	<h1 style="color: red;">Fiche élève 1/4</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 2
		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 : « Introduction et rappels historiques sur le chiffre de Vigenère »



Le **chiffre de Vigenère** est un système de chiffrement par substitution polyalphabétique, apparu au **XVI<sup>e</sup> siècle**. Il est souvent associé au diplomate et cryptographe français **Blaise de Vigenère** (1523–1596), qui en a publié la description détaillée en 1586 dans son ouvrage « *Traité des chiffres ou secrètes manières d'écrire.* »

À l'époque, la **cryptographie** était surtout dominée par les méthodes à substitution monoalphabétique, comme le **chiffre de César**, dans lesquelles chaque lettre est remplacée par une autre suivant un décalage fixe. Ces systèmes étaient relativement simples à casser grâce à l'**analyse fréquentielle** : il suffisait d'étudier la fréquence des lettres dans le message chiffré pour retrouver la clé.

Le chiffre de Vigenère introduit une rupture : il utilise **plusieurs alphabets de substitution** successifs, déterminés par une **clé**. Cette clé est composée de lettres (ou de nombres représentant un décalage), et elle est **répétée tout au long du message**. Chaque lettre de la clé indique combien de positions il faut décaler la lettre correspondante du texte clair dans l'alphabet.

Par exemple, si la clé est « **CLE** » :

- C (3<sup>e</sup> lettre de l'alphabet) → décalage de +2
- L (12<sup>e</sup>) → décalage de +11
- E (5<sup>e</sup>) → décalage de +4

Lettre clé	Décalage
C	+2
L	+11
E	+4

**Ces décalages se répètent pour chiffrer tout le texte.**

L'avantage de cette méthode résidait dans la **diversité des substitutions** : la même lettre du texte clair pouvait être chiffrée différemment selon sa position dans le texte, ce qui perturbait fortement l'analyse fréquentielle classique.

Pendant des siècles, le chiffre de Vigenère a été considéré comme **incassable** par de nombreux cryptographes et militaires, d'où **son surnom de chiffre indéchiffrable (le chiffre indéchiffrable)**.



# Fiche élève 2/4

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

Thème n°2 et 3

Cycle 4

Technologie

Séance 2

Cycle 4

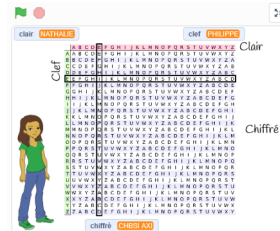
### Explication :

<https://ladigitale.dev/digiview/#/v/689ee6ddcc98b>



### Le cryptage des données :

<https://scratch.mit.edu/projects/857667380>



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

### Exercice 1 : Appliquer la méthode de cryptage ?

La clef est « **CLE** »

Le message à crypter est : « **VIGENERE** »

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

Réponse :

Lettre claire	Lettre clé	Décalage	Lettre chiffrée
V	C		
I	L		
G	E		
E	C		
N	L		
E	E		
R	C		
E	L		

Le tableau :

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



# Fiche élève 3/4

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

Thème n°2 et 3

Cycle 4

Technologie

Séance 2

Cycle 4

### Exercice 2 : Comment utiliser cette méthode de cryptage ?

Chiffrons le texte "**CHIFFRE DE VIGENERE**" avec la clef "**BACHELIER**"

(Cette clef est éventuellement répétée **plusieurs fois** pour être aussi longue que le texte clair).

#### Réponse :

Clair	C	H	I	F	F	R	E	D	E	V	I	G	E	N	E	R	E
Clef	B	A	C	H	E	L	I	E	R	B	A	C	H	E	L	I	E
Décalage																	
Chiffré																	

Vérifier avec le lien : <https://www.apprendre-en-ligne.net/crypto/vigenere/index.html>

### Exercice 3 : Comment utiliser cette méthode de cryptage ?

Saurez-vous trouver le message suivant chiffré grâce à la clé « **CRYPTOLOGIE** » ?

**NVQX MSOS RIVE JGTL HFBK UMPV BXGT ZFSI XKFL H**

Quel est le message en clair ?

#### Réponse : \_\_\_\_\_



### Exercice 4 : Comment utiliser cette méthode de cryptage ?

Saurez-vous **coder le message** ?

**LE TRESOR EST DANS UN COFFRE**

Supposons que le mot clé soit **JUPITER**. On commence par l'écrire sous le message à coder, en le **répétant si nécessaire** :

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

L	E	T	R	E	S	O	R	E	S	T	D	A	N	S	U	N	C	O	F	F	R	E
J	U	P	I	T	E	R	J	U	P	I	T	E	R	J	U	P	I	T	E	R	J	U
U	Y	I	A	..	..	..																



# ANNEXE 1 - 4/4

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

### Thème n°2 et 3

Cycle 4

Technologie

Séance 2

Cycle 4

Table de Vigenère.

	Lettre en clair																									
	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
<b>Lettre de la clé</b>	Lettres chiffrées (au croisement de la colonne <i>Lettre en clair</i> et de la ligne <i>Lettre de la clé</i> )																									
A	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
B	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	A
C	C	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
D	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
E	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	D
F	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
G	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	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	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