-421) = 9\,025\,798\,118\,400$ et $(2^2-1)(2^2-2)(31^2-1)(31^2-31)(4073^2-1)(4073^2-4073) = 1\,473\,860\,586\,963\,514\,982\,400$.

Nous n'entrerons pas plus dans le détail.

Il est également possible de compliquer davantage en prenant des paquets de 3 ou 4 par exemple et donc être amené à travailler avec des matrices de $GL_3(\mathbb{Z}/26\mathbb{Z})$ ou plus généralement $GL_n(\mathbb{Z}/26\mathbb{Z})$. Le principe est exactement le même. La seule difficulté réside dans le calcul du déterminant et de la détermination de l'inverse matricielle. Cela n'est pas le but de ce cours (mais ce n'est pas du tout or de portée).

6. RSA

Les cryptosystèmes que nous avons introduit jusque là ont tous une "grande faille" : dès que l'on connait la clef de chiffrement on peut trouver la clef de déchiffrement (et inversement). On parle de cryptosystème **symétrique**.

Le problème c'est que deux individus voulant échanger des informations secrètes doivent avant tout convenir de la méthode de chiffrement ainsi que la clef.

Si un pirate intercepte l'échange de clef, le cryptage devient inutile.

A l'opposé des cryptosystèmes symétrique il y a les cryptosystème **asymétrique** : il est difficile de déterminer la clef de déchiffrement même en connaissant la clef de chiffrement. L'exemple fameux de tel cryptosystème est la méthode RSA, initiales des inventeurs Rivest, Shamir et Adleman. Pour arriver à comprendre son fonctionnement nous avons besoin des nombres premiers.

6.1 Les nombres premiers

Définition 6.1.1

Un nombre premier est un nombre qui n'a que deux diviseurs positifs.

On note $\mathcal{P}$, l'ensemble des nombres premiers.

Ainsi un nombre premier est un nombre qui n'est divisible que par 1 et par lui-même sauf 1.

Par exemple 2, 13, 101.

Proposition 6.1.2 Lemme d'Euclide

Soient a, b des entiers et $p \in \mathcal{P}$.

$$p|ab \Longrightarrow (p|a) \vee (p|b)$$

Démonstration. Supposons que p ne divise pas a. Les seuls diviseurs de p et donc du $\mathrm{PGCD}(p, a)$ sont 1 et p et puisque p ne divise pas a on a nécessairement $\mathrm{PGCD}(p, a) = 1$. Le lemme de Gauss permet de conclure que $p|b$. □

Les nombres premiers sont au cœur de l'arithmétique. Ils forment les atomes de tous les nombres.

Théorème 6.1.3 Théorème fondamental de l'arithmétique - Gauss

Tout nombre entier non nul se décompose de manière unique, à l'ordre des facteur près, en produit fini de nombre premier.

Démonstration. Montrons l'existence par récurrence sur n. Le nombre 1 est produit d'un nombre fini de nombre premier : aucun (produit sur l'ensemble vide) ce qui prouve le cas initial.

Supposons que tout entier $n < N$ s'écrit comme produit fini de nombre premier et montrons qu'il en est de même pour N. Considérons le plus petit $p \in D(N)$ strictement supérieur à 1 qui existe car cet ensemble est une partie non vide de $\mathbb{N}$ et admet donc un plus petit élément.

Nécessairement p est un nombre premier par minimalité. Mais $N = N'p$ et puisque $N' < N$ il s'écrit comme produit de nombre premier et il en va donc de même pour N.

L'unicité se déduit du lemme d'Euclide. □

Théorème 6.1.4

$$\sharp(\mathcal{P}) = +\infty$$

Démonstration. Raisonnons par l'absurde et supposons que $p_1 < p_2 < \cdots < p_n$ sont les seuls premier. Considérons $N = 1 + p_1 \cdot p_2 \cdots p_n$. Le nombre N n'est pas un nombre premier (puisque strictement plus grand que le plus grand des nombres premiers). D'après le théorème fondamental de l'arithmétique, N est divisible par un nombre premier, p_k. Mais puisque $p_1 \cdot p_2 \cdots p_n$ est également divisible par p_k on en déduit que $1 = N - p_1 \cdot p_2 \cdots p_n$ est divisible par p_k et nécessairement $p_k = 1$ qui n'est pas un nombre premier. Absurde. □

Définition 6.1.5

Soit $p \in \mathcal{P}$ et $n \in \mathbb{N}_{>0}$. On appelle **valuation p-adique** de n la plus grande puissance de p qui apparait dans la décomposition en facteur premier de n. On la note $\nu_p(n)$.

Par exemple $\nu_2(12) = 2$, $\nu_3(12) = 1$ et $\nu_5(12) = 0$.

Corollaire 6.1.6

Soit $n \in \mathbb{N}_{>0}$. La famille $\{\nu_p(n)\}_{p\in\mathcal{P}}$ est une famille d'entier presque tous nul et

$$n = \prod_{p\in\mathcal{P}} p^{\nu_p(n)}$$

Démonstration. Cela se déduit du théorème fondamental de l'arithmétique. □

Proposition 6.1.7

Soient a et b des éléments de $\mathbb{N}_{>0}$ et $p \in \mathcal{P}$.

(i). $\nu_p(ab) = \nu_p(a) + \nu_p(b)$.

(ii). $a|b \iff \Big(\forall p \in \mathcal{P},\ \nu_p(a) \leqslant \nu_p(b)\Big)$.

(iii). $\nu_p(a^b) = b\nu_p(a)$.

(iv). $\nu_p(\mathrm{PGCD}(a,b)) = \min(\nu_p(a), \nu_p(b))$.

Démonstration.

(i). On a $a = \prod_{p\in\mathcal{P}} p^{\nu_p(a)}$ et $b = \prod_{p\in\mathcal{P}} p^{\nu_p(b)}$ d'où $ab = \prod_{p\in\mathcal{P}} p^{\nu_p(a)+\nu_p(b)}$.

(ii). Si $a|b$ alors il existe $k \neq 0$ tel que $b = ka$ ce qui implique d'après le premier point que $\nu_p(b) = \nu_p(k) + \nu_p(a)$ pour tout $p \in \mathcal{P}$. En particulier $\nu_p(b) \geqslant \nu_p(a)$. Réciproquement : posons $k = \prod_{p\in\mathcal{P}} p^{\nu_p(b)-\nu_p(a)}$.

Alors $b = ka$.

(iii). Beaucoup trop triviale.

(iv). C'est une conséquence de la construction du PGCD.

□

Théorème 6.1.8 Formule de Legendre

Soient $n \in \mathbb{N}_{>0}$ et $p \in \mathcal{P}$.

$$\nu_p(n!) = \sum_{i=1}^{\infty} \left[\frac{n}{p^i}\right]$$

où $[x]$ désigne la partie entière du réel x.

Démonstration. Soit $\alpha_i \in \mathbb{N}$ le plus grand entier tel que $\alpha_i p^i \leqslant n$. Dans ce cas le nombre d'entier inférieur ou égaux à n et divisible par p^i est $\alpha_i = \left[\frac{n}{p^i}\right]$.

Soit n_i le nombre d'entier entre 1 et n de valuation p-adique exactement égale à i. Naturellement $v_p(n!) = n_1 + 2n_2 + 3n_3$ etc...

Pour finir on observe que $\left[\frac{n}{p^i}\right] = n_i + n_{i+1}. \cdots$. □

Les nombres premiers bien que centraux en arithmétiques sont très peu connu. Voici une petite brochette de conjecture lié aux nombres premiers.

Goldbach. Tout nombre paire strictement supérieur à 2 s'écrit comme la somme de deux nombres premiers.

Legendre. Pour tout entier $n > 1$, il existe toujours un nombre premier entre n^2 et $(n+1)^2$.

Sophie Germain. Il existe une infinité de nombre premier p tel que $2p+1$ est également premier [10].

Mersenne. Il existe une infinité de nombre premier de la forme $2^n - 1$.

Fermat. Il existe une infinité de nombre premier de la forme $2^{2^n} + 1$

Fibonacci. Il existe une infinité de nombre premier qui apparaissent dans la suite de Fibonacci.

Riemann. ...

Malgré les mystères qui entourent ces nombres nous disposons de puissant résultat.

Lemme 6.1.9 : Soit $p \in \mathcal{P}$ et $0 < k < p$

$$\binom{p}{k} = \frac{p!}{k!(p-k)!} \text{ est divisible par } p$$

Démonstration. On observe que

$$k\binom{p}{k} = p\binom{p-1}{k-1}$$

Ainsi $p | k\binom{p}{k}$ et puisque k est premier à p le lemme de Gauss prouve que $p | \binom{p}{k}$. □

Théorème 6.1.10 Petit théorème de Fermat

Soit $p \in \mathcal{P}$ et $x \in \mathbb{N}$.

$$x^p \equiv_p x$$

Démonstration. On raisonne par récurrence sur x le cas initial étant trivial.
Supposons que pour un x quelconque fixé, $x^p \equiv_p x$. En developpant par le binôme de Newton on a

$$(x+1)^p = \sum_{k=0}^{p} \binom{p}{k} x^k = 1 + x^p + \sum_{k=1}^{p-1} \binom{p}{k}$$

Or entre 1 et $p-1$ tous les coefficients binomiaux sont multiples de p c'est à dire nuls modulo p. En conclusion $(x+1)^p \equiv_p x^p + 1$. Par hypothèse de récurrence, $(x+1)^p \equiv_p x + 1$. □

10. Monsieur Le Blanc

Corollaire 6.1.11

Soit $p \in \mathcal{P}$ et $x \in \mathbb{N}$ non multiple de p.

$$x^{p-1} \equiv_p 1$$

Démonstration. Le petit théorème de Fermat affirme que $x^p \equiv_p x$ c'est à dire qu'il existe $k \in \mathbb{Z}$ tel que $x^p - x = kp$ soit encore $x(x^{p-1} - 1) = kp$. Cette dernière égalité implique que $p|(x(x^{p-1} - x))$ or p et x sont premiers entre eux puisque p est premier et x non multiple de p. Le lemme de Gauss permet de conclure que $x^{p-1} - 1$ est multiple de p. □

6.2 Principe de chiffrement

Proposition 6.2.1

Soient $p < q$ deux nombres premier, e un nombre premier avec $\varphi = (p-1)(q-1)$ et d l'inverse de e modulo φ. Pour tout $x \in \mathbb{Z}$,

$$x^{de} \equiv_{pq} x$$

Démonstration. Puisque d est l'inverse de e modulo φ on en déduit $de \equiv_\varphi 1$. D'une autre manière, il existe $k \in \mathbb{Z}$ tel que $de = 1 + k(p-1)(q-1)$. Dans ce cas $x^{de} = x \times \left(x^{(p-1)(q-1)}\right)^k$.

Si x n'est pas multiple de p et de q alors le corollaire du petit théorème Fermat implique que $x^{p-1} \equiv_p 1$ soit encore $x^{(p-1)(q-1)} \equiv_p 1$. De même $x^{(p-1)(q-1)} \equiv_q 1$. Le lemme chinois implique alors que $x^{(p-1)(q-1)} \equiv_{pq} 1$ et donc $x^{de} \equiv_{pq} x$.

Si x est multiple de p mais pas de q alors le corollaire au petit théorème de Fermat implique que $x^{q-1} \equiv_q 1$ et donc $x^{k(p-1)(q-1)} \equiv_q 1$. Par définition il existe $\alpha \in \mathbb{Z}$ tel que $x^{k(p-1)(q-1)} = \alpha q + 1$. En multipliant par x on a $x^{1+k(p-1)(q-1)} = \alpha x q + x$ mais $xq \equiv_{pq} 0$ car x est multiple de p. Dans ce cas $x^{de} \equiv_{pq} x$.

Si x est multiple de q mais pas de p c'est le même raisonnement.

Si x est multiple de p et de q alors il est nul modulo pq et trivialement $x^{de} \equiv_{pq} x (\equiv_{pq} 0)$. □

Définition 6.2.2

Soient $p < q$ deux nombres premiers. Notons $n = pq$ et $\varphi(n) = (p-1)(q-1)$

Les données suivantes définissent le cryptosystème de RSA de base n.

Espace de clefs. $\mathcal{K}_{p,q} = (\mathbb{Z}/\varphi(n)\mathbb{Z})^\times$

Fonction de chiffrement. Quelque soit $e \in \mathcal{K}_{p,q}$ et $x \in \mathbb{Z}$, $C_e(x) \equiv_n x^e$

Fonction de déchiffrement. Quelque soit $e \in \mathcal{K}_{p,q}$ et $x \in \mathbb{Z}$, $D_e(x) \equiv_n x^{e^{-1}}$ où e^{-1} désigne l'inverse de e modulo $\varphi(n)$.

La proposition précédente justifie que la propriété de déchiffrement est satisfaite.

Dans la pratique la clef de chiffrement, la donnée (n, e), est appelé la **clef publique** et la clef de déchiffrement, la donnée (n, e^{-1}) est appelé la **clef privée**.

Prenons par exemple $p = 3$ et $q = 11$. Dans ce cas, $n = 33$ et $\varphi(33) = 20$. Le nombre $e = 13$ est un entier premier à 20 donc $(33, 13)$ est une clef publique. Chiffrons le message *PIKACHU*

Message	P	I	K	A	C	H	U
Codage	15	08	10	00	02	07	20
$x^{13} \bmod 33$	9	17	10	0	8	13	14

Ainsi le message chiffré est $9 - 17 - 10 - 0 - 8 - 13 - 14$.

Imaginons avoir reçu le message $8-0-29-0-14-8-31$ avec la même clef de chiffrement. L'inverse de 13 modulo 20 s'obtient en appliquant l'algorithme d'Euclide étendue. On trouve $13^{-1} \equiv_{20} 17$ Déchiffrons alors le message.

Message	08	00	29	00	09	14	08	31
$x^{17} \bmod 33$	02	00	17	00	15	20	02	04
Décodage	C	A	R	A	P	U	C	E

La sécurité de ce cryptosystème réside dans le fait que même si on connait la clef publique (n, e) il est difficile de trouver l'inverse de e car on ne connait pas φ (p et q en fait). Bien sur ce cryptosystème sera sûre avec de grande valeur pour p et q. Ainsi si vous savez qu'un message a été codé avec $(9068370463, 17)$ il sera difficile (du moins sans ordinateur) de trouver la clef privée.

Le paquetage est "automatique" avec cette méthode.

Si l'entier n est compris entre 26 et 2525 on travaillera par paquet de 2, s'il est entre 252526 et 25252525 on travaillera par paquet de 3 etc.

Prenons par exemple $p = 509$ et $q = 691$ alors $n = 351719$: on chiffrera par paquet de 3. Prenons $e = 7$ qui est bien premier avec $\varphi(351719) = 350520$.

Message	A	T	T	R	A	P	E	Z	L	E	S	T	O	U	S
Codage	00	19	19	17	00	15	04	25	11	04	18	19	14	20	18
Paquetage	1919			170015			42511			41819			142018		
$x^7 \bmod 351719$	27519			87444			106946			327923			329813		

et le message chiffré est $27519 - 87444 - 106946 - 327923 - 329813$.

6.3 Échange et signature

Madame A souhaite transmettre un message suivant le protocole RSA à monsieur B. Monsieur B a crié sur tous les toits que sa clef publique est (n_B, e_B) et a secrètement gardé sa clef privée (n_B, d_B). D'ailleurs madame A a fait la même chose avec sa clef publique (n_A, e_A) et privée (n_A, d_A).

Madame A code son message claire M avec la clef publique de monsieur B et publie sur son mur FB le message crypté. Tout le monde peut le voir mais seul monsieur B qui dispose de la clef de déchiffrement peut retrouver le message initial M.

Monsieur B voudrait être sûre que le message qu'il reçoit provient bien de madame A et pas d'un pirate qui se ferait passer pour elle. Madame A va alors signer son message avant de le chiffrer et de l'envoyer. Elle applique au message claire M sa clef privée (n_A, d_A) puis ensuite la clef publique (n_B, e_B) de monsieur B. En recevant le message, monsieur B va appliquer sa clef privée et obtenir un message encore chiffré. Il va alors appliquer la clef publique (n_A, e_A) de A qui est à la seule qui a pu utiliser sa clef privée pour signer ce message, pour retrouver le message claire M.

6.4 Exponentiation modulaire rapide

Bien que cette méthode de chiffrement soit sûre elle est soumise à une contrainte : le calcul des puissances modulaires, communément appelé **exponentiation modulaire**.

Reprenons l'exemple du déchiffrement introduit plus tôt. Avec une calculatrice on a $1919^7 = 9.5835149e+22$. Cet arrondi rend le déchiffrement impossible [11]. Il existe cependant une méthode rapide pour réaliser ces calculs sans arrondi ni problème du à la gestion de mémoire de la machine.

L'élément centrale de l'exponentiation modulaire rapide est le changement de base.

Théorème 6.4.1

Soient n et b des entiers tels que $b > 0$. Il existe un famille finie $\{a_0, a_1, \ldots, a_k\} \in [\![0, b[\![$ pour un certain $k \in \mathbb{N}$ tel que $n = \sum_{i=0}^{k} a_i b^i$

11. Et il s'agit d'un cas très simple

Démonstration. On raisonne par récurrence sur n, le cas initial $n = 0$ étant trivial. D'après le théorème de la division euclidienne $n = bq + r$ où $0 \leqslant r < b$. Naturellement $q < n$. Par hypothèse de récurrence $q = \sum_{i=0}^{k} a_i b^i$ pour un certain k. Ainsi $n = \sum_{i=0}^{k} a_i b^{i+1} + rb^0$ ce qui prouve le résultat. □

Définition 6.4.2

Soit $b \in \mathbb{N}_{>0}$. L'écriture en **base** b d'un entier $n \in \mathbb{N}$ est la donnée de la famille $\{a_0, a_1, \ldots, a_k\}$ du théorème précédent. On note

$$n = (a_k \ldots a_1 a_0)_b$$

La manière usuelle d'écrire les nombres est l'écriture en base 10 ou base décimale. Lorsque l'on ne précise pas la base, il s'agira de l'écriture décimale du nombre, c'est à dire $123 = (123)_{10}$

En observant la preuve du théorème précédent, on obtient un algorithme permettant d'écrire en base b quelconque : il suffit de réaliser des divisions euclidienne successives. Écrivons par exemple l'entier 123 en base 7.

- $123 = 7 \times 17 + \boxed{4}$
- $17 = 7 \times 2 + \boxed{3}$
- $2 = 7 \times 0 + \boxed{2}$

On a alors $123 = (234)_7$.

Définition 6.4.3

- L'écriture en base 2 est appelé le **binaire**.
- L'écriture en base 3 est appelé le **trinaire**.
- L'écriture en base 8 est appelé l'**octal**.
- L'écriture en base 16 est appelé l'**hexadécimal**.
- L'écriture en base 60 est appelé le **sexagésimal**.
- L'écriture en base 150 est appelé l'**indienne**.

Lorsque la base dépasse les 10 caractères usuelles de la numération, on ajoute des caractères. Par exemple, en hexadécimal, on l'habitude de compléter les chiffres de 0 à 9 par les lettres, A, B, C, D et E. Ainsi $(ABC)_{16} = \underbrace{10}_{A} \times 16^2 + \underbrace{11}_{B} \times 16^1 + \underbrace{12}_{C} = 2748$.

Algorithme d'exponentiation modulaire rapide

Cet algorithme permet de calculer très rapidement x^n modulo m. L'idée est d'écrire l'entier n en binaire (base 2).

Écrivons $n = \sum_{i=0}^{k} a_i 2^i$ où pour tout i, $a_i \in \{0, 1\}$. Dans ce cas, $x^n = \prod_{i=0}^{k} x^{2^i}$. L'avantage est que $(x^{2^i})^2 = x^{2^{i+1}}$. D'où l'algorithme.

§6.4.4 :

```
Écrire n en binaire : n = ∑_{i=0}^{k} a_i 2^i
Pour i de 0 à k
        Si i=0
             poser x[0] = x modulo m
        Sinon
             x[i] = x[i-1]*x[i-1] modulo m
        Fin Si
Fin pour
res = 1
Pour i de 0 à k
```

```
        Si a_i=1
             res = res*x[i] modulo m
        Fin Si
Fin pour
Renvoyer res
```

Par exemple calculons 19^{19} modulo 2017.

Ecriture binaire. La première étape consiste à écrire 19 en binaire ce qui se fait par division euclidienne successive. On trouve $19 = (10011)_2$.

Calcul des puissances de puissance de 2. On représente la situation dans un tableau

k	0	1	2	3	4
2^k					
mod					

où la dernière ligne est la seconde ligne modulo $m = 2017$. Le tableau va jusqu'à $k = 4$ car c'est la plus grande puissance de 2 qui apparait dans l'écriture binaire de 19. On l'initialise de la sorte

k	0	1	2	3	4
2^k	19				
mod	19				

On prend la valeur de la dernière ligne de la colonne k que l'on met au carré et que l'on inscrit dans à la seconde ligne de la colonne $k+1$ et on calcul la réduction modulo m à la dernière ligne.

k	0	1	2	3	4
2^k	19	361			
mod	19	361			

On itère le processus.

k	0	1	2	3	4
2^k	19	361	130321		
mod	19	361	1233		

k	0	1	2	3	4
2^k	19	361	130321	1520289	
mod	19	361	1233	1488	

k	0	1	2	3	4
2^k	19	361	130321	1520289	2214144
mod	19	361	1233	1488	1495

Conclusion. Les puissances de 2 apparaissant dans l'écriture binaire de 19 sont 0, 1 et 4 on a donc $19^{19} \equiv_{2017} 19 \times 361 \times 1495 \equiv_{2017} 808 \times 1495 \equiv_{2017} 1794$

7. Chiffrement DES

Le système de chiffrement DES, aujourd'hui désuet, est un algorithme de chiffrement par bloc qui a longtemps été utilisé pour le chiffrement des mot de passe UNIX. Il est aussi utilisé dans (d'ancien) décodeur de HBO [12].

1970 : Horst Feistel et ses collègues d'IBM, travaillant avec un système d'exploitation appelé *DEMONSTRATION*, propose un système de chiffrement par bloc pour la banque en ligne. Le Système *DEMONSTRATION* ne supportant pas les noms long est communément appelé *DEMON*. D'où le nom de cette méthode de chiffrement : *lucifer*.

1973 : le bureau des standards américain (NBS) lance un appel à la création d'un algorithme de chiffrement utilisable par les entreprises.

1976 : après quelques "modifications" de la part de l'agence de sécurité nationale américaine (NSA), le système *lucifer* rebaptisé *DES* pour *data encryption system*, est sélectionné par le NBS.

1994 : Don Coppersmith avoue qu'en 1974, les concepteurs d'IBM avaient trouvé avant l'heure une méthode d'attaque (appelée *attaque-T*, genre d'attaque différentielle), permettant de casser DES.

1998 : la machine *deep crack* (ayant couté environ 200 000€) permet de casser DES en force brute en 56h.

1999 : par l'intermédiaire de calcul distribué à travers le réseau, il a suffit de 22h pour casser DES en force brute (environ 100 000 machines connectées sur internet).

Dans tout ce chapitre nous ne travaillerons qu'en binaire.

7.1 Clef

La clef de DES est un nombre binaire sur 64 bits (8 octets) mais seul 56 bits sont actifs. En effet pour chaque octet un bit, le dernier, est réservé au contrôle de la clef. Il va permettre de s'assurer que l'octet comporte un nombre impaire de 1.

0	1	0	1	1	1	1	X		0	1	0	1	1	1	1	0
0	1	0	1	1	0	1	X		0	1	0	1	1	0	1	1
0	1	0	1	0	0	1	X		0	1	0	1	0	0	1	0
0	1	1	1	1	1	1	X		0	1	1	1	1	1	1	1
0	1	0	1	0	0	0	X	$\Longrightarrow$	0	1	0	1	0	0	0	1
0	0	0	1	1	0	1	X		0	0	0	1	1	0	1	0
1	0	1	1	1	1	0	X		1	0	1	1	1	1	0	0
1	0	0	1	0	0	0	X		1	0	0	1	0	0	0	1

Il n'y a donc que 56 bits de choix, ce que signifie, puisqu'un bit ne peut prendre que deux valeurs, qu'il y a 2^{56} clefs différentes. Ce qui représente environ 72 millions de milliard de clefs possible. Un ordinateur avec un algorithme permettant de tester une clef par seconde mettra donc environ 2 milliards d'année a tout tester.

7.2 Constante du chiffrement DES

La méthode de chiffrement DES peut être programmée dans une boite noire (dont on ne voit pas le code) avec un certain nombre de constate. Une attaque différentielle permet de ne pas prendre en compte la valeur des constantes utilisées dans cette boite. C'est pour cette raison que dans la pratique elles sont connues. Il y en a de trois natures : les fonctions de permutations, la fonction d'expansion et les matrices de substitutions.

Les fonctions de permutations. Ces fonctions que le notes dans un tableau vont permettre de mélanger les bits dans le mot. Par exemple la permutation $P = (4\ 1\ 3\ 2)$ se comprend par le placement en première position du quatrième bit, en seconde position du premier en troisième du troisième et en quatrième du second.

Si par exemple le message est $M =$ "1010" alors après application de la permutation P le nouveau message est $M' =$ "0110".

12. *Valar Morgulis*

Cinq permutations interviennent dans le système DES. Nous les notons en matrices bien qu'il faille les lire en ligne, nous n'avons simplement pas la place autrement.

La permutation initiale $\mathrm{PI} = \begin{pmatrix} 58 & 50 & 42 & 34 & 26 & 18 & 10 & 2 \\ 60 & 52 & 44 & 36 & 28 & 20 & 12 & 4 \\ 62 & 54 & 46 & 38 & 30 & 22 & 14 & 6 \\ 64 & 56 & 48 & 40 & 32 & 24 & 16 & 8 \\ 57 & 49 & 41 & 33 & 25 & 17 & 9 & 1 \\ 59 & 51 & 43 & 35 & 27 & 19 & 11 & 3 \\ 61 & 53 & 45 & 37 & 29 & 21 & 13 & 5 \\ 63 & 55 & 47 & 39 & 31 & 23 & 15 & 7 \end{pmatrix}$

La permutation initiale inverse qui fait simplement les association inverse de PI :

$$\mathrm{PI}^{-1} = \begin{pmatrix} 40 & 8 & 48 & 16 & 56 & 24 & 64 & 32 \\ 39 & 7 & 47 & 15 & 55 & 23 & 63 & 31 \\ 38 & 6 & 46 & 14 & 54 & 22 & 62 & 30 \\ 37 & 5 & 45 & 13 & 53 & 21 & 61 & 29 \\ 36 & 4 & 44 & 12 & 52 & 20 & 60 & 28 \\ 35 & 3 & 43 & 11 & 51 & 19 & 59 & 27 \\ 34 & 2 & 42 & 10 & 50 & 18 & 58 & 26 \\ 33 & 1 & 41 & 9 & 49 & 17 & 57 & 25 \end{pmatrix}$$

La permutation des rondes $\mathrm{P} = \begin{pmatrix} 16 & 7 & 20 & 21 & 29 & 12 & 28 & 17 \\ 1 & 15 & 23 & 26 & 5 & 18 & 31 & 10 \\ 2 & 8 & 24 & 14 & 32 & 27 & 3 & 9 \\ 19 & 13 & 30 & 6 & 22 & 11 & 4 & 25 \end{pmatrix}$

La première permutation des clefs

$$\mathrm{CP}_1 = \begin{pmatrix} 57 & 49 & 41 & 33 & 25 & 17 & 9 & 1 & 58 & 50 & 42 & 34 & 26 & 18 \\ 10 & 2 & 59 & 51 & 43 & 35 & 27 & 19 & 11 & 3 & 60 & 52 & 44 & 36 \\ 63 & 55 & 47 & 39 & 31 & 23 & 15 & 7 & 62 & 54 & 46 & 38 & 30 & 22 \\ 14 & 6 & 61 & 53 & 45 & 37 & 29 & 21 & 13 & 5 & 28 & 20 & 12 & 4 \end{pmatrix}$$

La seconde permutation des clefs

$$\mathrm{CP}_2 = \begin{pmatrix} 14 & 17 & 11 & 24 & 1 & 5 & 3 & 28 & 15 & 6 & 21 & 10 \\ 23 & 19 & 12 & 4 & 26 & 8 & 16 & 7 & 27 & 20 & 13 & 2 \\ 41 & 52 & 31 & 37 & 47 & 55 & 30 & 40 & 51 & 45 & 33 & 48 \\ 44 & 49 & 39 & 56 & 34 & 53 & 46 & 42 & 50 & 36 & 29 & 32 \end{pmatrix}$$

La fonction d'expansion va permettre de transformer un bloc de 32 bits en un bloc de 48 bits. Elle s'utilise comme les fonctions de permutation mais dupliquent en plus 16 bits.

$$E = \begin{pmatrix} 32 & 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 6 & 7 & 8 & 9 \\ 8 & 9 & 10 & 11 & 12 & 13 \\ 12 & 13 & 14 & 15 & 16 & 17 \\ 16 & 17 & 18 & 19 & 20 & 21 \\ 20 & 21 & 22 & 23 & 24 & 25 \\ 24 & 25 & 26 & 27 & 28 & 29 \\ 28 & 29 & 30 & 31 & 32 & 1 \end{pmatrix}$$

Les matrices de substitution sont aux nombres de 8 et sont des matrices de 4 lignes et 16 colonnes dont nous détaillerons l'utilisation le moment venu :

$$S1 = \begin{pmatrix} 14 & 4 & 13 & 1 & 2 & 15 & 11 & 8 & 3 & 10 & 6 & 12 & 5 & 9 & 0 & 7 \\ 0 & 15 & 7 & 4 & 14 & 2 & 13 & 1 & 10 & 6 & 12 & 11 & 9 & 5 & 3 & 8 \\ 4 & 1 & 14 & 8 & 13 & 6 & 2 & 11 & 15 & 12 & 9 & 7 & 3 & 10 & 5 & 0 \\ 15 & 12 & 8 & 2 & 4 & 9 & 1 & 7 & 5 & 11 & 3 & 14 & 10 & 0 & 6 & 13 \end{pmatrix}$$

$$S2 = \begin{pmatrix} 15 & 1 & 8 & 14 & 6 & 11 & 3 & 4 & 9 & 7 & 2 & 13 & 12 & 0 & 5 & 10 \\ 3 & 13 & 4 & 7 & 15 & 2 & 8 & 14 & 12 & 0 & 1 & 10 & 6 & 9 & 11 & 5 \\ 0 & 14 & 7 & 11 & 10 & 4 & 13 & 1 & 5 & 8 & 12 & 6 & 9 & 3 & 2 & 15 \\ 13 & 8 & 10 & 1 & 3 & 15 & 4 & 2 & 11 & 6 & 7 & 12 & 0 & 5 & 14 & 9 \end{pmatrix}$$

$$S3 = \begin{pmatrix} 10 & 0 & 9 & 14 & 6 & 3 & 15 & 5 & 1 & 13 & 12 & 7 & 11 & 4 & 2 & 8 \\ 13 & 7 & 0 & 9 & 3 & 4 & 6 & 10 & 2 & 8 & 5 & 14 & 12 & 11 & 15 & 1 \\ 13 & 6 & 4 & 9 & 8 & 15 & 3 & 0 & 11 & 1 & 2 & 12 & 5 & 10 & 14 & 7 \\ 1 & 10 & 13 & 0 & 6 & 9 & 8 & 7 & 4 & 15 & 14 & 3 & 11 & 5 & 2 & 12 \end{pmatrix}$$

$$S4 = \begin{pmatrix} 7 & 13 & 14 & 3 & 0 & 6 & 9 & 10 & 1 & 2 & 8 & 5 & 11 & 12 & 4 & 15 \\ 13 & 8 & 11 & 5 & 6 & 15 & 0 & 3 & 4 & 7 & 2 & 12 & 1 & 10 & 14 & 9 \\ 10 & 6 & 9 & 0 & 12 & 11 & 7 & 13 & 15 & 1 & 3 & 14 & 5 & 2 & 8 & 4 \\ 3 & 15 & 0 & 6 & 10 & 1 & 13 & 8 & 9 & 4 & 5 & 11 & 12 & 7 & 2 & 14 \end{pmatrix}$$

$$S5 = \begin{pmatrix} 2 & 12 & 4 & 1 & 7 & 10 & 11 & 6 & 8 & 5 & 3 & 15 & 13 & 0 & 14 & 9 \\ 14 & 11 & 2 & 12 & 4 & 7 & 13 & 1 & 5 & 0 & 15 & 10 & 3 & 9 & 8 & 6 \\ 4 & 2 & 1 & 11 & 10 & 13 & 7 & 8 & 15 & 9 & 12 & 5 & 6 & 3 & 0 & 14 \\ 11 & 8 & 12 & 7 & 1 & 14 & 2 & 13 & 6 & 15 & 0 & 9 & 10 & 4 & 5 & 3 \end{pmatrix}$$

$$S6 = \begin{pmatrix} 12 & 1 & 10 & 15 & 9 & 2 & 6 & 8 & 0 & 13 & 3 & 4 & 14 & 7 & 5 & 11 \\ 10 & 15 & 4 & 2 & 7 & 12 & 9 & 5 & 6 & 1 & 13 & 14 & 0 & 11 & 3 & 8 \\ 9 & 14 & 15 & 5 & 2 & 8 & 12 & 3 & 7 & 0 & 4 & 10 & 1 & 13 & 11 & 6 \\ 4 & 3 & 2 & 12 & 9 & 5 & 15 & 10 & 11 & 14 & 1 & 7 & 6 & 0 & 8 & 13 \end{pmatrix}$$

$$S7 = \begin{pmatrix} 4 & 11 & 2 & 14 & 15 & 0 & 8 & 13 & 3 & 12 & 9 & 7 & 5 & 10 & 6 & 1 \\ 13 & 0 & 11 & 7 & 4 & 9 & 1 & 10 & 14 & 3 & 5 & 12 & 2 & 15 & 8 & 6 \\ 1 & 4 & 11 & 13 & 12 & 3 & 7 & 14 & 10 & 15 & 6 & 8 & 0 & 5 & 9 & 2 \\ 6 & 11 & 13 & 8 & 1 & 4 & 10 & 7 & 9 & 5 & 0 & 15 & 14 & 2 & 3 & 12 \end{pmatrix}$$

$$S8 = \begin{pmatrix} 13 & 2 & 8 & 4 & 6 & 15 & 11 & 1 & 10 & 9 & 3 & 14 & 5 & 0 & 12 & 7 \\ 1 & 15 & 13 & 8 & 10 & 3 & 7 & 4 & 12 & 5 & 6 & 11 & 0 & 14 & 9 & 2 \\ 7 & 11 & 4 & 1 & 9 & 12 & 14 & 2 & 0 & 6 & 10 & 13 & 15 & 3 & 5 & 8 \\ 2 & 1 & 14 & 7 & 4 & 10 & 8 & 13 & 15 & 12 & 9 & 0 & 3 & 5 & 6 & 11 \end{pmatrix}$$

7.3 Logique propositionnelle

Le principe de chiffrement DES est très faible en terme de ressource de temps de calcul. Il n'y a que des substitutions, des conversions en binaire et des opérations de logique. Revenons sur les opérations de la logique.

Les trois opérations logiques élémentaires

Le *non* de la logique que l'on note $\neg p$ et dont la table est

p	$\neg p$
0	1
1	0

Le *ou* de la logique que l'on note $p + q$ et dont la table est

p	q	$p+q$
0	0	0
0	1	1
1	0	1
1	1	1

Le *et* de la logique que l'on note $p \times q$ ou plus simplement $p.q$ et dont la table est

p	q	$p.q$
0	0	0
0	1	0
1	0	0
1	1	1

On note 0 la proposition qui est toujours fausse, on l'appel la *contradiction*.
On note 1 la proposition qui est toujours vrai, on l'appel la *tautologie*.

Candimatica

Ces trois opérations satisfont certaines lois :

Proposition 7.3.1

Soient p, q et r des propositions

Commutativité. $p + q = q + p$, $p.q = q.p$

Associativité. $(p + q) + r = p + (q + r)$, $(p.q).r = p.(q.r)$

Neutralité. $p + 0 = p$, $p.1 = p$

Distributivité. $p.(q + r) = (p.q) + (p.r)$, $p + (q.r) = (p + q).(p + r)$

Idempotence. $p + p = p$, $p.p = p$

de Morgan $\neg(p + q) = (\neg p).(\neg q)$, $\neg(p.q) = (\neg p) + (\neg q)$

Absorption 1. $p + 1 = 1$, $p.0 = 0$

Tiers exclu. $p + (\neg p) = 1$

Involution. $\neg(\neg p) = p$

Contradiction. $p.(\neg p) = 0$

Absorption 2. $p + (p.q) = p$, $p.(p + q) = p$

Cette proposition se démontre en comparant par exemple les tables de vérité

Ou exclusif

Le *ou exclusif*, qui sera l'outil de la cryptographie DES, se comporte comme le *ou* classique à ceci près qu'il renvoie faux si les deux propositions sont vrais. On le note $p \oplus q$ et sa table de vérité est

p	q	$p \oplus q$
0	0	0
0	1	1
1	0	1
1	1	0

Théorème 7.3.2

1. $p \oplus q = (p + q).\neg(p.q)$
2. $p \oplus p = 0$
3. $p \oplus 0 = p$
4. $p \oplus 1 = \neg p$
5. $p \oplus \neg p = 1$
6. $p \oplus q = q \oplus p$
7. $p \oplus (q \oplus r) = (p \oplus q) \oplus r$
8. $(p \oplus q = 0) \Leftrightarrow (p = q)$
9. $\neg(p \oplus q) = (\neg p) \oplus q = p \oplus (\neg q) = (\neg p) \oplus (\neg q)$
10. $(p \oplus q = r) \Rightarrow (q \oplus r = p)$

Démonstration. Exercice □

7.4 Méthode de chiffrement

Création de 16 sous-clefs. La clef K est donnée sur 64 bits. On commence par supprimer les 8 bits de contrôle pour ne garder que les 56 bits utiles

$$\begin{array}{cccccccc} 0&1&0&1&1&1&1&0 \\ 0&1&0&1&1&0&1&1 \\ 0&1&0&1&0&0&1&0 \\ 0&1&1&1&1&1&1&1 \\ 0&1&0&1&0&0&0&1 \\ 0&0&0&1&1&0&1&0 \\ 1&0&1&1&1&1&0&0 \\ 1&0&0&1&0&0&0&1 \end{array} \Rightarrow \left.\begin{array}{ccccccc|c} 0&1&0&1&1&1&1&0 \\ 0&1&0&1&1&0&1&1 \\ 0&1&0&1&0&0&1&0 \\ 0&1&1&1&1&1&1&1 \\ 0&1&0&1&0&0&0&1 \\ 0&0&0&1&1&0&1&0 \\ 1&0&1&1&1&1&0&0 \\ 1&0&0&1&0&0&0&1 \end{array}\right.$$

On considère donc la clef de 56 bits $K = 01011110101101010100101111110101000000110110111101001000$
On va appliquer la première permutation CP_1 :

$$\text{CLEF} = \left\{ \begin{array}{|r||cccccccccccccc|} \hline \text{Position} & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ \hline \text{bit} & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ \hline \text{Position} & 15 & 16 & 17 & 18 & 19 & 20 & 21 & 22 & 23 & 24 & 25 & 26 & 27 & 28 \\ \hline \text{bit} & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ \hline \text{Position} & 29 & 30 & 31 & 32 & 33 & 34 & 35 & 36 & 37 & 38 & 39 & 40 & 41 & 42 \\ \hline \text{bit} & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ \hline \text{Position} & 43 & 44 & 45 & 46 & 47 & 48 & 49 & 50 & 51 & 52 & 53 & 54 & 55 & 56 \\ \hline \text{bit} & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ \hline \end{array} \right.$$

$$\text{CP}_1 = \begin{pmatrix} 57 & 49 & 41 & 33 & 25 & 17 & 9 & 1 & 58 & 50 & 42 & 34 & 26 & 18 \\ 10 & 2 & 59 & 51 & 43 & 35 & 27 & 19 & 11 & 3 & 60 & 52 & 44 & 36 \\ 63 & 55 & 47 & 39 & 31 & 23 & 15 & 7 & 62 & 54 & 46 & 38 & 30 & 22 \\ 14 & 6 & 61 & 53 & 45 & 37 & 29 & 21 & 13 & 5 & 28 & 20 & 12 & 4 \end{pmatrix}$$

$$\text{CP}_1[\text{CLEF}] = \left\{ \begin{array}{|r||cccccccccccccc|} \hline \text{Position} & \begin{matrix}1\\57\end{matrix} & \begin{matrix}2\\49\end{matrix} & \begin{matrix}3\\41\end{matrix} & \begin{matrix}4\\33\end{matrix} & \begin{matrix}5\\25\end{matrix} & \begin{matrix}6\\17\end{matrix} & \begin{matrix}7\\9\end{matrix} & \begin{matrix}8\\1\end{matrix} & \begin{matrix}9\\58\end{matrix} & \begin{matrix}10\\50\end{matrix} & \begin{matrix}11\\42\end{matrix} & \begin{matrix}12\\34\end{matrix} & \begin{matrix}13\\26\end{matrix} & \begin{matrix}14\\18\end{matrix} \\ \hline \text{bit} & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ \hline \text{Position} & \begin{matrix}15\\10\end{matrix} & \begin{matrix}16\\2\end{matrix} & \begin{matrix}17\\59\end{matrix} & \begin{matrix}18\\51\end{matrix} & \begin{matrix}19\\43\end{matrix} & \begin{matrix}20\\35\end{matrix} & \begin{matrix}21\\27\end{matrix} & \begin{matrix}22\\19\end{matrix} & \begin{matrix}23\\11\end{matrix} & \begin{matrix}24\\3\end{matrix} & \begin{matrix}25\\60\end{matrix} & \begin{matrix}26\\52\end{matrix} & \begin{matrix}27\\44\end{matrix} & \begin{matrix}28\\36\end{matrix} \\ \hline \text{bit} & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ \hline \text{Position} & \begin{matrix}29\\63\end{matrix} & \begin{matrix}30\\55\end{matrix} & \begin{matrix}31\\47\end{matrix} & \begin{matrix}32\\39\end{matrix} & \begin{matrix}33\\31\end{matrix} & \begin{matrix}34\\23\end{matrix} & \begin{matrix}35\\15\end{matrix} & \begin{matrix}36\\7\end{matrix} & \begin{matrix}37\\62\end{matrix} & \begin{matrix}38\\54\end{matrix} & \begin{matrix}39\\46\end{matrix} & \begin{matrix}40\\38\end{matrix} & \begin{matrix}41\\30\end{matrix} & \begin{matrix}42\\22\end{matrix} \\ \hline \text{bit} & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ \hline \text{Position} & \begin{matrix}43\\14\end{matrix} & \begin{matrix}44\\6\end{matrix} & \begin{matrix}45\\61\end{matrix} & \begin{matrix}46\\53\end{matrix} & \begin{matrix}47\\45\end{matrix} & \begin{matrix}48\\37\end{matrix} & \begin{matrix}49\\29\end{matrix} & \begin{matrix}50\\21\end{matrix} & \begin{matrix}51\\13\end{matrix} & \begin{matrix}52\\5\end{matrix} & \begin{matrix}53\\28\end{matrix} & \begin{matrix}54\\20\end{matrix} & \begin{matrix}55\\12\end{matrix} & \begin{matrix}56\\4\end{matrix} \\ \hline \text{bit} & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ \hline \end{array} \right.$$

On obtient alors le mélange : 11000000000111110100100011110010111101001001011010111111 On sépare la clef en deux partie de 28 bits :

$$\text{G} = 1100000000011111010010001111 \qquad \text{D} = 0010111101001001011010111111$$

On va alors réaliser le processus suivant pour obtenir 16 sous-clefs :
- Écraser G et D par leur décaler de 1 bit vers la gauche (le premier bit devenant le dernier).
- La clef K_1 est le résultat de la permutation par CP_2 de la concaténation de G et D.
- Écraser G et D par leur décaler de 1 bit vers la gauche.
- La clef K_2 est le résultat de la permutation par CP_2 de la concaténation de G et D.
- Écraser G et D par leur décaler de 1 bit vers la gauche.
- La clef K_3 est le résultat de la permutation par CP_2 de la concaténation de G et D.
- ...
- Écraser G et D par leur décaler de 1 bit vers la gauche.
- La clef K_16 est le résultat de la permutation par CP_2 de la concaténation de G et D.

La propriété de la permutation CP_2 est qu'elle supprime les bits 9, 18, 22, 25, 35, 38, 43 et 54 transformant le bloc de 56 bits en un bloc de 48 octets.

Dans notre exemple :

1. Décalage de 1 bit à gauche :

$$\text{G} = 1100000000011111010010001111 \quad \text{deviens} \quad \text{G} = 1000000000111111010010011111$$

$$\text{D} = 0010111101001001011010111111 \quad \text{deviens} \quad \text{D} = 0101111010010010110101111110$$

On concatène G et D et on applique le mélange CP_2 (comme nous l'avons fait pour CP_1) pour obtenir :

$$\text{K}_1 = 111110011000001010001110010101111111000011101001$$

2. Décalage de 1 bit à gauche :

$$G = 10000000001111110100100011111 \quad \text{deviens} \quad G = 00000000011111010010001111111$$

$$D = 01011110100100101101011111110 \quad \text{deviens} \quad D = 10111101001001011010111111100$$

On concatène G et D et on applique le mélange CP_2 pour obtenir :

$$K_2 = 10110001000111101010101001101000111011101101111$$

3. etc

Paquetage. On divise le message en paquet de 64 bits en complétant éventuellement les bits manquant par des 0 à la fin. Si par exemple le message est

$$M = \begin{array}{l} 1101110010111011111000100110101010 \\ 1110011011110111111000010001100 10 \\ 1001110100101011011010111110001 1 \\ 0011101011011111 \end{array}$$

Alors on le découpe en deux blocs :

$$M_1 = \begin{array}{l} 1101110010111011111000100110101010 \\ 1110011011110111111000010001100 10 \end{array} \qquad M_2 = \begin{array}{l} 1001110100101011011010111110001 1 \\ 0011101011011111000000000000000 0 \end{array}$$

Les opérations qui suivent se font sur chacun des blocs, nous ne les illustreront qu'avec le bloc de 64 bits M_1.

Permutation initiale. On applique au bloc la permutation initiale PI donnée plus haut. On rappel que cette permutation initiale correspond à un mélange des bits :

Position	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
bit	1	1	0	1	1	1	0	0	1	0	1	1	1	0	1	1
Position	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
bit	1	1	0	0	0	1	0	0	1	1	0	1	0	1	0	1
Position	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
bit	1	1	1	0	0	1	1	0	1	1	1	1	0	1	1	1
Position	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64
bit	1	1	0	0	0	0	1	0	0	0	1	1	0	0	1	0

$$\begin{pmatrix} 58 & 50 & 42 & 34 & 26 & 18 & 10 & 2 \\ 60 & 52 & 44 & 36 & 28 & 20 & 12 & 4 \\ 62 & 54 & 46 & 38 & 30 & 22 & 14 & 6 \\ 64 & 56 & 48 & 40 & 32 & 24 & 16 & 8 \\ 57 & 49 & 41 & 33 & 25 & 17 & 9 & 1 \\ 59 & 51 & 43 & 35 & 27 & 19 & 11 & 3 \\ 61 & 53 & 45 & 37 & 29 & 21 & 13 & 5 \\ 63 & 55 & 47 & 39 & 31 & 23 & 15 & 7 \end{pmatrix}$$

Ainsi, avec cette matrice de permutation, le premier bit du nouveau message est le bit 58, le second est le bit 50, le troisième le 42 et ainsi de suite. Le nouveau message deviens alors

Position	1 (58)	2 (50)	3 (42)	4 (34)	5 (26)	6 (18)	7 (10)	8 (2)	9 (60)	10 (52)	11 (44)	12 (36)	13 (28)	14 (20)	15 (12)	16 (4)
bit	0	1	1	1	1	1	0	1	1	0	1	0	1	0	1	1
Position	17 (62)	18 (54)	19 (46)	20 (38)	21 (30)	22 (22)	23 (14)	24 (6)	25 (64)	26 (56)	27 (48)	28 (40)	29 (32)	30 (24)	31 (16)	32 (8)
bit	0	0	1	1	1	1	0	1	0	0	1	0	1	0	1	0
Position	33 (57)	34 (49)	35 (41)	36 (33)	37 (25)	38 (17)	39 (9)	40 (1)	41 (59)	42 (51)	43 (43)	44 (35)	45 (27)	46 (19)	47 (11)	48 (3)
bit	0	1	1	1	1	1	1	1	1	0	1	1	0	0	1	0
Position	49 (61)	50 (53)	51 (45)	52 (37)	53 (29)	54 (21)	55 (13)	56 (5)	57 (63)	58 (55)	59 (47)	60 (39)	61 (31)	62 (23)	63 (15)	64 (7)
bit	0	0	0	0	0	0	1	1	1	1	1	1	0	0	1	0

Soit encore $PI[M_1] = 0111110110101011001111010010101001111111101100100000001111110010$

Gauche et droite. On note G la partie gauche de $PI[M_1]$ correspondant aux 32 premiers bits et D la partie droite correspondant aux 32 derniers.

$$G = 01111101101010110011110100101010 \qquad D = 01111111101100100000001111110010$$

Rondes. On va effectuer 16 *rondes*. Chacune de ces rondes suit le même schéma à ceci près qu'à la ronde k on utilisera le morceau K_k de la clef. Le schéma des rondes est le suivant :

1. On applique la fonction d'expansion au bloc D. On obtient un message $E[D]$ non plus sur 32 mais sur 48 bits que l'on regarde comme 12 blocs de 4 bits.
2. On calcul $E[D] \oplus K_k$ (lors de la ronde k) en additionnant (exclusivement) avec le morceau de clef.
3. On découpe ensuite $E[D] \oplus K_k$ en 8 blocs de 6 bits. Notons $B_1, \ldots, B_8$ ces 8 blocs. Le bloc $B_i = x_1x_2x_3x_4x_5x_6$ où les x_{machin} sont soit 0 soit 1. On considère l'entier n dont l'écriture binaire est x_1x_6. Il s'agit donc d'un entier entre 0 et 3. On considère m l'entier dont l'écriture binaire est $x_2x_3x_4x_5$ ce qui correspond à un entier entre 0 et 15. On va remplacer B_i par le nombre, que l'on écrira en binaire, à l'intersection de la $(n+1)$-ième ligne et $(m+1)$-ième colonne de la matrice de substitution S_i. Il s'agit, par construction d'un bloc de 4 bits.
4. Notons $\mathbb{S}$ l'application successive des matrices de substitution, de sorte que l'on note $\mathbb{S}[E[D] \oplus K_k]$ le message issue de l'itération précédente (en regroupant les 8 blocs de 4 bits). On applique alors la permutation des rondes. On note $P[\mathbb{S}[E[D] \oplus K_k]]$ le résultat
5. On remplace D par $P[\mathbb{S}[E[D] \oplus K_k]] \oplus G$ et G par D.

Réalisation la première ronde.

1.

Position	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
bit	0	1	1	1	1	1	1	1	1	0	1	1	0	0	1	0
Position	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
bit	0	0	0	0	0	0	1	1	1	1	1	1	0	0	1	0

$$\begin{pmatrix} 32 & 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 6 & 7 & 8 & 9 \\ 8 & 9 & 10 & 11 & 12 & 13 \\ 12 & 13 & 14 & 15 & 16 & 17 \\ 16 & 17 & 18 & 19 & 20 & 21 \\ 20 & 21 & 22 & 23 & 24 & 25 \\ 24 & 25 & 26 & 27 & 28 & 29 \\ 28 & 29 & 30 & 31 & 32 & 1 \end{pmatrix}$$

Position	1 (32)	2 (1)	3 (2)	4 (3)	5 (4)	6 (5)	7 (4)	8 (5)	9 (6)	10 (7)	11 (8)	12 (9)	13 (8)	14 (9)	15 (10)	16 (11)
bit	0	0	1	1	1	1	1	1	1	1	1	1	1	1	0	1
Position	17 (12)	18 (13)	19 (12)	20 (13)	21 (14)	22 (15)	23 (16)	24 (17)	25 (16)	26 (17)	27 (18)	28 (19)	29 (20)	30 (21)	31 (20)	32 (21)
bit	1	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0
Position	33 (22)	34 (23)	35 (24)	36 (25)	37 (24)	38 (25)	39 (26)	40 (27)	41 (28)	42 (29)	43 (28)	44 (29)	45 (30)	46 (31)	47 (32)	48 (1)
bit	0	1	1	1	1	1	1	1	1	0	1	0	0	1	0	0

Ainsi $E[D] = 00111111111111011010010000000000011111111010010 0$

2. On réalise le *ou exclusif* avec la clef K_1 :

$$\begin{array}{rl} & 00111111111111011010010000000000011111111010010 0 \\ \oplus & 11111001100000101000111001010111111100001110100 1 \\ \hline & 11000110011111111001010100101011110001111010011 01 \end{array}$$

Ainsi $E[D] \oplus K_1 = 11000110011111111001010100101011110001111010011 01$

3. On regarde $E[D] \oplus K_1$ en 8 blocs de 6 bits.

$$E[D] \oplus K_1 = 110001\ 100111\ 111100\ 101010\ 010101\ 111000\ 111101\ 001101$$

On va remplacer le bloc 110001 à l'aide S_1.

- Pour la ligne : le premier et dernier caractère forment 11 soit 3 en base 10.
- Pour la colonne : les autres caractères du bloc forment 1000 soit 8 en base 10.
- A l'intersection de la ligne $3+1$ et de la colonne $8+1$ de S_1 se trouve l'entier 5 qui, codé sur 4 bits, est 0101.

On va remplacer le bloc 100111 à l'aide S_2.
- Pour la ligne : le premier et dernier caractère forment 11 soit 3 en base 10.
- Pour la colonne : les autres caractères du bloc forment 0011 soit 3 en base 10.
- A l'intersection de la ligne $3+1$ et de la colonne $3+1$ de S_2 se trouve l'entier 1 qui, codé sur 4 bits, est 0001.

On va remplacer le bloc 111100 à l'aide S_3.
- Pour la ligne : le premier et dernier caractère forment 10 soit 2 en base 10.
- Pour la colonne : les autres caractères du bloc forment 1110 soit 14 en base 10.
- A l'intersection de la ligne $2+1$ et de la colonne $14+1$ de S_3 se trouve l'entier 14 qui, codé sur 4 bits, est 1110.

On va remplacer le bloc 101010 à l'aide S_4.
- Pour la ligne : le premier et dernier caractère forment 10 soit 2 en base 10.
- Pour la colonne : les autres caractères du bloc forment 0101 soit 5 en base 10.
- A l'intersection de la ligne $2+1$ et de la colonne $5+1$ de S_4 se trouve l'entier 11 qui, codé sur 4 bits, est 1011.

On va remplacer le bloc 010101 à l'aide S_5.
- Pour la ligne : le premier et dernier caractère forment 01 soit 1 en base 10.
- Pour la colonne : les autres caractères du bloc forment 1010 soit 10 en base 10.
- A l'intersection de la ligne $1+1$ et de la colonne $10+1$ de S_5 se trouve l'entier 15 qui, codé sur 4 bits, est 1111.

On va remplacer le bloc 111000 à l'aide S_6.
- Pour la ligne : le premier et dernier caractère forment 10 soit 2 en base 10.
- Pour la colonne : les autres caractères du bloc forment 1100 soit 12 en base 10.
- A l'intersection de la ligne $2+1$ et de la colonne $12+1$ de S_6 se trouve l'entier 1 qui, codé sur 4 bits, est 0001.

On va remplacer le bloc 111101 à l'aide S_7.
- Pour la ligne : le premier et dernier caractère forment 11 soit 3 en base 10.
- Pour la colonne : les autres caractères du bloc forment 1110 soit 14 en base 10.
- A l'intersection de la ligne $3+1$ et de la colonne $14+1$ de S_7 se trouve l'entier 3 qui, codé sur 4 bits, est 0011.

On va remplacer le bloc 001101 à l'aide S_8.
- Pour la ligne : le premier et dernier caractère forment 01 soit 1 en base 10.
- Pour la colonne : les autres caractères du bloc forment 0110 soit 6 en base 10.
- A l'intersection de la ligne $1+1$ et de la colonne $6+1$ de S_8 se trouve l'entier 7 qui, codé sur 4 bits, est 0111.

En conclusion nous obtenons le message :

$$\mathbb{S}[E[D] \oplus K_1] = 0101\ 0001\ 1110\ 1011\ 1111\ 0001\ 0011\ 0111$$

4. On applique la permutation des rondes $\mathbb{S}[E[D] \oplus K_1]$:

Position	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
bit	0	1	0	1	0	0	0	1	1	1	1	0	1	0	1	1
Position	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
bit	1	1	1	1	0	0	0	1	0	0	1	1	0	1	1	1

$$\begin{pmatrix} 16 & 7 & 20 & 21 & 29 & 12 & 28 & 17 \\ 1 & 15 & 23 & 26 & 5 & 18 & 31 & 10 \\ 2 & 8 & 24 & 14 & 32 & 27 & 3 & 9 \\ 19 & 13 & 30 & 6 & 22 & 11 & 4 & 25 \end{pmatrix}$$

Position	1 (16)	2 (7)	3 (20)	4 (21)	5 (29)	6 (12)	7 (28)	8 (17)	9 (1)	10 (15)	11 (23)	12 (26)	13 (5)	14 (18)	15 (31)	16 (10)
bit	1	0	1	0	0	0	1	1	0	1	0	0	0	1	1	1

Position	17 (2)	18 (8)	19 (24)	20 (14)	21 (32)	22 (27)	23 (3)	24 (9)	25 (19)	26 (13)	27 (30)	28 (6)	29 (22)	30 (11)	31 (4)	32 (25)
bit	1	1	1	0	1	1	0	1	1	1	1	0	0	1	1	0

Au final

$$P[\mathbb{S}[E[D] \oplus K_1]] = 10100011010001111110110111100110$$

5. Pour finir on réalise l'opération $P[\mathbb{S}[E[D] \oplus K_1]] \oplus G$ qui deviendra le nouveau D et le nouveau G sera l'ancien D.

	1	0	1	0	0	0	1	1	0	1	0	0	0	1	1	1	1	1	1	0	1	1	0	1	1	1	1	0	0	1	1	0
$\oplus$	0	1	1	1	1	1	0	1	1	0	1	0	1	0	1	1	0	0	1	1	1	1	0	1	0	0	1	0	1	0	1	0
	1	1	0	1	1	1	1	0	1	1	1	0	1	1	0	0	1	1	0	1	0	0	0	0	1	1	0	0	1	1	0	0

Et

$$G = 01111111101100100000001111110010 \qquad D = 11011110111011001101000011001100$$

On réitère alors ces rondes en changeant la clef à chaque tour.

Initialement.

$$G = 01111101101010110011110100101010 \qquad D = 01111111101100100000001111110010$$

A la fin de la ronde 1.

$$G = 01111111101100100000001111110010 \qquad D = 11011110111011001101000011001100$$

A la fin de la ronde 2.

$$G = 11011110111011001101000011001100 \qquad D = 01101111000010101101000101000010$$

A la fin de la ronde 3.

$$G = 01101111000010101101000101000010 \qquad D = 00010110110001011111000000000101$$

A la fin de la ronde 4.

$$G = 00010110110001011111000000000101 \qquad D = 11000010011110110010001010100101$$

A la fin de la ronde 5.

$$G = 11000010011110110010001010100101 \qquad D = 11011110001100011000100010010110$$

A la fin de la ronde 6.

$$G = 11011110001100011000100010010110 \qquad D = 00110000100011100000011111011101$$

A la fin de la ronde 7.

$$G = 00110000100011100000011111011101 \qquad D = 11011000000101101110110100111101$$

A la fin de la ronde 8.

$$G = 11011000000101101110110100111101 \qquad D = 10110001110000011011010001001001$$

A la fin de la ronde 9.

$$G = 10110001110000011011010001001001 \qquad D = 01100001011001111100011111101100$$

A la fin de la ronde 10.

$$G = 01100001011001111100011111101100 \qquad D = 00101111001001110101000100100100$$

A la fin de la ronde 11.

$$G = 00101111001001110101000100100100 \qquad D = 01000110000011010111100010111011$$

A la fin de la ronde 12.

$$G = 01000110000011010111100010111011 \qquad D = 00010111101001110010010111110111$$

A la fin de la ronde 13.

$$G = 00010111101001110010010111110111 \qquad D = 00101111100101010111011000111111$$

A la fin de la ronde 14.

$$G = 00101111100101010111011000111111 \qquad D = 01100111100101000101100001000001$$

A la fin de la ronde 15.

$$G = 01100111100101000101100001000001 \qquad D = 00110000110010100100001000011100$$

A la fin de la ronde 16.

$$G = 00110000110010100100001000011100 \qquad D = 11010101001001100001000100011010$$

Pour finir on recolle la partie gauche et droite et on fini avec le message

$$M_1' = 00110000110010100100001000011100110101010010011000010001000110 10$$

Permutation initiale inverse. On applique finalement à ce message M_1' la permutation initiale inverse qui fini alors par

$$PI^{-1}[M_1'] = 10001000001101101010000100010011110010110110000010010100100100 00$$

Qui correspond donc au message chiffré. On réitère ensuite l'intégralité de ce processus à tous les blocs du message.