	<h1 style="color: red;">Fiche élève 1/5</h1> <h2 style="color: green;">Comment sont cryptées les données avant d'être communiquées ?</h2> <h3>Thème n°2 et 3</h3>	Cycle 4
		Technologie Cycle 4
		Séance 1
		Sources Traam Académie de Nancy-Metz

### Compétences disciplinaires de Technologie : « Thème 2 et 3 » :

Compétences de fin de cycle	Repères de progressivité : 4 <sup>e</sup>
Comprendre et modifier un programme associé à une fonctionnalité d'un objet ou d'un système technique	Analyser les données et en déduire des modifications à apporter au programme  Compléter un programme pour répondre à une fonctionnalité d'un OST  Tester et valider, dans un environnement simulé ou réel, une modification du programme

### Introduction : « Histoire du cryptage des données – du code César à la clé Wi-Fi moderne »



**Le besoin de protéger l'information est presque aussi ancien que l'écriture elle-même.**

Dès l'Antiquité, les dirigeants, militaires et diplomates ont cherché à transmettre des messages confidentiels sans que l'ennemi puisse les comprendre. L'un des exemples les plus célèbres est **le code César** : utilisé par Jules César au 1er siècle av. J.-C., il consistait à décaler chaque lettre de l'alphabet d'un nombre fixe de positions (par exemple, un décalage de 3 transforme A en D, B en E, etc.). Simple mais efficace pour l'époque, il illustrait déjà l'idée centrale de tout chiffrement : **rendre un message illisible sans la clé.**

Au fil des siècles, d'autres méthodes sont apparues, comme le **chiffre de Vigenère** (XVI<sup>e</sup> siècle), qui utilisait une clé répétée pour appliquer plusieurs décalages successifs. Plus complexe à casser, il fut longtemps considéré comme incassable. Mais l'avancée des mathématiques et l'apparition des premières techniques de **cryptanalyse finirent par en venir à bout.**

Au XX<sup>e</sup> siècle, les besoins militaires lors des deux guerres mondiales ont accéléré l'innovation. L'exemple le plus marquant est sans doute la machine **Enigma**, utilisée par l'Allemagne nazie. Ce système électromécanique de rotors produisait un chiffrement polyalphabétique très complexe pour l'époque. Sa décryptanalyse par les Alliés, **grâce aux travaux d'Alan Turing** et de son équipe à Bletchley Park, fut décisive dans l'issue du conflit. Avec l'essor de l'informatique, le chiffrement est passé du domaine **mécanique au domaine électronique, puis numérique.**

L'arrivée d'Internet a popularisé la **cryptographie à clé publique**, qui permet à deux parties de communiquer de manière sécurisée **sans avoir à échanger au préalable une clé secrète.** Cela a rendu possibles le commerce en ligne, les signatures électroniques et le chiffrement de bout en bout dans la messagerie. Aujourd'hui, les méthodes de protection vont bien au-delà des substitutions et transpositions. Les algorithmes modernes combinent mathématiques avancées, gestion de clés complexes et protocoles robustes. Dans notre quotidien, le cryptage est partout : dans les connexions **HTTPS**, dans les applications de messagerie chiffrée, et même dans nos réseaux domestiques via les normes **Wi-Fi WPA3.**

La **clé Wi-Fi** que nous utilisons désormais n'est pas qu'un simple mot de passe : elle repose sur des suites de nombres générés aléatoirement et échangés de manière sécurisée, rendant le piratage extrêmement difficile pour quiconque n'a pas accès aux moyens de calcul d'un État ou d'une organisation spécialisée.

**Ainsi, du simple décalage alphabétique de César aux systèmes cryptographiques sophistiqués de notre époque, l'histoire du chiffrement est celle d'une course permanente entre ceux qui veulent protéger l'information et ceux qui cherchent à la percer.**



# Fiche élève 2/5

## Comment sont cryptées les données avant d'être communiquées ?

### Thème n°2 et 3

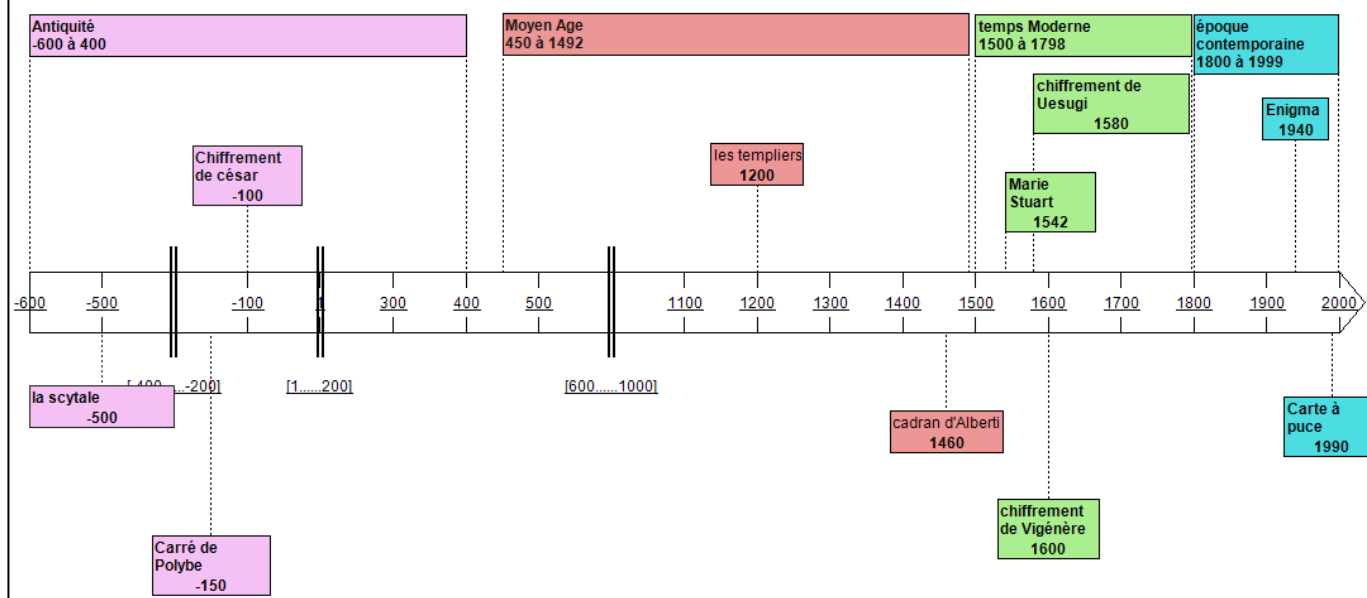
Cycle 4

Technologie

Séance 1

Cycle 4

frise chronologique de l'évolution de la cryptographie



**La situation de départ :**

<https://ladigitale.dev/digiview/#/v/689d952c60915>



**Le cryptage des données :**

<https://sites.ac-nancy-metz.fr/technologie-college/cryptoMahli/index.html>

<https://www.apprendre-en-ligne.net/crypto/cesar/index.html>



**Quelques définitions :**

La **cryptologie** est la science qui étudie l'ensemble des techniques liées à la protection de l'information. Elle regroupe deux domaines principaux : la **cryptographie**, qui concerne la création de codes secrets pour protéger les données, et la **cryptanalyse**, qui concerne l'étude et la détection des failles dans les systèmes de chiffrement afin de les casser.

La **cryptographie** est la branche de la cryptologie qui s'intéresse à la conception de techniques et d'algorithmes permettant de sécuriser les communications. Elle consiste à transformer les informations (texte clair) en un format illisible (texte chiffré) pour empêcher les personnes non autorisées d'accéder aux données, tout en permettant à la personne légitime de les déchiffrer à l'aide d'une clé secrète.

La **cryptanalyse** est l'étude et l'analyse des systèmes de chiffrement dans le but de découvrir des failles ou de casser un code. Elle vise à comprendre comment déchiffrer un message sans posséder la clé de décryptage. Les cryptanalystes cherchent souvent des méthodes pour attaquer des systèmes de chiffrement ou pour trouver des points faibles dans les algorithmes utilisés.





# Fiche élève 4/5

## Comment sont cryptées les données avant d'être communiquées ?

Thème n°2 et 3

Cycle 4

Technologie

Séance 1

Cycle 4

Quelle est la lettre la plus utilisée dans le texte à déchiffrer ? **Z**

Que peux-tu conclure ? : \_\_\_\_\_

\_\_\_\_\_

Le chiffre de César utilisé pour crypter le message est donc de :

\_\_\_\_\_

**Compléter le tableau de correspondance avec le décalage trouvé :**

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

Vidéo d'explication du code CESAR :

<https://ladigitale.dev/digiview/#/v/689d9c1f47334>



Utiliser Scratch pour tester :

<https://www.dcode.fr/chiffre-cesar>

<https://www.apprendre-en-ligne.net/crypto/cesar/index.html>

<https://scratch.mit.edu/projects/116204998/>



Déchiffrer le message  
le texte du message à déchiffrer

Utilise l'application «Menu : **Chiffre de César** CryptoMahli → **Créer/Utiliser l'alphabet de César** » pour analyser



\_\_\_\_\_

**C'est l'article** \_\_\_\_\_

Vérifier votre travail avec le programme SCRATCH : <https://scratch.mit.edu/projects/863678708/>



# Fiche élève 5/5

Comment sont cryptées les données avant d'être communiquées ?

Thème n°2 et 3

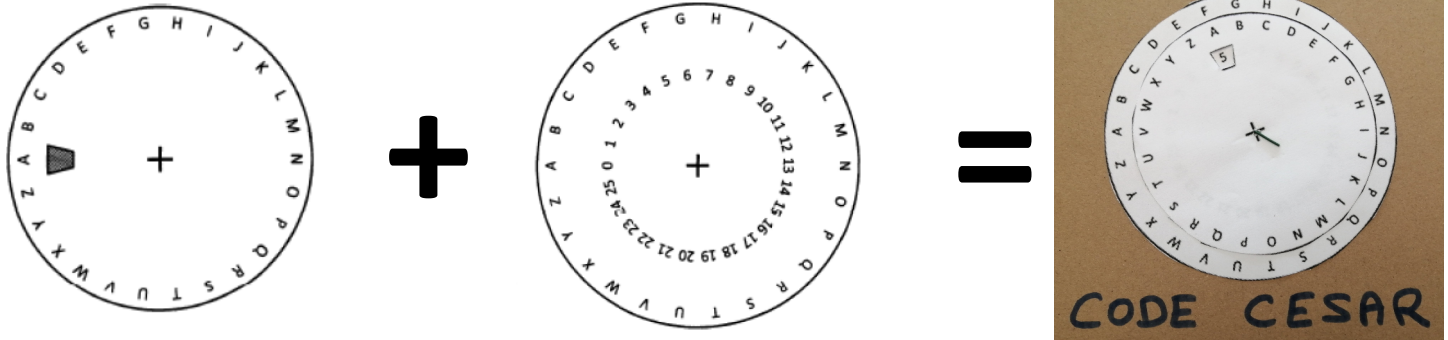
Cycle 4

Technologie

Séance 1

Cycle 4

**Exercice 2 : Découper l'annexe 1 afin de réaliser la maquette en papier du chiffre de César :**



**Travail 1 : Message : OZQJXHJXFWKZYJRUJWJZWIJXLFZQJX**

Quelle est la lettre la plus utilisée ? : \_\_\_\_\_

---



---



---



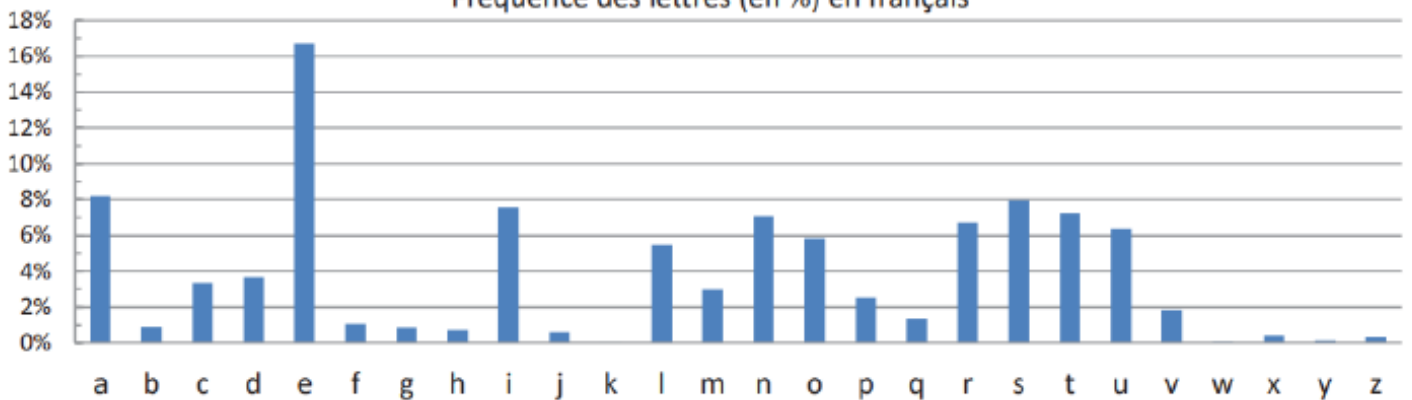
---



---



Fréquence des lettres (en %) en français





# ANNEXE 1

## Comment sont cryptées les données avant d'être communiquées ?

Thème n°2 et 3

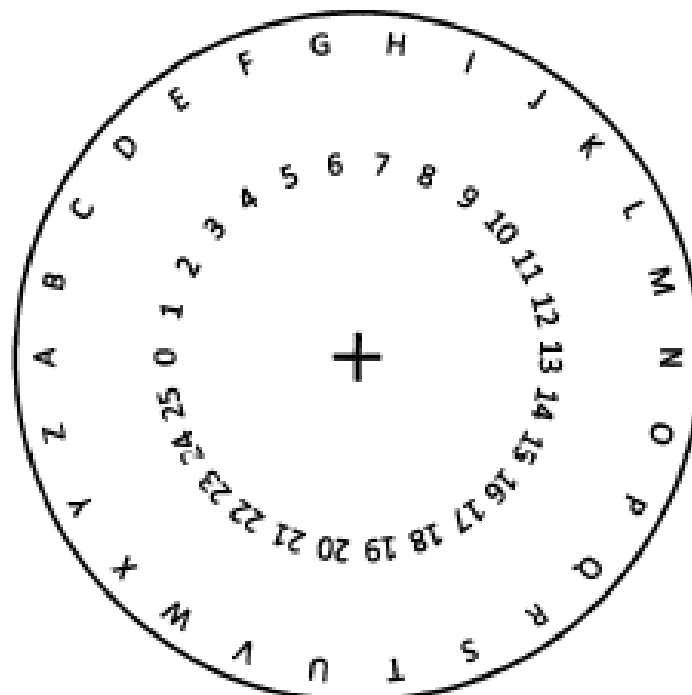
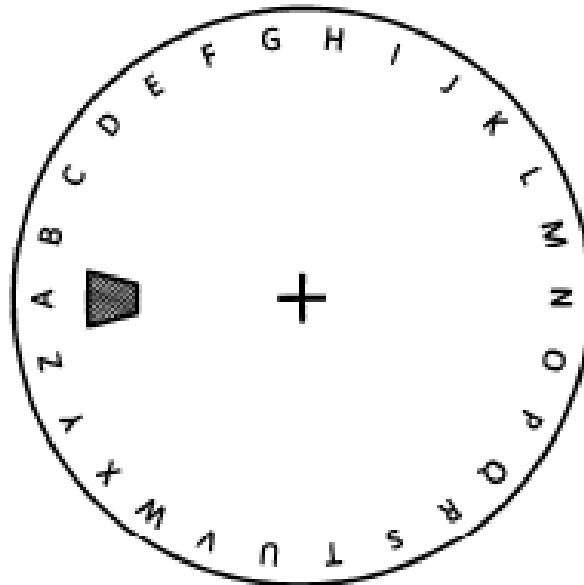
Cycle 4

Technologie

Séance 1

Cycle 4

Outil de chiffrement / déchiffrement  
Pour les messages utilisant le chiffre de César



1. Découpez les deux disques
2. A l'aide d'un cutter, découpez la fenêtre trapézoïdale du premier disque.
3. Poncez au compas les centres des deux disques (croix).
4. Assemblez les disques (le premier sur le deuxième) à l'aide d'une attache parisienne.