



**DEVOIR MAISON**  
Pour le .../.../...

4<sup>ème</sup>



**CRYPTAGE et DECRYPTAGE**

**Le Code César :** Depuis l'antiquité, les hommes ont toujours éprouvé le besoin de modifier un texte afin de le dissimuler à la vue des personnes non autorisées. Cette science s'appelle la *cryptographie*. L'un des premiers codages utilisés est le *code de César* qui doit son nom à l'empereur romain Jules César. Il consiste à décaler chaque lettre de l'alphabet de *trois* rangs :

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
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Le mot « **CRYPTOGRAPHIE** » devient après codage « **FUBSWRJUDSKLH** ».

Le mot codé « **FRGH GH FHVDU** » s'écrit « **CODE DE CESAR** » après décodage.

On peut, de la même façon, faire un codage en décalant les lettres de l'alphabet d'un autre nombre de rangs. Ce nombre sera appelé *la clé* du codage. Par exemple un codage de César de clé 8, signifie qu'on décale chaque lettre de 8 rangs, A est remplacé par I, B par J, etc...

- **Exercice N°1** : En utilisant un codage de César dont la clef est 3, décoder le texte :  
« **GDQV OD YLH LO IDXW VDYRLU FRPSWHU PDLV SDV VXU OHV DXWUHV** »
- **Exercice N°2** : En utilisant un codage de César dont la clef est 17, coder le texte :  
« **LES PETITS RUISSEAUX FONT DE GRANDES RIVIERES** »
- **Exercice N°3** : Un codage de César, transforme « **SUBSTITUTION** » en « **KMTKLALMLAGF** ». Quelle est la clé ?

**Décryptage d'un texte par analyse des fréquences :**

Si on ne connaît pas la clé, le code de César est assez facile à décrypter. Une méthode un peu longue, consiste à essayer toutes les clés possibles.

- **Exercice N°4** : Combien y a-t-il de clés possibles ?

Une autre est l'analyse des fréquences. Selon la langue, certaines lettres reviennent plus souvent que d'autres (en Français, par exemple, la lettre la plus utilisée est la lettre E). Ainsi la lettre apparaissant le plus souvent dans un texte crypté par le chiffrement de César correspondra vraisemblablement à la lettre E. Une simple soustraction donne alors la clé de cryptage.

Fréquences théoriques des lettres dans un texte (en %)												
E	S	A	I	N	T	R	U	L	O	D	C	P
17,52	8,17	8,01	7,35	7,22	7,07	6,69	6	5,77	5,43	3,91	3,23	2,94
M	V	Q	G	F	H	B	X	J	Y	Z	K	W
2,90	1,41	1,14	1,06	1,06	0,88	0,88	0,47	0,44	0,30	0,12	0,05	0,02

- **Exercice N°5** , Comment déchiffrer le texte suivant sans connaître la clef ?  
 « YRF RYRIRF QR PRGGR PYNFFR BAG QR OBAF ERFHYGNGF RA ZNGURZNGVDHRF »

*Marche à suivre* : Compléter le tableau suivant puis comparer la fréquence d'apparition des lettres dans ce texte (arrondir au centième) avec la fréquence théorique d'apparition des lettres d'un texte de la langue française. En déduire le décryptage du texte.

<b>Lettre</b>	A	B	C	D	E	F	G	H	I	J	K	L	M
<b>Nombre</b>													
<b>Fréquence</b>													
<b>Lettre</b>	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
<b>Nombre</b>													
<b>Fréquence</b>													

- **Exercice N°6** . Sur une scène de crime, dans une poubelle, sur du papier froissé, les enquêteurs ont trouvé le message suivant :  
 « DCZMPS O WAOUWBS IBS GCZIHWCB  
 DCIF HFOBGASHHFS ZSG ASGGOUSG  
 TCBQHWCBBOBH O Z OWRS RS HCFQVSG  
 SBTZOAASSG »



A l'aide d'un tableur, réaliser un tableau des effectifs et des fréquences d'apparition des lettres dans ce message. Insérer ensuite un diagramme en barres illustrant cette répartition.

Déchiffrer le message et faire des recherches, à l'aide d'internet, sur le nom y apparaissant.

Cet exercice pourra être envoyé par courriel de la manière suivante :

**À :** XXXXXX @laposte.net  
**Objet :** Devoir n°4 (NOM Prénom)  
**Joindre :** Le fichier avec le DM.

*Écrire ensuite le texte suivant :*  
 « Bonjour M. XXXXXX, voici en PIECE  
 JOINTE mon DM.  
 Bonne correction,  
 NOM Prénom »

<b>Destinataire :</b>	XXXXX@laposte.net
<b>Copie :</b>	
<b>Cci :</b>	
<b>Objet :</b>	devoirN°127 (NOM Prénom)
<b>Pièce(s) jointe(s) :</b>	1 fichier(s)   _devoir N°12...ods supprimer
<b>Vérifier l'orthographe</b>	Thème : Aucun    Priorité : Normale
police    taille    G / S A    [icônes de mise en forme]	
« Bonjour M. XXXXXX, voici en PIECE JOINTE mon DM. Bonne correction, NOM Prénom »	