Cryptographie

Chiffre de César

Quatrième

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 ⊕. 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 ⊕ 1 =	D ⊕ 9 =	T ⊕ 8 =	A ⊕ 26 =	R ⊕ 32 =
Z ⊕ 1 =	M ⊕ 8 =	M ⊕ 13 =	L ⊕ 27 =	L ⊕ 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 MATHEMATIQUES PEUVENT ETRE DEFINIES 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 ⊕ 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 ARRYY RFVAG 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 Isḥāq 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 divulgâcher l'intrigue d'une série...

Chiffre de César — Correction

À rédiger

Informations légales

- **Auteur :** Fabrice ARNAUD
- **Web :** pi.ac3j.fr
- **Mail :** contact@ac3j.fr
- **Dernière modification :** 30 avril 2026 à 12:51

Ce document a été écrit pour LaTeXavec l'éditeur VIM - Vi Improved Vim 9.1.967
Il a été compilé sous Linux Ubuntu Questing Quokka (Le Quokka en quête) 25.10 avec la distribution TeX Live 2024.20250309 et LuaTex 1.18.0

Le fichier source a été réalisé sous Linux Ubuntu avec l'éditeur Vim.

J'aimerais beaucoup rendre disponibles mes sources en TeX. Dans un monde idéal, je le ferai immédiatement. J'ai plusieurs fois constaté que des pilleurs du Net me volent mes fichiers pdf, retirent cette dernière page de licence, pour les mettre en ligne et parfois même les rendre payants. N'ayant pas les moyens de mettre un cabinet d'avocats sur cette contravention à la licence CC BY-NC-SA 4.0, je fais le choix de ne pas rendre mes sources disponibles.
La plupart des pdf proposés sur ce blog ne contiennent aucun filigrane, je ne les signe pas. Cela permet aux collègues, aux parents, aux élèves, de disposer d'un document anonyme dont chacun peut disposer en respectant la licence qui est particulièrement souple pour les utilisateurs non commerciaux. Je me suis contenté d'ajouter mes références sur cette dernière page. Seules les corrections d'examens contiennent un filigrane vertical. J'ai en effet constaté que certains sites peu scrupuleux, vendaient mes corrections alors qu'elles sont disponibles librement et gratuitement sur mon site. Cette solution est insatisfaisante, je n'ai pas trouvé mieux !
Les QR codes présents sur certains documents pointent vers le fichier pdf lui-même et sa correction. Ce lien ne pointe ni vers une page de mon blog ni vers une quelconque publicité. Vous pouvez le laisser si vous souhaitez que vos élèves accèdent au document en ligne avec sa correction.
Si vous êtes un enseignant et que vous diffusez ce document dans le cadre strict de votre établissement scolaire, inutile de vous poser des questions sur la licence ci-dessous ! Dans la mesure où vous limitez cette diffusion à votre classe ou un environnement numérique de travail privé, n'hésitez pas à vous servir !

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 même 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'Oeuvre 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 crée par **Fabrice ARNAUD (contact@ac3j.fr)** le 30 avril 2026 à 12:51.
Il est disponible en ligne sur **pi.ac3j.fr**, **Le blog de Fabrice ARNAUD**.
Adresse de l'article :