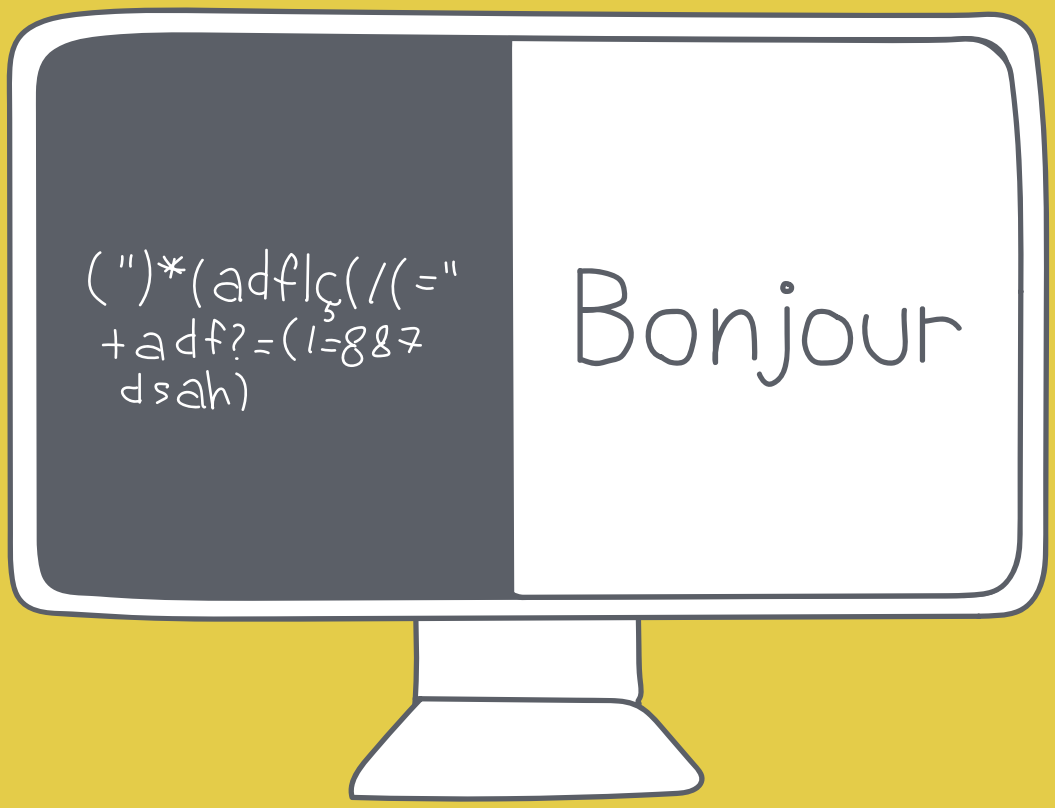
ENQUÊTE 4 · SI · 7e

COMMENT DÉCRYPTER UN MESSAGE CHIFFRÉ ?



<DÉ>CODAGE • ÉDUCATION NUMÉRIQUE • CYCLE 2 (7e-8e)
DEF-DGEO (VAUD, SUISSE)
2023 • DECODAGE.EDU-VD.CH • CC BY NC SA 4.0

PLAN D'ÉTUDES ROMAND

EN 22 - S'approprier les concepts de base de la science informatique…

2 … en encodant, décodant et en transformant des données

Informations et données

Cryptage et décryptage d'un message à l'aide de méthodes simples

Liens disciplinaires

MSN 22 – Nombres ; MSN 25 – Modélisation

INTENTIONS PÉDAGOGIQUES

Cette enquête montre aux élèves que l'on peut chiffrer un message pour le rendre incompréhensible et ainsi le transmettre de manière confidentielle à quelqu'un possédant la clé pour le déchiffrer. Mais qu'il existe également des procédés pour casser le chiffrement, abordés ici à travers une technique simple à mettre en œuvre.

Cette enquête prolonge l'activité faite sur le chiffrement de César en 6e en présentant un aspect différent, qui peut être vécu comme une complexité supplémentaire : il s'agit de traduire en clair un message chiffré sans connaître la clé de chiffrement (le décalage dans le cas du chiffrement de César), on parle alors de décryptage.

LA QUESTION DE L'ENQUÊTE : COMMENT DÉCRYPTER UN MESSAGE CHIFFRÉ ?	
ÉTAPE 1 - POUR COMPRENDRE Une première investigation pour comprendre la question.	Les élèves décodent des mots grâce à la technique du chiffrement de César. Mais certains d'entre eux résistent et les élèves doivent alors découvrir comment les déchiffrer.
ÉTAPE 2 - POUR RÉPONDRE Poursuite de l'investigation pour répondre à la question.	On exprime la possibilité que la clé de chiffrement n'est pas la bonne. Il faut donc un nouvel outil permettant de « casser le code ». Les élèves en construisent un et le testent.
ÉTAPE 3 - POUR CONCLURE Mise en forme de la réponse à la question.	Les élèves peuvent se rendre compte qu'on peut déchiffrer un message sans nécessairement en connaître la clé (décryptage).
ÉTAPE 4 - PROPOSER DES MESSAGES À DÉCHIFFRER (PROLONGEMENT)	Les élèves conçoivent des phrases à déchiffrer.

LA PROTECTION DES DONNÉES PERSONNELLES

Cette enquête est l'occasion d'aborder la question des données personnelles que l'on peut laisser en ligne et à la manière de les protéger. En effet, une multitude de sites et d'applications web cherchent à collecter les données de leurs utilisateurs pour avoir un maximum d'informations à leur égard : prénom, nom, âge, date de naissance, sexe, géolocalisation, centres d'intérêt, goûts, etc. La récolte de ces informations permet d'alimenter des algorithmes créés par les développeurs de ces sites et applications, en vue de proposer des contenus ciblés aux utilisateurs, pour les pousser à consommer davantage. Ce phénomène est abordé dans le scénario de 7e-8e : Réseaux sociaux, interactions et identité en ligne.

Or, certains usages requièrent que l'utilisateur partage ses données personnelles pour qu'il puisse être identifié. C'est le cas lorsque l'on achète des billets de transports pour voyager à l'étranger, lorsque l'on veut ouvrir un compte bancaire ou payer une facture en ligne. Bien que ces données soient récoltées par certaines entreprises et institutions, elles ne doivent pas être accessibles à tous. Pour les protéger, elles sont stockées sur des serveurs sécurisés et sont codées, de sorte à ce que seuls ceux qui en détiennent le code puissent les lire. C'est ce que l'on appelle le cryptage ou le chiffrement. Malgré cela, certains procédés permettent de décrypter des données sans en connaître la clé de cryptage. Ce phénomène fera l'objet de cette enquête.

À l'issue de ce travail, on encourage les élèves à se questionner quant aux données qu'ils partagent en ligne, lorsque l'occasion se présente dans leur quotidien : à quelles occasions me demande-t-on mon nom, mon prénom, mon âge, mon adresse mail, etc. ? Comment ces données sont-elles traitées ? Est-ce indispensable ? Si tel est le cas, sont-elles cryptées ?

Étape 1 - Pour comprendre

RÉSUMÉ	Les élèves décodent des mots grâce à la technique du chiffrement de César. Mais certains d'entre eux résistent et les élèves doivent alors découvrir comment les déchiffrer.
MODALITÉ	En groupes de 3-4 élèves
MATÉRIEL	• Fiche 1 : disque de César • Fiche 1.1 : disque de César (suite) • Fiche 2 : mots à déchiffrer • Fiche 2.1 : mots à déchiffrer « corrigé » • Fiche 2.2 : listes personnalisées
DURÉE	20 minutes

MODULARITÉ

RAPPEL : LE CODE DE CÉSAR

Le Code ou Chiffre de César est une méthode de chiffrement par substitution mono-alphabétique. Il s'agit de décaler les lettres d'un message en clair d'un certain nombre de rangs pour obtenir la lettre chiffrée. Ainsi, un A se transforme en D avec un décalage de trois rangs.

C'est un chiffrement peu sûr car il n'offre que 25 possibilités et qu'il ne résiste pas à des méthodes de décryptage basiques (comme l'attaque par force brute ou l'analyse de fréquence par exemple) mais il peut être utilisé comme élément d'une méthode plus complexe, le chiffrement de Vigenère par exemple 78-E4-01.

Le chiffrement de Vigenère est un chiffrement de César amélioré : il utilise non pas un mais 26 alphabets décalés, avec donc un décalage spécifique pour chaque lettre. Ce chiffrement est resté incassable pendant trois siècles mais, aujourd'hui les ordinateurs ont gagné en puissance et il n'est plus infrangible. Plus la puissance des ordinateurs augmente, plus les techniques de chiffrement existantes perdent en efficacité.

TEMPS 1.1 — EXPLICATIONS — 5 minutes

On annonce avoir un certain nombre de messages secrets à déchiffrer. Ils ont été chiffrés grâce à la technique du « Chiffrement de César » que certains ont peut-être vu en 6e. Répartir les élèves par groupes de 3-4 élèves et rappeler ou expliquer en quoi consiste cette technique, en s'appuyant sur l'outil fourni sur les *Fiches 1 et 1.1*.

Disque de chiffrement

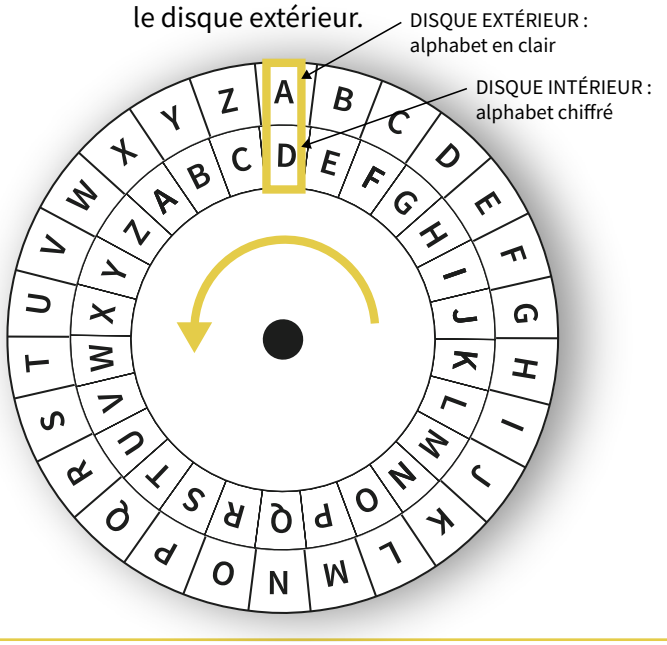
Ce disque est à réaliser auparavant par l'enseignant. Il faut en confectionner autant qu'il y a de groupes de travail. Son utilisation se fait selon le descriptif ci-dessous :

Le disque extérieur correspond à l'alphabet en clair.

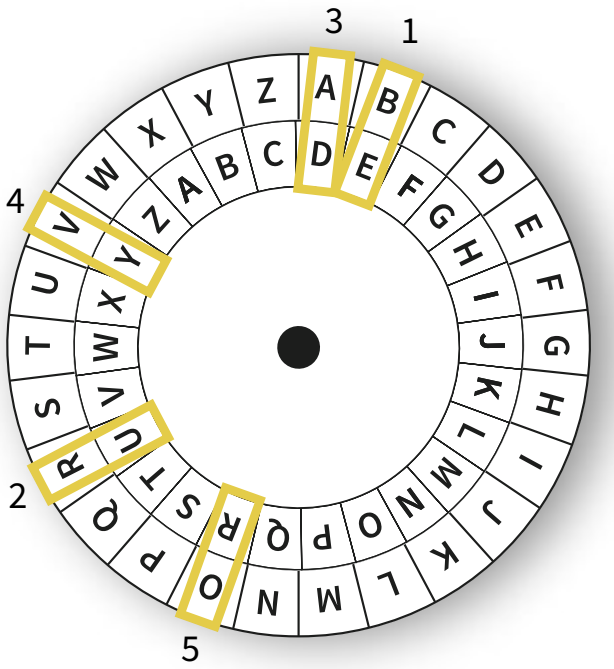
On décale le disque intérieur, dans le sens anti-horaire, du nombre de rang correspondant à la clé de chiffrement (ici trois).

Pour chiffrer un message, on regarde donc la lettre sur le disque extérieur et on note sa correspondance chiffrée (le D pour le A, le H pour le E, etc.).

Pour réaliser l'opération inverse, on regarde la lettre du message chiffré sur le disque intérieur et on note sa correspondance sur le disque extérieur.



On distribue un disque à chaque groupe pour visualiser le décalage des alphabets. On peut se servir d'un mot en exemple pour que les élèves comprennent le principe. Dans cet exemple, le disque intérieur a subi un décalage de trois lettres par rapport au disque supérieur (le D chiffré correspond au A déchiffré). On peut proposer le mot EUDYR à déchiffrer avec ce décalage.



LETTRES À DÉCHIFFRER		LETTRES DÉCHIFFRÉES
1re lettre	E →	B
2e lettre	U →	R
3e lettre	D →	A
4e lettre	Y →	V
5e lettre	R →	O

TEMPS 1.2 — DÉCHIFFRER — 15 minutes

On distribue à chaque groupe une liste de mots chiffrés avec la clé correspondante, voir *Fiche 2*. Les élèves doivent collaborer pour déchiffrer chaque mot. Par exemple : un élève donne la clé et dicte chaque lettre à déchiffrer, un autre élève paramètre le disque et lit les lettres ainsi déchiffrées à un troisième élève chargé de les écrire, les rôles pouvant permuter à chaque mot. On passe dans les différents groupes et on rappelle que les lettres chiffrées doivent être lues sur le disque intérieur et que la correspondance doit être trouvée sur le disque extérieur.

Les élèves vont se rendre compte que parmi la liste de mots déchiffrés, certains n'ont aucun sens (le dernier dans chaque liste).

Le corrigé se trouve sur la Fiche 2.1.

Il y a une fiche vierge à disposition (Fiche 2.2) afin de laisser le choix dans les mots à découvrir, on peut ainsi personnaliser les listes.

On trouve aussi des outils en ligne qui permettent d'effectuer automatiquement les chiffrements, en voici trois : *78-E4-02* ; *78-E4-03* ; *78-E4-04*.

Étape 2 - Pour répondre

RÉSUMÉ	On exprime la possibilité que certaines personnes cherchent à déchiffrer des messages qui ne leur sont pas destinés. Ces personnes ne connaissent donc pas la clé de chiffrement, comment procéder ? Il faut un nouvel outil permettant de « casser le code ». Les élèves en construisent un et le testent.
MODALITÉS	En collectif, en groupes de 3-4 élèves
MATÉRIEL	• Fiche 3 : tableau alphabétique • Fiche 4 : rouleau de César • Fiche 4.1 : rouleau de César (suite) • Cylindre • Rouleaux
DURÉE	20 minutes

TEMPS 2.1 — EXPLICATIONS — 5 minutes

On fait le point sur le fait que dans chaque groupe, il y a un mot qui n'a pas pu être déchiffré correctement. On demande aux élèves une explication plausible : la clé fournie n'est pas la bonne. Comment donc réussir à déchiffrer ce mot ? La proposition peut être de tester toutes les solutions possibles, mais cela prend du temps, d'autant plus si on a plusieurs mots dont on ne possède pas la clé. Il faudrait donc un autre outil que le disque permettant de visualiser rapidement toutes les solutions possibles.

TEMPS 2.2 — UN NOUVEL OUTIL — 15 minutes

On affiche au tableau les *Fiches 4 et 4.1* de fabrication du rouleau de César et on distribue à chaque groupe :

- les bandes de lettres à découper *Fiche 3* ou déjà découpées.
  On prend soin d'adapter en amont la taille des bandes au cylindre choisi ;
- un cylindre (de type boîte de conserve par exemple) ;
- des ciseaux, du scotch.

Les élèves fabriquent un rouleau de César et essaient d'en découvrir le fonctionnement.
Ils peuvent ensuite déchiffrer le mot manquant avec cet outil.

Étape 3 - Pour conclure

RÉSUMÉ	Les élèves peuvent se rendre compte qu'il est possible de déchiffrer un message sans nécessairement en connaître la clé (décryptage).
MODALITÉS	En groupes de 3-4 élèves, en collectif
MATÉRIEL	• Rouleaux de César construits par les élèves
DURÉE	5 minutes

TEMPS 3.1 DÉCHIFFRER SANS CONNAÎTRE LA CLÉ 5 minutes

On récolte dans chaque groupe les mots ainsi déchiffrés, avec les bonnes clés de chiffrement. On propose à l'ensemble des groupes une phrase chiffrée dont on ne connaît pas la clé. Le premier groupe à « casser le code » gagne le défi. On peut éventuellement compliquer le défi en changeant de clé à chaque mot.

DÉFI : LEKI DU HUKIIYHUP ZQCQYI Q TUSXYVVHUH SU CUIIQWU.

RÉPONSE : VOUS NE REUSSIREZ JAMAIS A DECHIFFRER CE MESSAGE.

CLÉ : 16

On conclut que pour « casser un message secret », en connaissant la méthode utilisée, on peut utiliser un outil qui va passer en revue rapidement toutes les solutions possibles. Cela s'appelle l'attaque par force brute. Cependant cela n'est faisable à la main qu'avec des chiffrements simples, sinon il faut des ordinateurs puissants et du temps, plusieurs années, plusieurs milliers d'années, selon la longueur du message et la méthode avec laquelle on l'a chiffrée.

LA CRYPTANALYSE

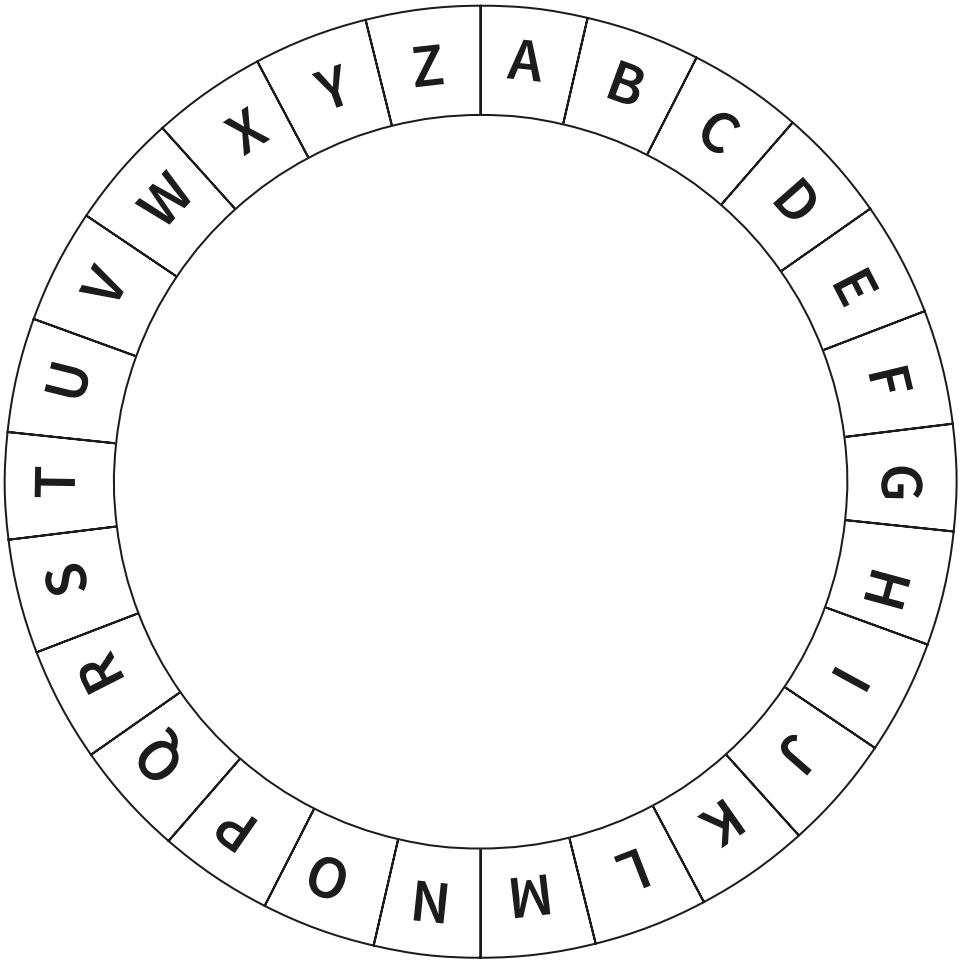
Le chiffrement de César est facile à décrypter, il ne fonctionnait à l'époque que si les ennemis de Jules César étaient peu familiers avec ce qu'on appelle la cryptanalyse : technique qui consiste à déduire un texte en clair d'un texte chiffré sans posséder la clé de chiffrement.

Étape 4 - Proposer des messages à déchiffrer
(prolongement)

RÉSUMÉ	Les élèves conçoivent des phrases à déchiffrer.
MODALITÉ	En individuel
MATÉRIEL	• Disques et rouleaux de César
DURÉE	30 minutes

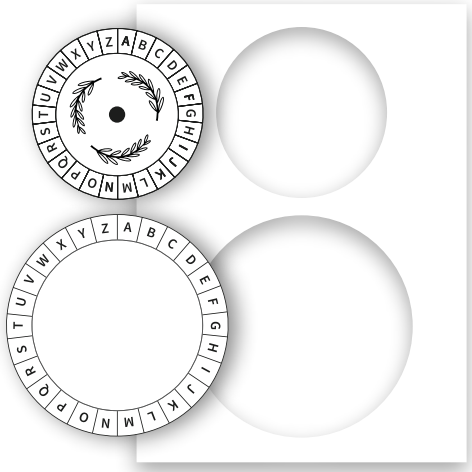
Comme prolongement, on demande aux élèves de créer des phrases chiffrées à l'aide du disque de César et de les transmettre sans donner la clé. Chaque camarade essaie d'en déchiffrer une à l'aide d'un rouleau de César.

Disque de César

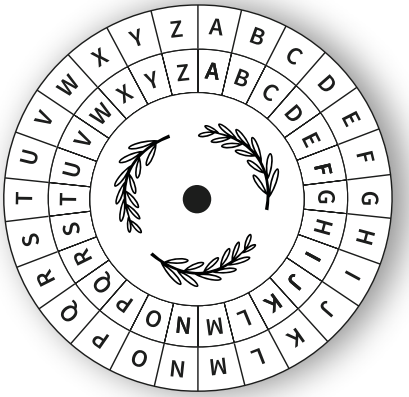


Disque de César (suite)

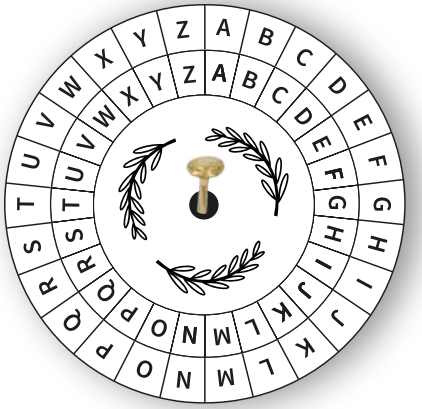
1 - Découper les deux disques. Éventuellement les plastifier.



2 - Superposer le plus petit sur le plus grand.

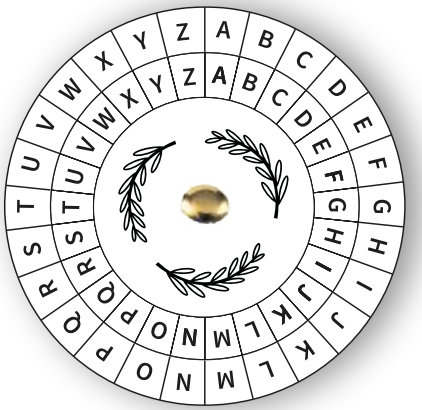


3 - À l'aide d'un compas, percer un trou au centre.



4 - Faire passer une attache parisienne pour les solidariser.

5 - Chiffrer.



Mots à déchiffrer

GROUPE 1 (la clé de chiffrement se trouve entre parenthèses)

Mots à déchiffrer	Mots déchiffrés
(4) LMWXSMVI	
(10) DBYECCO	
(6) IOYKGAD	
(20) ZYOCFFY	
(15) BPIWTBPIXFJTH	
(9) DQODQMFUAZ	

GROUPE 2 (la clé de chiffrement se trouve entre parenthèses)

Mots à déchiffrer	Mots déchiffrés
(5) XTNWJJX	
(11) XLETYPP	
(8) KIVBQVM	
(19) CHNKGXX	
(13) INPNAPRF	
(11) RGIVJ DZUZ	

GROUPE 3 (la clé de chiffrement se trouve entre parenthèses)

Mots à déchiffrer	Mots déchiffrés
(6) KRKBKY	
(9) YAXONBBNDA	
(4) IGSPIW	
(21) HDIDNOMZ	
(12) BDQEUPQZF	
(14) UZIVTKZFE	

GROUPE 4 (la clé de chiffrement se trouve entre parenthèses)

Mots à déchiffrer	Mots déchiffrés
(7) YHJJVBYJPY	
(10) NOMYEZOB	
(5) XTZQNLSJW	
(17) UVJJZEVI	
(15) SXHRJITG	
(8) EPPSRKIV	

GROUPE 5 (la clé de chiffrement se trouve entre parenthèses)

Mots à déchiffrer	Mots déchiffrés
(4) EYXSVMWIV	
(10) ZOBWODDBO	
(6) BUARUOX	
(20) LYZOMYL	
(15) XCITGSXGT	
(13) MNLRMNA	

GROUPE 6 (la clé de chiffrement se trouve entre parenthèses)

Mots à déchiffrer	Mots déchiffrés
(5) AJWYJX	
(11) APETEPD	
(8) ZIXQLMA	
(19) WXEBVTMX	
(13) VZZRAFR	
(12) RDJGQTH	

Retour

CORRIGÉ

Mots à déchiffrer

GROUPE 1 (la clé de chiffrement se trouve entre parenthèses)

Mots à déchiffrer	Mots déchiffrés
(4) LMWXSMVI	HISTOIRE
(10) DBYECCO	TROUSSE
(6) IOYKGAD	CISEAUX
(20) ZYOCFFY	FEUILLE
(15) BPIWTBPIXFJTH	MATHEMATIQUES
(9) DQODQMFUAZ	UHFUHDWLRQ (la bonne clé est 12 et doit donner RECREATION)

GROUPE 2 (la clé de chiffrement se trouve entre parenthèses)

Mots à déchiffrer	Mots déchiffrés
(5) XTNWJJX	SOIREES
(11) XLETYPP	MATINEE
(8) KIVBQVM	CANTINE
(19) CHNKGXX	JOURNEE
(13) INPNAPRF	VACANCES
(11) RGIVJ DZUZ	CRTGU OKFK (la bonne clé est 17 et doit donner APRESMIDI)

GROUPE 3 (la clé de chiffrement se trouve entre parenthèses)

Mots à déchiffrer	Mots déchiffrés
(6) KRKBKY	ELEVES
(9) YAXONBBNDA	PROFESSEUR
(4) IGSPIW	ECOLES
(21) HDIDNOMZ	MINISTRE
(12) BDQEUPQZF	PRESIDENT
(14) UZIVTKZFE	INWJHYNTS (la bonne clé est 17 et doit donner DIRECTION)

GROUPE 4 (la clé de chiffrement se trouve entre parenthèses)

Mots à déchiffrer	Mots déchiffrés
(7) YHJJVBYJPY	RACCOURCIR
(10) NOMYEZOB	DÉCOUPER
(5) XTZQNLSJW	SOULIGNER
(17) UVJJZEVI	DESSINER
(15) SXHRJITG	DISCUTER
(8) EPPSRKIV	MXXAZSQD (la bonne clé est 4 et doit donner ALLONGER)

GROUPE 5 (la clé de chiffrement se trouve entre parenthèses)

Mots à déchiffrer	Mots déchiffrés
(4) EYXSVMWIV	AUTORISER
(10) ZOBWODDBO	PERMETTRE
(6) BUARUOX	VOULOIR
(20) LYZOMYL	REFUSER
(15) XCITGSXGT	INTERDIRE
(13) MNLRMNA	ZAYEZAN (la bonne clé est 9 et doit donner DECIDER)

GROUPE 6 (la clé de chiffrement se trouve entre parenthèses)

Mots à déchiffrer	Mots déchiffrés
(5) AJWYJX	VERTES
(11) APETEPD	PETITES
(8) ZIXQLMA	RAPIDES
(19) WXEBVTMX	DELICATE
(13) VZZRAFR	IMMENSE
(12) RDJGQTH	DPVSCFT (la bonne clé est 15 et doit donner COURTES)

Listes personnalisées

GROUPE ☐ (la clé de chiffrement se trouve entre parenthèses)	
Mots à déchiffrer	Mots déchiffrés
(4)	
(10)	
(6)	
(20)	
(15)	
(9)	

GROUPE ☐ (la clé de chiffrement se trouve entre parenthèses)	
Mots à déchiffrer	Mots déchiffrés
(5)	
(11)	
(8)	
(19)	
(13)	
(11)	

GROUPE ☐ (la clé de chiffrement se trouve entre parenthèses)	
Mots à déchiffrer	Mots déchiffrés
(6)	
(9)	
(4)	
(21)	
(12)	
(14)	

GROUPE ☐ (la clé de chiffrement se trouve entre parenthèses)	
Mots à déchiffrer	Mots déchiffrés
(7)	
(10)	
(5)	
(17)	
(15)	
(8)	

GROUPE ☐ (la clé de chiffrement se trouve entre parenthèses)	
Mots à déchiffrer	Mots déchiffrés
(4)	
(10)	
(6)	
(20)	
(15)	
(13)	

GROUPE ☐ (la clé de chiffrement se trouve entre parenthèses)	
Mots à déchiffrer	Mots déchiffrés
(5)	
(11)	
(8)	
(19)	
(13)	
(12)	

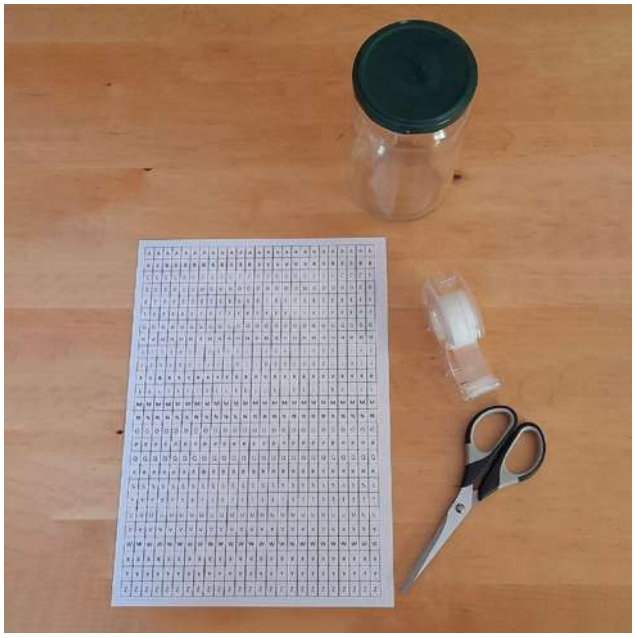
Tableau alphabétique

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

Retour

Rouleau de César

ÉTAPE 1 : se munir d'un contenant cylindrique de type boîte de conserve ou bocal. Mesurer la circonférence du contenant.



ÉTAPE 2 : imprimer le tableau alphabétique de la fiche précédente avec une hauteur correspondant à la circonférence mesurée précédemment.

ÉTAPE 3 : rassembler tableau, cylindre, ciseaux et ruban adhésif.

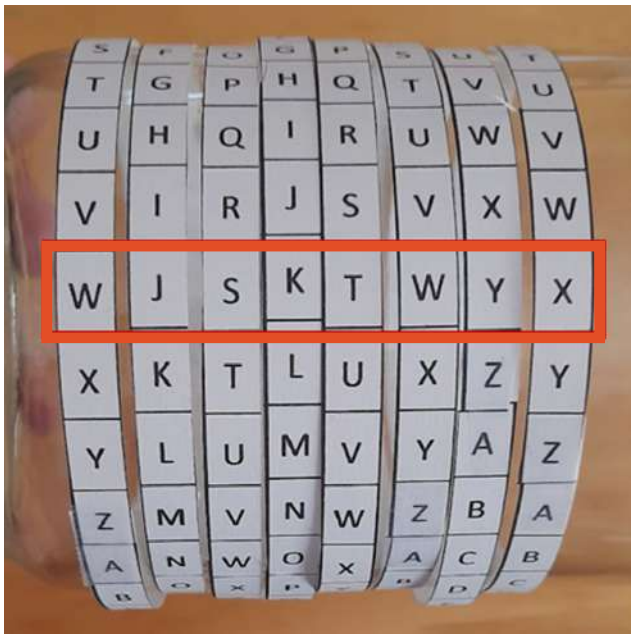
ÉTAPE 4 : découper les bandes dans le tableau.

ÉTAPE 5 : relier les extrémités de chaque bande entre elles.

Retour

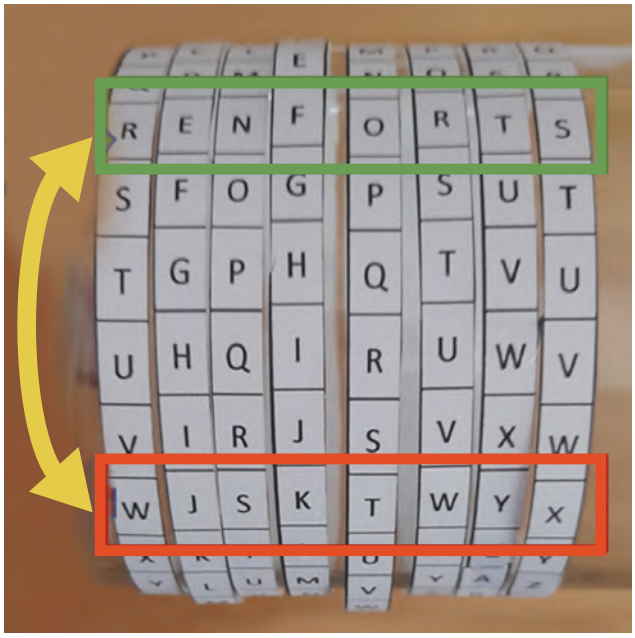
Rouleau de César (suite)

ÉTAPE 6 : placer les bandes les unes après les autres autour du cylindre.



ÉTAPE 7 : décaler chaque bande pour aligner les lettres du mot à décoder.

ÉTAPE 8 : tourner délicatement le cylindre (sans bouger les bandes de lettres) pour repérer le mot ainsi déchiffré.



Exemple avec le décryptage du mot WJSKTWYX.
Le mot RENFORTS apparaît au 5e décalage.