

**ADDITIONNER UNE LETTRE ET UN NOMBRE**

Nous allons créer une nouvelle opération mathématique, l'addition entre les lettres de l'alphabet et les nombres entiers. Pour ne pas confondre cette opération étrange avec l'addition habituelle, nous allons utiliser un nouveau symbole \oplus . Avant d'effectuer cette opération il est nécessaire de numéroter les 26 lettres de l'alphabet de la manière suivante :

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Pour ajouter un nombre entier à une lettre on applique l'algorithme suivant :

- effectuer la somme du numéro de la lettre et du nombre entier;
- si la somme est comprise entre 0 et 25, ne rien faire;
- sinon retirer 26 à cette somme jusqu'à obtenir un nombre entier compris entre 0 et 25 (il faut parfois effectuer plusieurs fois cette soustraction!);
- le résultat est la lettre qui correspond au numéro obtenu.

Effectuer les additions suivantes :

$A \oplus 1 =$

$D \oplus 9 =$

$T \oplus 8 =$

$A \oplus 26 =$

$R \oplus 32 =$

$Z \oplus 1 =$

$M \oplus 8 =$

$M \oplus 13 =$

$L \oplus 27 =$

$L \oplus 100 =$

LE CHIFFRE DE CÉSAR

On appelle *chiffre de César* toutes les méthodes de cryptage qui consistent à décaler les lettres de l'alphabet d'un nombre de rang fixé ce qui revient à ajouter un nombre entier secret aux lettres en utilisant la méthode précédente. Le nombre entier secret s'appelle **la clé de cryptage**. La connaissance de cette clé permet de décrypter le message. L'histoire atteste que l'empereur romain Jules Cesar (Rome -102 — Rome -44) utilisait ce chiffre en décalant les lettres de 3 rangs.

Combien il y a-t-il de clés de cryptages différentes pour un chiffre de César?

Cryptez la citation suivante du logicien britannique Bertrand Russel (Trellech 1872 — Penrhyndeudraeth 1970) en utilisant le chiffre de César dont la clé est 10.

« LES MATHÉMATIQUES PEUVENT ÊTRE DÉFINIES COMME UNE SCIENCE DANS LAQUELLE ON NE SAIT JAMAIS DE QUOI ON PARLE NI SI CE QU'ON DIT EST VRAI »

Pour vous aider dans cette tâche, vous devez compléter le tableau suivant. Avant cela calculez $A \oplus 10 =$.

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

Cryptage :

CRYPTANALYSE D'UN CHIFFRE DE CÉSAR

Voici une citation du journaliste Laurent Lemire chiffrée avec un code de César :

YRFZN GURZN GVDHR FABAG CRHGR GEREV RANIB VENIR PYNIV
RDHBG VQVRA ARRYR RRVAG RERFF RAGAR NAZBV AFQVN OYRZR
AGYRF ZVYVG NVERF QRCHV FDHRY YRFCR EZRGG RAGQR PNYPH
YREYN GENWR PGBVE RQHAC EBWRP GVYR

👉 Quelles sont les cinq lettres qui apparaissent le plus dans ce texte chiffré?

Voici les lettres de l'alphabet français les plus fréquentes dans un texte quelconque :

E	A	I	S	T	N	R	U	L	O	D	M	P	C	V	Q	G
16%	9%	8%	8%	7%	7%	6%	6%	5%	4%	3%	3%	3%	3%	2%	1%	1%

Le philosophe arabe Abū Yūsuf Ya'qūb ibn Ishāq al-Kindī dit Al-Kindi (Koufa 801 — Bagdad 873) au IX^e siècle fait la plus ancienne description de l'analyse fréquentielle. Il est très probable que cette analyse soit née des travaux effectués pour reconstituer la chronologie des révélations du Coran¹. Il expose alors les fondements de cette méthode de cryptanalyse dans son traité intitulé Manuscrit sur le déchiffrement des messages cryptographiques. Il montre qu'un message chiffré conserve la trace du message clair original en gardant les fréquences d'apparitions de certaines lettres.

👉 En observant la fréquence d'apparition des lettres dans le texte chiffré, déterminer la clé correspondant à ce code de César.

👉 Compléter le tableau suivant :

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

👉 Déchiffrer ensuite ce message.

Décryptage :

Le ROT13 (rotate by 13 places) est un cas particulier du chiffre de César, un algorithme simpliste de chiffrement de texte. Comme son nom l'indique, il s'agit d'un décalage de 13 caractères de chaque lettre du texte à chiffrer. Son principal aspect pratique est que le codage et le décodage se font exactement de la même manière. Bien qu'il ne soit pas évident de lire un texte une fois qu'il est chiffré avec ROT13, ce chiffrement est inapproprié pour conserver des secrets en sécurité. Il est plutôt utilisé dans les pages web pour ne pas dévoiler à tous des solutions de jeux, des fins de films ou pour ne pas divulguer l'intrigue d'une série...



CRYPTOGRAPHIE

 **CHIFFRE DE CÉSAR** — Correction 



À rédiger



CRYPTOGRAPHIE



INTENTIONS PÉDAGOGIQUES

INFORMATIONS LÉGALES

- **Auteur** : Fabrice ARNAUD
- **Web** : pi.ac3j.fr
- **Mail** : contact@ac3j.fr
- **Dernière modification** : 2 septembre 2025 à 6:42

Ce document a été écrit pour L^AT_EX avec l'éditeur VIM - Vi Improved Vim 9.1.
Il a été compilé sous Linux Ubuntu Noble Numbat 24.04 avec la distribution TeX Live 2023.20240207-101 et LuaHBTeX 1.17.0

Pour compiler ce document, un fichier comprenant la plupart des macros est nécessaires. Ce fichier, Entete.tex, est encore trop mal rédigé pour qu'il puisse être mis en ligne. Il est en cours de réécriture et permettra ensuite le partage des sources dans de bonnes conditions.
Le fichier source a été réalisé sous Linux Ubuntu avec l'éditeur Vim. Il utilise une balise spécifique à Vim pour permettre une organisation du fichier sous forme de replis. Cette balise %{{{ ... %}}} est un commentaire pour L^AT_EX, elle n'est pas nécessaire à sa compilation. Vous pouvez l'utiliser avec Vim en lui précisant que ce code définit un repli. Je vous laisse consulter la documentation officielle de Vim à ce sujet.

LICENCE CC BY-NC-SA 4.0



Attribution Pas d'Utilisation Commerciale Partage dans les Mêmes Conditions 4.0 International

Ce document est placé sous licence CC-BY-NC-SA 4.0 qui impose certaines conditions de ré-utilisation.

Vous êtes autorisé à :

- Partager** — copier, distribuer et communiquer le matériel par tous moyens et sous tous formats
- Adapter** — remixer, transformer et créer à partir du matériel

L'Offrant ne peut retirer les autorisations concédées par la licence tant que vous appliquez les termes de cette licence.

Selon les conditions suivantes :

- Attribution** — Vous devez créditer l'Œuvre, intégrer un lien vers la licence et indiquer si des modifications ont été effectuées à l'Œuvre. Vous devez indiquer ces informations par tous les moyens raisonnables, sans toutefois suggérer que l'Offrant vous soutient ou soutient la façon dont vous avez utilisé son œuvre.
- Pas d'Utilisation Commerciale** — Vous n'êtes pas autorisé à faire un usage commercial de cette Œuvre, tout ou partie du matériel la composant.
- Partage dans les Mêmes Conditions** — Dans le cas où vous effectuez un remix, que vous transformez, ou créez à partir du matériel composant l'Œuvre originale, vous devez diffuser l'œuvre modifiée dans les mêmes conditions, c'est à dire avec la même licence avec laquelle l'œuvre originale a été diffusée.
- Pas de restrictions complémentaires** — Vous n'êtes pas autorisé à appliquer des conditions légales ou des mesures techniques qui restreindraient légalement autrui à utiliser l'Œuvre dans les conditions décrites par la licence.

Consulter : <https://creativecommons.org/licenses/by-nc-sa/4.0/deed.fr>

Comment créditer cette Œuvre ?

Ce document, , a été créé par **Fabrice ARNAUD (contact@ac3j.fr)** le 2 septembre 2025 à 6:42.

Il est disponible en ligne sur **pi.ac3j.fr**, **Le blog de Fabrice ARNAUD**.

Adresse de l'article : .