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.

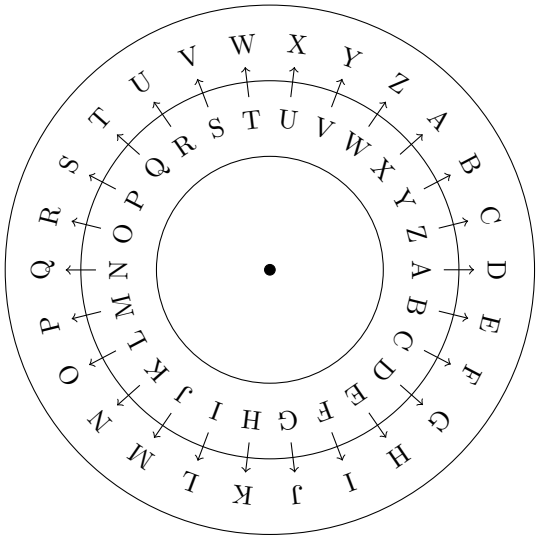
Définition 1.1. Le **chiffrement par décalage** d'ordre n consiste à remplacer toutes les lettres du message par les lettres correspondantes n rang plus loin dans l'alphabet.

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 pt 1) Par quelles lettres va-t-on remplacer B, C et D ?
On remplace par E, F et G respectivement.

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

1 pt



2) Coder le mot `CRYPTOGRAPHIE` à l'aide du disque de codage précédent.
F U B S W R J U D S K L H

1 pt 3) Décrypter à l'aide du disque de codage le message suivant : `MXOHV FHVDU`
JULES CESAR

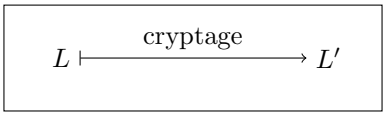
Le nombre 3 est appelé la **clé** *du code de César du message précédent.*

1 pt *Exemple.* 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. M B I Z D Y Q B K Z R S O

1 pt 2) Le message suivant `QLHU CPSHY` a été codé avec la méthode chiffrement par décalage d'ordre 7. Décrypter le. JEAN VILAR

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 permuttent 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 $f(x) = 3x + 1$.

2 pt 1) Calculer les images de 0, 1, 2, 8, 9 par la fonction f.
$f(0) = 1$, $f(1) = 4$, $f(2) = 7$, $f(8) = 25$, $f(9) = 28$.

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.

1 pt 2) Par quelles lettres va-t-on remplacer les lettres B, C, D et I ?
$B \to E$, $C \to H$, $D \to K$ et $I \to Z$

1 pt 3) Quel problème se pose avec la lettre J (de rang 9) ?
Il n'y a pas de lettre de rang 28.

Pour régler le probleme 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
$f(x) = 3x + 1$ modulo 26	1	4	7	10	13	16	19	21	25	28 - 26 = **2**	5	8	11
Code L'	B	E	H	K	N	Q	T	W	Z	C	F	I	L

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
$f(x) = 3x + 1$ modulo 26	14	17	20	23	26 - 26 = 0	3	6	9	12	15	18	21	24
Code L'	O	R	U	X	A	D	G	J	M	P	S	V	Y

2 pt 4) Compléter le tableau précédent.

2 pt 5) À l'aide du tableau précédent, coder le mot `CRYPTOGRAPHIE`. H A V U G R T A B U W Z N

1 pt 6) Décrypter le message : `HWZQQANLNOG BQQZON`. CHIFFREMENT AFFINE

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`).

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

`XBL Q'HPTL H MHPYL HWWYLUKYL BU UVTIYL BAPSL HBE ZHNLZ`

La lettre H qui se retrouve seul correspond sans doute à A. On en déduit que la clé devrait être 7. En effet, si on décode avec cette clé, on obtient le message :
QUE J AIME A FAIRE APPRENDRE UN NOMBRE UTILE AUX SAGES.
Remarque : Si on écrit le nombre de lettres de chaque mots du message précédent, on obtient la suite suivante : 3,1415926535 les premières décimales du nombre π.

Exercice 2 (***).

2 pt 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.
R S P E G X T S D E A H F

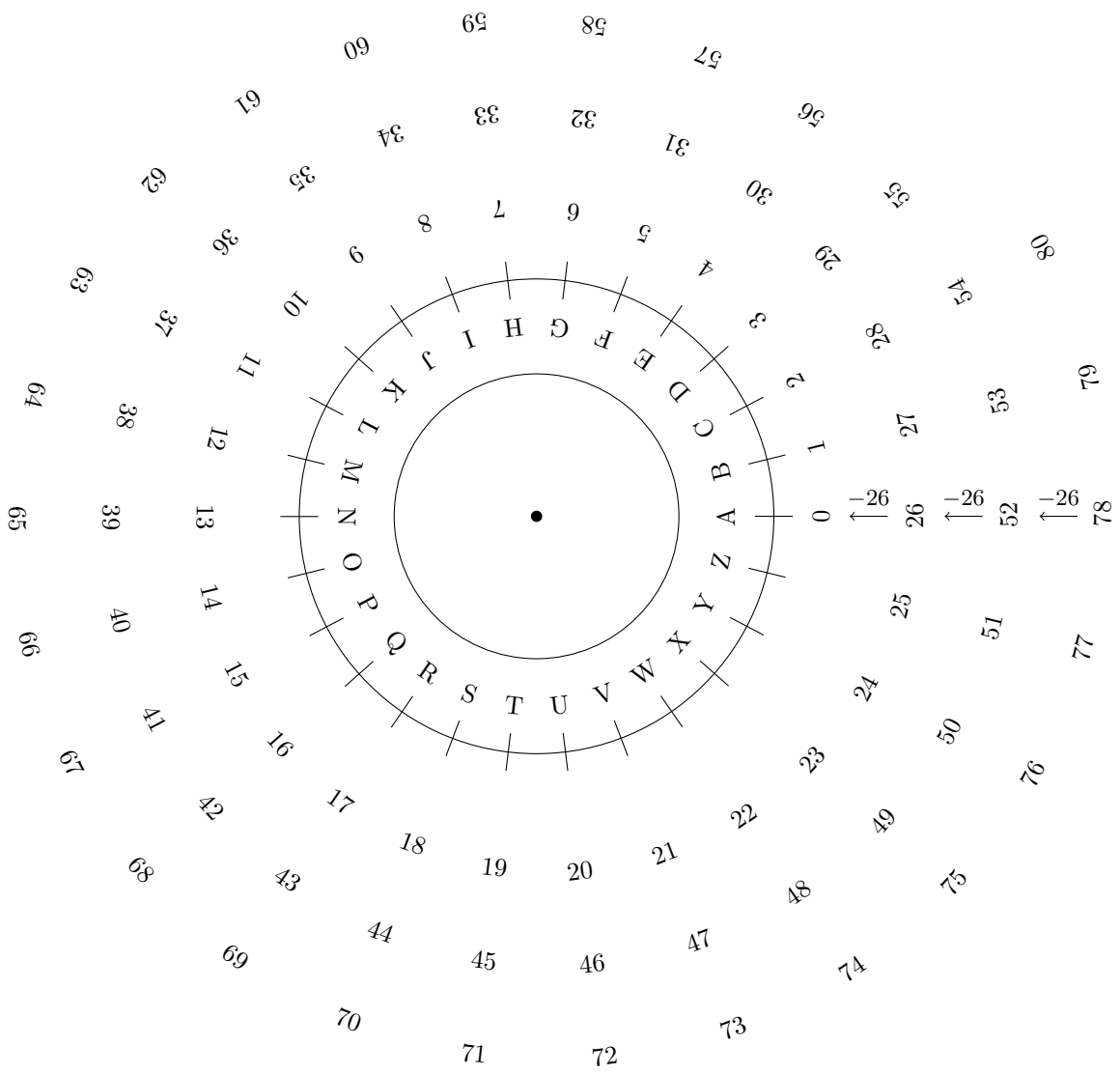
1 pt 2) On considère la fonction affine f définie par $f(x) = x + 3$. Coder le mot CRYPTOGRAPHIE à l'aide de la méthode de chiffrement affine associée à f.
F U B S W R J U D S K L H
Que se passe-t-il lorsque $a = 1$ avec la méthode de chiffrement affine associée à $f(x) = ax + b$?
Le chiffrement affine avec $a = 1$ correspond au chiffrement par décalage de clé b.

1 pt 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 FJXFNDNJBFPRJ.

+1 pt a) Par quelles lettres sont remplacées les lettres C et P ?
Les deux lettres seront remplacées par la lettre F.

+1 pt b) Quel problème rencontre-t-on pour le décodage ?
Pour décoder la lettre F par exemple, il faut faire un choix entre C ou P. Ce qui rend impossible le décodage dans le cas général.

+1 pt c) Déterminer le pgcd de $a = 2$ et 26. Conjecturer une condition sur a.
Le pgcd de 2 et 26 est 2. Avant avec $a = 3$ et 7, le codage était possible. Or 3 et 7 sont premiers avec 26.
On conjecture donc que a doit être premier à 26 (le nombre de lettres de l'alphabet).



Le reste de la division Euclidienne de 26, 52, 78 par 26 est 0. On résumera ce fait ainsi :

$$0 \equiv 26 \equiv 52 \equiv 78 \quad \text{modulo } 26$$