De l'origine de l'alphabet à la protection des données :
Coder pour mieux communiquer

CODER POUR PROTÉGER

Mallette pédagogique 3

CETTE MALLETTE A ÉTÉ RÉALISÉE PAR

Les Maths en Scène
Les Maths où on ne les attend pas !

EN PARTENARIAT AVEC

Evrêk'Alès

FINANCÉE PAR

La Région Occitanie
Pyrénées · Méditerranée

INTRODUCTION

Dans ce jeu coopératif, les élèves plongent dans l'histoire fascinante de la **cryptographie**, depuis les premières méthodes antiques jusqu'aux techniques plus sophistiquées et automatisées du début du XX^{e} siècle.

À travers une série d'énigmes, ils apprennent à chiffrer et déchiffrer des messages, découvrant les techniques utilisées pour **protéger l'information** à travers les âges et les contextes.

L'atelier est à la fois ludique et immersif : il place les élèves dans une situation où la sécurité de l'information est essentielle, tout en stimulant leur logique, leur coopération et leur créativité.

En guise de récompense, l'activité leur permet de découvrir les portraits de femmes et d'hommes qui œuvrent aujourd'hui dans la **cybersécurité** — de la cryptographie à la protection des données personnelles.

Les élèves découvrent ainsi les métiers de ce domaine et comprennent leur rôle fondamental dans la société moderne.

SOMMAIRE

Mise en place

Niveau : 4ème à la Terminale
Durée : 45 minutes
Compétences :
Effectif : 10 à 20 élèves

- Comprendre le principe de chiffrement.
- Saisir des instructions implicites.
- Prendre des initiatives.

Matériel

- 1 Pochette Animateur avec :
  - 1 Lettre de lancement
  - 5 Lettres Felicitations
  - 1 Fiche réponses
- 6 Boites à code
Ensemble pavé tactile et carte microbit
  - 1 pour chaque atelier
  - 1 pour le code final
- 5 Article Histoire à afficher
- Constellation à projeter
Fiche dans le dossier Annexe
Vidéoprojecteur non fourni

- 5 Pochettes Atelier avec :
  - 1 Lettre Enigme
  - 1 Frise chronologique
  - Matériel spécifique
    - Scytale : 4 Tubes et 3 Rubans
    - César : Cadran Alberti
    - Vigenère : Table Vigenère
    - Pig Pen : Symboles à compléter
    - Enigma : Cadran Enigma

Installation

- Former cinq îlots de tables (pour pouvoir installer 2 à 4 élèves par ilôt).
- Sur chaque ilôt, déposer une Pochette Atelier et la Boîte à code qui lui est associée.
- Mise en route des boites à code :
  - insérer la carte microbit dans le bloc central
  - connecter le pavé tactile au bloc central par la fiche P1/15
  - mettre sous tension en appuyant longuement sur le boutonà l'arrière de la carte microbit. Le nom du code doit défiler.
- Afficher les articles Histoire aux murs dans la classe.
- Projeter la constellation sur tableau blanc

Consignes et déroulé

- Installer les élèves par groupes (de 2 à 4) sur chaque ilôts.

- Lire à la classe la lettre de lancement qui présente le scénario général : l'agente Delastelle, capturée par un groupe malveillant, confie aux élèves la mission de retrouver le code protégeant les documents de l'Organisation à partir du matériel à leurs disposition.

- Chaque groupe résout son énigme à l'aide du matériel. La phrase déchiffrée donne une indication sur le code numérique à rechercher. La réponse se trouve parmi les articles Histoire affichés au mur. Cette étape est résolue si le message "CODE BON =) " s'affiche une fois qu'ils ont tapé leur réponse sur le pavé tactile.

- Lorsque le groupe a résolu son énigme, l'animateur leur distribue la lettre "bis" de félicitations.
  A partir du nom de métier caché dans la première lettre et des instructions de la lettre "bis", les élèvent tracent au tableau, directement sur la constellation, un chiffre qu'ils doivent retenir.

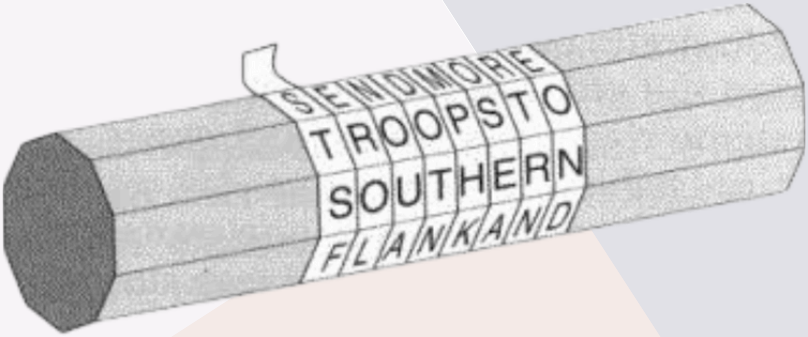
- La lettre "bis" leur fournit également un indice sur l'ordre des chiffres du code final. La frise à leur disposition, leur permet de classer chronologiquement l'émergence de chacune de ces techniques de chiffrement.

- En mettant en commun et en ordonnant leur chiffres, ils trouvent le code final. Ainsi, les données relatives aux agent des l'organisation sont préservées : ils ont alors accès aux portraits des métiers de la cryptographie.

- Prévoir un temps d'échange sur la sécurité des données et les métiers du numériques.

La scytale

La scytale est un bâton de bois permettant de chiffrer et de déchiffrer un message. Utilisée par les Spartiates à des fins militaires, au moins à partir du Ve siècle avant J.-C., elle constitue l'une des plus anciennes méthodes de chiffrement connues.



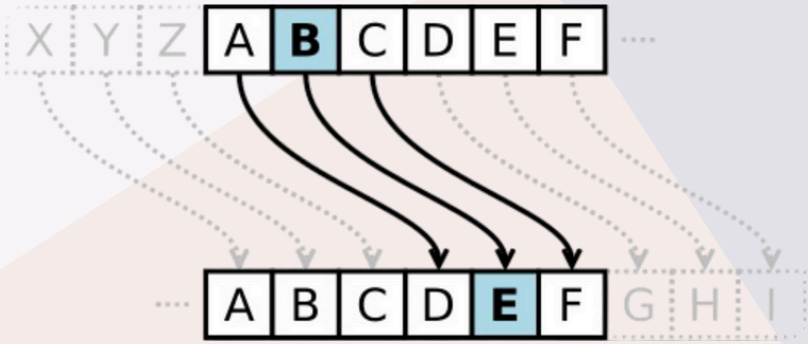
Pour chiffrer un texte, on enroule une bande, souvent en cuir, autour de la scytale afin d'inscrire une lettre sur chaque tour. Des caractères supplémentaires sont ajoutés entre les lettres du message original pour empêcher toute restitution à la simple lecture de la bande.
Pour déchiffrer, il faut disposer d'une scytale de même diamètre afin d'enrouler à nouveau la bande de la même manière et ainsi retrouver le contenu initial.

Il s'agit d'une méthode de **chiffrement par transposition**, qui consiste à modifier l'ordre des lettres sans en changer la nature. Cependant, la résistance de ce code reste faible : puisqu'aucune substitution de lettres n'est effectuée, le message pouvait être reconstitué relativement facilement avec quelques astuces.

Le code César

Le code de César, ou chiffrement par décalage, est l'une des méthodes de chiffrement les plus anciennes et les plus simples. Elle fut utilisée notamment par Jules César pour protéger certaines de ses correspondances.

Le principe est très simple : chaque lettre du texte original est remplacée par une autre lettre située à une distance fixe dans l'ordre de l'alphabet. César utilisait par exemple un décalage de 3. Ainsi, la lettre A devient D, B devient E, etc. Pour les dernières lettres de l'alphabet, on recommence au début : il s'agit donc d'une permutation circulaire.



Exemple : Le mot "CESAR", avec un décalage de 3, devient "FHVDU".

Il s'agit d'un chiffrement par **substitution monoalphabétique** : chaque lettre du texte chiffré correspond toujours à une seule lettre du texte original.

Une méthode pour le déchiffrer consiste à utiliser l'analyse de fréquences. En français, la lettre E est la plus courante : elle représente plus de 15 % des lettres d'un texte, soit plus d'une sur sept.
Ainsi, en observant la lettre qui apparaît le plus souvent dans un texte chiffré, on peut supposer qu'il s'agit du E et en déduire le décalage utilisé pour le chiffrement.

Le chiffrement Vigenère

Le chiffrement de Vigenère utilise une clé alphabétique, qui peut correspondre à un mot ou à une phrase. Pour chiffrer un message, on utilise successivement chaque lettre de la clé afin de déterminer le décalage à appliquer pour la substitution de chaque lettre du texte.

Principe du chiffrement de Vigenère :

- La clé est répétée autant de fois que nécessaire pour couvrir l'ensemble du message.
- Chaque lettre du texte original est décalée dans l'alphabet d'un nombre de positions égal à la valeur de la lettre correspondante dans la clé (A=0, B=1, ..., Z=25). Si la lettre de la clé est A, la lettre du texte reste inchangée.
- Comme pour le chiffrement de César, le décalage est circulaire : après Z, on recommence à A.

Exemple de chiffrement :

Texte	V	I	G	E	N	E	R	E
Clé	C	L	E	C	L	E	C	L
Rang clé	2	11	4	2	11	4	2	11
Texte chiffré	X	T	K	G	Y	I	T	P

"C" est la 3e lettre de l'alphabet. On décale la lettre "V" de 2 rangs dans l'alphabet et on obtient "X".

Ce chiffrement est une **substitution polyalphabétique**, ce qui signifie qu'une même lettre du texte chiffré peut correspondre à plusieurs lettres différentes du texte original, selon la lettre de la clé utilisée pour déterminer le décalage.

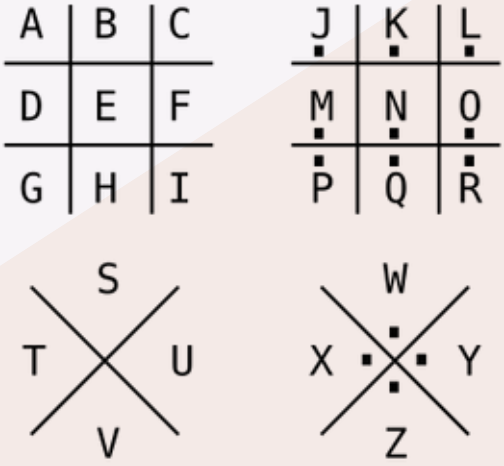
Cela rend le texte beaucoup plus difficile à déchiffrer sans connaître la clé et rend également inutile l'analyse des fréquences. Plus la clé est longue et comporte des lettres variées , plus le message est difficile à déchiffrer.

PigPen

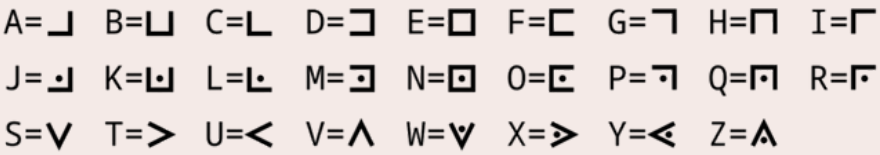
Le chiffrement Pigpen (ou «Parc à cochons»), également appelé chiffrement des francs-maçons, est une méthode de **substitution monoalphabétique** dans laquelle chaque lettre est remplacée par un symbole géométrique.

Il est surtout connu pour son utilisation par les francs-maçons, qui l'employaient pour communiquer de manière confidentielle.

Ce chiffrement repose sur une construction géométrique mnémotechnique : on utilise des grilles de 2x2 ou 3x3 dans lesquelles les lettres de l'alphabet sont disposées.



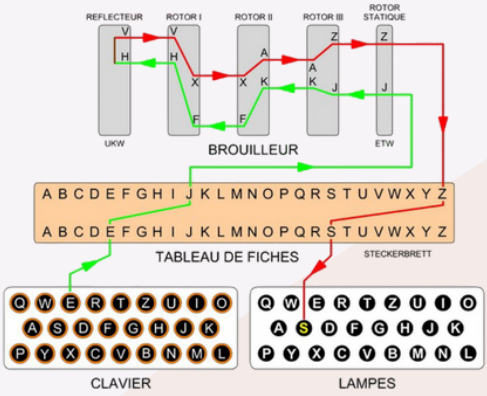
Chaque lettre est représentée par le symbole correspondant à sa position dans la grille, formant ainsi un alphabet qui évoque visuellement un parc à cochons, d'où le nom du chiffrement.



Des variantes plus complexes existent, par exemple en modifiant l'ordre des lettres.

La machine Enigma

Inventée par l'ingénieur allemand Arthur Scherbius à partir d'un brevet de 1919, la machine Enigma est un dispositif électromécanique automatisant le chiffrement et de déchiffrement. Celle-ci se présente sous la forme d'une machine à écrire :



Lorsqu'on appuie sur une touche, la lettre chiffrée apparaît sur un panneau lumineux. Le résultat dépend de la position de trois pièces mobiles, appelées rotors, dont la position définit la configuration du réseau de substitution alphabétique. On peut en observer un exemple dans l'image adjacente.

Les rotors sont connecté les uns aux autres tels des engrenages. A chaque frappe, un mécanisme interne fait tourner le premier rotor d'un cran. Toutes les 26 frappes, le deuxième rotor avance à son tour, et toutes les 676 frappes (26 au carré), c'est le troisième rotor qui se déplace. Ces rotations modifient continuellement les connexions électriques à l'intérieur de la machine : une même touche peut alors produire un grand nombre de lettres différentes. Il s'agit donc d'une méthode de **substitution polyalphabétique**.

Par la suite, une version plus complexe fut développée, équipée d'un tableau de connexions qui renforçait encore la difficulté du décryptage. Enigma fut ainsi massivement utilisée pour les communications de l'Allemagne nazie durant la Seconde Guerre mondiale.

Sa complexité venait du nombre colossal de réglages possibles, modifiés chaque jour par l'armée allemande.

Solutions

- **Scytale :** Enroulé autour petit tube bleu, le ruban commençant par la lettre “D” indique “Date siège Athènes”, correspondant à l’an 404 av J.C dans l’article “Lysandre, stratège spartiate”.
  Métier caché : Analyste
  Chiffre à trouver dans la constellation : 6

- **César :** Phrase à déchiffrer : “Le code est la date du siège d’Alesia”, correspondant à l’an 52 av J.C dans l’article “Alésia, bataille décisive de la guerre des Gaules”.
  Métier caché : Chercheur
  Chiffre à trouver dans la constellation : 0

- **Vigenère :** Phrase à déchiffrer avec “CLE” pour clé : “Date décès Vigenère”, correspondant à 1596 dans l’article “Blaise de Vigenère, érudit de la renaissance”.
  Métier caché : Cryptologue
  Chiffre à trouver dans la constellation : 9

- **PigPen :** Phrase à déchiffrer : “Première loge maçonnique française”, correspondant à 1725 dans l’article “Naissance de la franc-maçonnerie française”.
  Métier caché : Testeur
  Chiffre à trouver dans la constellation : 1

- **Enigma :** Phrase à déchiffrer : “Brevet Enigma”, correspondant à 1919 dans l’article “Mission : Décrypter Enigma”.
  Métier caché : Architecte
  Chiffre à trouver dans la constellation : 0

- **Enigme finale :** On remet les chiffres dans l’ordre chronologique des méthodes de chiffrement ce qui nous donne : 60910.

Sources

Scytale :

- https://fr.wikipedia.org/wiki/Scytale
- https://www.researchgate.net/figure
- https://fr.wikipedia.org/wiki/Chiffrement_par_transposition

César :

- https://fr.wikipedia.org/wiki/Chiffrement_par_d%C3%A9calage
- https://fr.wikipedia.org/wiki/Chiffrement_par_substitution
- https://fr.wikipedia.org/wiki/Analyse_fr%C3%A9quentielle
- https://www.apprendre-en-ligne.net/crypto/stat/francais.html
- https://maths.ac-amiens.fr/IMG/pdf/frequences.pdf

Vigenère :

- https://fr.wikipedia.org/wiki/Chiffre_de_Vigen%C3%A8re
- https://fr.wikipedia.org/wiki/Chiffrement_par_substitution

Pig Pen :

- https://fr.wikipedia.org/wiki/Chiffre_des_francs-ma%C3%A7ons
- https://www.apprendre-en-ligne.net/crypto/subst/pigpen.html

Enigma :

- https://fr.wikipedia.org/wiki/Enigma_(machine)
- https://www.apprendre-en-ligne.net/crypto/Enigma/index.html

Compétences

Collège- mathématiques cycle 4

Domaine 1 : Langages mathématiques, scientifiques et informatiques

Passer du langage courant à un langage scientifique ou technique et vice versa.

Passer d'un registre de représentation à un autre (tableau, graphique, croquis, symbole, schéma, etc.).

Domaine 2 : Les méthodes et outils pour apprendre

Définir et respecter une organisation et un partage des tâches dans le cadre d'un travail de groupe.

Rechercher des informations dans différents médias (presse écrite, audiovisuelle, web) et ressources documentaires.

Domaine 3 : La formation de la personne et du citoyen

Formuler une opinion, prendre de la distance avec celle-ci, la confronter à celle d'autrui et en discuter.

Utiliser les médias et l'information de manière responsable et raisonnée.

Domaine 4 : Les systèmes naturels et les systèmes techniques

Extraire, organiser les informations utiles et les transcrire dans un langage adapté.

Communiquer sur ses démarches, ses résultats et ses choix, en argumentant.

Expliquer un comportement responsable dans le domaine de la santé, de la sécurité et de l'environnement.

Domaine 5 : Les représentations du monde et l'activité humaine

Contextualiser un document, un texte, une œuvre, un(e) artiste, un personnage, une découverte scientifique, un fait artistique ou une notion dans le temps et dans une ou plusieurs aires géographiques et culturelles.

Exercer son regard critique sur divers œuvres et documents.

Élaborer un raisonnement et l'exprimer en utilisant des langages divers.

Collège- mathématiques cycle 4

Trois compétences principales :

Utiliser différents langages.

Organiser efficacement un travail de groupe.

Situer les savoirs dans leur contexte historique et culturel.

Lycée

SNT, Codage de l'information

Représenter et décoder une information codée.

Décalage, codage/décodage, logique modulaire simple.

SNT/NSI, Cryptographie

Comprendre la vulnérabilité d'un code et le casser.

SNT, Données structurées

Substitution polyalphabétique, clé, chiffrement/déchiffrement.

SNT, Représentations symboliques

Lire/produire des codages symboliques non alphabétiques.

NSI, Histoire de l'informatique

Comprendre un système de chiffrement mécanique, notion de rotor.

RETROUVEZ NOS TROIS MALLETTES PEDAGOGIQUES

- CODER LA PAROLE (mallette 1)
- CODER POUR DIFFUSER (mallette 2)
- CODER POUR PROTEGER (mallette 3)

Emprunt Gratuit.

Contacter la médiatrice de l'association :

- par téléphone : 0665141741
- par mail : médiation@lesmathsenscene.fr

CETTE MALLETTE A ÉTÉ RÉALISÉE PAR

Les Maths en Scène
Les Maths où on ne les attend pas !

EN PARTENARIAT AVEC

Evrêk'Alès

FINANCÉE PAR

La Région Occitanie
Pyrénées · Méditerranée