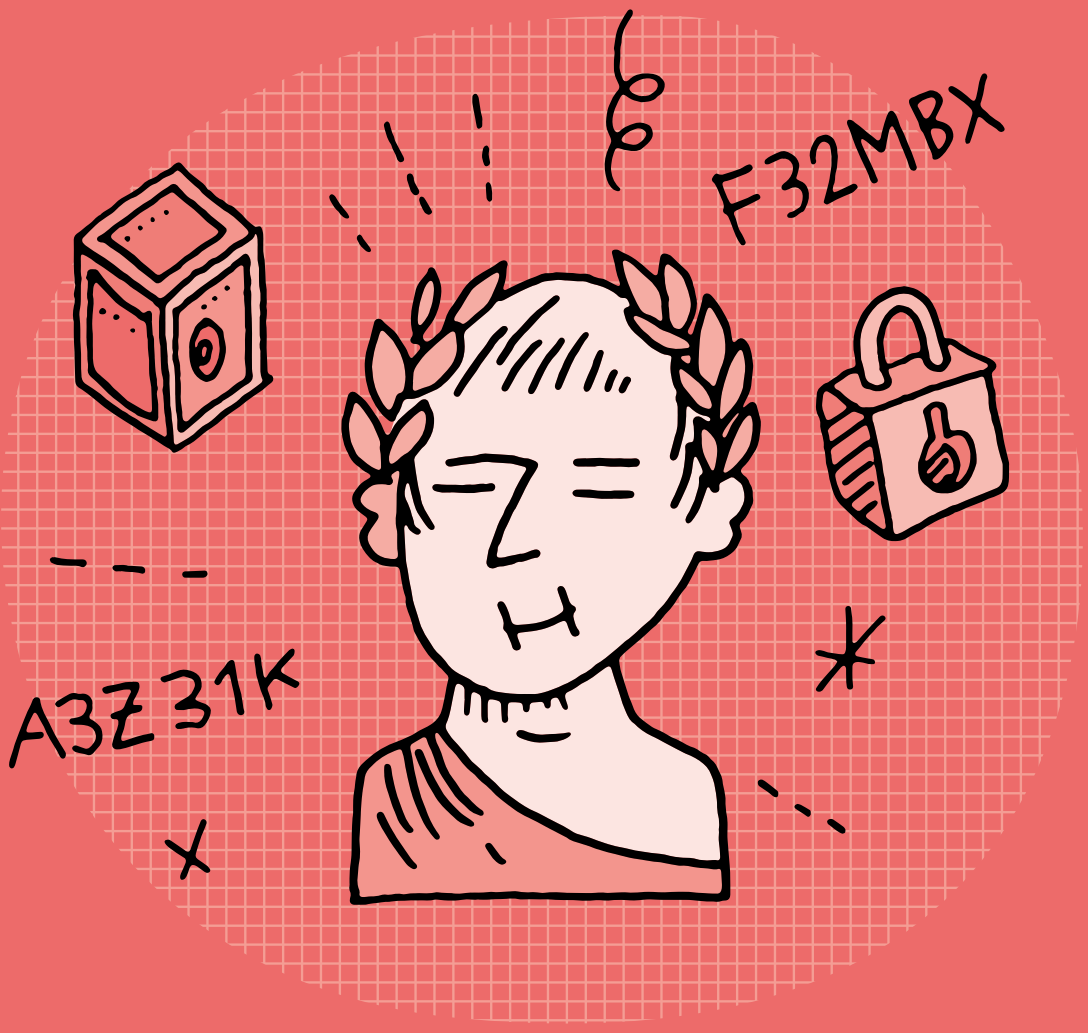
Enquête 5 • SI • 6e

Comment l'empereur romain Jules César protégeait-il ses messages secrets ?



SI • 6e
Comment l'empereur romain Jules César protégeait-il ses messages secrets ?

Objectifs du Plan d'études romand (PER):

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

2 … en encodant, décodant et en transformant des données

Information et données

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

Liens disciplinaires:

- L128 – Écriture et instruments de la communication
- SHS 22 – Trace et mémoire

Intentions pédagogiques:

Cette enquête vise à montrer aux élèves que l'on peut chiffrer un message pour le rendre incompréhensible et ainsi le transmettre de manière confidentielle. Il est possible de le déchiffrer si l'on possède la clé. Il existe cependant des possibilités pour casser le chiffrement. On aborde donc la cryptographie par une technique simple à mettre en œuvre en classe.

La question de l'enquête:

Comment l'empereur romain Jules César protégeait-il ses messages secrets?

Étape	Résumé	Matériel
1. Pour comprendre la question **Durée:** 10 minutes	**Début de l'investigation:** • Comparer deux messages interceptés, un lisible et un autre chiffré selon la méthode du chiffrement de César. • Visionner une vidéo explicative pour situer le contexte.	• fiche 1 (matériel de classe) • fiche 2 (à projeter ou 1 par élève) • vidéo *Cryptographie César* (partie 1) [56-45-01] • affichage numérique
2. Pour répondre à la question **Durée:** 25 minutes	**Poursuite de l'investigation:** • Tenter de percer le mystère du message selon différentes méthodes. • Déchiffrer le message.	• fiches 3, 4 et 7 (1 par élève) • attache parisienne • vidéo *Cryptographie César* (partie 2) [56-45-02] • affichage numérique
3. Pour conclure **Durée:** 15 minutes	**Conclusion:** • Tester la méthode de chiffrement en envoyant et en déchiffrant des messages codés.	• disque de chiffrement réalisé lors de l'étape 2 (1 par élève) • fiche 5 (1 par élève) • fiche 6 (à projeter) • vidéo *Cryptographie César* (partie 3) [56-45-03] • affichage numérique

Étape 1
Pour comprendre la question

Résumé :
- Comparer deux messages interceptés, un lisible et un autre chiffré selon la méthode du chiffrement de César.
- Visionner une vidéo explicative pour situer le contexte.

Matériel :
- fiche 1 (matériel de classe)
- fiche 2 (à projeter ou 1 par élève)
- vidéo *Cryptographie César* (partie 1) [56-45-01]
- affichage numérique

Temps 1.1 : Intercepter un message

Modalités de travail : en collectif

Durée : 5 minutes

On annonce qu'on a écrit un message sur un papier (préalablement découpé et plié) et qu'on va le donner à une personne de la classe (voir message 1 de la fiche 1). L'élève qui reçoit le message le lit mentalement. On reprend le message et on annonce qu'on va le transmettre à une deuxième personne qui pourra le lire dans sa tête. Et ainsi de suite. Cependant, si le message est intercepté par quelqu'un d'autre avant d'arriver chez son destinataire, alors cette personne pourra le lire à l'ensemble de la classe. On jette volontairement le papier de manière à ce qu'il n'arrive pas chez son destinataire. Le message est alors dévoilé et lu à la classe :

CODE POUR OUVRIR LE COFFRE-FORT : 279671

On explique à la classe que l'on aurait voulu que ce message reste secret. On va alors envoyer un nouveau message selon les mêmes modalités que précédemment mais il sera écrit comme le faisait Jules César, le célèbre empereur romain (voir message 2 de la fiche 1).

QJX WJSKTWYX FWWNAJSY F Q'FZGJ.

On rejoue l'envoi du message. L'élève qui intercepte cette fois le message 2 essaie de le lire à la classe, puis vient l'écrire au tableau pour que tout le monde le visualise bien. On explique que cette méthode était employée par Jules César pour envoyer des messages sans que ces ennemis puissent les lire. On énonce alors aux élèves la question « Mais comment faisait-il ? » permettant ainsi d'introduire le temps 1.2.

Pour ancrer davantage ce temps 1.1, on peut imaginer que dans la classe se trouve un coffre-fort représenté par une boîte fermée par un cadenas, dans laquelle on a glissé un trésor. Le premier message envoyé à l'une des personnes de la classe contient donc le code du cadenas. La personne qui a eu connaissance du message peut venir ouvrir la boîte et découvrir le trésor. Mais l'élève qui a intercepté le message dans un second temps va également pouvoir venir ouvrir la boîte révélant la nécessité de coder le message.

Cryptographie : La cryptographie est le domaine qui étudie la manière dont des communications ou des données numériques peuvent être protégées pour empêcher d'y accéder.

Cryptage : Le cryptage est un terme à l'usage plutôt déconseillé, on lui préfère le terme de chiffrement. De nombreuses sources demandent également de ne pas utiliser le verbe crypter, jugé peu rigoureux, et de lui préférer le verbe chiffrer.

Chiffrement : Procédé de cryptographie par lequel on rend des données incompréhensibles à toute personne qui ne possède pas la clé de déchiffrement.

Déchiffrement : Procédé qui permet de récupérer les données originelles d'un message précédemment chiffré. Pour cela, il faut connaître la clé de déchiffrement.

Clé de chiffrement : Suite de caractères qui permet de chiffrer et déchiffrer un message. Si la clé est la même pour les deux opérations, on parle de chiffrement/déchiffrement symétrique, si les clés sont différentes, on parle de chiffrement/déchiffrement asymétrique.

Décryptage : Procédé qui consiste à retrouver le message clair correspondant à un message chiffré sans posséder la clé de déchiffrement. À l'inverse de cryptage, décryptage peut être employé, dans le cas défini ci-avant. En anglais, on parle de *casser* le message secret (*break*, *crack*).

Temps 1.2 : Mais comment faisait César ?

Modalités de travail : en collectif

Durée : 5 minutes

On propose aux élèves de visionner la première partie d'une vidéo [56-45-01] permettant d'expliquer ce que faisait César. Cette première partie ne sert qu'à contextualiser l'envoi de messages secrets, sans donner la clé de l'explication.

On pourra donner quelques éléments de vocabulaire aux élèves : la Gaule - capituler - Jules César - Cicéron. La fiche 2 peut être utile à cet effet. Il est recommandé de projeter une première fois la vidéo, d'expliciter avec les élèves les éléments de vocabulaire précisés ci-dessus (voire d'autres, si les élèves le demandent), puis de la projeter une seconde fois.

La vidéo à projeter est une production de **Science Tips** pour le compte du Commissariat à l'Énergie Atomique (CEA), organisme de recherche scientifique français dans les domaines de l'énergie, de la défense, des technologies de l'information et de la communication, des sciences de la matière, des sciences de la vie et de la santé.

Elle est disponible en intégralité (2'14) *via* ce lien court : [56-45-04].

Pour les besoins de cette enquête, la vidéo a été découpée en trois parties :
- Partie 1 : contextualisation [56-45-01]
- Partie 2 : réponse à la question [56-45-02]
- Partie 3 : pour aller plus loin [56-45-03]

Étape 2
Pour répondre à la question

Résumé :
- Tenter de percer le mystère du message selon différentes méthodes.
- Déchiffrer le message.

Matériel :
- fiches 3, 4 et 7 (1 par élève)
- attache parisienne
- vidéo *Cryptographie César* (partie 2) [56-45-02]
- affichage numérique

Temps 2.1 : Essais

Modalités de travail : en collectif

Durée : 5 minutes

On demande aux élèves d'essayer de décoder le message écrit au tableau :

QJX WJSKTWYX FWWNAJSY F Q'FZGJ.

On demande aux élèves quelle pourrait être la signification de ce message (le message signifie : LES RENFORTS ARRIVENT À L'AUBE.)

Les élèves vont vraisemblablement tester plusieurs hypothèses en laissant libre cours à leur imagination. Il est peu probable qu'elles et ils se basent sur de véritables stratégies (fréquences des lettres, recherche de mots probables), mais on peut les amener à repérer des indices dans la phrase : **lettres doubles**, **mots de deux ou trois lettres**, **lettres isolées**…

QJX WJSKTWYX FWWNAJSY F Q'FZGJ.

Temps 2.2 : Infographie et vidéo

Modalités de travail : en collectif

Durée : 5 minutes

On distribue le document de la fiche 3 et on leur propose de le lire silencieusement. On demande ensuite si certaines et certains ont trouvé un indice permettant de déchiffrer le message. Le texte qui permet de comprendre le chiffrement du message se trouve dans la partie consacrée à Jules César : « Il s'agit de décaler les lettres de l'alphabet d'un certain nombre de cases, connu uniquement de l'expéditrice ou l'expéditeur et de la ou du destinataire du message. Ainsi, si ce nombre est de 3, alors A devient D, B devient E… ».

Pour confirmer ce que les élèves ont trouvé, on projette la deuxième partie de la vidéo [56-45-02].

Après la vidéo, on précisera que dans celle-ci on parle de coder un message pour le rendre incompréhensible à qui ne sait pas comment faire pour le lire, que le terme précis est **chiffrer**, qu'on effectue un **chiffrement** avec un système particulier, la **clé de chiffrement**, et qu'il faut posséder cette clé pour **déchiffrer** le message.

On pourra compléter ce temps (ou le faire à la fin de l'enquête) en faisant décalquer par les élèves la carte muette de la Suisse, disponible en fiche 7, pour la superposer sur la carte romaine disponible également en fiche 7, et ainsi montrer l'influence de la culture de l'empire romain sur la zone d'influence correspondant à la Suisse (prévoir du papier calque).

Temps 2.3 : Disque de chiffrement

Modalités de travail : en binômes

Durée : 5 minutes

On demande aux élèves de se mettre par deux et on distribue à chaque élève un disque de chiffrement découpé et réalisé auparavant (voir fiche 4). On demande ensuite à une, un ou plusieurs élèves d'expliquer comment ce disque peut fonctionner. On fait reformuler plusieurs élèves pour s'assurer que tout le monde a compris son principe.

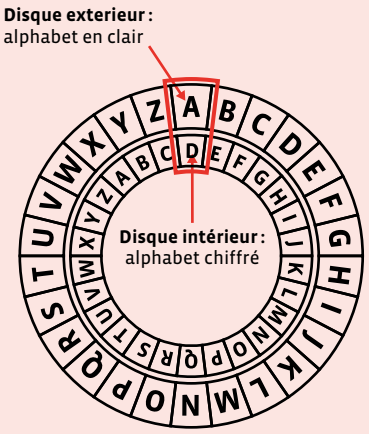
Disque de chiffrement : Ce disque peut faire l'objet, a priori ou a posteriori de la séance, d'une réalisation par les élèves qui associe arts visuels, travaux manuels (tracés, découpage, lettres stylisées éventuellement), technologie (réalisation d'un objet technique) ou mathématiques (mesures d'angles, calculs liés au cercle…).

Son utilisation se fait selon le descriptif suivant :

Le disque extérieur correspond à l'alphabet en clair. On décale le disque intérieur du nombre de rang correspondant à la clé de chiffrement (ici 3).

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…).

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



Temps 2.4 : Déchiffrer

Modalités de travail : en binômes

Durée : 10 minutes

On laisse ensuite les élèves tester plusieurs décalages jusqu'à ce qu'elles et ils trouvent la solution (le décalage choisi pour le message du début est de 5). On peut instaurer une forme de compétition et le premier binôme ayant réussi pourra alors donner la clé de chiffrement à la classe entière qui testera alors sa validité.

QJX WJSKTWYX FWWNAJSY F Q'FZGJ. = LES RENFORTS ARRIVENT À L'AUBE.

Étape 3
Pour conclure (validation, mise en forme)

Résumé :
- Tester la méthode de chiffrement en envoyant et en déchiffrant des messages codés.

Matériel :
- disque de chiffrement réalisé lors de l'étape 2 (1 par élève)
- fiche 5 (1 par élève)
- fiche 6 (à projeter)
- vidéo *Cryptographie César* (partie 3) [56-45-03]
- affichage numérique

Temps 3.1 : S'envoyer des messages

Modalités de travail : en binômes

Durée : 10 minutes

Les élèves vont devoir décider d'une clé de chiffrement. Ce travail va leur permettre de découvrir la notion de bug. Il suffit d'un bug dans le codage du message pour produire un message non conforme. D'où la nécessité de mettre en place des procédures de vérification, permettant de s'assurer que le message est le même aux deux bouts de la chaîne d'information.

Modularité

Les élèves se mettent par deux et décident d'une clé de chiffrement (correspondant au nombre de décalage des deux alphabets de la roue de chiffrement). Les binômes retournent ensuite à leur place respective et on distribue les disques de chiffrement ainsi que la fiche 5 afin que chaque élève ait le matériel à disposition. On demande aux élèves de rédiger leurs messages à destination de leur binôme et de le chiffrer. Le message doit être assez court : 48 lettres (caractères) maximum (en comptant les espaces et les signes de ponctuation comme des lettres). Chaque élève prépare son message. Une fois le message chiffré, chaque binôme s'échange le message sans se parler. Chaque élève essaie alors de déchiffrer le message de son binôme à l'aide des outils fournis. On s'assurera qu'expéditrice ou expéditeur et destinataire utilisent bien la même clé de chiffrement (nombre de décalage).

Si l'organisation proposée ci-dessus ne convient pas car les déplacements dans la classe sont problématiques, on peut procéder comme dans le scénario 4 *Codage de données, codage binaire* (séance 2 : Pixel Paravent) et placer une séparation entre deux élèves.

On pourra également montrer aux élèves qu'il y a d'autres outils pour utiliser le chiffrement de César (voir fiche 6 à projeter).

Temps 3.2: Casser le code (décrypter)

Modalités de travail: en collectif

Durée: 5 minutes

Ce travail sur le décryptage peut également faire comprendre aux élèves la nécessité d'avoir des mots de passe dits **robustes**. En effet, si leurs mots de passe sont trop simples (leur prénom, date de naissance, suite de nombre comme 1234...), ils seront faciles à trouver.

Responsabilité

De plus, cette enquête met l'accent sur la confidentialité des informations. Un parallèle peut être fait avec les identifiants et/ou mots de passe. Si les élèves les communiquent, elles et ils ne savent pas ce qu'en feront les personnes qui les ont récupérés, d'où l'importance de garder ces données pour soi uniquement. Ces données sont confidentielles.

Charte Éducation numérique

Je garde secrets mes identifiants et mots de passe et je ne communique pas d'informations personnelles sur Internet (nom, prénom, adresse...).

charte-numerique.edu-vd.ch

Illustration: T. Schyrr (CC)

On peut prendre le message d'une ou d'un élève sans connaître la clé de chiffrement et tester toutes les possibilités (26). Cette méthode s'appelle une attaque par force brute. Elle peut être réalisée grâce à des sites [56-45-05] qui proposent de décrypter un message chiffré avec la méthode de César.

Les élèves s'apercevront ainsi qu'une méthode de chiffrement offre souvent des failles que l'on peut exploiter pour percer le mystère...

Attaque par force brute: une des méthodes utilisée pour déchiffrer un message s'appelle l'attaque par force brute: il s'agit de tester toutes les combinaisons possibles.

Cela nécessite cependant de connaître la méthode utilisée pour chiffrer le message.

Dans le cas du chiffrement de César, les élèves peuvent tenter de tester tous les décalages possibles (26 combinaisons car 26 lettres dans l'alphabet) pour percer le mystère d'un message.

Prolongement

On peut projeter la troisième et dernière partie de la vidéo [56-45-03].

Pour déchiffrer un message utilisant la méthode de César, on peut aussi procéder à une analyse de fréquence des lettres. Il s'agit de repérer dans le message la lettre la plus fréquemment utilisée et de regarder le décalage entre cette lettre et le E qui est la lettre la plus courante dans la langue française. Pour exemple, cette analyse fonctionne très bien avec le message utilisé lors de la première étape:

- QJX WJSKTWYX FWWNAJSY F Q'FZGJ
- Lettres les plus utilisées: J (4 fois) et W (4 fois)
- Décalage entre le E et le J: 5 (clé de chiffrement)
- Décalage entre le E et le W: 18 (peut être testé mais ne donnera pas de résultat)

Analyse fréquentielle : L'analyse fréquentielle est une méthode de cryptanalyse dont la description la plus ancienne est réalisée par Al-Kindi au IXe siècle. Elle consiste à examiner la fréquence des lettres employées dans un message chiffré. Cette méthode est fréquemment utilisée pour décoder des messages chiffrés par substitution, dont un exemple très simple est le chiffre de César.

L'analyse fréquentielle est basée sur le fait que, dans chaque langue, certaines lettres ou combinaisons de lettres apparaissent avec une certaine fréquence. Par exemple, en français, le *e* est la lettre la plus utilisée, suivie du a et du s. Inversement, le w est peu utilisé.

Ces informations permettent aux cryptanalystes de faire des hypothèses sur le texte clair, à condition que l'algorithme de chiffrement conserve la répartition des fréquences, ce qui est le cas pour des substitutions mono-alphabétiques et poly-alphabétiques.

Une deuxième condition nécessaire pour appliquer cette technique est la longueur du cryptogramme. En effet, un texte trop court ne reflète pas obligatoirement la répartition générale des fréquences des lettres. De plus, si la clé est de la même longueur que le message, il ne pourra y avoir de répétition de lettre et l'analyse fréquentielle deviendra impossible.

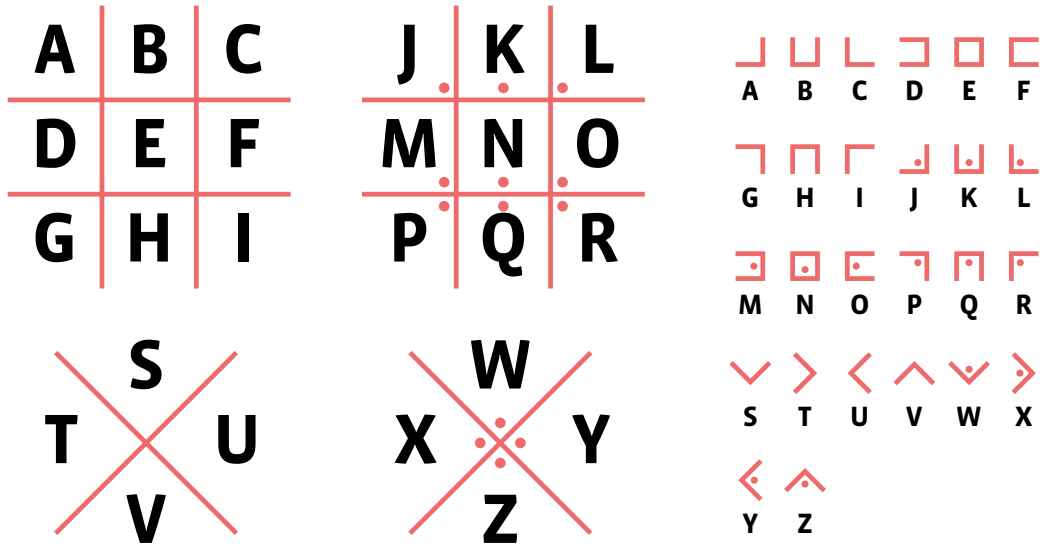
source: Wikipédia [56-45-06]

Une fois quelques messages déchiffrés, les élèves se rendent compte qu'il faut complexifier le chiffrement. On peut leur proposer quelques pistes :

- Changer la clé de chiffrement à chaque lettre. On peut s'aider d'un nombre pour cela. Par exemple, avec 284 on opère un décalage de 2 pour la première lettre, de 8 pour la deuxième, de 4 pour la suivante, puis à nouveau de 2 pour la suivante et ainsi de suite… On appelle cette technique le chiffre de Vigenère.
- Concevoir une table de chiffrage avec des lettres aléatoires et/ou des nombres :

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

- Utiliser un autre code où les lettres sont remplacées par des symboles, comme le code des templiers ou ses variantes, par exemple :



LES RENFORTS ARRIVENT A L'AUBE

Fiche 1

Messages

Message 1

1

CODE POUR OUVRIR LE COFFRE-FORT : 279671

Message 2

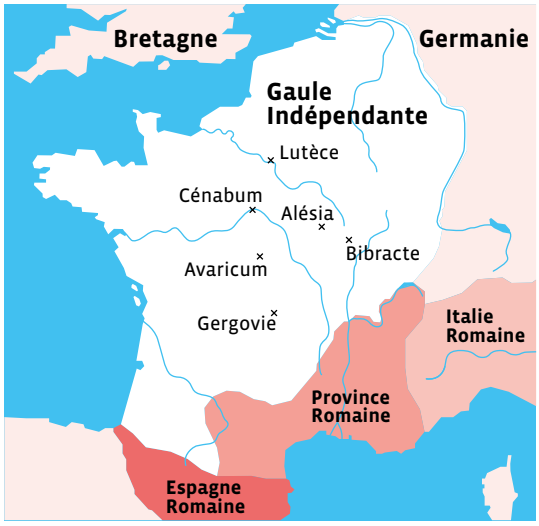
2

QJX WJSKTWYX FWWNAJSY F Q'FZGJ.

Fiche 2

Prénom : .....

Contexte historique



La Suisse, la Belgique et la France que l'on connaît aujourd'hui n'ont pas toujours eu les mêmes frontières, ni les villes les mêmes noms. Auparavant, on parlait d'Helvétie, de Gaule belgique et de Gaule. Ces pays ont fait l'objet, au temps de Jules César (premier siècle avant Jésus-Christ), de conquêtes de la part de l'Empire romain (actuelle Italie).

Jules César est un empereur romain, né en 100 avant Jésus-Christ et mort en 44 avant Jésus-Christ à Rome.
Il étend l'Empire romain en menant des batailles et en conquérant notamment la Gaule et une partie de la Germanie (actuelle Allemagne).

Cicéron est un homme d'État romain. Allié de Jules César dans un premier temps, il décide de devenir un opposant dans un second temps.

Capituler : accepter la défaite, s'avouer vaincu et rendre les armes.

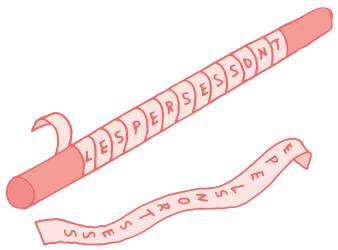
Petite histoire de la cryptographie

Ve siècle av. JC

Pendant l'Antiquité, les habitants de Sparte (une ancienne ville grecque) utilisaient un bâton de bois pour enrouler une lanière de cuir sur laquelle on écrivait un message.

Une fois déroulée, le message était illisible. Il fallait posséder un bâton du même diamètre pour enrouler à nouveau la lanière et lire le message.

Ce sont les premiers pas connus de la cryptographie.



Ier siècle av. JC

Le célèbre empereur romain, **Jules César**; a donné son nom à une technique de chiffrement: le chiffre de César. Il s'agit de décaler les lettres de l'alphabet d'un certain nombre de cases, connu uniquement de l'expéditeur et du destinataire du message.

Ainsi, si ce nombre est de 3, alors A devient D, B devient E... C'est la plus ancienne méthode de substitution mono-alphabétique.

IXe siècle

Al-Kindi (801-873), un philosophe arabe, a écrit le premier ouvrage de cryptographie (ou déchiffrement) connu. Ce livre a été retrouvé en 1987 dans des archives à Istanbul (Turquie).

Ce texte décrit notamment la possibilité de déchiffrer un message en se basant sur la fréquence des lettres dans le message chiffré.

1586

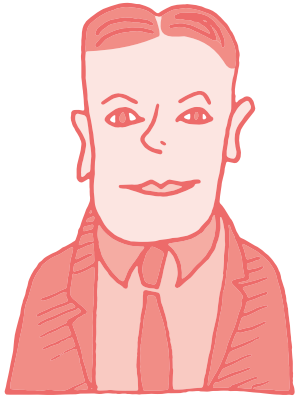
Blaise de Vigenère (1523-1596), diplomate français, a créé une technique qui consiste à remplacer une lettre par une autre en fonction de sa position dans le message (on parle de substitution polyalphabétique).

Une même lettre peut ainsi être remplacée par plusieurs lettres différentes.

1942

Alan Turing (1912-1954), brillant mathématicien britannique, a réussi à déchiffrer le code des messages allemands pendant la seconde guerre mondiale.

Ces messages étaient chiffrés à l'aide de la machine Enigma aux un million de milliards de combinaisons possibles.

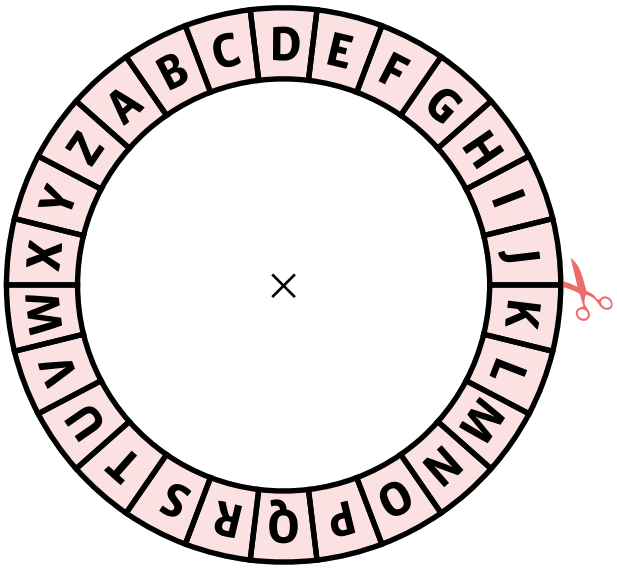


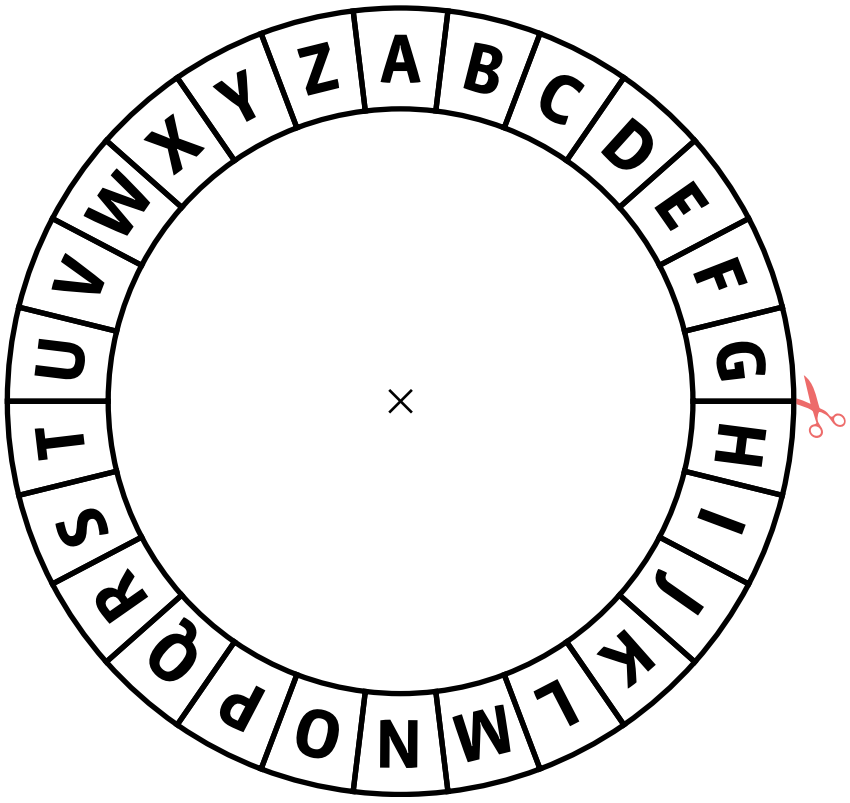
Infographie

Prénom : .....

Fiche 4

Disque de chiffrement





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 niveau du point bleu.

4. Faire passer une attache parisienne pour les solidariser.

5. Chiffrer.

Fiche 5

Prénom : .....

Chiffrer / déchiffrer un message

1. Écris le message à envoyer (48 caractères, espaces incluses) :

Message initial : → _____

2. Choisis le nombre de décalage : → _____
   Chiffre ton message initial à l'aide du disque de chiffrement et du tableau suivant.

Message initial																		
Message chiffré																		
Message initial																		
Message chiffré																		
Message initial																		
Message chiffré																		

3. Récris le message chiffré sur une feuille.
   Donne cette feuille à ton binôme (avec la clé).

4. Récupère le message chiffré de ton binôme.
   Écris la clé de chiffrement communiquée : → _____
   Déchiffre le message à l'aide du disque de chiffrement et du tableau suivant.

Message chiffré																		
Message déchiffré																		
Message chiffré																		
Message déchiffré																		
Message chiffré																		
Message déchiffré																		

5. Écris le message reçu déchiffré :

→ _____

Fiche 5

Exemple

Chiffrer / déchiffrer un message

1. Écris le message à envoyer (48 caractères, espaces incluses):

Message initial: → *Rendez-vous à seize heures au grand arbre.*

2. Choisis le nombre de décalage: → *8*

Chiffre ton message initial à l'aide du disque de chiffrement et du tableau suivant.

Message initial	R	E	N	D	E	Z	–	V	O	U	S		A		S	E
Message chiffré	Z	M	V	L	M	H	–	D	W	C	A		I		A	M
Message initial	I	Z	E		H	E	U	R	E	S		A	U		G	R
Message chiffré	G	H	M		P	M	C	Z	M	A		I	C		O	Z
Message initial	A	N	D		A	R	B	R	E	.						
Message chiffré	I	V	L		I	Z	J	Z	M	.						

3. Récris le message chiffré sur une feuille.

Donne cette feuille à ton binôme (avec la clé).

ZMVLMH-DWCA I AMGHM PMCZMA IC OZIVL IZJZM.

4. Récupère le message chiffré de ton binôme.

L'IKKWZL, R'G AMZIQ.

Écris la clé de chiffrement communiquée: → *8*

Déchiffre le message à l'aide du disque de chiffrement et du tableau suivant.

Message chiffré	L	'	I	K	K	W	Z	L	,		R	'	G		A	M
Message déchiffré	D	'	A	C	C	O	R	D	,		J	'	Y		S	E
Message chiffré	Z	I	Q	.												
Message déchiffré	R	A	I	.												
Message chiffré																
Message déchiffré																

5. Écris le message reçu déchiffré:

→ *D'accord, j'y serai.*

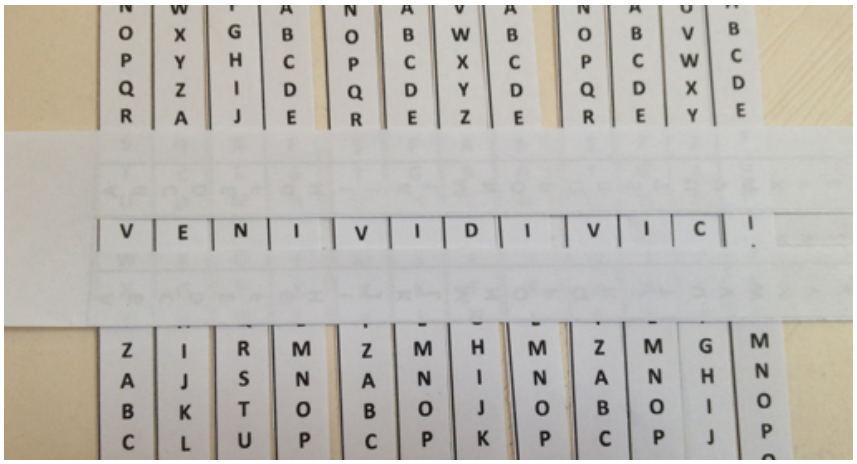
Fiche 6

À projeter

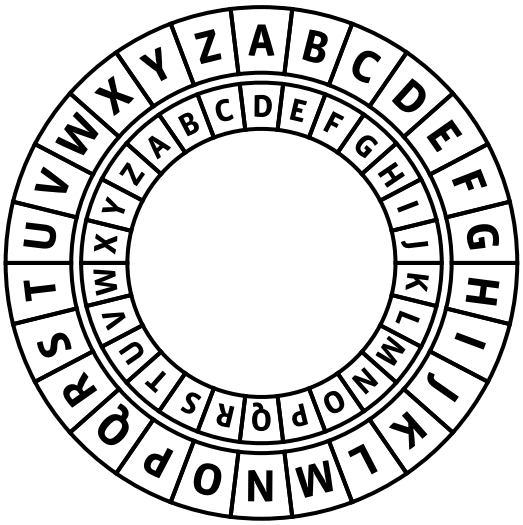
Outils de chiffrage de type *Code César*

Rouleau à chiffrer (scytale)

Réglettes



Disque de chiffrement



Fiche 7

Prénom : .....

Carte de l'Empire Romain et Carte de la Suisse