Éléments de cryptologie

Cours et exercices

Définition

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

La **cryptanalyse** est une science qui consiste à tenter de déchiffrer un cryptogramme.

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

Définition

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

Cryptologie de César

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. Ce nombre est appelé **la clef** (de cryptage) ; 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*.

Traitons un autre exemple et cryptons le mot *ZAKARIA* avec 4 pour clef.

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*.

Le cadre *mathématiquement légal* de ce type de calcul est les **congruences**.

Définition

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

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

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 $-1 - 1 = -2 = 2 \times (-1)$.

Exercice 1

Parmi les propositions, lesquelles sont vraies.

1. $15 \equiv_8 7$
2. $99 \equiv_2 -1$
3. $654 \equiv_3 0$
4. $3 \equiv_3 3$
5. $873 \equiv_5 555$
6. $8704 \equiv_{13} 791$
7. $-8 \equiv_9 1$
8. $-984 \equiv_{19} 17$

Exercice 2

Dans chacun des cas, déterminer x modulo n (déterminer le plus petit entier positif y tel que $x \equiv_n y$).

1. $x = 555$, $n = 12$
2. $x = 983$, $n = 45$
3. $x = 3078$, $n = 487$
4. $x = 573$, $n = 159$

Théorème (Opérations)

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

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

Par exemple :

- $25 \equiv_4 1$ 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 $10^{2016} \equiv_9 1$

Exercice 3

Simplifier les expressions suivantes.

1. 123^{122} modulo 124
2. $2014 \times 2015 \times 2016$ modulo 2017
3. 2792^{217} modulo 5
4. 133^{39} modulo 10
5. 99^{100} modulo 42
6. 2^{1147} modulo 17

Exercice 4

Montrer que pour tout $n \in \mathbb{N}$, $9^n - 2^n$ est multiple de 7.

Exercice 5

Montrer que pour tout entier $n \in \mathbb{N}$, $6^n + 13^{n+1}$ est divisible par 7.

Exercice 6

1. Montrer que $34^{57} - 1$ est un multiple de 11.
2. Montrer que $9518^{42} - 4$ est divisible par 5.

Exercice 7

Crypter le mot *MATHEMATIQUES* par la méthode de César avec 19 comme clef.

Exercice 8

Crypter le mot *ZEBRE* par la méthode de César avec 25 comme clef.

Exercice 9

On a utilisé la méthode de César avec 25 comme clef pour obtenir *BDRSBGZTCBZAQTKD*. Quel était le message original ?

Cryptanalyse de César - BRUTE FORCE

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...

Exercice 10

Crypter le message *VIVELACRYPTO* par la méthode de César par paquet de 3 avec 190091 comme clef.

Exercice 11

On a utilisé la méthode de César par paquet de 3 avec 250025 comme clef pour obtenir *208907-107501-39318-48312-77499*. Quel était le message original ?

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 [1] 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* [2]

Exercice 12

Ce message a été codé par la méthode de César : *2138-523-1651-1650-712-1434-1834-2338-412-721-212-708*. Quel était le message original ?

1. "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.

2. 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.