1, 2, 3, codez ! - Activités cycle 3 - Séance 3.4: Comment assurer la confidentialité de nos échanges ?

Résumé	Afin de protéger leurs communications, les élèves s'initient au chiffrement, à l'aide d'un algorithme simple (dit « de César »), consistant à décaler les lettes d'un message.
Notions	« Information » • Chiffrer un message signifie le transformer pour qu'il ne soit compréhensible que par la personne à laquelle il est destiné. • Le Chiffrement de César est une méthode facile à utiliser, mais également facile à casser.
Matériel	Pour chaque élève • Fiche 44 • Fiche 45 Pour chaque groupe • Fiche 46 (uniquement si l'on fait le prolongement consistant à fabriquer un outil pour chiffrer / déchiffrer un message)
Lexique	Chiffrement
Durée :	1h30

Situation déclenchante

L'enseignant rappelle le contexte de la mission spatiale : « *L'équipe d'exploration et la base doivent communiquer régulièrement. La base communique aussi en permanence avec la Terre. Mais il faut être certain que les messages ne puissent pas être interceptés par des puissances hostiles qui pourraient espionner les résultats voire menacer la sécurité de l'équipage. Comment pourrait-on faire ?* »
La classe débat des méthodes de confidentialité : les mots « langage secret » ou « langage codé » surgissent très rapidement. Il y a un risque de confusion ici entre le codage présenté dans les séances précédentes (au sens de « numérisation binaire ») et son utilisation ici (au sens de « chiffrement ») . L'enseignant introduit alors un vocable nouveau : on parle de « langage **chiffré** ». Le « chiffrement », consiste à modifier un texte pour le rendre moins intelligible, afin d'empêcher les personnes non autorisées à accéder au contenu du texte.

Expérimentation : déchiffrons le message des explorateurs (en classe entière)

L'enseignant distribue aux élèves la phrase chiffrée de la Fiche 44 : « Voici un message envoyé par les explorateurs à la base. Pouvez-vous déchiffrer ce message ? »

> **Note pédagogique :**
> Pour simplifier le chiffrement et nous focaliser sur la méthode plus que sur le résultat, nous n'incluons pas (à dessein) la ponctuation.

La classe repère vite que le message est écrit à l'envers. En le lisant de droite à gauche, on découvre le contenu :

EQUIPE CONCURRENTE REPEREE CHIFFRONS LES COMMUNICATIONS

La classe aura remarqué l'aisance avec laquelle elle a « cassé» ce premier chiffrement. Le chiffrement en « écriture miroir » n'est donc pas un chiffrement très sécurisé. Nous allons étudier un chiffrement un peu plus compliqué, l'un des premiers chiffrements utilisés dans l'Histoire.

Expérimentation : déchiffrons le message de la base (en classe entière)

L'enseignant distribue alors la Fiche 45. « *En réponse au message alarmiste des explorateurs, la base a répondu ceci. Pouvez-vous déchiffrer ce message ?* »
Il est évident, cette fois-ci, que le message n'est pas chiffré en « écriture miroir ». Si les élèves ont du mal à comprendre comment déchiffrer ce message, l'enseignant peut les aiguiller progressivement de plusieurs façons :

- *Quels sont les mots les plus courts ? À quoi peuvent-ils correspondre en français ?* Les mots les plus courts de la langue française sont « a », « à », « y », mais on peut également retrouver des formes contractées « l' », « d' », etc. Les mots de 2 lettres sont également peu nombreux (le, la, on…)
- *Quelle est la lettre la plus courante dans un texte rédigé en français ?* (réponse : la lettre E) *Qu'en est-il ici ?* Dans le texte chiffré ici, c'est la lettre H. On peut donc supposer que « H » substitue systématiquement toutes les lettres « E » du message initial.

Le chiffrement utilisé ici, appelé « Chiffrement de César », décale dans l'alphabet toutes les lettres de 3 positions : le A devient D, le B devient E, le C devient F, le E devient H, le X devient A, le Z devient C. On parle également de « permutation circulaire ». Déchiffré, le message devient :

MESSAGE BIEN RECU UTILISONS LE CHIFFREMENT DE CESAR

> **Notes scientifiques :**
>
> - Le Chiffrement de César doit son nom à Jules César, qui l'utilisait pour ses communications secrètes, par exemple pendant la Guerre des Gaules.
> - La clef de ce chiffrement désigne le décalage des lettres. Dans le Chiffrement de César, les lettres sont en effet toutes décalées d'un certain rang (la clef). Dans l'exemple utilisé, la clef est +3, ce qui signifie que, pour crypter le message, il faut simplement décaler toutes les lettres de 3 rangs dans l'alphabet (A devient D, B devient E... W devient Z, X devient A, Y devient B…).
> - Avec une clé égale à 0, les lettres ne sont pas décalées, et donc le message chiffré est identique à l'original. Avec une clé égale à -3, on décale les lettres dans l'autre sens (A devient X, B devient Y…)… ce que l'on fait pour décrypter un message chiffré avec une clef de +3 !

Expérimentation : recherche d'autres chiffrements (par groupes)

La troisième partie de cette séance permet aux élèves de réinvestir les concepts abordés jusqu'à présent. L'enseignant propose : « *Maintenant, vous devez, par groupes, améliorer le Chiffrement de César pour brouiller vos messages.* » Dans un premier temps, les élèves tentent de chiffrer, puis de déchiffrer des messages courts qu'ils improvisent. Dans un second temps, les groupes échangent des messages chiffrés, et tentent de casser le chiffrement de leurs voisins.

> **Note scientifique :**
> Il existe de très nombreuses méthodes de chiffrement. Il est probable que les premiers essais des élèves s'orientent vers un changement de la clef du Chiffrement de César. Une variante du Chiffrement de César qui pourrait surgir pendant les expérimentations correspondrait à une clef variable selon un motif bien précis : par exemple, la première lettre du message pourrait être décalée de +1, la seconde de +2, la troisième de +3, puis la quatrième serait à nouveau décalée de +1, la cinquième de +2, et ainsi de suite… Les possibilités sont infinies. Les élèves peuvent aussi penser à supprimer les espaces, ce qui empêche le repérage des mots courts et rend donc plus difficile l'identification de la clef utilisée dans le Chiffrement de César.

Mise en commun

Un élève par groupe vient présenter la méthode de chiffrement que son groupe a élaborée. La classe débat ensuite des raisons pour lesquelles leur chiffrement a été facile ou difficile à casser. Cela permet au fur et à mesure de voir qu'il existe plusieurs stratégies de chiffrement. La classe peut éventuellement élaborer un chiffrement commun, et rédiger un petit texte, à diffuser auprès des classes voisines pour en tester la solidité !

Conclusion et traces écrites

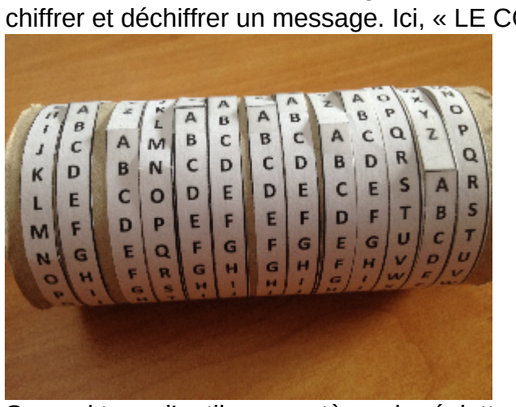
La classe synthétise collectivement ce qui a été appris au cours de cette séance :

- *Chiffrer un message signifie le transformer pour qu'il ne soit compréhensible que par la personne à laquelle il est destiné.*
- *Le Chiffrement de César est une méthode facile à utiliser, mais également facile à casser.*

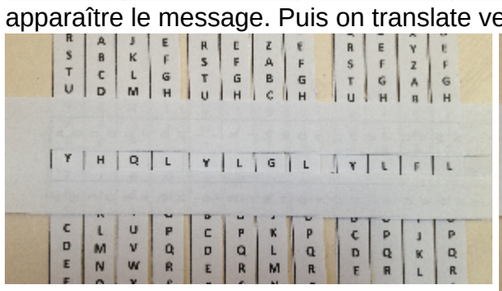
Les élèves notent ces conclusions dans leur cahier de sciences. L'enseignant, quant-à-lui, met à jour l'affiche « qu'est-ce que l'informatique ? ».

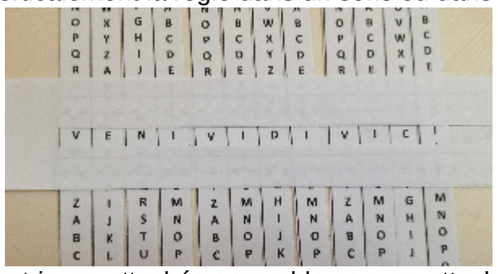
Prolongement

- Une étude documentaire sur Alan Turing parait très appropriée après un travail sur le chiffrement ! Il a en effet dirigé l'équipe qui a cassé le fameux code secret Enigma des nazis et, à cette occasion, a participé au développement de machines qui ont mené à l'ordinateur. Voir, à ce sujet, l'éclairage scientifique.
- Réaliser des outils de chiffrement / déchiffrement :
  - Premier type d'outil : un cylindre avec des roues égrenant l'alphabet. Sur l'image ci-dessous, des languettes de 138x5mm ont été imprimées avec toutes les lettres de A à Z, puis enroulées autour d'un rouleau de carton. Les languettes sont scotchées sur elles-mêmes, et pas du tout au carton, afin de pouvoir utiliser celui-ci comme axe. En faisant tourner les roues, on peut rapidement chiffrer et déchiffrer un message. Ici, « LE CODE DE CESAR » (lisible sur la ligne centrale) devient « MF DPEF EF DFTBS » avec une clef +1 (ligne immédiatement en dessous), et ainsi de suite.



  - Second type d'outil : un système de réglettes posées les unes à côté des autres. Chaque languette contient deux fois l'alphabet. En s'aidant d'une règle, on aligne les réglettes pour faire apparaître le message. Puis on translate verticalement la règle dans un sens ou dans l'autre pour lire le message chiffré.





  - Troisième type d'outil : deux disques concentriques attachés ensemble par une attache-parisienne. Sur les pourtours des disques ont été placées les lettres de l'alphabet. En faisant pivoter un disque par rapport à l'autre, il est facile de chiffrer et déchiffrer rapidement n'importe quelle lettre.

Classe de CM2 de Kévin Faix (Le Krémlin Bicêtre)

<< Séance III-3.3 Séquence III-3 Séance III-3.5 >>
