

CRYPTOGRAPHIE 1 : CODAGE D'UN MESSAGE



Le chat de Philippe Geluck

De nos jours, le codage d'un message pour le transmettre secrètement est devenu courant, par exemple lors de la communication de données personnelles sur un site web sécurisé (voir https://interstices.info/jcms/int_63483/a-propos-de-la-cryptographie). Dans cette activité, nous allons voir différentes façons de coder un message.

1 Le code de César

Le chiffrement par décalage aussi connu comme le chiffre de César est une méthode très simple (et la plus ancienne) de cryptage d'un message utilisée par Jules Cesar dans ses correspondances secrètes.

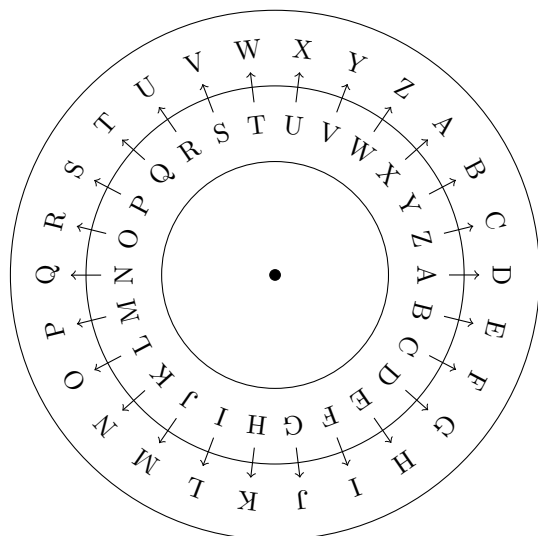
Définition 1.1. Le **chiffrement par décalage** d'ordre n consiste à remplacer toutes les lettres du message par les lettres correspondantes n rang plus loin dans l'alphabet.

Exemple. Le chiffrement par décalage d'ordre 3 :

Avec cette méthode de codage, la première lettre de l'alphabet A sera remplacée par la 4e lettre de l'alphabet soit D .

- 1) Par quelles lettres va-t-on remplacer B , C et D ?

La figure suivante illustre les associations entre les lettres pour le chiffrement par décalage d'ordre 3



- 2) Coder le mot CRYPTOGRAPHIE à l'aide du disque de codage précédent.
- 3) Décrypter à l'aide du disque de codage le message suivant : MXOHV FHVDU

Le nombre 3 est appelé la clé du code de César du message précédent.

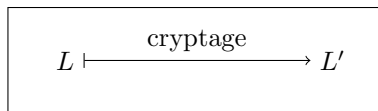
Exemple. Le chiffrement par décalage d'ordre 10 :

- 1) Découper le disque en annexe et le placer sur le disque précédent pour vous aider à crypter le message suivant : CRYPTOGRAPHIE avec la méthode de chiffrement par décalage d'ordre 10.

2) Le message suivant QLHU CPSHY a été codé avec la méthode de chiffrement par décalage d'ordre 7. Décrypter le.

Il n'y a que 26 façons différentes de crypter un message avec le code de César (chiffrement par décalage). Cela en fait donc un code très peu sûr. Pourtant, en raison de sa grande simplicité, le code de César fut encore employé par les officiers sudistes pendant la guerre de Sécession, et même par l'armée russe en 1915.

Maintenant, nous allons voir une autre façon de coder les messages. Avant, on peut déjà remarquer que pour coder un message, il nous faut une application qui permutent les lettres entre elles telle que deux lettres différentes soient bien associées à deux lettres différentes. Le **cryptage** est une *fonction* :



2 Chiffrement affine

Nous allons associer aux différentes lettres de l'alphabet leur rang dans l'alphabet (mais en commençant à compter par 0) :

Lettre	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Rang	0	1	2	3	4	5	6	7	8																24	25

On considère la fonction affine f définie par $f(x) = 3x + 1$.

1) Calculer les images de 0, 1, 2, 8, 9 par la fonction f .

Pour crypter notre message, nous allons remplacer la lettre A (de rang 0) par la lettre B (de rang $f(0) = 1$) et ainsi de suite.

2) Par quelles lettres va-t-on remplacer les lettres B, C, D et I ?

3) Quel problème se pose avec la lettre J (de rang 9)?

Pour régler le problème précédent, nous allons remplacer $f(9) = 28$ par $28 - 26 = 2$. Ainsi, nous remplacerons la lettre J par la lettre C (de rang 2).

Voici le tableau de codage des lettres de l'alphabet :

Lettre L	A	B	C	D	E	F	G	H	I	J	K	L	M
Rang x	0	1	2	3	4	5	6	7	8	9	10	11	12
$f(x) = 3x + 1 \text{ modulo } 26$	1	4	7	10					25	$28 - 26 = 2$	5	8	
Code L'	B	E	H	K					Z	C	F	I	

Lettre L	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Rang x	13	14	15	16	17	18	19	20	21	22	23	24	25
$f(x) = 3x + 1 \text{ modulo } 26$	14			23	$26 - 26 = 0$	3							24
Code L'	O			X	A	D							Y

4) Compléter le tableau précédent.

5) À l'aide du tableau précédent, coder le mot CRYPTOGRAPHIE. -----

6) Décrypter le message : HWZQQANLNOG BQQZON. -----

Définition 2.1. Le **chiffrement affine** consiste à remplacer les lettres une par une avec la méthode suivante : la lettre de rang x est remplacée par la lettre de rang $f(x) = ax + b$ modulo 26.

Remarque. Il existe encore d'autres méthodes de chiffrement, par exemple : Le chiffre de Vigenère (voir http://fr.wikipedia.org/wiki/Chiffre_de_Vigenère).

Exercice 1. Le message suivant a été codé avec la méthode de chiffrement par décalage.

XBL Q'HPTL H MHPYL HWYLUKYL BU UVTIYL BAPSL HBE ZHNLZ

Décrypter le message.

Exercice 2 (*)**.

1) On considère la fonction affine f définie par $f(x) = 7x + 3$. Coder le mot CRYPTOGRAPHIE à l'aide de la méthode de chiffrement affine associée à f .

2) On considère la fonction affine f définie par $f(x) = x + 3$. Coder le mot CRYPTOGRAPHIE à l'aide de la méthode de chiffrement affine associée à f .

Que se passe-t-il lorsque $a = 1$ avec la méthode de chiffrement affine associée à $f(x) = ax + b$?

3) On considère la fonction affine f définie par $f(x) = 2x + 1$. Le mot CRYPTOGRAPHIE par la méthode de chiffrement affine associée à f devient FJXFNDNJBFP RJ.

a) Par quelles lettres sont remplacées les lettres C et P? -----

b) Quel problème rencontre-t-on pour le décodage? -----

c) Déterminer le pgcd de $a = 2$ et 26. Conjecturer une condition sur a .

