FONDATION La main à la pâte
POUR L'ÉDUCATION À LA SCIENCE

Cycle 4

Cryptographie débranchée (dans le projet, lister en lien avec la suivante)

Une séquence du projet *1,2,3... CODEZ !*

Résumé

Cette séquence de cryptographie entièrement débranchée (sans ordinateur) permet aux élèves de découvrir le chiffrement de César, puis le chiffrement par substitution monoalphabétique. Ils apprennent à cryptanalyser (i.e. « casser ») ces chiffrements, notamment grâce à l'analyse fréquentielle. Les élèves cherchent ensuite à corriger le principal point faible de ces méthodes de chiffrement (l'échange de la clé) et découvrent l'intérêt du chiffrement asymétrique utilisant clé publique et clé privée. Enfin, ils débattent des enjeux sociétaux de la cryptographie.

Projet « Cryptographie »

Tout au long de ce travail, les élèves découvrent et s'approprient de nombreux concepts propres à l'informatique, comme les notions d'information, d'algorithme, de langage (*cf.* scénario conceptuel, page 3), et s'initient à la programmation.

Disciplines concernées et liens avec les programmes

Les programmes de 2016 introduisent des notions d'informatique aussi bien en mathématiques qu'en technologie. Nous conseillons de mener ce projet dans le cadre du cours de mathématiques afin de cibler l'enseignement de technologie vers des projets qui mettent davantage en avant l'aspect matériel, comme la robotique (*cf.* pages 66 et 67).
Les programmes 2016 de mathématiques comportent un chapitre « algorithmique et programmation » qui justifie parfaitement un tel projet :

Mathématiques

Au cycle 4, les élèves s'initient à la programmation, en développant dans une démarche de projet quelques programmes simples, sans viser une connaissance experte et exhaustive d'un langage ou d'un logiciel particulier. En créant un programme, ils développent des méthodes de programmation, revisitent les notions de variables et de fonctions sous une forme différente, et s'entraînent au raisonnement.
– Décomposer un problème en sous-problèmes afin de structurer un programme ; reconnaître des schémas.
– Écrire, mettre au point (tester, corriger) et exécuter un programme en réponse à un problème donné.
– Écrire un programme dans lequel des actions sont déclenchées par des événements extérieurs.
– Programmer des scripts se déroulant en parallèle.
  • Notions d'algorithme et de programme.
  • Notion de variable informatique.
  • Déclenchement d'une action par un évènement, séquences d'instructions, boucles, instructions conditionnelles.
  • Notion de message échangé entre objets.
– Exemples de situations, d'activités et de ressources pour l'élève
  • Initiation au chiffrement (Morse, chiffre de César, code ASCII)
Outre ces compétences en informatique, le projet permet de travailler d'autres compétences plus classiques en mathématiques, notamment :
– Organisation et gestion de données, fonctions
  • Calculer des effectifs, des fréquences.
  • Tableaux, représentations graphiques (diagrammes en bâtons, diagrammes circulaires, histogrammes).

Éducation aux médias et à l'information

– Utiliser les médias de manière responsable

• Comprendre ce que sont l'identité et la trace numériques.

• Se familiariser avec les notions d'espace privé et d'espace public.

• Se questionner sur les enjeux démocratiques liés à la production participative d'informations et à l'information journalistique.

Le professeur de mathématiques peut mener le projet seul, ou en collaboration avec d'autres professeurs (notamment de français et, dans une moindre mesure, de technologie et de physique-chimie). Ces prolongements sont indiqués séance par séance et peuvent servir de base à la construction d'un projet pluridisciplinaire, plus volumineux, dans le cadre des EPI.

Objectifs

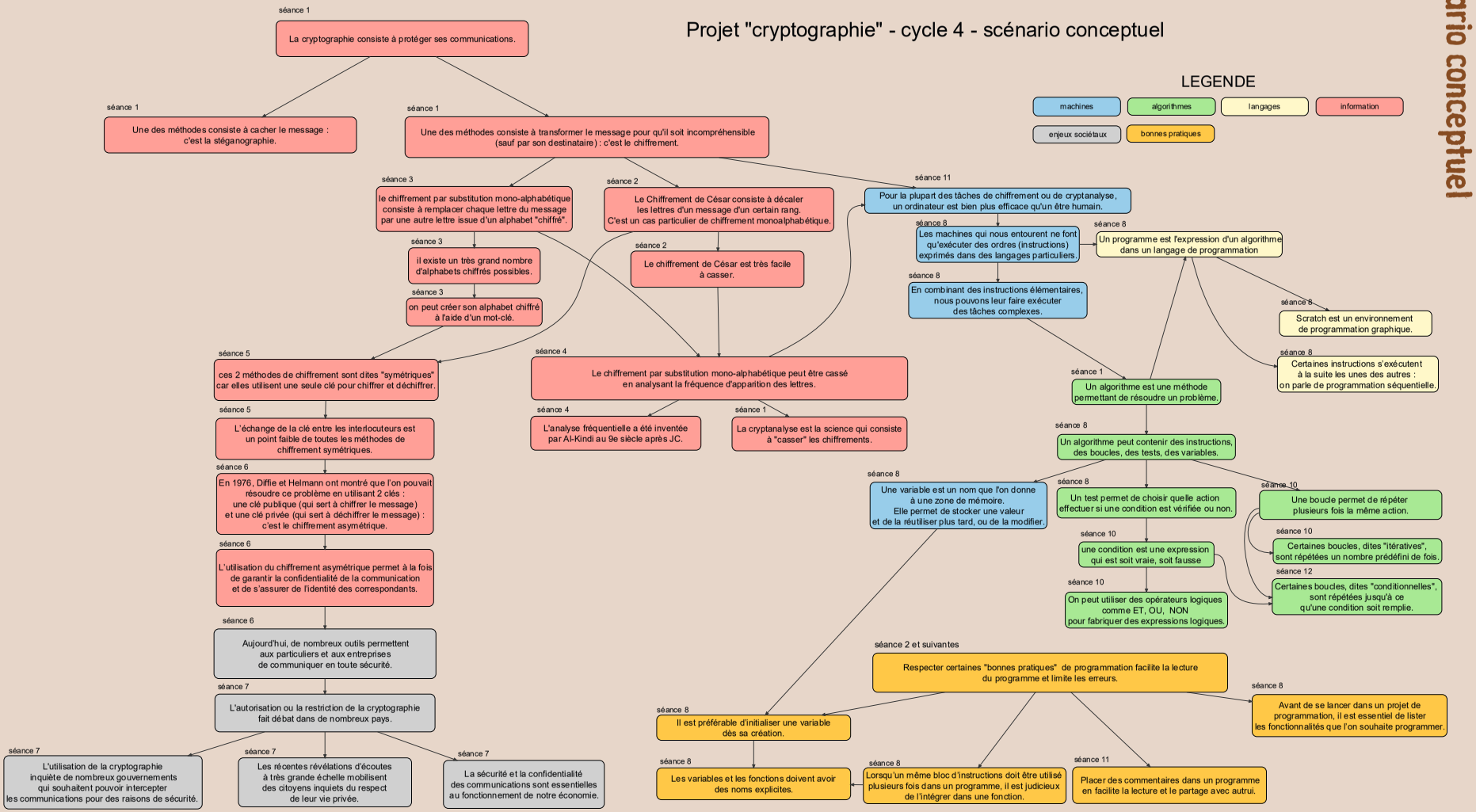
L'objectif du projet est de familiariser les élèves avec les méthodes et les enjeux de la cryptographie.
La première séquence, entièrement débranchée (sans ordinateur), leur permet de découvrir le chiffrement de César, puis le chiffrement par substitution mono-alphabétique. Ils apprennent à cryptanalyser (*i.e.* « casser ») ces chiffrements, notamment grâce à l'analyse fréquentielle. Les élèves cherchent ensuite à corriger le principal point faible de ces méthodes de chiffrement (l'échange de la clé) et découvrent l'intérêt du chiffrement asymétrique utilisant clé publique et clé privée. Enfin, ils débattent des enjeux sociétaux de la cryptographie.
La seconde séquence, optionnelle, propose aux élèves de programmer (dans l'environnement *Scratch*[1]) le chiffrement de César (chiffrer/déchiffrer) et l'analyse fréquentielle (trouver les fréquences de chaque lettre dans un texte, et afficher ce résultat sous la forme d'un graphique). Cette séquence permet une appropriation de tous les concepts de programmation utiles au collège : séquences, boucles, tests, variables (variables simples et tableaux), fonctions…

	Séance	Titre	Page	Résumé
	Séance 1	Comment communiquer secrètement ?	119	Les élèves cherchent plusieurs méthodes permettant de crypter un message, et discutent de la fiabilité de ces méthodes.
	Séance 2	Le chiffrement de César	125	Les élèves s'initient à la cryptanalyse : ils doivent décrypter un message sans savoir, a priori, comment ce message a été crypté. Ils découvrent le chiffrement de César, forme très simple de cryptage par substitution mono-alphabétique.
	Séance 3	Chiffrement mono-alphabétique : explosion du nombre de clés possibles	131	Les élèves généralisent le chiffrement de César à n'importe quel chiffrement par substitution mono-alphabétique. Ils apprennent comment chiffrer un message à l'aide d'un mot-clé ou d'une phrase-clé, et calculent le nombre (énorme) d'alphabets chiffrés possibles.
	Séance 4	Casser le chiffrement mono-alphabétique : l'analyse de fréquence d'Al-Kindi	136	Les élèves découvrent et appliquent la méthode d'analyse fréquentielle inventée par Al-Kindi, nécessitant des allers-retours entre la statistique et la linguistique.

1. Pour plus d'informations sur la programmation en *Scratch* (ou ses alternatives) : pourquoi, comment, etc., ainsi que pour une séance d'initiation (à insérer en début de séquence 2 si besoin), voir le chapitre « Introduction générale à *Scratch* », page 68.

	Séance 5	Comment communiquer sans échanger la clé ?	147	Les élèves modélisent les échanges entre 2 personnes à l'aide de cadenas et de clés. Ils prennent conscience du point faible de la plupart des méthodes de chiffrement : l'échange de la clé ; et comprennent que l'usage de plusieurs clés permet de résoudre ce problème. C'est le principe du chiffrement asymétrique.
	Séance 6	Clé publique, clé privée	150	Les élèves perfectionnent leur algorithme de chiffrement asymétrique, en utilisant des clés publiques (qui servent à chiffrer) et des clés privées (qui servent à déchiffrer).
	Séance 7	La cryptographie, amie ou ennemie ?	154	Les élèves participent à un « atelier philo » portant sur les enjeux actuels de la cryptographie. Faut-il l'autoriser, au risque d'empêcher les agences de sécurité de faire leur travail ? Faut-il l'interdire, au risque de voir disparaître notre vie privée ?
	Séance 8	Programmer le chiffrement de César (1/4)	159	Les élèves explicitent l'algorithme et listent les étapes qui vont structurer leur projet de programmation du chiffrement de César. Ils programment, dans l'environnement *Scratch*, une première fonction permettant de trouver la lettre correspondant à un rang dans l'alphabet.
	Séance 9	Programmer le chiffrement de César (2/4)	165	Les élèves modifient leur programme précédent pour introduire une « fonction » (bloc personnalisé).
	Séance 10	Programmer le chiffrement de César (3/4)	169	Les élèves avancent leur programme du chiffrement de César : ils sont capables de trouver le rang d'une lettre, puis de chiffrer cette lettre en décalant le rang d'un certain nombre (la clé).
	Séance 11	Programmer le chiffrement de César (4/4)	172	Les élèves terminent leur programme du chiffrement de César, qui permet désormais de chiffrer un message entier, en tenant compte des espaces, de la ponctuation et des accents. Ils apprennent également à commenter un programme de façon à le rendre lisible et compréhensible. Une activité de prolongement est proposée afin de les aider à manipuler les opérateurs logiques.
	Séance 12	Programmer l'analyse fréquentielle	180	Les élèves élaborent un nouveau programme qui permet de calculer les fréquences de chaque lettre d'un message, de façon à faciliter sa cryptanalyse.
	Séance 13	(optionnelle) Programmer l'affichage de l'histogramme des fréquences (1/2)	186	Les élèves perfectionnent leur programme précédent pour qu'il affiche l'histogramme des fréquences du texte analysé. Ils tracent les axes du graphique et utilisent des costumes (notions propres à *Scratch*) afin de légender l'axe des abscisses.
	Séance 14	(optionnelle) Programmer l'affichage de l'histogramme des fréquences (2/2)	190	Les élèves terminent leur programme en lui faisant tracer le graphique correspondant à l'histogramme des fréquences.

Projet "cryptographie" - cycle 4 - scénario conceptuel



Séquence 1 : de Jules César à Al-Kindi : chiffrement et cryptanalyse

	Séance	Titre	Page	Résumé
	Séance 1	Comment communiquer secrètement ?	119	Les élèves cherchent plusieurs méthodes permettant de crypter un message, et discutent de la fiabilité de ces méthodes.
	Séance 2	Le chiffrement de César	125	Les élèves s'initient à la cryptanalyse : ils doivent décrypter un message sans savoir, a priori, comment ce message a été crypté. Ils découvrent le chiffrement de César, forme très simple de cryptage par substitution mono-alphabétique.
	Séance 3	Chiffrement mono-alphabétique : explosion du nombre de clés possibles	131	Les élèves généralisent le chiffrement de César à n'importe quel chiffrement par substitution mono-alphabétique. Ils apprennent comment chiffrer un message à l'aide d'un mot-clé ou d'une phrase-clé, et calculent le nombre (énorme) d'alphabets chiffrés possibles.
	Séance 4	Casser le chiffrement mono-alphabétique : l'analyse de fréquence d'Al-Kindi	136	Les élèves découvrent et appliquent la méthode d'analyse fréquentielle inventée par Al-Kindi, nécessitant des allers-retours entre la statistique et la linguistique.
	Séance 5	Comment communiquer sans échanger la clé ?	147	Les élèves modélisent les échanges entre 2 personnes à l'aide de cadenas et de clés. Ils prennent conscience du point faible de la plupart des méthodes de chiffrement : l'échange de la clé ; et comprennent que l'usage de plusieurs clés permet de résoudre ce problème. C'est le principe du chiffrement asymétrique.
	Séance 6	Clé publique, clé privée	150	Les élèves perfectionnent leur algorithme de chiffrement asymétrique, en utilisant des clés publiques (qui servent à chiffrer) et des clés privées (qui servent à déchiffrer).
	Séance 7	La cryptographie, amie ou ennemie ?	154	Les élèves participent à un « atelier philo » portant sur les enjeux actuels de la cryptographie. Faut-il l'autoriser, au risque d'empêcher les agences de sécurité de faire leur travail ? Faut-il l'interdire, au risque de voir disparaître notre vie privée ?

Séance 1 – Comment communiquer secrètement ?

Discipline dominante	Mathématiques
Résumé	Les élèves cherchent plusieurs méthodes permettant de crypter un message, et discutent de la fiabilité de ces méthodes.
Notions *(cf. scénario conceptuel, page 117)*	Information : • La cryptographie consiste à protéger ses communications : – Soit en transformant le message pour qu'il soit incompréhensible (sauf par son destinataire) : c'est le chiffrement ; – Soit en dissimulant le message : c'est la stéganographie. • La cryptanalyse est la science qui consiste à « casser » les chiffrements. Algorithme : • Un algorithme est une méthode permettant de résoudre un problème.
Matériel	Pour chaque élève : • Fiche 1, page 123 • (facultatif), Fiche 2, page 124 • (facultatif) miroirs

Situation déclenchante

Le professeur évoque le débat sociétal actuel autour de la confidentialité des échanges (écoutes téléphoniques, surveillance d'Internet) et replace ce débat dans un contexte historique plus large : les hommes ont toujours voulu protéger leurs communications (pour envoyer des lettres amoureuses, des ordres militaires, ou des informations diplomatiques) tandis qu'ils ont, en parallèle, toujours voulu percer les secrets de leurs voisins et/ou ennemis.

Le professeur demande aux élèves de prendre 5 minutes pour écrire ce à quoi leur fait penser le mot « cryptographie ». Il met en commun leurs propositions au tableau. Quelques exemples de réponses fréquentes au cycle 4 : cryptogramme, informatique, algorithme, crypter, décrypter, coder, décoder, pirater, nombre premier, CB, robot, sécurité, protection des données…

Il propose ensuite aux élèves un défi simple : comment écrire un message, par exemple un SMS, à un ami sans que ce message puisse être compris par d'autres personnes (en particulier, les parents, les professeurs, etc.).

La discussion collective fait ressortir le besoin, pour l'émetteur du message et son destinataire, de se mettre d'accord sur un « code » (on précisera le vocabulaire plus tard).

Recherche (par groupes)

Les élèves, répartis par petits groupes (4 élèves, par exemple), doivent réfléchir à un code leur permettant de communiquer secrètement. Ils doivent expliciter leur méthode et l'agrémenter d'un exemple avec une question et une réponse.

Note : pour plus de simplicité, on ne cherche pas à différencier les majuscules et les minuscules, et on ignore les caractères accentués.

Mise en commun

Le professeur organise une mise en commun au cours de laquelle les différents binômes présentent leurs propositions, qui sont discutées collectivement. On cherche à savoir, par exemple, si le « code » :

- permet de communiquer (les 2 protagonistes se comprennent-ils ? y a-t-il des ambiguïtés ?) ;
- est facile à apprendre et à utiliser ;
- est difficile à « casser » pour une personne extérieure qui ne connaîtrait pas ce code.

Exemples de proposition d'élèves :

- Mélanger l'ordre des lettres du message : écrire de droite à gauche, écrire en « verlan », écriture « miroir » (dans laquelle l'ordre, mais aussi la forme des lettres, est inversée). Si cette proposition apparait, distribuer des miroirs aux élèves pour qu'ils puissent manipuler.
- Cacher le message à l'intérieur d'un autre : écriture en dent de scie
- Supprimer certains caractères (par exemple les voyelles).
- Remplacer les lettres du message par des chiffres (A ➜ 01, B à ➜ 02…). Attention, si on remplace simplement A par « 1 », le chiffrement est facile, mais le déchiffrement est ambigu : « 13 » signifie-t-il « 1 » puis « 3 », c'est-à-dire A puis C, ou la treizième lettre, c'est-à-dire M ? Pour lever l'ambiguïté, il faut utiliser 2 chiffres pour chaque lettre.
- Remplacer les lettres par des symboles non chiffrés, comme dans le code morse (traits, points, espaces)
- Utiliser une langue étrangère peu répandue (le navajo, par exemple).
- Utiliser une langue que l'on invente pour les besoins de notre communication. Ce ne sont pas les lettres qui sont remplacées par des chiffres ou autres symboles, mais des mots qui sont remplacés par d'autres.
- Parler dans sa propre langue, mais en supprimant les espaces, les caractères accentués et la ponctuation.

Si certaines de ces propositions ne sont pas faites par les élèves, ne pas les introduire maintenant : ce sera fait plus tard dans la séance.

Notes pédagogiques

Au cours de cette discussion, quelques éléments de vocabulaire sont précisés :

- « Crypter » un message signifie le brouiller pour que son contenu ne soit compréhensible que par son destinataire. Le message n'a donc pas besoin d'être caché. Cette activité s'appelle la cryptographie (on utilise les verbes « crypter » et « décrypter »). La cryptanalyse consiste à trouver la méthode permettant de décrypter un message qui ne nous est pas destiné.
  – Lorsque les mots sont échangés avec d'autres mots ou expressions (exemple : « Jupiter » désigne le professeur de mathématiques), ce cryptage s'appelle un « code ». On utilise les verbes « coder » et « décoder ».
  – Lorsque ce sont les lettres qui sont remplacées (et non les mots), soit par d'autres lettres, soit par d'autres types de signes, on parle de « chiffrement ». On utilise les verbes « chiffrer » et « déchiffrer ».
- On peut aussi chercher à cacher le message, plutôt qu'à le rendre inintelligible. Dans ce cas, le message est transmis « en clair », mais c'est le supportdu message qui est caché (par exemple, un bout de papier roulé dans un stylo). Cette activité s'appelle la stéganographie. Elle a été très utilisée dans l'antiquité et peut faire l'objet de séances spécifiques (*cf.* « prolongements » proposés à la fin de cette séance).
- Certaines propositions des élèves (comme le code morse) ne relèvent ni de la cryptographie ni de la stéganographie. Il ne s'agit pas de cacher le message ou de

le rendre confidentiel, mais simplement de lui trouver un support qui soit pratique. Le morse associe des lettres à des impulsions électriques plus ou moins brèves car c'est un moyen commode de communiquer par le télégramme. Le morse peut être un bon moyen d'étudier l'encodage de l'information, mais pas la cryptographie.

Exercices

Le professeur distribue la Fiche 1 à chaque élève. Cette fiche présente plusieurs messages cryptés (chiffrés ou codés) par des méthodes différentes. Les élèves doivent retrouver le message clair.
La Fiche 2 fournit une table de correspondance permettant de faciliter le travail de l'exercice 3. Le professeur la distribue, ou non, selon l'aisance des élèves dans cet exercice.
Les exercices sont corrigés collectivement.

- Exercice 1 : il s'agit d'une simple écriture miroir (de droite à gauche)
  - Message crypté : SERTTEL SEL RESREVNI D TIFFUS LI
  - Message clair : IL SUFFIT D INVERSER LES LETTRES
- Exercice 2 : même chose, mais la suppression des espaces rend le message plus difficile à saisir
  - Message crypté : RUDSULPTSECSECAPSESELSNAS
  - Message clair, sans les espaces : SANSLESESPACESCESTPLUSDUR
  - Message clair, avec les espaces : SANS LES ESPACES C EST PLUS DUR
- Exercice 3 : il s'agit d'une simple correspondance entre les lettres et leur rang dans l'alphabet (A ➜ 01, B ➜ 02…)
  - Message crypté : 15112021031514140109191201121608010205 20
  - Message clair : OKTUCONNAISLALPHABET
  - Message clair avec les espaces : OK TU CONNAIS L ALPHABET

L'exercice 3 permet de constater que chiffrer l'alphabet à l'aide de nombres à 2 chiffres laisse la possibilité de chiffrer d'autres caractères (minuscules, caractères accentués…) car seuls 26 nombres ont été utilisés, sur un total de 100 nombres possibles (de 00 à 99).

Conclusion

Le professeur fait remarquer un point commun à toutes les méthodes de cryptage (codage ou chiffrement) étudiées ici : passer du texte clair au texte crypté nécessite le même type d'opération que de passer du texte crypté au texte clair. Il peut préciser que ce n'est pas toujours le cas (*cf.* Séance 5).
La classe définit collectivement les concepts-clés cités dans l'en-tête de cette séance : cryptographie, cryptanalyse, chiffrement, stéganographie et algorithme.

Prolongements EPI

- En français : étude du rôle de la ponctuation dans la compréhension d'un texte.
- En mathématiques : l'encodage (code morse, ASCII, binaire)

La classe peut étudier comment l'information peut être encodée de façon à pouvoir être stockée et transmise facilement. Le morse offre un bon exemple historique, l'ASCII et le binaire sont plus en phase avec l'informatique d'aujourd'hui.

- En physique-chimie, et en mathématiques : stéganographie

Notre projet traite de façon approfondie la problématique du chiffrement. La classe peut le prolonger en ajoutant quelques séances de mathématiques et/ou de physique-chimie pour étudier la stéganographie.

– En physique-chimie : fabriquer de l'encre « sympathique » (avec du lait ou du jus de citron : le message se révèle à la chaleur)
– En mathématiques : cacher une information à l'intérieur d'une image (format pbm). Cela nécessite 3 à 4 séances, car les élèves doivent d'abord travailler sur la représentation d'une image (encodage des pixels) ainsi que sur l'encodage des textes en ASCII et en binaire. Une fois ces compétences acquises, on peut encoder un message dans la parité des pixels d'une image en niveau de gris, par exemple (256 niveaux de gris sont suffisants). À l'œil, on ne remarque rien, tandis qu'en ouvrant l'image dans un éditeur de texte, on peut récupérer l'information cachée (après un décodage binaire ➜ ASCII).

FICHE 1
Quelques messages cryptés à remettre au clair

Consigne : Peux-tu cryptanalyser les messages suivants ?

Message 1 : SERTTEL SEL RESREVNI D TIFFUS LI

Message 2 : RUDSULPTSECSECAPSESELSNAS

Message 3 : 151120210315141401091912011216080102052 0

Consigne : Peux-tu cryptanalyser les messages suivants ?

Message 1 : SERTTEL SEL RESREVNI D TIFFUS LI

Message 2 : RUDSULPTSECSECAPSESELSNAS

Message 3 : 1511202103151414010919120112160801020520

Consigne : Peux-tu cryptanalyser les messages suivants ?

Message 1 : SERTTEL SEL RESREVNI D TIFFUS LI

Message 2 : RUDSULPTSECSECAPSESELSNAS

Message 3 : 1511202103151414010919120112160801020520

Consigne : Peux-tu cryptanalyser les messages suivants ?

Message 1 : SERTTEL SEL RESREVNI D TIFFUS LI

Message 2 : RUDSULPTSECSECAPSESELSNAS

Message 3 : 1511202103151414010919120112160801020520

FICHE 2
Table de correspondance

Table de correspondance entre caractères utilisés dans les messages et nombres servant à les coder :

caractère	a	b	c	d	e	f	g	h
nombre	01	02	03	04	05	06	07	08

caractère	i	j	k	l	m	n	o	p
nombre	09	10	11	12	13	14	15	16

caractère	q	r	s	t	u	v	w	x
nombre	17	18	19	20	21	22	23	24

caractère	y	z
nombre	25	26

Table de correspondance entre caractères utilisés dans les messages et nombres servant à les coder :

caractère	a	b	c	d	e	f	g	h
nombre	01	02	03	04	05	06	07	08

caractère	i	j	k	l	m	n	o	p
nombre	09	10	11	12	13	14	15	16

caractère	q	r	s	t	u	v	w	x
nombre	17	18	19	20	21	22	23	24

caractère	y	z
nombre	25	26

Table de correspondance entre caractères utilisés dans les messages et nombres servant à les coder :

caractère	a	b	c	d	e	f	g	h
nombre	01	02	03	04	05	06	07	08

caractère	i	j	k	l	m	n	o	p
nombre	09	10	11	12	13	14	15	16

caractère	q	r	s	t	u	v	w	x
nombre	17	18	19	20	21	22	23	24

caractère	y	z
nombre	25	26

Séance 2 – Le chiffrement de César

Discipline dominante	Mathématiques
Résumé	Les élèves s'initient à la cryptanalyse : ils doivent décrypter un message sans savoir, a priori, comment ce message a été crypté. Ils découvrent le chiffrement de César, forme très simple de cryptage par substitution mono-alphabétique.
Notions *(cf. scénario conceptuel, page 117)*	Information : • Le Chiffrement de César consiste à décaler les lettres d'un message d'un certain rang. • Il est très facile à casser.
Matériel	Pour chaque élève : • Fiche 3, page 129 • Fiche 4, page 130

Situation déclenchante

Le professeur revient sur la nécessité de communiquer secrètement, en particulier lorsqu'il faut transmettre des ordres militaires (si notre ennemi connaît les manœuvres de notre armée à l'avance, l'effet de surprise est perdu et la défaite bien plus probable).

Il affiche le message crypté suivant au tableau, et demande aux élèves d'essayer de le cryptanalyser :

QLBKP, H TPKP, KLZ YLUMVYAZ CPLUULUA WHY SH TLY

Note scientifique

• Rappel sur le vocabulaire :

– Si l'on connaît la méthode de cryptage (ce qui est le cas quand on est le destinataire légitime du message), retrouver le texte clair s'appelle « décoder » ou « déchiffrer » (selon le type de cryptage utilisé) ou, plus généralement, « décrypter » le message.

– Si l'on n'est pas le destinataire légitime du message (et que l'on ignore a priori comment il a été crypté), tenter de retrouver le texte clair s'appelle « cryptanalyser » le message.

• Convention : il est d'usage, en cryptographie, d'écrire les textes clairs en minuscule et les textes chiffrés en majuscule. Nous adopterons cette convention à partir de maintenant. Afin de simplifier le travail de cryptanalyse, nous garderons la ponctuation et les espaces, et ignorerons les caractères accentués (« é » serait traité comme « e »).

Recherche (par binômes)

Les élèves, répartis par binômes, tentent de cryptanalyser le message affiché au tableau. Il est probable qu'ils pensent aux méthodes identifiées à la séance précédente (comme l'écriture miroir par exemple). À moins d'avoir déjà étudié le chiffrement de César par le passé, il est peu probable qu'ils y arrivent du premier coup.

Mise en commun

Après un temps de tâtonnement, la classe cherche, collectivement, comment cryptanalyser ce message. Le professeur peut guider les élèves en leur demandant quelle est la lettre la plus fréquente en français (le « e »), et quelle est la lettre la plus fréquente dans ce texte (le « L »). Que se passe-t-il si l'on fait correspondre tous les « L » du message avec des « e » ? On obtient :

Q**e**BKP, H TPKP, K**e**Z Y**e**UMVYAZ CP**e**UU**e**UA WHY SH T**e**Y

pour plus de lisibilité, on a mis la lettre « e » en minuscule, et en gras.

On peut remarquer que le E et le L sont décalés de 7 rangs dans l'alphabet. Et si la méthode de cryptage consistait simplement à décaler toutes les lettres de 7 rangs ? Essayons sur les mots courts, pour voir si cela fonctionne. Passer de « L » à « e » nécessite de reculer de 7 rangs. Avec la même méthode,

- Le second mot du message « H » devient « a ». Ce qui est cohérent puisque « a » est le mot à une lettre le plus fréquent en français
- le 4e mot du message, « K**e**Z », se transforme en « des » (qui est également un mot fréquent) ;
- le dernier mot du message, « T**e**Y », se transforme en « mer » (idem).

Cette étape nous confirme que nous sommes sur la bonne voie et nous incite à décrypter tout le message de cette façon. On obtient alors :

jeudi, a midi, des renforts viennent par la mer

(rappel : nous ne prenons pas en compte les accents, et écrivons les textes clairs en minusule)

La classe en conclut alors qu'elle a réussi à cryptanalyser le message, en cherchant la lettre la plus fréquente et en s'aidant des mots courts. Le professeur explique que cette méthode s'appelle le chiffrement de César, car Jules César l'utilisait fréquemment pour transmettre des messages secrets (diplomatiques ou militaires). Le professeur fait remarquer que l'on n'est pas obligé de décaler les lettres de 7 rangs, et qu'on peut utiliser n'importe quel décalage. Le décalage s'appelle la « clé ». Connaître la valeur de la clé permet de décrypter très facilement le message.

Note pédagogique

Jules César utilisait plusieurs clés différentes dans ses correspondances diplomatiques ou militaires. Le plus connu est le décalage de 3 rangs. C'est lui qu'on appelle en général « chiffrement de César ». Ici, nous avons choisi un décalage de 7 rangs, et non pas 3, pour éviter que certains élèves, qui auraient déjà entendu parler du chiffrement de César, ne trouvent la solution immédiatement.

Exercice (par binôme)

Les élèves s'entraînent au chiffrement de César par binômes :

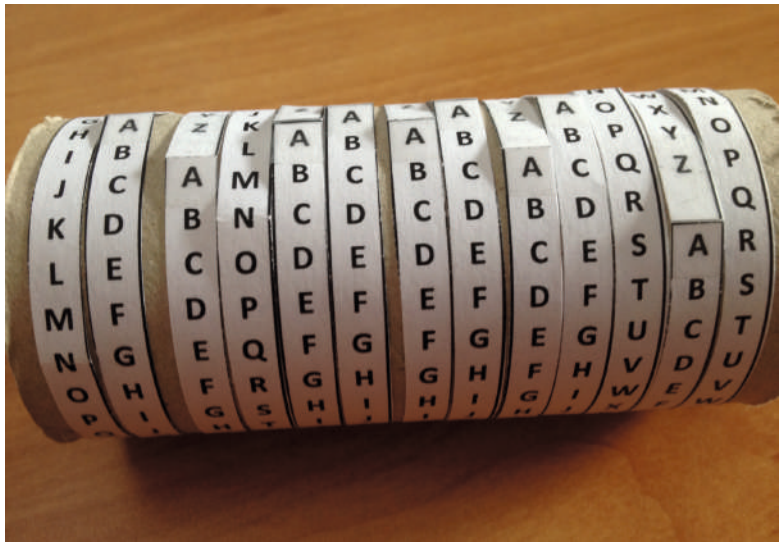
- Chaque élève choisit une clé et chiffre un message d'une dizaine de lettres (c'est suffisant pour s'entraîner !) ;
- Il transmet le message chiffré et la clé à son voisin, qui décale les lettres dans le sens inverse et déchiffre ainsi le message.

Conception d'une machine à chiffrer / déchiffrer (collectivement)

Si l'on ne connaît pas la valeur de la clé, on peut chercher à la deviner (c'est ce que nous avons fait en cherchant la lettre la plus fréquente), ou on peut tester toutes les clés possibles. Le professeur demande

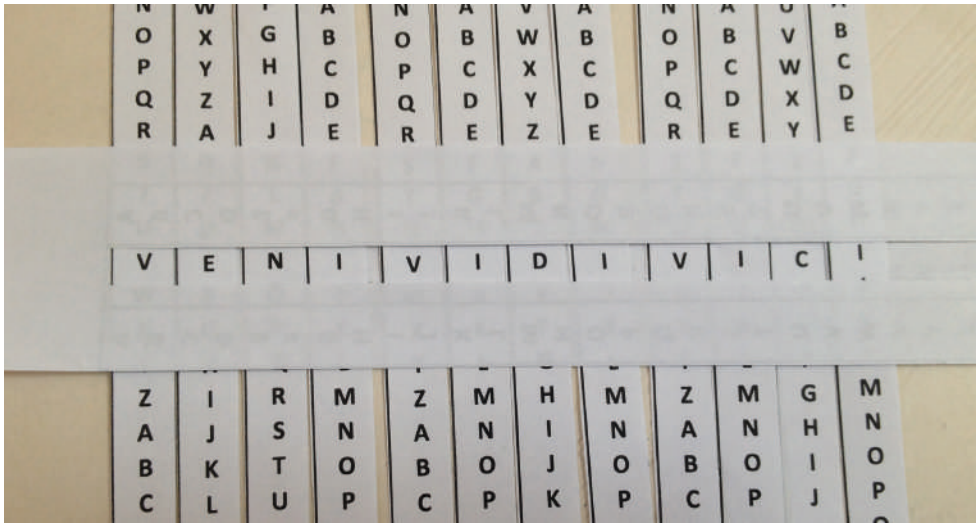
aux élèves combien de clés sont possibles dans le chiffrement de César. La réponse est 25, car on peut décaler l'alphabet d'1 lettre (clé = +1), de 2 lettres jusqu'à 25 lettres (pour une clé = +25, le A devient Z). La clé = +26 n'a aucun intérêt, puisqu'elle transforme A en A, B en B Le message crypté est identique au message clair.
Si l'on sait que le message a été crypté selon le chiffrement de César, alors il n'y a que 25 clés à tester, ce qui n'est pas si long que cela ! Le professeur demande à la classe de réfléchir à un système permettant de lire d'un coup les 25 messages possibles, afin de trouver instantanément quel est le bon.

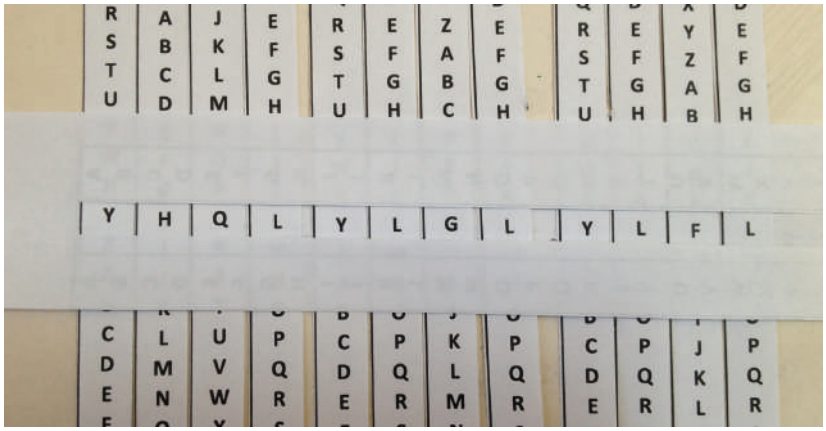
Premier type d'outil : un rouleau à chiffrer.

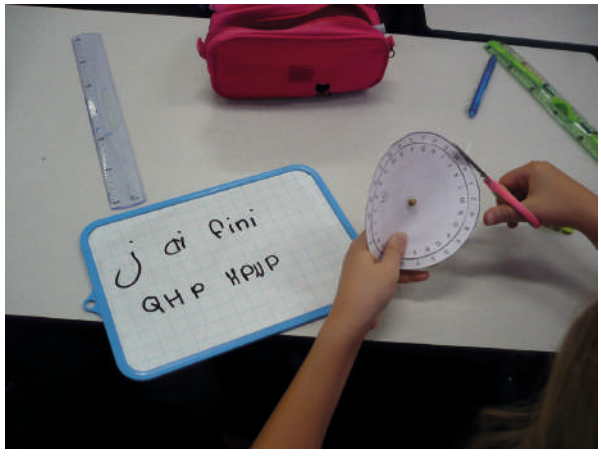


Sur l'image ci-dessous, des languettes de 138x5mm ont été imprimées avec toutes les lettres de A à Z, puis enroulées autour d'un rouleau de carton. Les languettes sont scotchées sur elles-mêmes, et pas du tout au carton, afin de pouvoir utiliser celui-ci comme axe. En faisant tourner les roues, on peut 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. Les languettes peuvent être imprimées directement à l'aide de la Fiche 3.

Second type d'outil : un système de réglettes posées les unes à côté des autres.
Chaque languette contient deux fois l'alphabet (de manière à reboucler sur A après la lettre Z car ici, contrairement au rouleau, la languette n'est pas repliée sur elle-même). En s'aidant d'une règle, on aligne les réglettes pour faire apparaître le message. Puis, en immobilisant les réglettes, on translate verticalement la règle dans un sens ou dans l'autre pour lire le message chiffré. Note : « VENI VIDI VICI » est la célèbre maxime de Jules César (Je suis venu, j'ai vu, j'ai vaincu).







Troisième type d'outil : un disque à chiffrer.
Cet outil est constitué de 2 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 de déchiffrer rapidement n'importe quelle lettre. Les disques peuvent être facilement imprimés et découpés grâce à la Fiche 4.

Utilisation d'une machine à chiffrer / déchiffrer (individuellement)

Chaque élève fabrique sa machine à chiffrer, selon un des 3 modèles décrits ci-dessus (ou selon une autre idée qui peut avoir émergé en classe !).

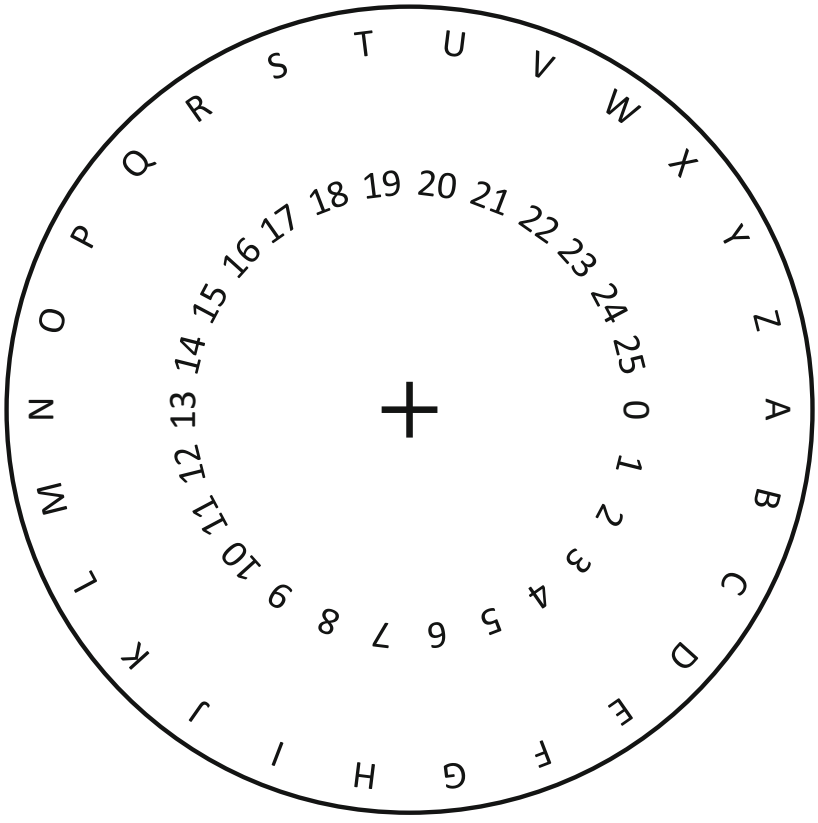
Prolongement

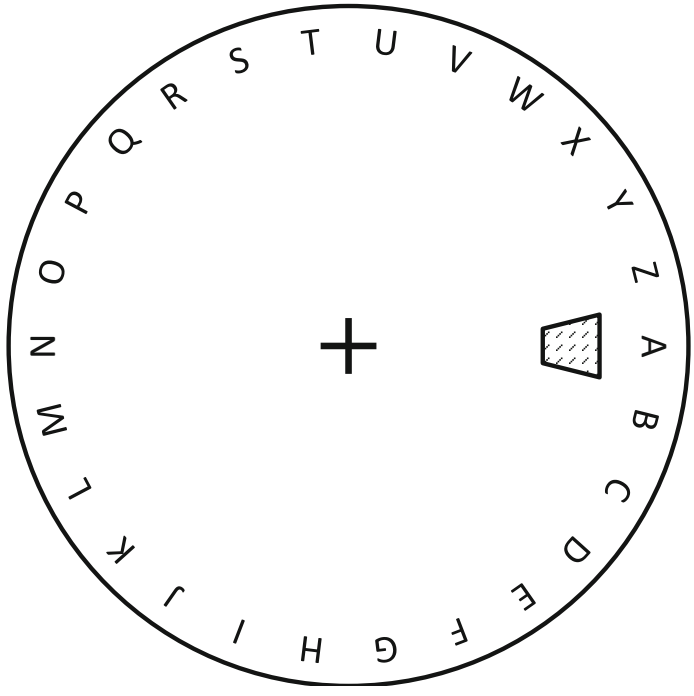
En mathématiques ou en technologie : fabriquer d'autres outils de cryptographie. Par exemple, une scytale (il s'agit d'un chiffrement par transposition, dans lesquelles les lettres sont mélangées, et non d'un chiffrement par substitution, qui consiste à remplacer les lettres par d'autres…).

FICHE 3
Fabriquer un rouleau à chiffrer/déchiffrer

A	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	Z
A	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	Z

FICHE 4
Fabriquer un disque à chiffrer / déchiffrer





Séance 3 – Chiffrement mono-alphabétique : explosion du nombre de clés possibles

Discipline dominante	Mathématiques
Résumé	Les élèves généralisent le chiffrement de César à n'importe quel chiffrement par substitution mono-alphabétique. Ils apprennent comment chiffrer un message à l'aide d'un mot-clé ou d'une phrase-clé, et calculent le nombre (énorme) d'alphabets chiffrés possibles.
Notions *(cf. scénario conceptuel, page 117)*	Information : • Le chiffrement par substitution mono-alphabétique consiste à remplacer chaque lettre du message par une autre lettre issue d'un alphabet « chiffré ». • Il existe un très grand nombre d'alphabets chiffrés possibles. • On peut créer son alphabet chiffré à l'aide d'un mot-clé.
Matériel	Pour chaque élève : • Fiche 5, page 135

Situation déclenchante

Le professeur rappelle ce qui a été vu à la séance précédente : le chiffrement de César consiste à décaler les lettres de l'alphabet d'un certain rang (la « clé »), toujours le même. Ce chiffrement est très facile à casser, car il n'y a que 25 clés possibles.

Il propose de raffiner ce chiffrement, en faisant correspondre à chaque lettre une autre lettre, mais sans s'obliger à respecter le même décalage à chaque fois. En pratique, cela revient à faire correspondre 2 alphabets : un alphabet « clair » (dans l'ordre) et un alphabet « chiffré » (mélangé).

Exercice (individuellement)

Le professeur distribue la Fiche 5 à chaque élève et leur demande d'effectuer les 2 premiers exercices.

La solution de l'exercice 1 est :

- Message clair : bonne chance pour casser ce code
- Message crypté : TCUUI KMJUKI HCYW KJVVIW KI KCJI

La solution de l'exercice 2 est :

- Message crypté : D JB EBUB
- Message clair : j ai fini

Les élèves apprennent ainsi à utiliser la table de correspondance dans les 2 sens (pour chiffrer et déchiffrer).

Combien de clés possibles ? (collectivement)

Après avoir corrigé les 2 premiers exercices de la Fiche 5, le professeur explique qu'il s'agit d'un chiffrement par substitution mono-alphabétique : à chaque lettre de l'alphabet, on en substitue une autre (et une seule). Il fait remarquer que le chiffrement de César est une version très simplifiée du chiffrement mono-alphabétique.

Note scientifique

Le chiffrement de César est bien un cas particulier de chiffrement par substitution mono-alphabétique. On peut appréhender ceci de 2 façons :

• Parmi tous les chiffrements mono-alphabétiques possibles, le chiffrement de César s'obtient en réalisant une permutation circulaire sur l'alphabet clair, ce qui est bien un sous-ensemble de tous les mélanges possibles.

• Autre manière de considérer le problème : le chiffrement de César est un chiffrement mono-alphabétique dont la clé est un mot à 1 seule lettre. Par exemple, le chiffrement de César de rang 3 est un chiffrement mono-alphabétique dont la clé est « D » (« A » décalé de 3 rangs). La notion de clé sera approfondie plus loin dans cette séance.

Il pose plusieurs questions de manière à guider les élèves, collectivement, dans le calcul du nombre de clés possibles dans un chiffrement mono-alphabétique.

• Question 1 : combien de possibilités a-t-on pour chiffrer la lettre « A » ? Réponse : 26.

• Question 2 : une fois que l'on a choisi une lettre qui correspond à « A » (par exemple, « K »), combien de possibilités reste-t-il pour chiffrer la lettre « B » ? Réponse : 25 (car « K » est déjà prise).

• Question 3 : une fois qu'on a choisi la correspondance pour A et pour B, combien de possibilités a-t-on pour la lettre C ? Réponse : 24

• Question 4 : combien de correspondances peut-on fabriquer entre l'alphabet de départ (« clair ») et l'alphabet d'arrivée (« crypté ») ? Réponse : 26x25x24x23… x2x1.

Note pédagogique

En cas de difficulté à comprendre l'usage de la multiplication dans la question 4, ne pas hésiter à utiliser une représentation en arbre.

Le professeur explique que ce nombre peut également s'écrire « 26 ! » et se prononce « factorielle 26 ».
Les élèves calculent (à l'aide de la calculatrice scientifique ou d'un tableur) :

• 1 ! = 1
• 2 ! = 1 x 2 = 2
• 3 ! = 1 x 2 x 3 = 6
• 4 ! = 1 x 2 x 3 x 4 = 24
• 5 ! = 1 x 2 x 3 x 4 x 5 = 120
• 6 ! = 720
• 7 ! = 5 040
• 8 ! = 40 320
• 9 ! = 362 880
• 10 ! = 3 628 800

…

• 26 ! ≃ $4x10^{26}$, c'est-à-dire 400 000 000 000 000 000 000 000 000

Le nombre de clés possibles n'est plus 26 (comme dans le chiffrement de César), mais 400 millions de milliards de milliards !

Exercice (individuellement)

Le professeur donne aux élèves l'exercice 3 de la Fiche 5 qui permet, par ailleurs, de travailler sur les puissances de 10.

Corrigé :

• Exercice 3a : on mettra 5 x $4x10^{26}$ secondes, soit $1,5x10^{21}$ ans (ou encore 100 milliards de fois l'âge de l'univers) à tester toutes les clés.

• Exercice 3b : si tous les êtres humains coopèrent, on mettra 8 milliards de fois moins de temps, soit encore 12 fois l'âge de l'univers.

• Exercice 3c : le plus puissant des supercalculateurs actuels mettra $4x10^{11}$ secondes, soit 300 000 ans, pour tester toutes les clés possibles.

Après avoir corrigé l'exercice 3, la classe réalise que le nombre vertigineux de clés possibles a rendu cette méthode de chiffrement incassable pendant des siècles (du moins si on supprime les espaces, car sinon on peut se servir des mots courts pour deviner certaines lettres). C'est l'invention par Al-Kindi, au 9e siècle après J.-C., de l'analyse fréquentielle qui a rendu ce chiffrement obsolète. Cette méthode fait l'objet de la séance suivante.

Chiffrement à l'aide d'un mot-clé ou d'une phrase-clé (collectivement)

Cependant, dans la pratique, il faut que l'émetteur et le destinataire du message s'accordent à trouver quel alphabet utiliser, ce qui peut être compliqué :

• Prendre un alphabet mélangé aléatoirement nécessite que chacun apprenne par cœur cet alphabet aléatoire, ce qui est très difficile, et facilement source d'erreur ;

• La solution consistant à noter cet alphabet (table de correspondance de la Fiche 5) n'est pas non plus satisfaisante : il suffit qu'un espion trouve le papier sur lequel on l'a noté pour avoir la clé permettant de déchiffrer tous les messages.

Une solution possible consiste à ne pas utiliser un alphabet aléatoire, mais un mot-clé, ou une phrase-clé. Le professeur explique la méthode à l'aide d'un exemple. Si la clé est « JULES CESAR », on remplit l'alphabet chiffré par les lettres de la clé, en ignorant les espaces et en ignorant les lettres qui ont déjà été utilisées ! (c'est indispensable si l'on veut que chaque lettre soit substituée par une seule lettre possible.)

« JULES CESAR » devient alors « JULESCAR »

Étape 1 : on remplit le tableau avec les lettres de la phrase-clé « nettoyée ».

Alphabet 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
Alphabet chiffré	J	U	L	E	S	C	A	R																		

Étape 2 : on complète l'alphabet en démarrant là où s'arrête la phrase-clé, et en omettant les lettres déjà utilisées.

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

Ainsi, il est très facile de reconstruire l'alphabet chiffré, et l'on n'a plus qu'à retenir un mot ou une phrase, ce qui est bien plus facile que d'apprendre un enchaînement aléatoire de 26 lettres !
Avec la clé « JULES CESAR », le texte « VENI VIDI VICI » devient donc MSZT MTET MTLT.

Note pédagogique

La méthode décrite ci-dessus est celle qui est communément adoptée en cryptographie, c'est pourquoi nous l'utiliserons par la suite. Il faut néanmoins comprendre que cette méthode est une convention et qu'il est parfaitement possible de créer un autre alphabet chiffré. Par exemple, à la fin du mot-clé, plutôt que de continuer l'alphabet comme expliqué ci-dessus, on pourrait décider de le reprendre du début (par la lettre A, sauf si elle a été utilisée). À noter que dans ce cas, la fin de l'alphabet sera inchangée : ce qui rend le texte chiffré en partie lisible et donc bien plus facile à cryptanalyser.

Entraînement (par binôme)

Chaque binôme utilise l'exercice 4 de la Fiche 5 pour s'exercer au chiffrement par substitution mono-alphabétique. Il s'agit, dans un premier temps, de trouver une clé de chiffrement, puis de générer l'alphabet chiffré, et enfin de chiffrer un message court. Ce message est transmis au voisin, qui doit le déchiffrer (attention, il faut transmettre le message chiffré, mais aussi la clé !)

Note scientifique

L'usage du chiffrement par substitution mono-alphabétique est en réalité bien antérieur à Jules César : on le voit apparaître dans le *Kama Sutra* (écrit au 5e après J.-C.… mais sur la base d'un manuscrit datant du IVe siècle avant J.-C.). Parmi les nombreux arts que devait maîtriser une concubine, le numéro 45 (*mlecchita-vikalpà*) consistait à savoir communiquer secrètement avec son amant !

Conclusion

La classe définit collectivement les concepts-clés cités dans l'en-tête de cette séance : chiffrement mono-alphabétique, clé, alphabet chiffré.

FICHE 5
Exercices de chiffrement mono-alphabétique

Exercice 1
À l'aide du tableau de correspondance ci-dessous, chiffre le message : « bonne chance pour casser ce code »

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

Exercice 2
À l'aide du même tableau de correspondance, déchiffre le message « D JB EBUB »

Exercice 3a
Sachant qu'il existe $4x10^{26}$ (4 suivi de 26 zéros) clés possibles pour le chiffrement mono-alphabétique, combien de temps faudrait-il pour qu'un individu teste toutes les clés et déchiffre ainsi le message ? On suppose qu'une personne met seulement 5 secondes pour tester une clé (générer le message en clair et le lire pour voir s'il a une signification).

Exercice 3b
Et si tous les êtres humains travaillaient ensemble pour résoudre ce problème, combien de temps cela prendrait-il ?

Exercice 3c
Et si on utilisait le plus puissant des supercalculateurs (Tianhe-2, de l'armée chinoise), capable de tester 10^{15} clés par seconde, combien de temps cela prendrait-il ?

Exercice 4
Choisis un mot-clé ou une phrase-clé et remplit l'alphabet chiffré ci-dessous. Attention à ne pas utiliser la même lettre plusieurs fois !
Utilise cette nouvelle table de correspondance pour chiffrer un message court. Transmets ce message à ton voisin (ainsi que la clé) et vérifie qu'il déchiffre bien ton message.

Alphabet 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
Alphabet chiffré																										

Séance 4 – Casser le chiffrement mono-alphabétique : l'analyse de fréquence d'Al-Kindi

Discipline dominante	Mathématiques
Résumé	Les élèves découvrent et appliquent la méthode d'analyse fréquentielle inventée par Al-Kindi, nécessitant des allers-retours entre la statistique et la linguistique.
Notions *(cf. scénario conceptuel, page 117)*	Information : • Le chiffrement par substitution mono-alphabétique peut être cassé en analysant la fréquence d'apparition des lettres. • L'analyse fréquentielle a été inventée par Al-Kindi au 9e siècle après J.-C.
Matériel	Pour chaque élève : • (Facultatif) un jeu de Scrabble© Pour chaque élève : • Fiche 6, page 144 • Fiche 7, page 145 • Fiche 8, page 146

Situation déclenchante

Le professeur revient sur ce qui a été vu lors de la séance précédente : en raison du très grand nombre de clés possibles, le chiffrement par substitution mono-alphabétique semble incassable. En effet, essayer toutes les clés prendrait des milliers d'années (avec un supercalculateur) ou des milliards d'années (à la main).

Il annonce pourtant que ce chiffrement n'est plus utilisé depuis le Moyen-Âge, car un savant perse a trouvé une méthode permettant de trouver la clé rapidement (Al-Kindi, 9è siècle après J.-C.).

Le professeur demande à la classe comment Al-Kindi a bien pu s'y prendre. S'ils n'ont aucune idée, il les guide en leur demandant d'expliquer comment ils avaient « cassé » le chiffrement de César (*cf.* Séance 2, page 125).

Outre la possibilité d'essayer toutes les clés possibles, la classe avait repéré quelle était la lettre la plus fréquente dans la langue française (le « E »), puis elle avait fait l'hypothèse que toutes les lettres avaient subi le même décalage que le « E ». Cette hypothèse n'est plus justifiée dans le cadre d'un chiffrement mono-alphabétique quelconque : chaque lettre peut, a priori, correspondre à n'importe quelle autre. Il faut donc s'aider de plusieurs lettres fréquentes, et pas d'une seule.

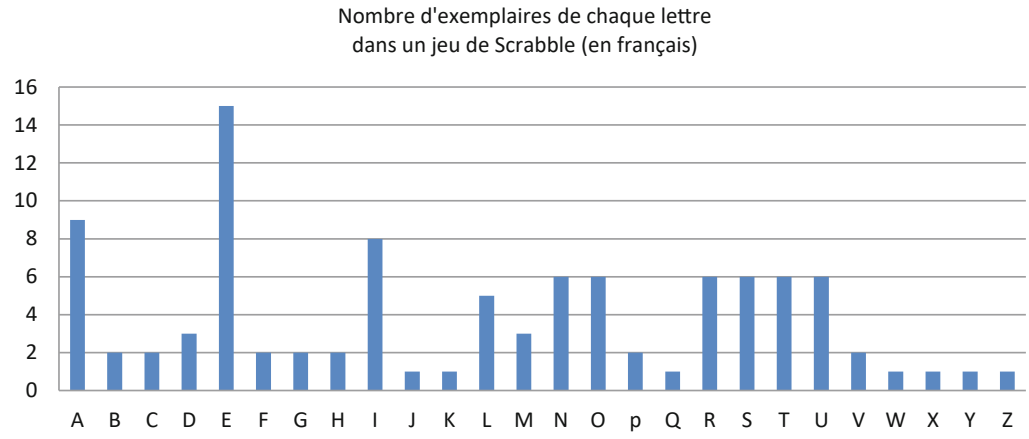
Trouver les lettres les plus fréquentes en français (collectivement, puis par binôme)

Le professeur demande si les élèves savent quelles sont les lettres les plus fréquentes en français et, dans le cas contraire, comment ils pourraient le déterminer.

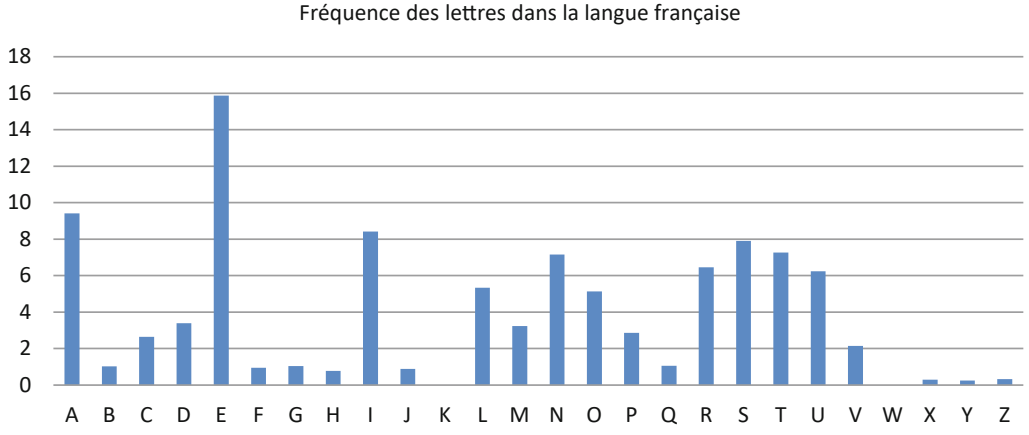
Une première manière d'approcher le problème consiste à examiner un jeu de Scrabble. Les lettres possèdent chacune une valeur et, bien entendu, les lettres les plus rares rapportent le plus de points (il est plus difficile de placer un W qu'un E dans un mot français !). Par ailleurs, on remarque que les lettres qui rapportent le moins de points (donc, a priori, les plus fréquentes), sont présentes en de nombreux exemplaires dans le jeu.

Lettre au Scrabble© (valeur de chaque lettre en indice)	A_1	B_3	C_3	D_2	E_1	F_4	G_2	H_4	I_1	J_8	K_{10}	L_1	M_2	N_1	O_1	P_3	Q_8	R_1	S_1	T_1	U_1	V_4	W_{10}	X_{10}	Y_{10}	Z_{10}
Nombre d'exemplaires de chaque lettre.	9	2	2	3	15	2	2	2	8	1	1	5	3	6	6	2	1	6	6	6	6	2	1	1	1	1

Après avoir fait examiner les pièces par les élèves, il affiche la répartition des lettres au tableau et demande aux élèves, par binôme, de créer un histogramme.



Cet histogramme est très proche de celui obtenu pour la langue française en général :



Notes scientifiques

• Il n'est pas possible de donner un histogramme de référence unique pour une langue donnée, quelle qu'elle soit, car les lettres les plus fréquemment employées dépendent du type de texte et du registre d'écriture (télégramme diplomatique, œuvre littéraire, encyclopédie, langage familier). Cependant, les différences d'un registre à l'autre peuvent être négligées dans un tel projet pédagogique.

• Les histogrammes de référence figurant sur la Fiche 7 ont été produits en analysant de grands corpus de texte (dictionnaires, œuvres littéraires)[1]. Nous les avons modifiés pour tenir compte de notre alphabet simplifié (les statistiques pour la lettre « e » regroupent également celles des lettres « é », « è », « ê »).

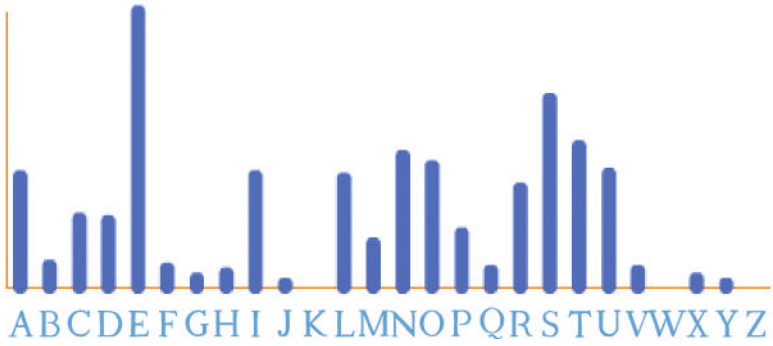
1. Source : https://en.wikipedia.org/wiki/Letter_frequency

Mise en commun

Après avoir corrigé les productions des élèves, le professeur demande à la classe si cette fréquence constatée pour le Scrabble reflète la fréquence des lettres de la langue française. Il propose, pour le savoir, d'analyser un texte figurant dans l'exercice 1 de la Fiche 6 (il s'agit du préambule à la Déclaration universelle des droits de l'homme et du citoyen de 1789).

Pour gagner du temps, chaque élève ne travaille que sur 2 ou 3 lettres seulement (ce qui permet, malgré tout, de comparer les productions de plusieurs élèves pour une même lettre et ainsi de détecter d'éventuelles erreurs).

Finalement, un histogramme est produit collectivement (figure ci-dessous) :



Note : ce graphique a été généré à l'aide du programme *Scratch* produit à la séquence 3, page 75. Ici, l'axe n'est pas gradué car seule la forme générale de l'histogramme nous intéresse.

On remarque que, même pour ce texte relativement court, l'histogramme obtenu ressemble à celui du jeu de Scrabble© ou de l'histogramme de référence de la langue française. Il semble que, dès qu'un texte devient suffisamment long (de l'ordre de la centaine de lettres), on retrouve le schéma suivant :

- La lettre e est la plus fréquente. C'est la seule dont la fréquence dépasse 15 %.
- Elle est suivie des lettres a (9 %), i (8 %), s (8 %), t (7 %), n (7 %) et r (6 %).
- Seules huit lettres affichent une fréquence inférieure à 1 % : f, h, j, k, w, x, y et z (onze lettres au total affichent une fréquence inférieure à 2 %).

Cryptanalyse pas à pas (par groupes ou collectivement)

Le professeur distribue aux élèves l'exercice 2 de la Fiche 6, qui propose d'effectuer la cryptanalyse d'un texte assez court (21 mots, 114 caractères, espaces et ponctuation non compris). La cryptanalyse est un exercice qui mêle mathématiques (analyse fréquentielle, basée sur la statistique) et linguistique (connaissance de la langue française, des lettres et des mots les plus fréquents, etc.).

Notes scientifiques

- Contrairement à ce que l'on peut imaginer a priori, il est beaucoup plus facile de cryptanalyser un texte long qu'un texte court. Plus le texte est long, plus on se rapproche de l'histogramme de référence, et plus la statistique permet, seule ou quasiment, de cryptanalyser le texte.
- Avec un texte assez court, comme ici, il est nécessaire de faire de nombreux allers-retours entre la statistique et la linguistique pour parvenir à le cryptanalyser. Cependant, comme on le voit ci-dessous, on y arrive très bien !

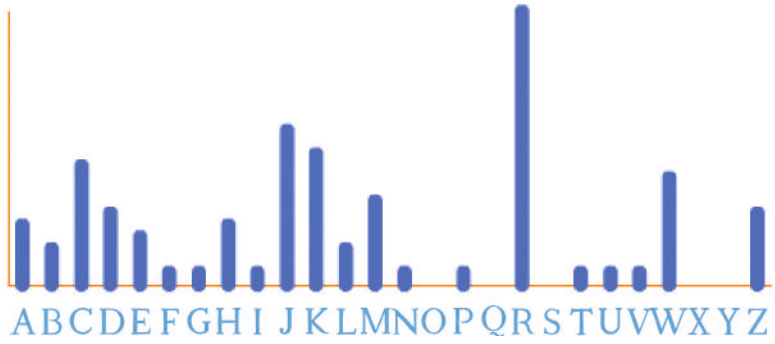
Notes pédagogiques

• Réaliser, seul, un tel exercice pour la première fois est hors de portée d'élèves de collège. En revanche, réalisé collectivement (ou en petits groupes avec des temps de mise en commun), il permet d'acquérir la « gymnastique » permettant, ensuite, d'être plus autonome.

• En fonction de l'aisance des élèves, le professeur choisira de proposer cet exercice sous forme de défi (à réaliser en autonomie, par petits groupes). Dans tous les cas, il ne faudra pas hésiter à les guider s'ils sont bloqués. Pour cette raison, nous explicitons ci-dessous une méthode « pas à pas ».

Étape 1 : réaliser l'histogramme du texte

Cette étape, déjà réalisée à plusieurs reprises au cours de cette séance, ne comporte plus aucune difficulté. Elle peut être réalisée comme précédemment, chaque lettre étant comptée par un élève.
On obtient :



Étape 2 : chercher la lettre la plus fréquente

Une lettre se détache très nettement (le « R »), suivie par 4-5 lettres de fréquence élevée, tandis que 13 lettres ont une fréquence très faible. Le schéma semble similaire à l'histogramme de référence, on peut donc supposer que le texte clair est écrit en français (ou en anglais, en allemand, en espagnol… qui ont des histogrammes assez semblables, comme le montre la Fiche 7).
Dans ce cas, on peut faire l'hypothèse (raisonnable) que le « R » chiffre la lettre « e ».
Si l'on remplace les « R » par des « e », le message devient :

Z**e**J VDAA**e**J CLWJJ**e**CK **e**K E**e**A**e**MH**e**CK ZWIH**e**J **e**K **e**ULMP **e**C EHDWKJ. Z**e**J EWJKWCBKWDCJ
JDBWLZ**e**J C**e** F**e**MN**e**CK **e**KH**e** TDCE**ee**J GM**e** JMH Z'MKWZWK**e** BDAAMC**e**.

Étape 3 : chercher les mots courts

Ici, pour rendre le travail plus facile, on a laissé les espaces et la ponctuation ce qui permet de rechercher les mots courts, peu nombreux.
Il y a 2 mots de 2 lettres dans ce message : **e**K (répété 2 fois), **e**C et C**e**. En français, les mots de 2 lettres les plus fréquents sont (dans l'ordre) : de, il, le, et, je, la, ne, un, en, ce, se, sa, du. Etant donnée la position de la lettre « e » dans les mots de 2 lettres présents ici, on peut faire l'hypothèse que :

• « eK » correspond à « et » (K ➜ t)

• « eC » pourrait correspondre à « en » (C ➜ n). « Ce » correspond à « de » ou « le » ou « ne » (C ➜ d ou C ➜ l ou C ➜ n). On peut donc faire l'hypothèse que C ➜ n.

Selon cette hypothèse, le texte devient :

ZeJ VDAAeJ nLWJJent et EeAeMHent ZWIHeJ et eULMP en EHDWtJ. ZeJ EWJtWnBtWDnJ JDBWLZeJ ne FeMNent etHe TDnEeeJ GMe JMH Z'MtWZWte BDAAMne.

On commence à reconnaître des structures familières (les 3e, 5e et 15e mots finissent par « ent », comme un verbe à la 3e personne du pluriel), ce qui nous encourage à poursuivre : notre hypothèse, jusque-là, semble correcte !

> **Note pédagogique**
> Obtenir la liste des mots de 2 ou 3 lettres en langue française est aisé car c'est un sujet qui intéresse les amateurs de Scrabble© ! Voir ici, par exemple : https://www.listesdemots.com

Dans le même esprit, on peut rechercher les mots de 3 lettres. Le texte en compte 3 : ZeJ (répété 2 fois), GMe et JMH. En français, les mots de 3 lettres les plus fréquents sont (dans l'ordre) : que, les, son, mon, pas, lui, une, des, qui, est. Notre mot « ZeJ » pourrait bien être « les » (plus probable, car plus fréquent) ou « des ».

Si l'on fait l'hypothèse que ZeJ ➜ les (Z ➜ l et J ➜ s), notre texte devient :

les VDAA**es** n**l**W**ssent et** E**e**A**e**MH**ent** **l**WI**l**H**es et e**ULMP **en** EHDW**ts**. **les** EW**st**W**n**B**t**WD**ns** **s**DBWL**les ne** F**e**MN**ent et**H**e** TD**n**E**ees** GM**e** **s**MH **l'**M**t**W**l**W**te** BDAAM**ne**.

Et si GMe ➜ que (mot de 3 lettres finissant par e le plus fréquent), alors le texte devient (avec G ➜ q et M ➜ u) :

les VDAA**es** n**l**W**ssent et** E**e**A**eu**H**ent** **l**WI**l**H**es et e**UL**u**P **en** EHDW**ts**. **les** EW**st**W**n**B**t**WD**ns** **s**DBWL**les ne** F**eu**N**ent et**H**e** TD**n**E**ees que su**H **l'ut**W**l**W**te** BDAA**une**.

Étape 4 : chercher les doublets

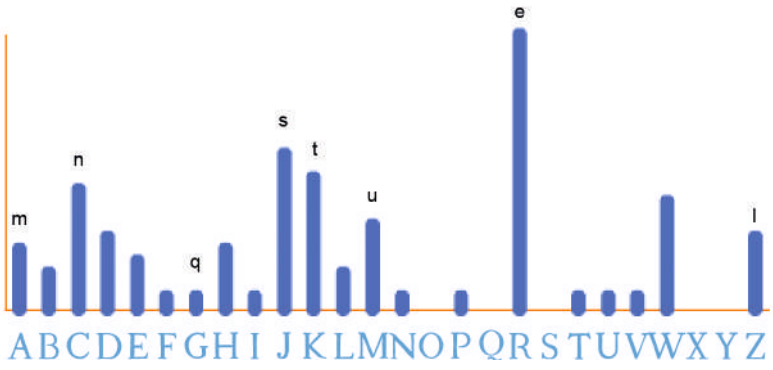
Les paires de lettres répétées sont souvent très utiles pour cryptanalyser un tel texte. Les doublets présents dans le texte sont : AA (répété 2 fois) et ss (en clair, car on l'a déjà déchiffré). En français, les doublets les plus fréquents sont : ss, ll, mm, rr, tt, nn, pp, ee, cc et ff.

Puisque les lettres s et l sont déjà trouvées, on peut essayer de remplacer AA par mm. Donc, si A ➜ m, le texte devient :

les VD**mmes** n**l**W**ssent et** E**emeu**H**ent** **l**WI**l**H**es et e**UL**u**P **en** EHDW**ts**. **les** EW**st**W**n**B**t**WD**ns** **s**DBWL**les ne** F**eu**N**ent et**H**e** TD**n**E**ees que su**H **l'ut**W**l**W**te** BD**mmune**.

Étape 5 : revenir au tableau de fréquences

Les lettres que nous avons déjà trouvées sont :



Or, on sait qu'en français, après la lettre e, les lettres les plus fréquentes sont a, i, s, t. Puisque s et t ont été trouvées (et correspondent bien à des pics), il est fort probable que a et i soient cachées derrière la lettre la plus fréquente restante (W).

Si on fait l'hypothèse que W ➜ a, alors le texte devient :

les VD**mmes n**L**assent et** E**emeu**H**ent la**I**H**es **et e**UL**u**P **en** EHD**ats**. **les** E**astan**B**ta**D**ns s**DB**a**L**les ne** F**eu**N**ent et**H**e** TD**n**E**ees que su**H **l'utalate** BD**mmune**.

Le 3e mot ne semble pas exister en français, ni l'avant dernier. L'hypothèse ne semble pas justifiée. Essayons W ➜ i. Le texte devient :

les VD**mmes n**L**issent et** E**emeu**H**ent li**I**H**es **et e**UL**u**P **en** EHD**its**. **les** E**istin**B**ti**D**ns s**DB**i**L**les ne** F**eu**N**ent et**H**e** TD**n**E**ees que su**H **l'utilite** BD**mmune**.

Formidable ! On reconnaît le mot « utilité » à l'avant-dernière place en partant de la fin.

Le 3e mot « nLissent » pourrait être « naissent ». Dans ce cas, L ➜ a, ce qui donne :

les VD**mmes naissent et** E**emeu**H**ent li**I**H**es **et e**U**au**P **en** EHD**its**. **les** E**istin**B**ti**D**ns s**DB**iales ne** F**eu**N**ent et**H**e** TD**n**E**ees que su**H **l'utilite** BD**mmune**.

De retour à l'histogramme des fréquences, parmi les lettres les plus fréquentes (a, i, s, t, n et r), il ne nous reste plus que r à trouver. Le pic restant pourrait correspondre à H ou C. C a déjà été trouvé (il correspond à n). Reste H. Si H ➜ r. Alors, le texte devient :

les VD**mmes naissent et** E**emeurent li**I**res et e**U**au**P **en** E**r**D**its**. **les** E**istin**B**ti**D**ns s**DB**iales ne** F**eu**N**ent etre** TD**n**E**ees que sur l'utilite** BD**mmune**.

On reconnait les mots « être » et « sur » dans la seconde phrase (remarque : on aurait pu trouver cela en regardant les mots de 3 lettres qui commencent par « su » il y avait des chances pour que cela soit « sur » !). Le 6e mot de la première phrase pourrait bien être « libre ». Dans ce cas (l ➜ b), on aurait :

les VD**mmes naissent et** E**emeurent libres et e**U**au**P **en** E**r**D**its**. **les** E**istin**B**ti**D**ns s**DB**iales ne** F**eu**N**ent etre** TD**n**E**ees que sur l'utilite** BD**mmune**.

Dès lors, le déchiffrement devient très facile : le 5e mot est « demeurent » (E ➜ d).

les VD**mmes naissent et demeurent libres et e**U**au**P **en dr**D**its**. **les distin**B**ti**D**ns s**DB**iales ne** F**eu**N**ent etre** TD**ndees que sur l'utilite** BD**mmune**.

Le contexte nous aide : le second mot est probablement « hommes », et le dernier mot de la première phrase « droit ». Dans ce cas (V ➜ h, D ➜ o), on a :

les hommes naissent et demeurent libres et eU**au**P **en droits**. **les distin**B**tions so**B**iales ne** F**eu**N**ent etre** T**ondees que sur l'utilite** B**ommune**.

Le travail est quasi achevé, il suffit de considérer que le 8e mot est « égaux » (U ➜ g et P ➜ x). Plus loin, on devine « distinctions sociales » (B ➜ c). La dernière étape est :

les hommes naissent et demeurent libres et egaux en droits. les distinctions sociales ne F**eu**N**ent etre** T**ondees que sur l'utilite commune**.

Par élimination, on en déduit que « Feuvent » correspond à « peuvent » et « Tondees » à « fondees ».

Nous avons donc réussi, sans connaître la clé, à cryptanalyser ce texte, malgré les millions de milliards de milliards de clés possibles !

Ce texte est bien sûr le premier article de la Déclaration des droits de l'homme (sans les accents) : *les hommes naissent et demeurent libres et egaux en droits. les distinctions sociales ne peuvent etre fondees que sur l'utilite commune.*

Quelle était la clé ?

Une fois la cryptanalyse terminée, il est très simple de trouver la clé. On connaît quasiment toutes les correspondances entre les 2 alphabets (clair et chiffré).

Alphabet 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
Alphabet chiffré	L	I	B	E	R	T	U	V	W	?	?	Z	A	C	D	F	G	H	J	K	M	N	?	P	?	?

Les quelques cases restantes sont très faciles à remplir.
La clé est donc : LIBERT (le mot-clé était LIBERTE).

Notes scientifiques

D'autres statistiques peuvent nous guider pour l'analyse fréquentielle. Par exemple :
• La fréquence des lettres en fonction de leur position dans les mots. En anglais, les mots commencent bien plus souvent par les lettres « t », « a » ou « s » que par « e », même si « e » est la lettre la plus courante.
• La fréquence des paires de lettres ou « bigrammes ». En français, les bigrammes les plus fréquents sont « es », « de », « le », « en » et « re ». La recherche des « bigrammes » et des « trigrammes » (les plus fréquents sont « ent » et « les ») s'impose dès lors que le texte ne contient plus d'espace ni de ponctuation pour séparer les mots (rappel : nous avons gardé, ici, les espaces et la ponctuation par souci de simplification). Attention cependant : certains bigrammes apparents n'existent pas car ils sont à cheval sur 2 mots !

Etude documentaire (individuellement)

Le professeur distribue la Fiche 8 à chaque élève. La fiche est lue individuellement, puis discutée en classe entière. Cette discussion permet notamment de faire ressortir :
• La faiblesse de certaines méthodes de chiffrement qui, bien que proposant un nombre de clés très important, peuvent être cassées avec un peu d'astuce ;
• La course permanente entre les cryptographes et les cryptanalystes ;
• Les enjeux actuels de la cryptographie (enjeux qui seront débattus plus en détail à la fin de la séquence, page 154).

Conclusion

La classe élabore une conclusion collective qui peut être, par exemple :
• L'algorithme est le plus important. Mieux vaut un bon algorithme[2] et une machine médiocre qu'un algorithme médiocre et une bonne machine !
• L'analyse fréquentielle nécessite de faire des allers-retours entre la statistique et la connaissance de la langue (linguistique).

2. Sur cet aspect, voir l'éclairage scientifique, page 10.

Prolongements EPI

• En français :

– Lire *Les Hommes dansants*, une des 56 nouvelles d'Arthur Conan Doyle mettant en scène le détective Sherlock Holmes. La cryptanalyse est au cœur de cette nouvelle (*cf.* prolongement en mathématiques proposé ci-dessous).

– Étudier quelques textes et remarquer que l'histogramme des fréquences peut varier sensiblement selon le registre de langage (familier, soutenu, etc.). Remarquer aussi que, dans un texte aussi atypique que *La Disparition* de G. Perec, l'histogramme des fréquences ressemble tout de même fortement à l'histogramme de référence pour la langue française, mis à part le « e » qui a disparu.

• En langue vivante :

– Étudier quelques textes et remarquer que les fréquences des lettres sont différentes de celles de la langue française (cependant, la lettre « e » reste largement dominante dans toutes ces langues, comme on le voit sur la Fiche 7).

• En histoire :

– Étudier les conditions qui ont permis l'essor des sciences arabes, au point de parler d'un « âge d'or » : stabilité politique, prospérité économique, tolérance religieuse

• En mathématiques :

– Pour comprendre que l'analyse de fréquence marche quels que soient les symboles utilisés (pas seulement des lettres), faire la cryptanalyse d'un « texte » composé d'une suite de dessins. Par exemple, un des messages figurant dans la nouvelle *Les Hommes dansants* (*cf.* prolongement en français proposé ci-dessus) :

– Pour aller au-delà du chiffrement mono-alphabétique, on peut étudier :

- Le chiffrement de Vigenère (le chiffrement utilise plusieurs alphabets différents)
- Le chiffrement de Playfair (le chiffrement se fait par bigrammes, et non par lettres individuelles)

FICHE 6
Analyse fréquentielle

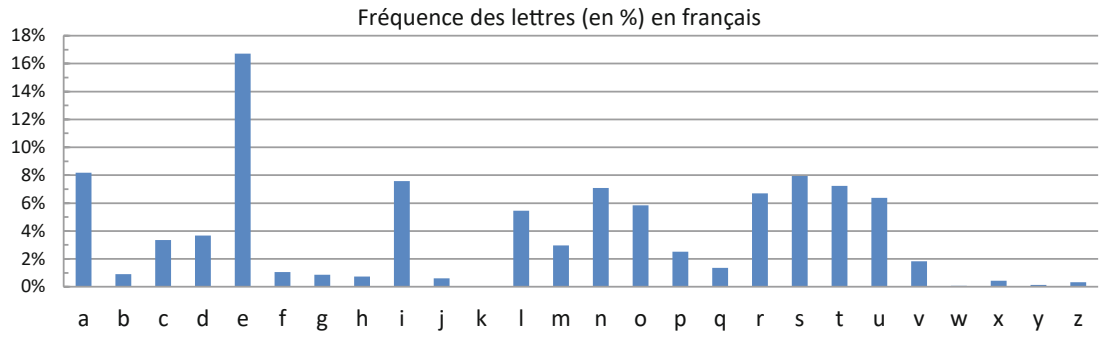
Exercice 1 : Relève la fréquence d'apparition de toutes les lettres de ce texte (il s'agit du préambule à la Déclaration universelle des droits de l'homme et du citoyen de 1789).
Les representants du peuple francais, constitues en assemblee Nationale, considerant que l'ignorance, l'oubli ou le mepris des droits de l'Homme sont les seules causes des malheurs publics et de la corruption des gouvernements, ont resolu d'exposer, dans une declaration solennelle, les droits naturels, inalienables et sacres de l'Homme, afin que cette declaration, constamment presente a tous les membres du corps social, leur rappelle sans cesse leurs droits et leurs devoirs ; afin que les actes du pouvoir legislatif, et ceux du pouvoir executif, pouvant etre a chaque instant compares avec le but de toute institution politique, en soient plus respectes ; afin que les reclamations des citoyens, fondees desormais sur des principes simples et incontestables, tournent toujours au maintien de la Constitution et au bonheur de tous.
(Note : pour simplifier le travail, nous avons supprimé les accents dans ce texte.)

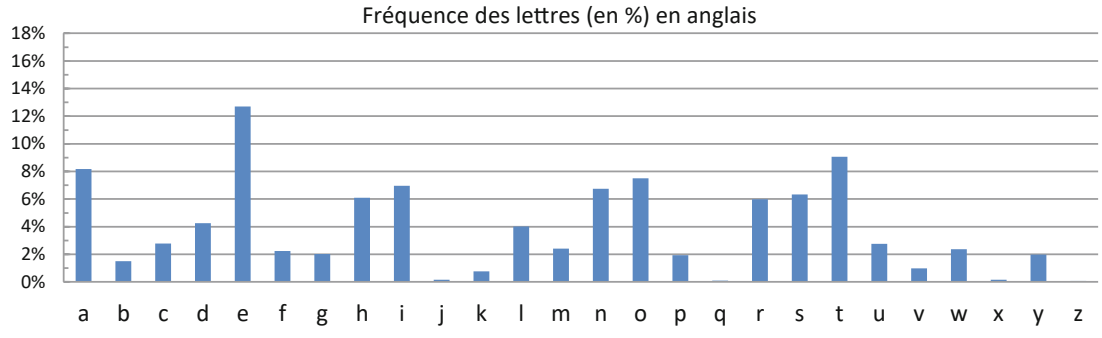
Exercice 2 : Voici un texte chiffré par substitution mono-alphabétique. La clé n'est pas connue. Défi : cryptanalysez ce texte.
ZRJ VDAARJ CLWJJRCK RK ERARMHRCK ZWIHRJ RK RULMP RC EHDWKJ. ZRJ EWJKWCBKWDCJ JDBWLZRJ CR FRMNRCK RKHR TDCERRJ GMR JMH Z'MKWZWKR BDAAMCR.

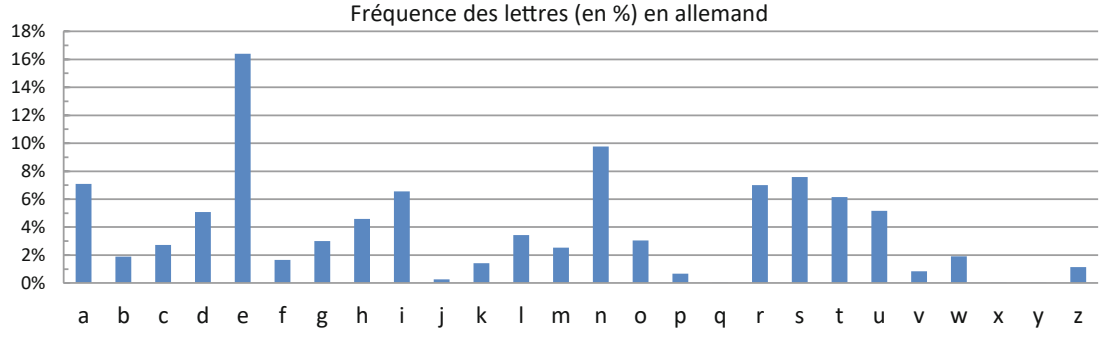
Exercice 1 : Relève la fréquence d'apparition de toutes les lettres de ce texte (il s'agit du préambule à la Déclaration universelle des droits de l'homme et du citoyen de 1789).
Les representants du peuple francais, constitues en assemblee Nationale, considerant que l'ignorance, l'oubli ou le mepris des droits de l'Homme sont les seules causes des malheurs publics et de la corruption des gouvernements, ont resolu d'exposer, dans une declaration solennelle, les droits naturels, inalienables et sacres de l'Homme, afin que cette declaration, constamment presente a tous les membres du corps social, leur rappelle sans cesse leurs droits et leurs devoirs ; afin que les actes du pouvoir legislatif, et ceux du pouvoir executif, pouvant etre a chaque instant compares avec le but de toute institution politique, en soient plus respectes ; afin que les reclamations des citoyens, fondees desormais sur des principes simples et incontestables, tournent toujours au maintien de la Constitution et au bonheur de tous.
(Note : pour simplifier le travail, nous avons supprimé les accents dans ce texte.)

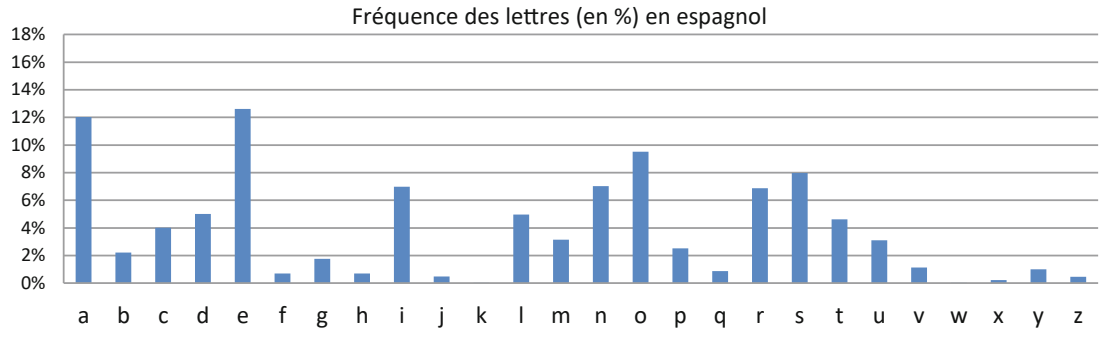
Exercice 2 : Voici un texte chiffré par substitution mono-alphabétique. La clé n'est pas connue. Défi : cryptanalysez ce texte.
ZRJ VDAARJ CLWJJRCK RK ERARMHRCK ZWIHRJ RK RULMP RC EHDWKJ. ZRJ EWJKWCBKWDCJ JDBWLZRJ CR FRMNRCK RKHR TDCERRJ GMR JMH Z'MKWZWKR BDAAMCR.

FICHE 7
Quelques histogrammes de référence









FICHE 8
César et Al-Kindi, les premiers acteurs de la cryptographie

Les hommes ont toujours voulu protéger leurs communications, qu'il s'agisse d'envoyer des ordres militaires, d'espionner les puissances ennemies, de faire du commerce ou même d'échanger des lettres amoureuses. À l'époque de Jules César, très peu de personnes savent lire, et sa méthode de chiffrement, pourtant très simple, suffit dans la plupart des cas.

Au sortir de l'antiquité, ce chiffrement s'est raffiné : plutôt que simplement décaler l'alphabet, on mélange les lettres apparemment au hasard (en réalité, on utilise un mot- ou une phrase-clé). Les possibilités sont immenses et il est impossible, si l'on ne connait pas la clé, d'essayer tous les alphabets possibles. Ce chiffrement par « substitution mono-alphabétique » (à une lettre « en clair » correspond une, et une seule, lettre chiffrée) restera inviolé pendant près de 1 000 ans, jusqu'à ce qu'Al-Kindi invente une méthode (appelée « analyse de fréquence ») qui permet de le briser en quelques minutes.

Al-Kindi, de son vrai nom Abū Yūsuf Ya'qūb ibn Isāq al-Kindī, est l'un des plus grands savants arabes, auteur de plus de 290 manuscrits sur l'astronomie, les mathématiques, la médecine, la philosophie… Au IXe siècle après J.-C., alors que l'Occident s'enferme dans l'obscurantisme, les sciences arabes connaissent leur âge d'or. Al-Kindi remarque que certaines lettres sont beaucoup plus fréquentes que d'autres et que le chiffrement mono-alphabétique ne modifie pas ces fréquences. Par exemple, si « e » est chiffré en « L », la lettre « L » aura la même fréquence, dans le message chiffré, que la lettre « e » dans le message clair. Connaissant la fréquence des lettres dans une langue, il devient facile de retrouver le texte clair, si celui-ci est assez long. Al-Kindi devient le premier cryptanalyste de l'histoire.

Il faudra attendre le XVe siècle pour que Léon Battista Alberti invente le chiffrement par substitution poly-alphabétique, puis que Blaise de Vigenère le perfectionne. Cette méthode utilise plusieurs alphabets chiffrés et résiste à l'analyse de fréquence. Elle fera autorité pendant 3 siècles jusqu'à ce que Charles Babbage découvre une méthode pour la briser.

Depuis, la course continue entre les cryptographes (qui inventent des chiffrements) et les cryptanalystes (qui attaquent ces chiffrements). La cryptographie s'est mécanisée, puis informatisée. Les cryptographes actuels sont davantage mathématiciens que linguistes, mais les enjeux restent les mêmes. Cependant, comme nous le verrons, depuis l'essor d'Internet et la numérisation de nos communications, ces enjeux ont pris une dimension nouvelle :

- D'un côté, les États peuvent intercepter toutes les communications (e-mail, téléphone…) échangées entre deux individus, et souhaitent limiter l'usage de la cryptographie pour préserver la sécurité (espionner les terroristes, en particulier).
- D'un autre côté, les citoyens prennent conscience de l'importance qu'il y a de préserver leur intimité, qu'il s'agisse de leur vie de famille, leur santé, leurs opinions politiques, croyances religieuses, orientations sexuelles… Que peuvent devenir ces informations dans les mains d'un employeur, d'un assureur ou d'un gouvernement non démocratique ?

Séance 5 – Comment communiquer sans échanger la clé ?

Discipline dominante	Mathématiques
Résumé	Les élèves modélisent les échanges entre deux personnes à l'aide de cadenas et de clés. Ils prennent conscience du point faible de la plupart des méthodes de chiffrement : l'échange de la clé ; et comprennent que l'usage de plusieurs clés permet de résoudre ce problème. C'est le principe du chiffrement asymétrique.
Notions *(cf. scénario conceptuel, page 117)*	Information : • Le chiffrement de César et le chiffrement par substitution mono-alphabétique sont dits « symétriques » car ils utilisent une seule clé pour chiffrer et déchiffrer. • L'échange de la clé entre les interlocuteurs est un point faible de toutes les méthodes de chiffrement symétriques (qui utilisent la même clé pour chiffrer ou déchiffrer).
Matériel	Pour chaque groupe : • 1 boîte • 2 cadenas, chacun possédant sa propre clé. Si possible, utiliser des cadenas de couleurs différentes, avec les clés assorties.

Situation initiale

La classe fait le point sur ce qu'elle a appris en matière de cryptographie :
• le chiffrement de César est très facile à casser, à la fois car le nombre de clés possibles est très faible (donc on peut les tester toutes très rapidement) et parce qu'il ne résiste pas à l'analyse fréquentielle ;
• le chiffrement par substitution mono-alphabétique possède un nombre de clés très élevé, mais il est facile à casser (pour des messages de longueur suffisante) à l'aide de l'analyse fréquentielle ;
• Il existe des méthodes de chiffrement qui résistent à l'analyse fréquentielle (ceux pour lesquelles une même lettre peut être chiffrée en plusieurs lettres différentes).
Le professeur fait remarquer que toutes ces méthodes de chiffrement possèdent un point faible : la transmission de la clé. Pour que le destinataire du message puisse le déchiffrer, il faut qu'il possède la clé de chiffrement. Le professeur demande aux élèves comment il est possible de se mettre d'accord sur une clé avec son interlocuteur, et la classe examine les points faibles des méthodes proposées par les élèves :
• Noter la clé sur un papier, que l'on transmet à l'interlocuteur : si le papier est intercepté, c'est fichu ! (On peut évoquer les « cabinets noirs » qui, dans chaque pays, interceptaient les courriers postaux pour espionner les communications, en particulier venant ou allant à des ambassades).
• Transmettre la clé oralement à son interlocuteur, qui l'apprend par cœur : cela nécessite de pouvoir rencontrer son interlocuteur. Aujourd'hui, on veut communiquer rapidement avec des personnes à l'autre bout de la planète. Comment justifier de prendre un billet d'avion juste pour communiquer la clé d'un futur échange ? Ce système peut fonctionner en théorie, mais sera très lent et couteux. C'est comme cela que fonctionne le téléphone rouge : avant chaque nouvelle communication, une nouvelle clé est générée aléatoirement, puis échangée par voie diplomatique (ce qui prend du temps

et nécessite un acheminement hautement sécurisé). L'important étant que la clé soit très longue (à peu près aussi longue que le message à chiffrer) et qu'elle soit nouvelle pour chaque nouveau message. Ce chiffrement est inviolable, mais très couteux : seules les communications les plus importantes peuvent justifier un tel coût.

• Changer souvent de clé. Avantage : si quelqu'un découvre une clé, il ne pourra décoder que les messages du jour, et pas ceux du lendemain). Inconvénient : il faut noter les différentes clés et se les transmettre et l'on retombe sur les difficultés rencontrées précédemment.

Recherche (par groupes)

Le professeur propose aux élèves de modéliser la communication entre 2 personnes à l'aide d'une boîte (qui renferme le message que l'on veut transmettre) et de cadenas (qui symbolisent des méthodes de chiffrement). On peut mettre en place plusieurs méthodes de chiffrement (*i.e.* utiliser plusieurs cadenas). Chaque groupe reçoit une boîte, 2 cadenas, chacun des cadenas ayant sa propre clé.

La situation est la suivante : Alice cherche à envoyer un message à Bob, sans qu'Ève puisse intercepter ce message.

Les élèves doivent chercher quelles sont les opérations à réaliser (et dans quel ordre) par Alice et par Bob pour que le message puisse être correctement déchiffré à l'arrivée, sans jamais voyager en clair.

Note scientifique

Alice, Bob et Ève sont des figures inventées par Ron Rivest en 1978 dans un article décrivant le système RSA (dont il est question sur la Fiche 9, page 153). Depuis, ces 3 prénoms sont couramment utilisées pour illustrer les méthodes de cryptographie.

Notes pédagogiques

• Il est peu probable que les élèves parviennent, seuls, à trouver l'algorithme. Ce petit temps de tâtonnement nous semble cependant important pour leur faire réfléchir avant de les guider (légèrement) vers la solution.

• Une façon de les guider peut être de les faire jouer au jeu « loup/chèvre/chou » : Un batelier doit faire traverser une rivière à un loup, une chèvre et un chou. Attention : il n'y a qu'une place sur le bateau. De plus, si le loup et la chèvre sont ensemble sur la même rive lorsque le batelier s'éloigne, le loup mange la chèvre. Même chose avec la chèvre et le chou. Comment faire ? Il s'agit d'un problème similaire, avec une contrainte sur le voyage. Ici, il s'agit de ne jamais laisser seuls le loup et la chèvre, ou la chèvre et la laitue ; tandis que dans notre problème d'origine, il s'agit de ne jamais faire voyager le coffre sans aucun cadenas.

Après une dizaine de minutes de tâtonnement, le professeur les met sur la voie : il explique que le problème de l'échange de clé vient du fait que les 2 interlocuteurs utilisent la même clé.

Il propose d'explorer ce qui se passe si chacun possède son propre cadenas et sa propre clé. Les élèves tâtonnent à nouveau une dizaine de minutes en explorant cette configuration :

• Alice possède un cadenas, et une clé (qui n'ouvre que son propre cadenas).

• Idem pour Bob

• Ils doivent se communiquer la boîte en faisant en sorte qu'elle soit toujours fermée par un cadenas, et qu'elle puisse être ouverte à la fin (par Bob).

Mise en commun

Le professeur organise la mise en commun au cours de laquelle quelques groupes viennent présenter leur méthode. Chacune est discutée.

La méthode qui fonctionne (ou plutôt, qui semble fonctionner, comme on le verra à la séance suivante) est :

• Étape 1 : situation initiale : Alice veut envoyer un message à Bob. Chacun possède un cadenas et une clé privée (son propre algorithme de chiffrement).

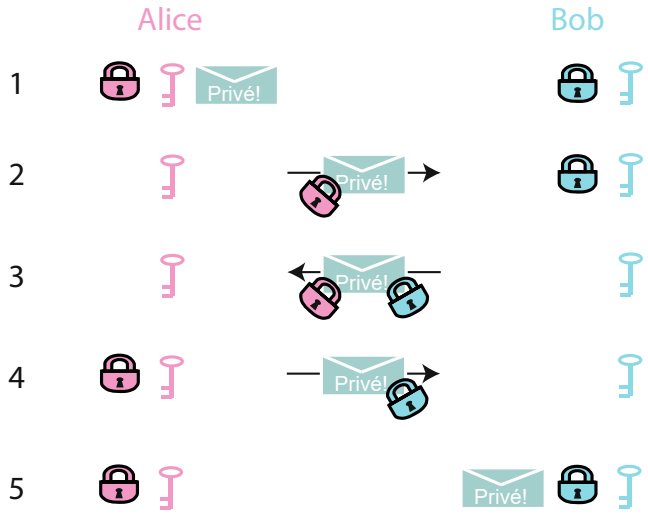
• Étape 2 : Alice pose son cadenas et envoie ce message chiffré à Bob.

• Étape 3 : Bob ne peut pas ouvrir le cadenas d'Alice (il n'a pas la clé d'Alice) : il pose son propre cadenas et renvoie le message (chiffré à la fois par Alice et par Bob) à Alice.

• Étape 4 : Alice retire son cadenas (elle déchiffre le message à l'aide de sa clé) et le renvoie à Bob.

• Étape 5 : cette fois, Bob peut retirer le dernier cadenas (puisque c'est le sien : il a la clé !) et lire ainsi le message contenu dans la boîte.

Elle peut s'illustrer comme ceci :



Le professeur fait remarquer aux élèves qu'Alice et Bob ont réussi à communiquer secrètement et ce, sans jamais communiquer leur clé !

Exercice

Chaque groupe répète la manœuvre plusieurs fois de manière à ce qu'elle soit bien comprise par tous les élèves.

Notes scientifiques

• Cette méthode possède un point faible, qui est discuté (et résolu) dans la séance suivante.

• Les cadenas représentent des fonctions mathématiques de chiffrement (et les clés les valeurs qui permettent de déchiffrer). Cette méthode de communication sans échange de clé suppose donc que les méthodes de chiffrement utilisées (donc les fonctions mathématiques) soit commutatives.

Séance 6 – Clé publique, clé privée

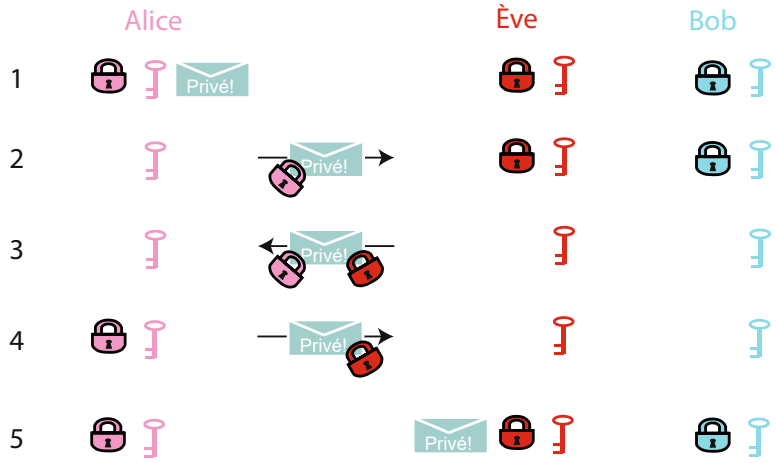
Discipline dominante	Mathématiques
Résumé	Les élèves perfectionnent leur algorithme de chiffrement asymétrique, en utilisant des clés publiques (qui servent à chiffrer) et des clés privées (qui servent à déchiffrer).
Notions *(cf. scénario conceptuel, page 117)*	Information : • En 1976, Diffie et Helmann ont montré que l'on pouvait résoudre le problème de l'échange des clés en utilisant 2 clés : une clé publique (qui sert à chiffrer le message) et une clé privée (qui sert à déchiffrer le message) : c'est le chiffrement asymétrique. • L'utilisation du chiffrement asymétrique permet à la fois de garantir la confidentialité de la communication, et de s'assurer de l'identité des correspondants. • Aujourd'hui, de nombreux outils permettent aux particuliers et aux entreprises de communiquer en toute sécurité.
Matériel	Pour chaque groupe : • Idem Séance 5, mais avec un 3e cadenas (et sa clé) en plus Pour chaque élève : • Fiche 9, page 153

Situation initiale

Le professeur demande à 2 élèves de refaire une démonstration à la classe de la méthode d'échange des clés vue à la séance précédente.

Il demande alors aux élèves si ceux-ci peuvent identifier le point faible de cet échange. Si les élèves ne trouvent pas par eux-mêmes, il les guide en leur demandant ce qui se passe si Ève (qui tente de percer le secret de la correspondance entre Alice et Bob) intercepte le premier message (étape 2, ci-avant).

Si ça n'est pas Bob qui reçoit le message, mais Ève, alors Ève peut se faire passer pour Bob, sans que lui-même le sache (il ne saura même pas qu'Alice a tenté de communiquer avec lui). Ève, usurpant l'identité de Bob, pose son propre cadenas et le renvoie à Alice. Alice, pensant recevoir la réponse de Bob, retire son cadenas. À l'étape suivante, Ève reçoit le message et peut le déchiffrer. On peut illustrer cette interception comme cela :



Ainsi, l'utilisation d'une double clé privée permet de communiquer secrètement sans avoir besoin d'échanger sa clé, mais ne résiste pas à l'interception par un tiers. Et ceci pour une raison simple : aucun interlocuteur ne peut vérifier l'identité de l'autre. Rappelons que l'utilisateur, quel qu'il soit, ne « voit » pas les cadenas (ni leur couleur), mais simplement une chaîne de caractères chiffrée, qui ressemble beaucoup à un texte aléatoire.

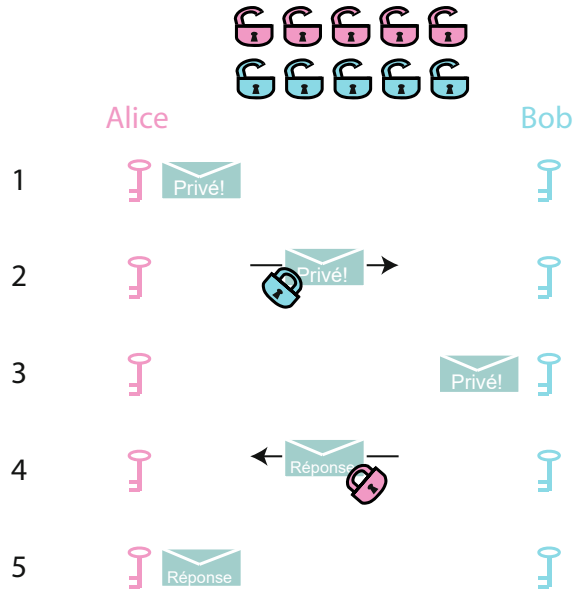
Introduction de la clé publique (collectivement)

Le professeur explique que cette méthode se résout en introduisant 2 clés pour chaque personne, une clé publique (que tout le monde peut connaître) et une clé privée. Le point important est que ces 2 clés ne permettent pas de faire la même chose :

- La clé publique permet uniquement de chiffrer le message ;
- La clé privée permet, seule, de le déchiffrer.

Cette méthode nécessite, en pratique, d'utiliser des fonctions asymétriques (*cf.* prolongement). Pour notre analogie du cadenas et des clés : la clé publique est similaire au cadenas ouvert (en fermant le cadenas, on chiffre le message), tandis que la clé privée est représentée par la clé du cadenas. Ainsi, Alice et Bob mettent à la disposition de tout le monde leur cadenas, mais pas leur clé. Dans ce cas, Alice envoie simplement son message en utilisant le cadenas de Bob (sa clé publique). Bob est le seul à disposer de la clé permettant de déchiffrer ce message ; il le fait et, s'il souhaite répondre à Alice, il utilise le cadenas d'Alice.

Ève peut intercepter n'importe quel message : puisqu'elle ne dispose pas des clés privées d'Alice ou de Bob, elle ne pourra déchiffrer ni le message original, ni sa réponse.



Exercice

Comme à la séance précédente, les élèves s'exercent quelques minutes à ce chiffrement asymétrique.

Notes scientifiques

- Le problème avec la solution sans clé publique (*cf.* séance précédente) est que Alice et Bob ne partagent aucune information, aucun moyen d'identification, et que, du coup, tout ce que Bob peut faire, Ève peut aussi le faire en se faisant passer pour Bob, et Alice n'a pas moyen de savoir si elle communique avec le vrai ou le faux Bob. Avec le système de clé publique/privée, Alice et Bob partagent une information (qu'ils ont eu via une tierce partie de confiance par exemple) : la clé publique de l'autre. Alice sait donc que si elle met le cadenas de Bob sur un message, seul lui pourra le déchiffrer
- La cryptographie asymétrique permet non seulement de chiffrer (et déchiffrer) des messages, mais aussi de s'identifier. Alice peut chiffrer sa signature avec sa clé privée et tout un chacun peut vérifier (à l'aide de sa clé publique) que la signature est bien celle d'Alice.

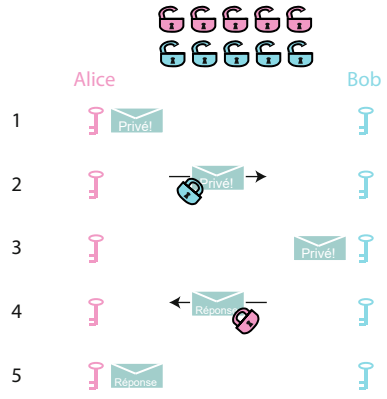
Etude documentaire (individuellement)

Le professeur distribue la Fiche 9 à chaque élève. La fiche est lue individuellement, puis discutée en classe entière. Cette discussion permet notamment de faire ressortir le lien entre la puissance de calcul disponible et le niveau de sécurité atteint (plus cette puissance de calcul augmente, et plus il faut augmenter la taille des clés pour garder un niveau de sécurité acceptable). La fin de la fiche documentaire reprend, et développe, les enjeux actuels de la cryptographie qui avaient été approchés sur la Fiche 8. Ces informations préparent au débat qui aura lieu lors de la séance suivante.

FICHE 9
Histoire de la cryptographie à clé publique

Dans les années 1960, l'informatique se développe et ouvre de nouvelles possibilités. La cryptographie, jusque-là réservée aux seules agences gouvernementales, devient accessible aux entreprises, voire aux particuliers. Mais, si deux personnes souhaitent communiquer secrètement, elles doivent se mettre d'accord sur une clé servant au chiffrement et au déchiffrement. L'échange des clés, qui a toujours été un casse-tête dans l'histoire de la cryptographie, devient un problème insurmontable à mesure que la cryptographie se démocratise.

Whitfield Diffie et Martin Hellman vont résoudre ce problème en 1976, dans un article intitulé New directions in cryptography resté fameux. Ces deux mathématiciens montrent qu'il est possible de communiquer secrètement en utilisant un chiffrement asymétrique. Le chiffrement asymétrique utilise 2 clés, l'une publique, l'autre privée. La clé publique permet de chiffrer le message, mais seule la clé privée permet de le déchiffrer.



Deux ans plus tard, Ron Rivest, Adi Shamir et Leonard Adleman améliorent cette idée pour créer l'algorithme RSA (nommé d'après leurs initiales). L'algorithme RSA utilise, pour simplifier, un très grand nombre, N, que l'on peut décomposer comme le produit de 2 nombres premiers *p* et *q*. N=*p*x*q*. N est la clé publique, tandis que *p* et *q* constituent la clé privée. N permet de chiffrer un message, mais l'opération de déchiffrement nécessite de connaître *p* et *q*. La sécurité de RSA repose sur le fait qu'il est très difficile de calculer les diviseurs d'un très grand nombre (on dit aussi « factoriser » un nombre). Même avec les meilleurs calculateurs, la factorisation peut prendre des années si le nombre est suffisamment grand. Pour cette raison, RSA est l'algorithme de chiffrement le plus utilisé dans le monde.

RSA est très sûr mais nécessite des moyens de calcul importants. Paul Zimmermann a résolu ce problème en 1991 en inventant un logiciel appelé PGP (*pretty good privacy*) qui est un compromis entre un chiffrement « classique » à clé privée et un chiffrement RSA. PGP a permis de démocratiser la cryptographie en la rendant accessible aux ordinateurs grand public. Cela lui a valu des poursuites judiciaires de la part du gouvernement américain. Certains gouvernements tentent en effet de limiter l'usage de la cryptographie de manière à pouvoir continuer d'intercepter les communications. Pour cela, ils exigent en général :

• Soit de limiter la taille des clés utilisées : une clé de taille « moyenne » est trop difficile à casser pour un ordinateur classique, mais pas pour un supercalculateur. Ainsi, la confidentialité est assurée vis-à-vis des particuliers, mais pas des agences gouvernementales ni des très grandes entreprises qui possèdent des supercalculateurs.

• Soit de déposer ses clés privées dans un « coffre » géré par un organisme « de confiance » (une agence gouvernementale par exemple). Ainsi, les communications sont secrètes pour tout le monde sauf pour ceux qui ont accès au coffre.

Longtemps réservée aux armées et aux diplomates, la cryptographie est aujourd'hui utilisée par de nombreux services : les banques (cartes bancaires, transactions sécurisées sur Internet), le commerce électronique, les messageries électroniques (carte SIM, e-mail…), les services médicaux (carte Vitale…), le vote électronique, etc.

Séance 7 – La cryptographie, amie ou ennemie ?

Discipline dominante	Atelier philo
Résumé	Les élèves participent à un « atelier philo » portant sur les enjeux actuels de la cryptographie. Faut-il autoriser la cryptographie, au risque d'empêcher les agences de sécurité de faire leur travail ? Faut-il l'interdire, au risque de voir disparaître notre vie privée ?
Notions *(cf. scénario conceptuel, page 117)*	Enjeux sociétaux : • L'autorisation ou la restriction de la cryptographie fait débat dans de nombreux pays. • L'utilisation de la cryptographie inquiète de nombreux gouvernements qui souhaitent pouvoir intercepter les communications pour des raisons de sécurité. • Les récentes révélations d'écoutes à très grande échelle mobilisent des citoyens inquiets du respect de leur vie privée. • La sécurité et la confidentialité des communications sont essentielles au fonctionnement de notre économie.
Matériel	Pour chaque élève : • Fiche 10, page 157 Pour la classe : • Fonds documentaire préparé à l'avance (cf. « préparation », ci-après)

Préparation de l'atelier philosophique

Le professeur organise cette séance de façon particulière, sous la forme d'un « atelier philo ».
Idéalement, il est assisté du professeur documentaliste qui, en plus de guider les élèves dans leurs recherches documentaires, co-anime le débat. Sa position « extérieure » peut aider à l'expression de l'opinion de chacun et garantir le respect de cette opinion.
L'objectif d'une telle séance n'est en effet pas d'aboutir à une conclusion tranchée que chacun sera tenu d'adopter, mais de faire prendre conscience aux élèves de la complexité du dilemme auquel sont confrontées nos sociétés actuelles et de leur permettre de se forger une opinion argumentée.

Notes pédagogiques

• Différentes méthodes existent pour mener un atelier philosophique en classe. Celle qui est utilisée s'inspire de la méthode AGSAS-Lévine© qui est présentée dans l'ouvrage *L'enfant philosophe, avenir de l'humanité ?* de Jacques Lévine paru chez ESF Éditeur.
• Pour la préparation de cette séance, les deux professeurs auront sélectionné quelques ressources documentaires (notamment articles de presse) afin de nourrir la seconde étape du travail. Les sources ne manquent pas. En 2015, par exemple, David Cameron a souhaité faire interdire le chiffrement en Angleterre. Cette même année, la France a voté la loi sur le renseignement qui oblige toute entreprise fournissant un service de chiffrement à communiquer au gouvernement les clés de déchiffrement en cas de demande.

L'organisation de la salle doit refléter le caractère particulier de cette séance :
• Les chaises sont placées en cercle de façon à aménager un espace de parole (les tables sont repoussées à l'extérieur du cercle, contre les murs de la salle)
• Les élèves prennent place sur ces chaises, dans le cercle.
• Les professeurs se placent en dehors du cercle : ils n'interviennent pas au cours de l'atelier.

Rappel des règles de l'« atelier philo »

Que les élèves aient déjà expérimenté ce type de travail ou non, le professeur explique ou fait rappeler aux élèves le déroulement et les règles inhérentes à l'« atelier philo » :
• Le professeur énonce le thème de l'atelier et chacun réfléchit pendant une minute à l'avis qu'il a sur cette question. Puis, les élèves disposent de 9 minutes pour s'exprimer sur le sujet, temps au cours duquel le professeur ne prend pas la parole. Un dispositif d'enregistrement est placé au centre du cercle car l'« atelier philo » sera ensuite transcrit (sans indiquer les prénoms des personnes qui s'expriment) et distribué à chacun.
• Les élèves sont libres de dire ce qui leur passe par la tête, tout en essayant de prendre de la hauteur par rapport au sujet. Il n'y a pas de bonne ou de mauvaise réponse. L'« atelier philo » est l'occasion de penser par soi-même, d'observer le cheminement individuel et collectif de la pensée.
• On ne peut s'exprimer que lorsqu'on a le « bâton de parole ». Celui-ci passe de main en main et il n'est pas obligatoire de dire quelque chose quand il arrive jusqu'à soi. Si l'élève n'a pas envie de parler, il transmet le bâton de parole à son voisin.
• Une des règles fondamentales est le respect de la parole d'autrui. On a le droit de ne pas être d'accord avec quelqu'un, mais on n'a pas le droit de se moquer ou de juger ce qui a été formulé, ni de parler avec vulgarité. On doit écouter ce que disent les autres.
Une fois ces règles énoncées, le professeur peut demander si certains élèves ne se sentent pas capables de les respecter, auquel cas ils sont priés de sortir de l'espace de parole. Ils ne seront alors pas autorisés à intervenir pendant l'atelier.

Déroulement de l'atelier

Le professeur annonce le thème de l'atelier : *faut-il autoriser l'usage, par tout un chacun, des outils de cryptographie ?*
Pendant que les élèves réfléchissent quelques instants, le dispositif d'enregistrement audio est déclenché.
Le professeur demande qui veut commencer et donne le « bâton de parole » à l'élève qui souhaite s'exprimer en premier, puis sort de l'espace de parole. Il peut aussi, s'il le souhaite, donner ce bâton de parole à un élève au hasard.
Le bâton passe de main en main. Chacun parle à son tour s'il le désire jusqu'à ce que le temps imparti soit écoulé.
À la fin des 10 minutes, l'enseignant demande si les élèves qui ne se sont pas exprimés pendant l'atelier souhaitent le faire, puis si certains veulent donner leur ressenti par rapport au déroulement de l'atelier : qualité de l'écoute, intérêt de ce qui a été formulé, etc.

Aller plus loin : examen des arguments du débat public sur le chiffrement

Après le déroulement de l'atelier proprement dit, les professeurs reviennent dans le cercle et proposent aux élèves d'écouter l'enregistrement.

Les professeurs proposent aux élèves de lire quelques documents choisis à l'avance (coupures de presse, voir la note pédagogique en début de séance).

Voici un recueil des arguments pour ou contre les plus fréquemment rencontrés dans le débat public sur la cryptographie et la surveillance.

• Arguments pour l'interdiction (ou la limitation) des outils de cryptographie :

– Prévention des actes terroristes : les services de sécurité ont besoin de pouvoir espionner les e-mails, sms, appels téléphoniques des personnes suspectées de vouloir commettre des actes terroristes, afin d'empêcher ces actes ou de trouver les responsables après coup.

– Disparition des réseaux criminels : de nombreux réseaux organisent leurs activités criminelles via Internet : trafic d'armes, trafic de drogue, trafic d'êtres humains, pédophilie. Espionner les communications permet de démanteler ces réseaux.

– Certaines législations prévoient un compromis en autorisant la cryptographie mais en obligeant les prestataires des services de cryptographie (comme, par exemple, les agences qui délivrent les clés publiques et privées) à fournir tous les renseignements nécessaires aux services gouvernementaux.

– « Ceux qui n'ont rien à cacher n'ont pas besoin de crypter leurs communications ».

• Arguments pour la légalisation (et même l'encouragement) des outils de cryptographie pour le plus grand nombre :

– Les terroristes et réseaux criminels utilisent déjà les outils de cryptographie à même de protéger leurs communications. Interdire l'accès à ces outils par le grand public revient à restreindre les libertés sans pour autant lutter efficacement contre les criminels.

– L'analyse de trafic permet déjà d'exploiter de nombreux renseignements grâce aux métadonnées (savoir qui a communiqué avec qui, quand, combien de temps, etc.) sans qu'il y ait besoin de connaître le contenu des messages.

– La cryptographie est la seule façon de garantir le respect de la vie privée à une époque où toutes nos données personnelles transitent par des serveurs informatiques. La convention européenne des droits de l'homme reconnaît d'ailleurs que le respect de la confidentialité des communications est un droit.

– Le développement du commerce, et plus généralement le bon fonctionnement de l'économie, nécessite que les personnes (ou entreprises) puissent communiquer de façon confidentielle en toute confiance. Sans cryptographie, tout le monde pourrait pirater une carte bancaire, ou usurper une identité et ainsi recevoir des renseignements (ou de l'argent) à la place de quelqu'un d'autre.

– De nombreuses professions (journalistes, avocats, huissiers, médecins, cadres commerciaux) sont tenus au secret professionnel et doivent crypter leurs données de façon à empêcher la divulgation d'informations confidentielles sur le web ou dans la presse.

Conclusion

Quel que soit le positionnement de chacun, à la fin de cette séance, sur la nécessité de libérer le chiffrement ou au contraire de l'interdire (ou, cas intermédiaire, de le limiter et l'encadrer), les élèves et professeurs discutent de la façon dont ils peuvent, eux, protéger leurs propres données.

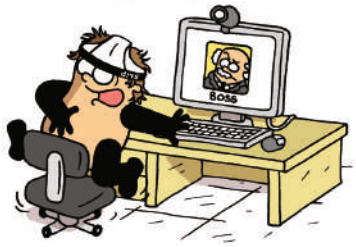
Cette discussion finale peut se faire à l'aide d'un document, comme par exemple celui élaboré par la CNIL (particulièrement bien adapté à un public adolescent), que l'on trouve sur la Fiche 10.

FICHE 10
Dix conseils pour rester Net sur le Web

10 conseils de la CNIL pour rester Net sur le web

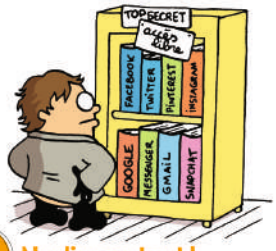
1 Réfléchis avant de publier !

Sur internet, tout le monde peut voir ce que tu mets en ligne : infos, photos, opinions.



2 Respecte les autres !

Tu es responsable de ce que tu publies en ligne alors modère tes propos sur les réseaux sociaux, forums... Ne fais pas aux autres ce que tu n'aimerais pas que l'on te fasse.



3 Ne dis pas tout !

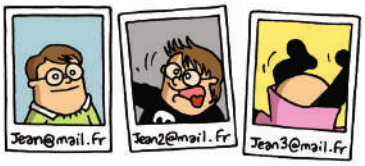
Donne le minimum d'informations personnelles sur internet. Ne communique ni tes opinions politiques, ni ta religion, ni ton numéro de téléphone...

4 Sécurise tes comptes !

Paramètre toujours tes profils sur les réseaux sociaux afin de rester maître des informations que tu souhaites partager.

5 Crée-toi plusieurs adresses e-mail !

Tu peux utiliser une boîte e-mail pour tes amis et une autre boîte e-mail pour les jeux et les réseaux sociaux.



6 Attention aux photos et aux vidéos !

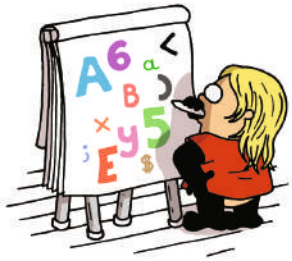
Ne publie pas de photos gênantes de tes amis ou de toi-même car leur diffusion est incontrôlable.

7 Utilise un pseudonyme !

Seuls tes amis et ta famille sauront qu'il s'agit de toi.

8 Attention aux mots de passe !

Ne les communique à personne et choisis-les un peu compliqués : ni ta date ni ton surnom !



9 Fais le ménage dans tes historiques !

Efface régulièrement tes historiques de navigation et pense à utiliser la navigation privée si tu utilises un ordinateur qui n'est pas le tien.

10 Vérifie tes traces !

Tape régulièrement ton nom dans un moteur de recherche pour découvrir quelles informations te concernant circulent sur internet.

CNIL
Commission Nationale de l'Informatique et des Libertés

Retrouvez d'autres conseils et astuces sur www.cnil.fr et sur www.educnum.fr ! #EducNum

Cette ressource est issue du projet thématique *1,2,3... CODEZ !*, paru aux Éditions Le Pommier.

Retrouvez l'intégralité de ce projet sur : https://www.fondation-lamap.org/projets-thematiques.

Fondation *La main à la pâte*
43 rue de Rennes
75006 Paris
01 85 08 71 79
contact@fondation-lamap.org

Site : www.fondation-lamap.org

FONDATION La main à la pâte
POUR L'ÉDUCATION À LA SCIENCE