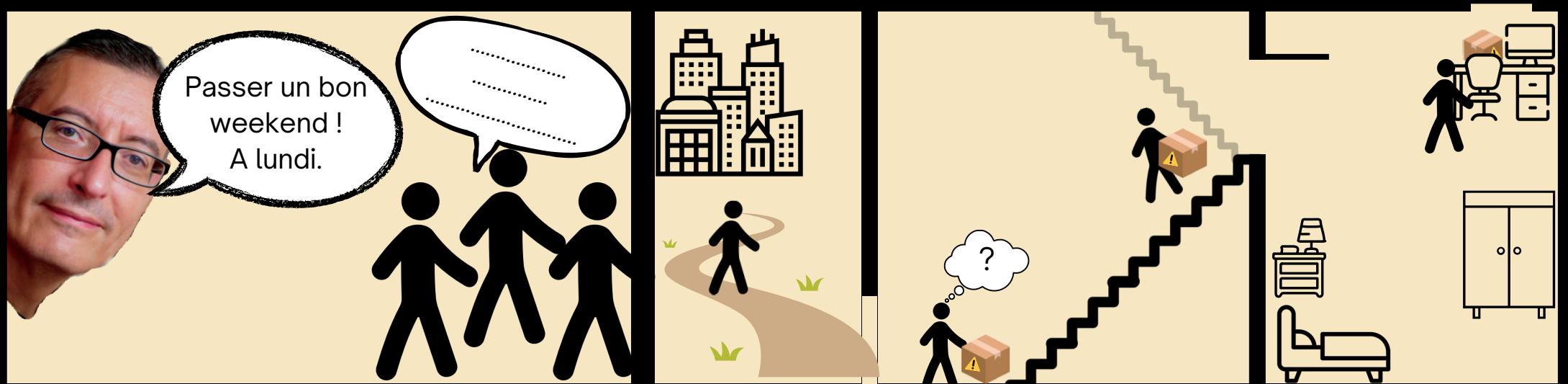


1 UN VENDREDI APRÈS LES COURS...



seluagsederreugal



2

GAULE, 14 MARS 54 AV. J.-C.

Nous sommes actuellement en pleine campagne militaire du proconsul romain Jules César pour étendre la république romaine sur l'ensemble de la gaule.



BIEN JOUÉ !

Tu as retrouvé le clair (=message avant chiffrement). On dit que tu as décrypté (ou cassé) le code secret.



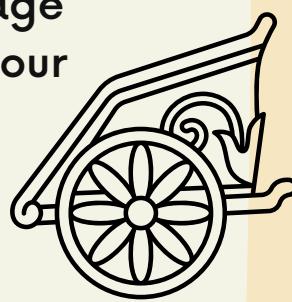
Nous avons intercepté un papyrus en provenance d'un curieux étranger. Il était transporté par un esclave à destination de Jules César lui-même. Une partie du message est illisible, il semble chiffré. Nous soupçonnons que nous ayons affaire à un chiffrement par décalage.



CHIFFREMENT PAR DÉCALAGE ?

C'est un chiffrement très simple, mais plutôt efficace à l'époque, car beaucoup était illétré.

Il consiste tous simplement à choisir un nombre qui correspond au décalage dans l'alphabet et à l'appliquer pour chaque lettre du message.



Voici un exemple avec un décalage de 3 sur le message "Jules Cesar".

Jules Cesar = Mxohv Fhvdu

Auê César

Je te fais part de quelque chose d'une importance vitale te concernant.

Un complot te visant s'est formé, et à pour projet de t'assassiner.

Prend garde, il ne te reste que peu de temps.

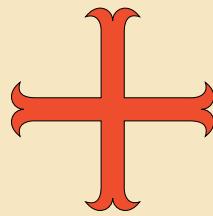
oh frqflloh gh Wurbhu



INFO BONUS



Le chiffrement par décalage porte aussi le nom de chiffre de césar, car il était utilisé par Jules César, avec un décalage de 3.



3 FRANCE, TROYES XIIÈME SIÈCLE

Nous sommes en pleine période de la création de l'ordre du Temple par le concile de Troyes. C'était un ordre religieux et militaire issu de la chevalerie du Moyen Âge, dont les membres sont appelés les Templiers.



Nous avons trouvé des traces près de cette porte de l'homme qui nous a enfermés. Elle semble bloquée. Mais d'étrange symbole s'y trouve. Nous semblons avoir affaire à un chiffrement par substitution.



Il semble que ce soit lié à un chiffrement qu'utilisaient les templiers à l'époque pour rendre illisible leur texte. La seule information dont nous disposons est ces dessins.



INFO BONUS

Au départ, la mission de cet ordre était d'assurer la sécurité des pèlerins en Terre Sainte. Mais très vite, les templiers se détournèrent de cet objectif pour préférer s'enrichir, devenant les trésoriers du roi et du Pape. C'est pour coder les lettres de crédit qu'ils s'échangeaient, qu'ils utilisèrent ce code.



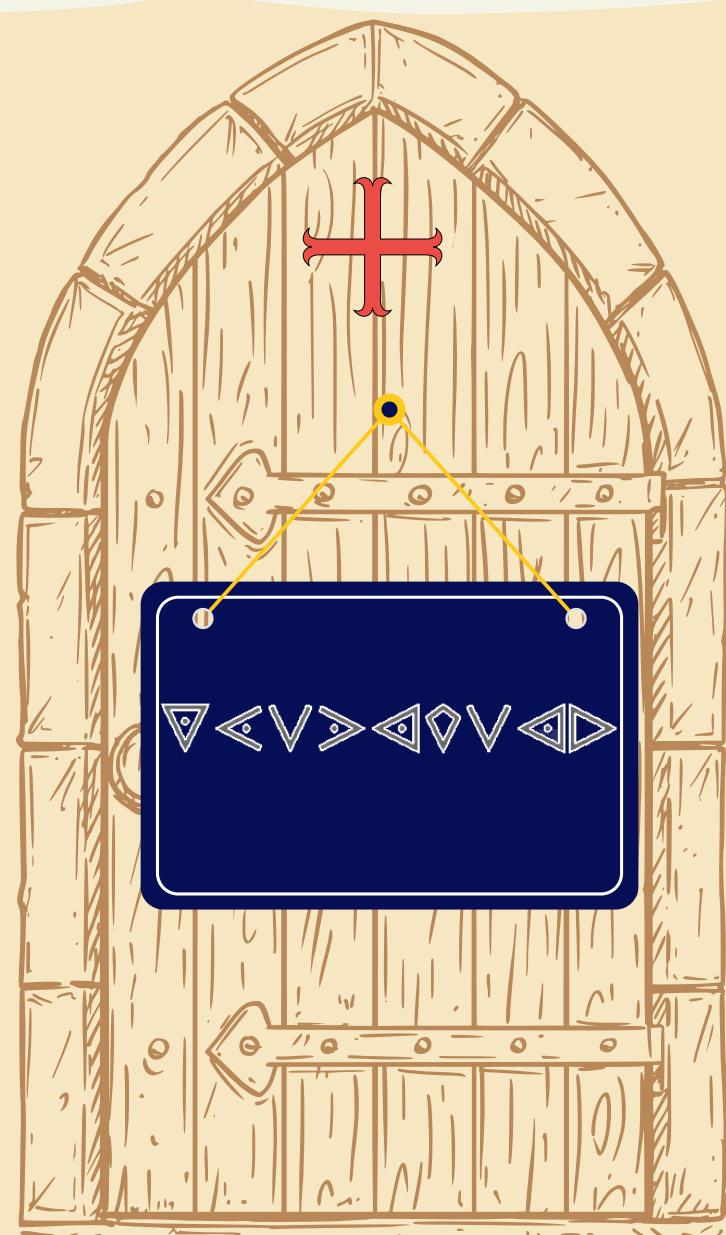
BIEN JOUÉ !

L'une des premières utilisations du chiffrement par substitution se trouve dans le Kamasutra. Un chapitre y est dédié pour permettre aux femmes de dissimuler leurs liaisons.



CHIFFREMENT PAR SUBSTITUTION ?

C'est une généralisation du chiffrement par décalage vu précédemment. Nous remplaçons encore une fois une lettre par une autre, mais ici, nous pouvons choisir pour chaque lettre de l'alphabet celle qui la remplacera.





4 SPARTE VÈME SIÈCLE AV. J.-C.

En plein cœur des guerres médiques, les Spartes doivent se défendre contre les invasions successives des Perses et d'Athènes.



BIEN JOUÉ !

Plus tard, les francs-maçons utiliseront une technique semblable pour créer le chiffre pigpen.



Nous avons réussi à mettre la main sur plusieurs bandes de messages mystérieux et incompréhensibles. Il semble que cette fois ci le chiffrement utilisé est un chiffrement par transposition (ou permutation). Tu l'as déjà rencontré lors du test que nous t'avons fait passer.

CHIFFREMENT PAR TRANSPOSITION ?

Le chiffre par transposition est, avec le chiffre par substitution, une des briques les plus utilisées par les chiffrements plus élaboré. Celle-ci consiste tout simplement à changer l'ordre des lettres dans le message.

spartiate = rtiaspate

Ici, la méthode de chiffrement est plus ingénieuse. Elle utilise une scytale, qui est un objet qui permet de facilement chiffrer et déchiffrer. Nous avons 2 modèles de scytale et 2 bandelettes. Il nous suffit de trouver la bonne association pour retrouver le message caché.



INFO BONUS



En 404 av. J.-C., Lysandre un général de Sparte, vit arriver un messager ensanglanté revenant de Perse. Il récupéra la ceinture de ce messager pour l'entourer autour de sa scytale. Il apprit alors que les Perses allaient lancer une attaque. Cela permit aux Spartes de se préparer à les repousser.





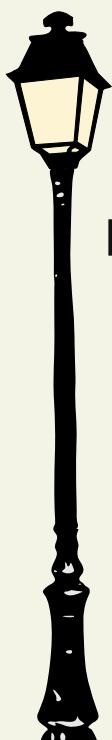
5

FRANCE : PARIS 1586

Blaise de Vigenère va révolutionner la cryptographie cette année en décrivant une méthode de chiffrement par substitution dans son livre intitulé « *Traité des chiffres* »



Étrange...
Ce tableau ne devrait pas être ici, il a été peint bien après 1586, en 1856.
Oh, un bout de papier est accroché derrière. Il semble que nous ayons encore affaire à un message chiffré.
Il semble que ce soit un chiffrement par substitution polyalphabétique.



BIEN JOUÉ !

La scytale était le premier dispositif de cryptographie militaire connu.



SUBSTITUTION POLYALPHABÉTIQUE ?

Il y a deux types de substitution : monoalphabétique et polyalphabétique. Dans le premier, une lettre est toujours remplacée par la même lettre. Le second peut lui combiner d'autres paramètres pour choisir la nouvelle lettre (comme sa position dans le message). Cela fait qu'une même lettre pourra être remplacée par différentes lettres.



zzwwavgk
clé = trésor

INFO BONUS

Ce n'est pas Vigenère qui créa le premier chiffrement par substitution polyalphabétique, on peut citer Giovan Battista Bellaso dont il parle dans son livre « *La Cifra del Sig* » publié en 1553.





6

ÉTATS-UNIS, VIRGINIE 1845

En plein expansionnisme porté par la "Destinée manifeste", les États-Unis alimentent peu à peu leur position de leader mondial.

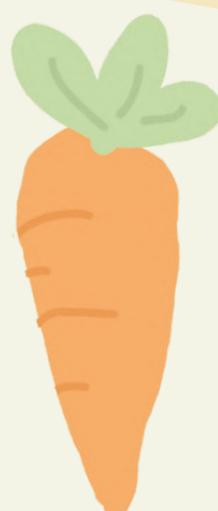


BIEN JOUÉ !

Le chiffrement de Vignère a résisté durant trois siècles aux cryptanalystes.



Nous voilà dans une grande plaine du sud ouest de la Virginie. Waouh, elle est remplie de lapin à queue blanche. Bizarre, ce lapin-ci a l'air d'avoir une lettre attaché autour de sa taille.



Sur le dos de l'enveloppe, on peut lire

1, 9, 16, 19, 63 lapin

À l'intérieur, il y a une lettre remplie de nombre et un long texte sur les ... lapins ?



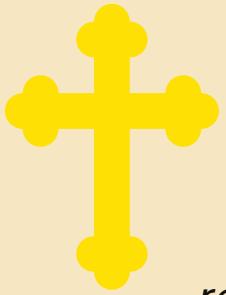
72, 3

45, 12, 68, 5, 71, 23,
24, 131, 73, 32, 41

129, 49, 76, 7, 31, 74,
66

INFO BONUS

Ce chiffre tient son nom de son créateur Thomas J. Beale. Il aurait découvert lors d'une expédition, un gisement d'or et d'argent. Voulant mettre ce butin à l'abri, il le cacha et donna trois lettres chiffrées à son ami Robert Morris contenant respectivement l'emplacement du trésor, son contenu et la liste des bénéficiaires. Malheureusement, les clés pour déchiffrer ces lettres ne lui furent jamais parvenues. Seule la deuxième lettre a pu être déchiffré avec comme clé la Déclaration d'indépendance des États-Unis d'Amérique.



7

ITALIE, ROME 1466

C'est cette année, que Leon Battista Alberti va révolutionner la cryptographie, jusqu'à être considéré, comme le père de la cryptographie occidentale.



Tiens, voilà un disque étrange. Il est accompagné d'un bout de papier incompréhensible. Ce disque me fait penser au célèbre disque d'Alberti.

zlln&mzdrtbqdsqeyiag

clé = s



BIEN JOUÉ !

"De componendis cifris" est le tout premier traité de cryptographie et a été écrit par Leon Battista Alberti.



DISQUE D'ALBERTI ?

C'est un cadran composé d'un cercle extérieur fixe et un cercle intérieur mobile. Ce qui rend ce chiffrement connu est qu'il a l'avantage d'être plus robuste, car le cercle est déplacé au cours du chiffrement, ce qui fait qu'une lettre ne sera pas toujours chiffrée par la même lettre.

Voici comment chiffrer un message.

On prend chaque lettre à partir du cercle extérieur (lettres majuscules) pour la remplacer par la lettre du cercle intérieur (lettres minuscules) juste en dessous. Il est chiffré par groupe de 3 lettres. À chaque fois que 3 lettres sont chiffrées, il faut tourner le cadran intérieur de 2 cases dans le sens antihoraire. Lorsque le message est entièrement chiffré, il faudra envoyer le chiffré et la dernière lettre du clair. Cela permettra à la personne de positionner correctement le disque intérieur pour commencer le déchiffrement du message.



INFO BONUS

Les chiffres sur le cercle extérieur sont une autre invention d'Alberti appelée le surchiffrement codique. Cette méthode consiste à créer toutes les combinaisons possibles avec 1, 2, 3 et 4, de 11 à 4444 soit 336. On associe un mot à une combinaison. Imaginons que 243 est associé au mot lapin, alors ce mot peut être chiffré par "aec" ou "knl" selon la position initiale du disque.





8

ALLEMAGNE 1918

Nous sommes vers la fin de la première guerre mondiale. À cette période, les gens regorgent d'inventivité pour créer des chiffrements difficilement cassable pour l'ennemi.



Attention, des soldats allemands. Vite allons nous cacher dans cet abri.



xx **** vv
FA *** FX ***



Tiens, cette radio émet un étrange message. Cela me fait penser au chiffre ADFGVX. Oh... étrange, il n'y a plus de son.



CHIFFRE ADFGVX?

Ce chiffre est composé de 2 étapes.

- La première étape consiste en une substitution de chaque lettre du clair par un binôme composé des lettres "A, D, F, G, V, X".
- La deuxième étape consiste à faire une transposition du résultat obtenu à l'étape précédente grâce à un mot, qui représente la clé du système.



Il nous faut donc trouver la fréquence qui diffuse le message et la clé. Un post-it est collé derrière la radio. Cela semble être une énigme, peut-être que la résoudre nous sera utile.



Mammifère herbivore de petite taille,
Me trouvant généralement en montagne.
De mes 4 estomacs, je suis la star du désherbage.

Exploratrice et intelligente,
Des ISICG, j'en suis devenu le symbole.
Ajouter 10 pi à la somme de mes caractères donne l'emplacement de mes vibrations.

Qui suis-je ?



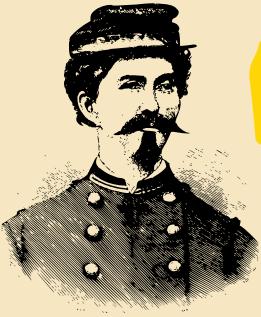
BIEN JOUÉ !

Même si les chiffres polyalphabétiques n'apparaissent qu'à la fin du XVI^e siècle, nous pouvons dire que Leon Battista Alberti en a créé les prémisses.



INFO BONUS

Ce chiffrement a été inventé par un lieutenant allemand Fritz Nebel et utilisé le 5 mars afin de sécuriser les communications radiophoniques pour l'offensive allemande sur Paris.



9

ETATS-UNIS 1863

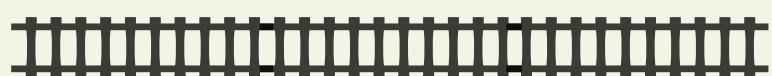
Nous sommes en pleine guerre de sécession opposant les états du Sud à ceux du Nord. Cette guerre fera environ 800.000 morts.



Nous voilà sur les prémisses d'un chemin de fer qui sera le premier à être transcontinental, reliant l'océan Atlantique à l'océan Pacifique sur plus de 3000 kilomètres et dont la construction prendra fin en 1869.

Tiens, voilà un papier intrigant. Il contient un message incompréhensible.

Tous ces rails me rappellent un drôle de chiffrement appelé Rail Fence.



CHIFFRE DE RAIL FENCE ?

C'est un chiffre par transposition qui utilise plusieurs lignes. Par exemple, pour 3 lignes, la première lettre est écrite sur la première ligne, la seconde sur la deuxième, la troisième sur la dernière, la quatrième sur la deuxième... À la fin, les lettres sont concaténées ligne par ligne.

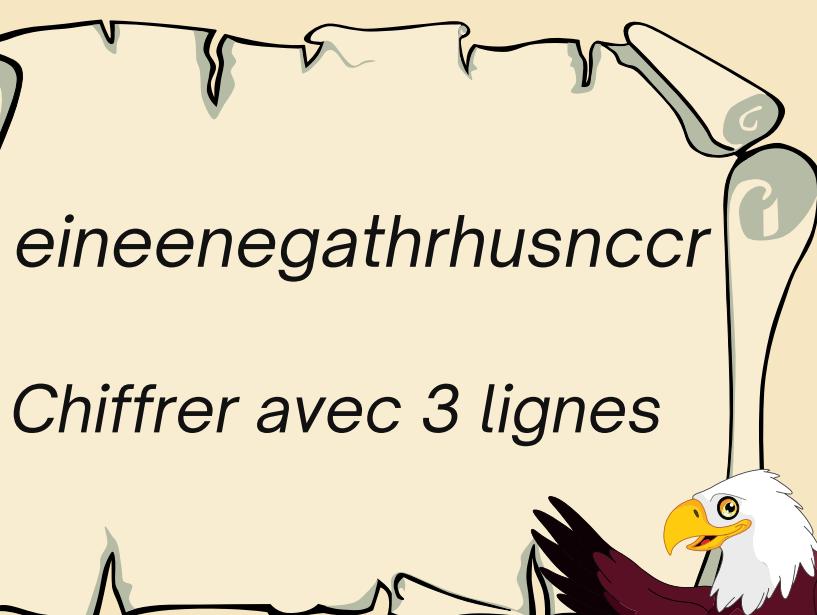
Avec 2 lignes, nous pouvons chiffrer train par :

t a n
r i → tanri

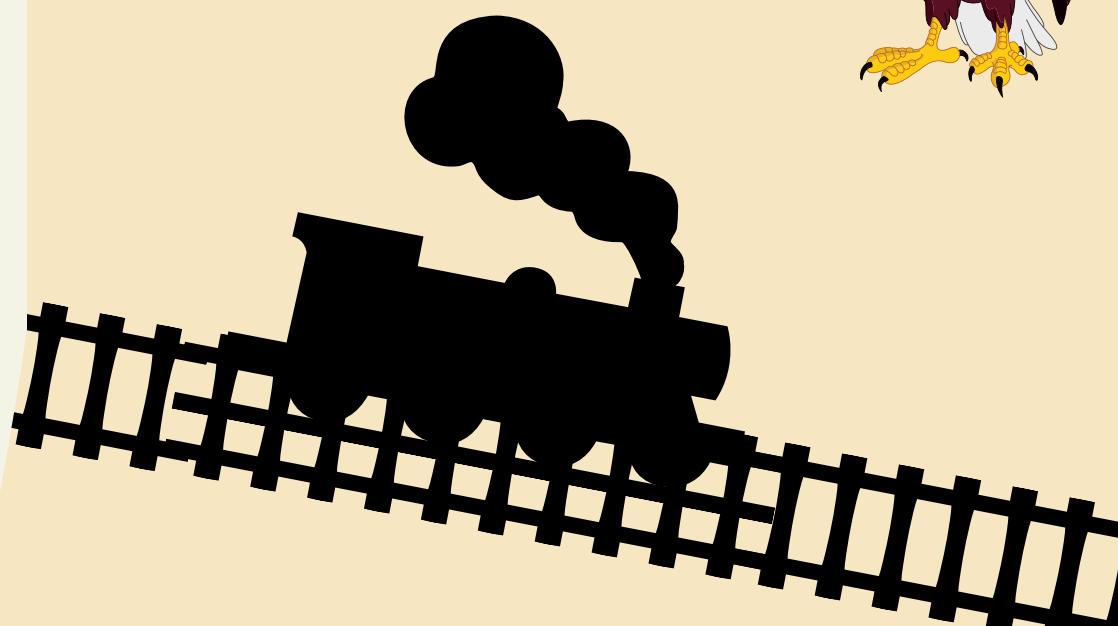


BIEN JOUÉ !

Pour en revenir au chiffrement, il fut cassé début juin par le lieutenant Georges Painvin. Cela conféra un énorme avantage à l'armée française qui mit en échec l'offensive allemande.



Chiffrer avec 3 lignes



INFO BONUS

La première utilisation de ce chiffre est antérieur au Moyen-Age. Le développement de chiffre plus puissant le rendit inutile. Pourtant, il a eu un regain d'utilisation, en étant utilisé par les espions confédérés et fédéraux pour chiffrer leurs dépêches pendant la guerre de sécession.



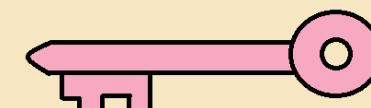
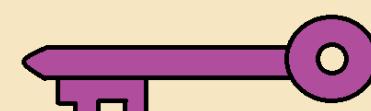
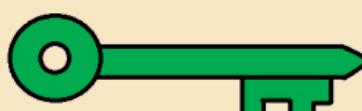
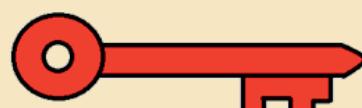
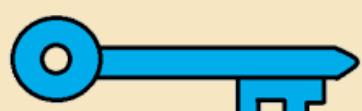


10 ENTRE LES DIMENSIONS



BIEN JOUÉ !

Ce chiffre est aussi connu sous le nom de chiffre zigzag.



Dépêchons-nous, il n'est peut-être pas trop tard





Je ne pensais pas qu'un de mes étudiants voudraient m'empêcher d'accomplir mon plan. Mais malheureusement pour vous, il est trop tard. Grâce à cette clé, mes étudiants auront toujours 20/20.



Nous pouvons encore le stopper en réussissant des épreuves. Sers-toi des compétences acquises au cours de notre voyage pour résoudre ces chiffrements.





K

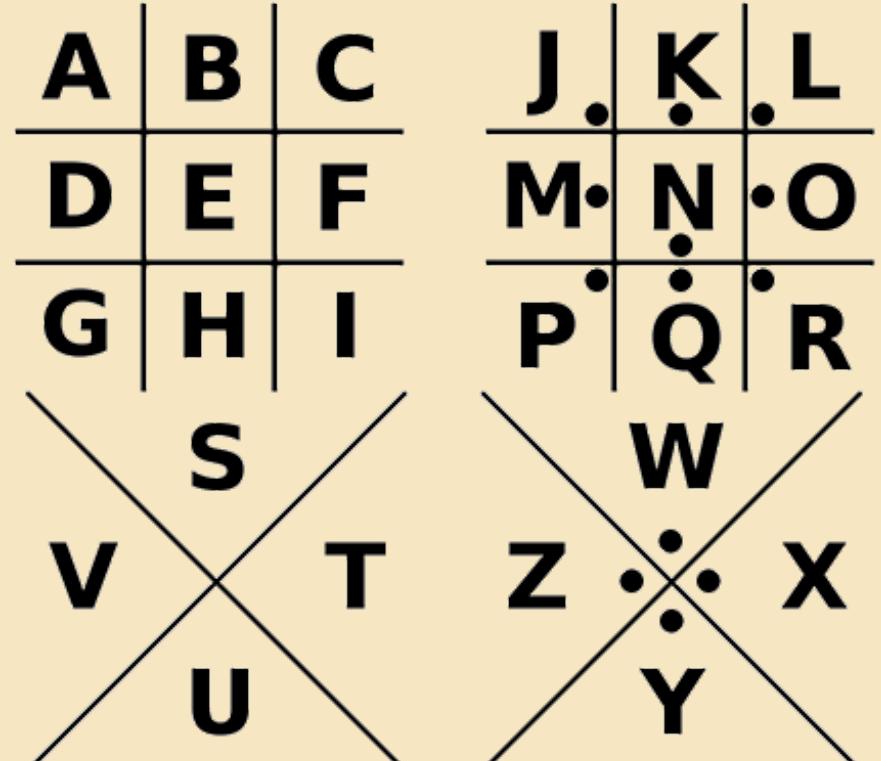


Dmzkqvombwzqf

C█F█J█O█L█E█J█L█E█O█

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I	J
3	L	M			
4					

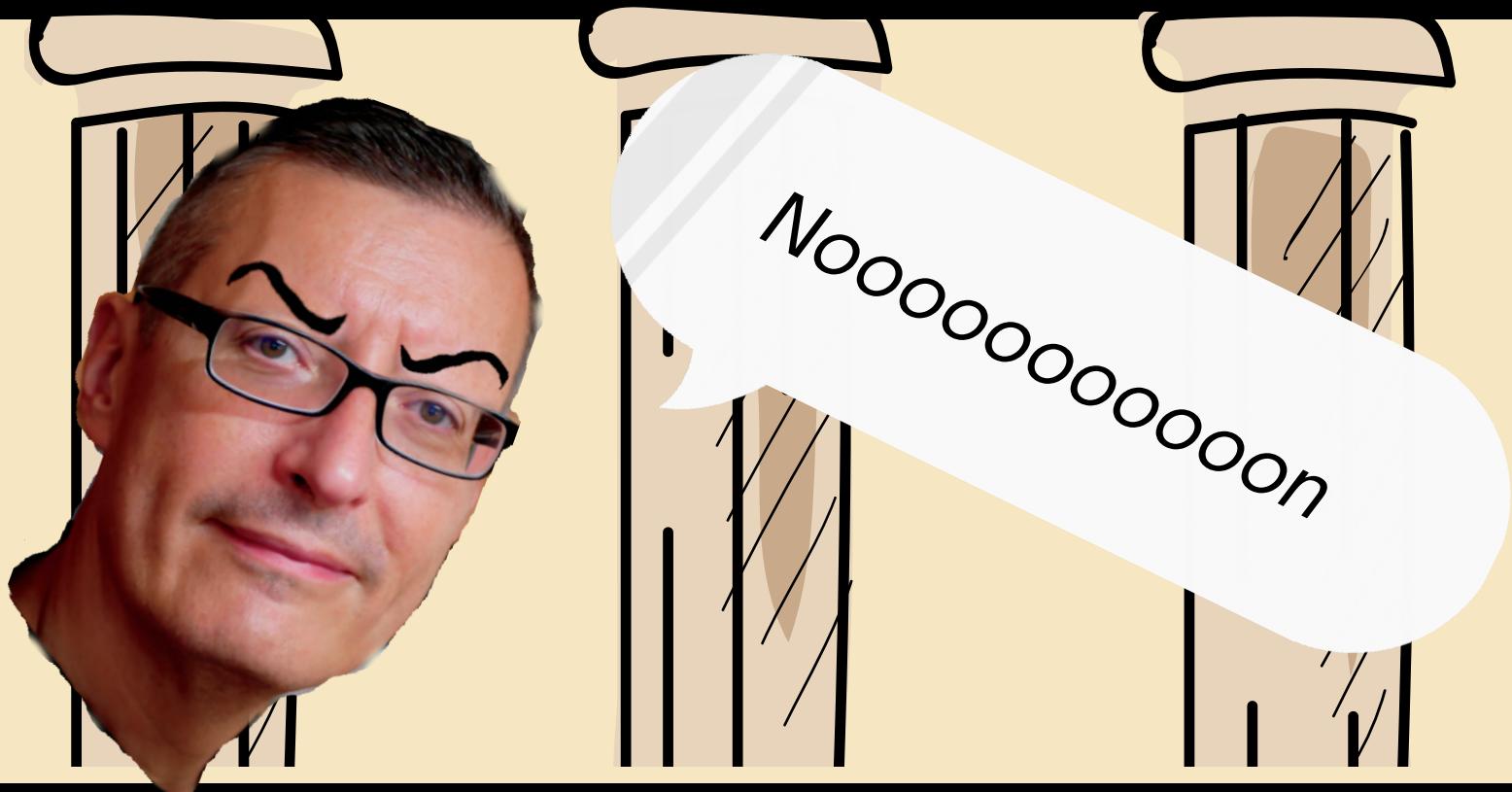
131142421514153
53431541215



POTION
TRANSLUMINEUSE



7 8 9 10 11 12
11 4 3 4 5 6



Bravo, tu as
arrêté les plans
de Mr Bonnefoi.

Nous n'y serions
jamais arrivés sans toi.



Et c'est ainsi que l'aventure pour empêcher les ambitions de Mr Bonnefoi prit fin.

Finalement, Mr Bonnefoi comprit que transformer le monde n'était pas la meilleure solution pour la réussite de ses étudiants.

À la place, il devint un grand professeur soucieux de leurs réussites pour que tous puissent valider leur année.



Fin