ACADÉMIE DE NORMANDIE *Liberté Égalité Fraternité*	**Fiche professeur 1/5** **Comment sont cryptées les données avant d'être communiquées ?** **Thème n°2 et 3**	**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 : 4e
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 Ier 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** (XVIe 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 XXe 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.

ACADÉMIE DE NORMANDIE
Liberté Égalité Fraternité

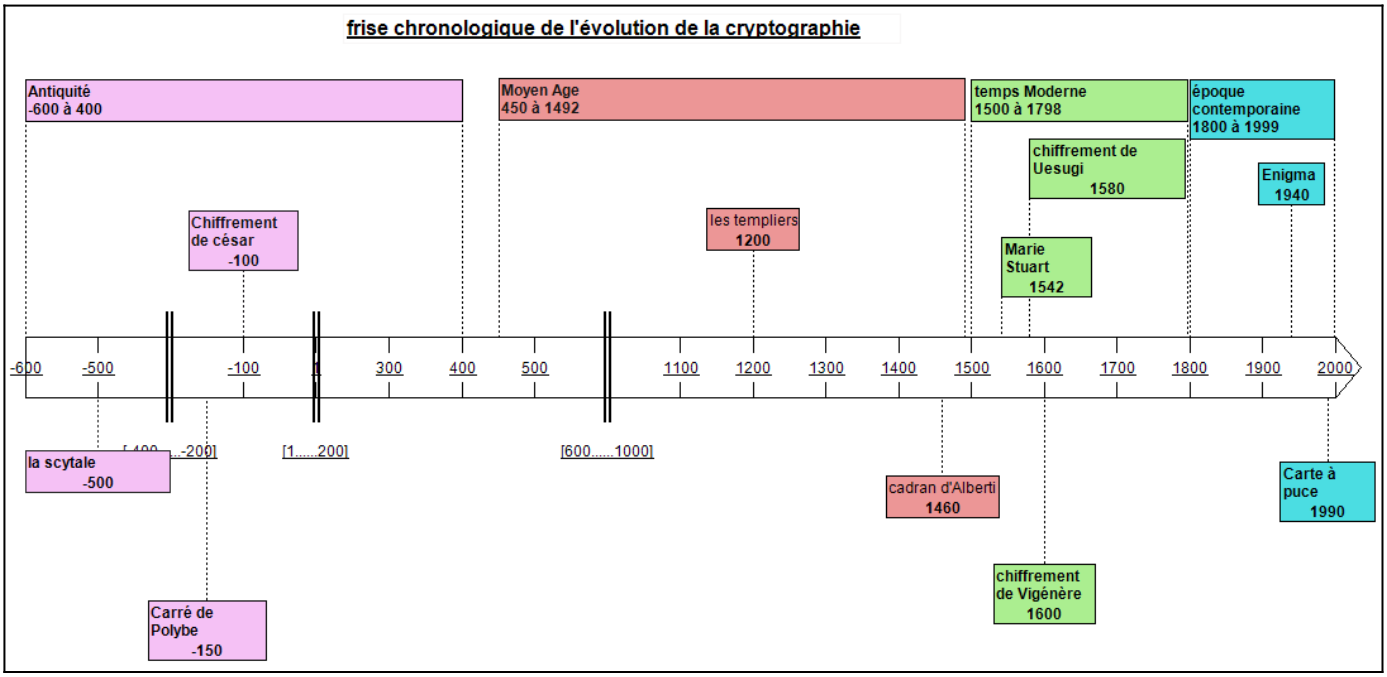
Fiche professeur 2/5

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 :	Le cryptage des données :
https://ladigitale.dev/digiview/#/v/689d952c60915	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.

ACADÉMIE DE NORMANDIE *Liberté Égalité Fraternité*	**Fiche professeur 3/5** **Comment sont cryptées les données avant d'être communiquées ?** **Thème n°2 et 3**	**Cycle 4** **Technologie** **Séance 1** **Cycle 4**

Exercice 1 : Comment un procédé de cryptage peut-il être vaincu ?

Ce message a été chiffré en appliquant le code César à un texte écrit en français. On ne connaît pas le **chiffre de César** qui a été utilisé, **Saurais-tu le déchiffrer en un minimum de temps ?**

OJPNGZNZOMZNCPHVDINIVDNNZIOGDWMZNZOZBVPSZI
YDBIDOZZOZIYMJDONDGNNJIOYJPZNYZMVDNJIZOYZXJIN
XDZIXZZOYJDQZIOVBDMGZNPINZIQZMNGZNVPOMZN

Analyse fréquentielle d'un texte :

En fonction de la langue dans laquelle un texte est écrit, certaines lettres apparaissent plus souvent que d'autre. Le tableau ci-dessous donne **la fréquence** d'apparition de **chaque lettre** de l'alphabet dans un écrit en français.

	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
Français	9,42	1,02	2,64	3,39	15,87	0,95	1,04	0,77	8,41	0,89	0,00	5,34	3,24	7,15	5,14	2,86	1,06	6,46	7,90	7,26	6,24	2,15	0,00	0,30	0,24	0,32

*Fréquence = nombre de fois qu'une lettre se répète **pour 100 caractères***

Quelle est la lettre la plus utilisée dans ce tableau ? E

Complète le tableau ci-dessous en y inscrivant, les lettres de l'alphabet français classées par ordre décroissant du nombre de fois qu'elles apparaissent dans un texte :

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

Analyse du message à déchiffrer :

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

Nombre d'apparitions de chaque lettre dans le texte :

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	3	1	11	0	0	5	1	13	7	0	0	7	18	12	6	2	0	1	0	0	6	1	3	6	24

ACADÉMIE DE NORMANDIE *Liberté Égalité Fraternité*	**Fiche professeur 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 ? : La lettre la plus utilisée dans ce texte écrit en français est E.

La lettre la plus utilisée dans le texte à déchiffrer est Z. Donc la lettre Z du texte chiffré correspond à la lettre E dans le texte du message à trouver

Le chiffre de César utilisé pour crypter le message est donc de : **5 à droite**

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

Vidéo d'explication du code CESAR :	Utiliser Scratch pour tester :
https://ladigitale.dev/digiview/#/v/689d9c1f47334	https://www.dcode.fr/chiffre-cesar https://www.apprendre-en-ligne.net/crypto/cesar/index.html https://scratch.mit.edu/projects/116204998/

Aide

Déchiffrer le message

Utilise l'application «Menu : **Chiffre de César** CryptoMahli→ **Créer/Utiliser l'alphabet de César** » pour analyser le texte du message à déchiffrer

TOUSLESETRESHUMAINSNAISSENTLIBRESETEGAUXENDIGNITEETEN DROITS ILSSONTDOUESDERAISONETDECONSCIENCEETDOIVENTAGIRLESUNSENVERSLESAUTRES

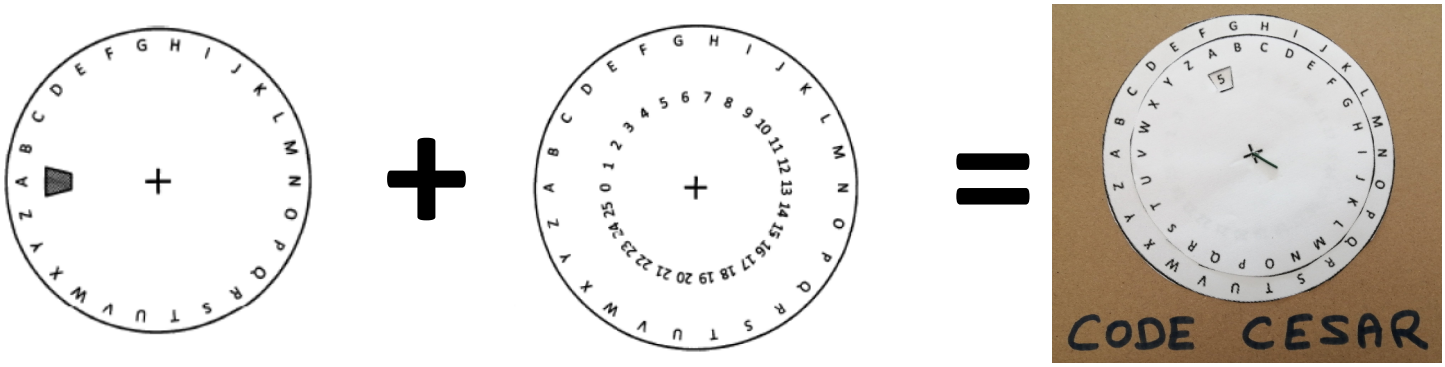
« TOUS LES ETRES HUMAINS NAISSENT LIBRES ET EGAUX EN DIGNITE ET EN DROITS. ILS SONT DOUES DE RAISON ET DE CONSCIENCE ET DOIVENT AGIR LES UNS ENVERS LES AUTRES »

C'est l'article 1 de la Déclaration universelle des droits de l'homme.

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

ACADÉMIE DE NORMANDIE *Liberté Égalité Fraternité*	**Fiche professeur 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 ? : **La lettre la plus utilisée dans ce message est le J**

Puisque le J remplace le E, le message a donc été codé avec un décalage de (+5).

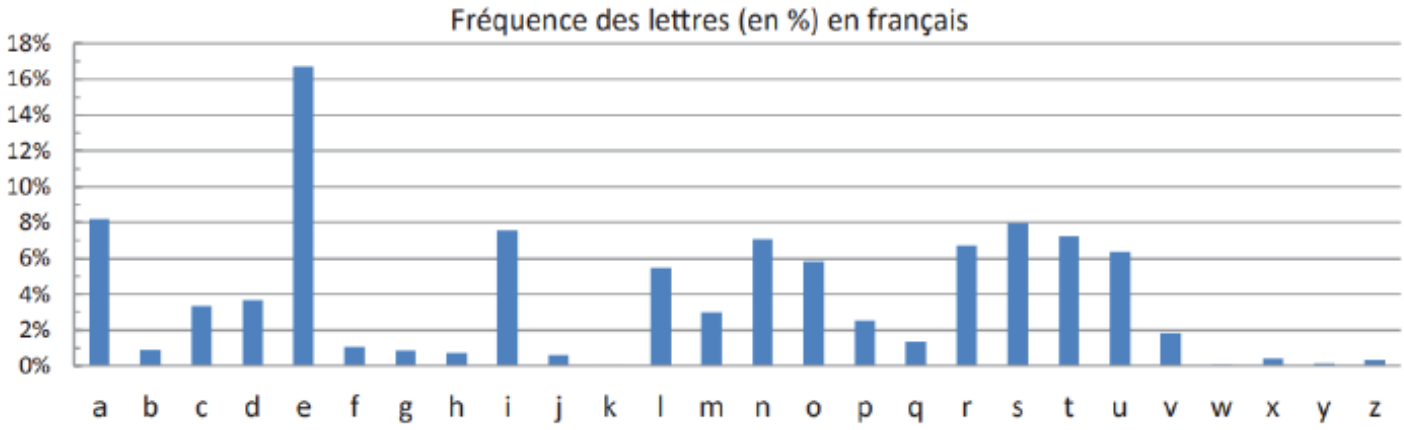
E -> F -> G -> H -> I -> J

Pour déchiffrer, il suffit donc de lui appliquer un décalage de (-5), ce qui donne :

OZQJXHJXFWKZYJRUJWJZWIJXLFZQJX

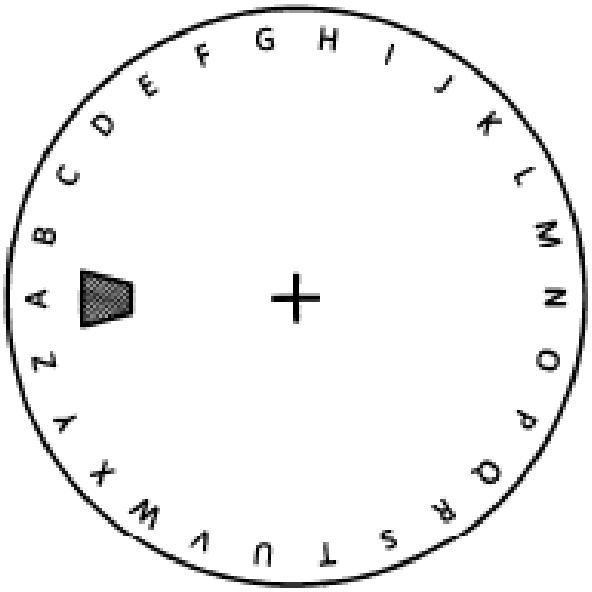
JULESCESARFUTEMPEREURDESGAULES

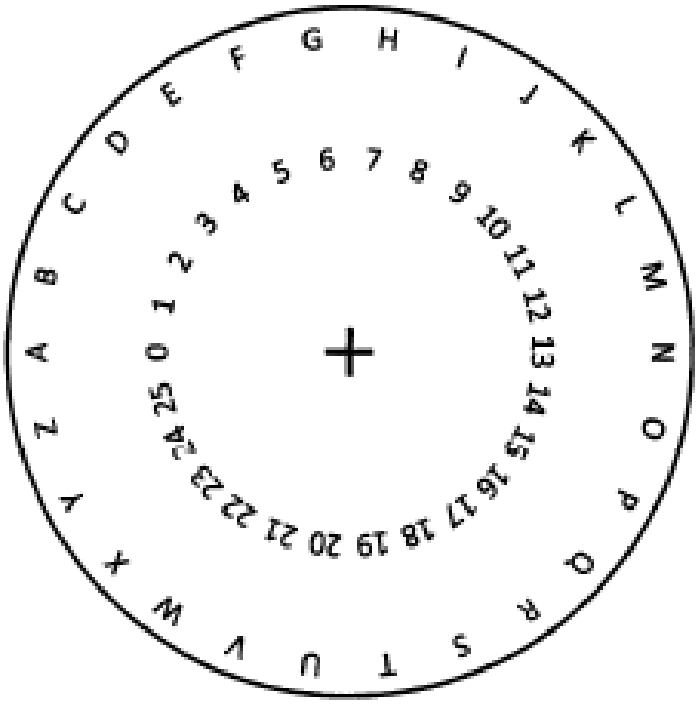
Jules César fut empereur des Gaules.



ACADÉMIE DE NORMANDIE *Liberté Égalité Fraternité*	**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. Percez au compas les centres des deux disques (croix).
4. Assemblez les disques (le premier sur le deuxième) à l'aide d'une attache parisienne.