Informatique débranchée : chiffrement par décalage Comment communiquer secrètement au temps de César ?

1 Contexte

De nos jours, de nombreuses données ont besoin d'être protégées pour faire face à l'espionnage et à la surveillance. Dans un contexte concernant plus les élèves, pouvoir transmettre des messages en étant sûrs de ne pouvoir être reconnu par personne d'autre que le destinataire peut être utile.
Le but de cette activité est de faire découvrir aux élèves une méthode leur permettant de modifier des messages de manière à ce qu'ils ne soient compréhensibles que par le destinataire. C'est ce que l'on nomme la cryptographie.
La méthode que nous allons voir ici est très ancienne puisqu'elle était déjà utilisée par Jules César pour communiquer secrètement avec ses généraux dans l'Antiquité.

2 Descriptif

- Durée : 1 heure
- Matériel requis : tableau de la salle pour pouvoir donner certaines explications aux élèves. Les élèves auront seulement besoin d'avoir de quoi écrire et du papier.
- Compétences requises : bien maîtriser l'alphabet, les élèves doivent par exemple pouvoir être capables de donner assez rapidement la quatrième lettre après la lettre f dans l'alphabet.
- Objectif : comprendre et appliquer la méthode de chiffrement proposée.

3 Cœur de l'activité autour du chiffrement monoalphabétique

3.1 Introduction (environ 15 minutes)

Le but de cette partie est de laisser les élèves chercher par eux-mêmes un moyen de s'échanger entre eux des messages écrits sans qu'ils puissent être reconnus par des personnes extérieures (sans leur donner de méthode afin qu'ils soient confrontés au problème).
Les élèves pourraient être répartis en groupes de quatre et dans chaque groupe former des binômes. Dans chaque binôme, un élève reçoit un mot et les deux élèves doivent se mettre d'accord sur une méthode pour que le premier élève puisse transmettre le mot au second (à l'aide d'un crayon et d'une feuille uniquement) sans que l'autre binôme ne puisse parvenir à le trouver.
L'objectif de cette partie est seulement de faire comprendre aux élèves le problème étudié afin qu'ils en comprennent le principe.

3.2 Explication de la méthode (environ 10 minutes)

Fonctionnement du chiffrement par décalage :

Dans cette méthode, on obtient le texte chiffré en substituant chaque lettre du texte original par une lettre de l'alphabet obtenue toujours de la même manière. On peut par exemple décider que la i ème lettre de l'alphabet sera codée par la i+3 ème lettre de l'alphabet (ici on appelle +3 la "clef").
Dans le cas par exemple d'un décalage à droite, pour les dernières lettres, il faut reprendre au début. Par exemple avec un décalage de +3, A devient D, B est remplacé par E, et ainsi de suite jusqu'à V qui est remplacé par Z, W par A, Y par B et enfin Z par C.

Explication de la méthode aux élèves :

Pour cela, on pourrait écrire sur le tableau un mot simple normalement puis juste en-dessous le même mot avec un décalage de par exemple une lettre et essayer de faire trouver le principe aux élèves. Une fois qu'ils commencent à être sur la piste, le procédé pourra leur être expliqué précisément.
Par exemple :

Mot initial :	A	N	A	N	A	S	et	B	A	N	A	N	E
Clef :													
+1	B	O	B	O	B	T		C	B	O	B	O	F
+2	C	P	C	P	C	U		D	C	P	C	P	G
+5	F	S	F	S	F	X		G	F	S	F	S	J
-1	Z	M	Z	M	Z	R		A	Z	M	Z	M	D
-3	X	K	X	K	X	P		Y	X	K	X	K	B

3.3 Expérimentation (environ 20 minutes)

Une fois la méthode comprise, les élèves peuvent se mettre par groupes comme dans l'introduction pour expérimenter la méthode.
D'abord ils pourront tester des décalages simples afin de bien comprendre le fonctionnement du procédé en s'échangeant des messages codés par binôme. Dans un second temps, en se remettant par groupes de quatre, chaque binôme devra de son côté se mettre d'accord sur une clef puis un élève de chaque binôme devra écrire un message au second, et devra être compris par celui-ci mais pas par les membres de l'autre binôme. Par exemple, le "codeur" devra coder un mot d'une longueur courte (par exemple 5 lettres maximum) et l'autre binôme aura 15 secondes pour le déchiffrer avant de devoir donner le mot au destinataire qui connaît la clef utilisée. Cela permettra aux élèves de réfléchir à des méthodes pour décrypter des messages en cherchant comment détecter la clef utilisée. Les élèves pourront être guidés afin qu'ils s'essayent à des décalages moins évidents que d'une ou deux lettres.
Dans cette partie, les élèves devront donc à la fois chiffrer et déchiffrer des messages simples sans toujours connaître la clef utilisée.

3.4 Déchiffrement (environ 20 minutes)

Pour terminer, les élèves recevront des phrases courtes chiffrées, et leur but sera de les décrypter (sans connaître la clef utilisée). Cela est faisable en essayant de deviner le décalage utilisé, en reconnaissant des motifs (deux lettres identiques consécutives par exemple) ou dans le pire des cas en testant tous les décalages possibles.
Cette partie a pour but de faire comprendre aux élèves qu'il n'est pas bien difficile de déchiffrer un message même si l'on ne connaît pas la clef, et permet donc de leur montrer que cette méthode simple n'est pas viable pour coder des données sensibles.

4 Si une seconde séance était possible : activité autour du chiffrement polyalphabétique

4.1 Les limites du chiffrement monoalphabétique

On peut facilement détecter de combien sont décalées les lettres (par analyse de fréquences ou en testant tous les décalages), il faut donc trouver un codage plus efficace.

4.2 Fonctionnement du chiffrement par décalage polyalphabétique :

Cette fois-ci, au lieu de toujours appliquer le même décalage, on procède d'une manière moins régulière afin de mieux brouiller le texte original.
Il faut d'abord choisir une clef qui est une suite de quelques chiffres (par exemple : 1 2 3). Ensuite, en partant du texte d'origine, pour la première lettre on utilise comme décalage le premier chiffre de la clef, pour la deuxième lettre on utilise le second chiffre de la clef et ainsi de suite jusqu'à arriver à la fin de la clef, on revient alors au début de celle-ci pour savoir de combien il faut décaler la lettre.
Pour la clef 1 2 3, il faut donc décaler la première lettre de 1 lettre, la deuxième lettre de 2 lettres, la troisième de 3 lettres, puis la quatrième lettre de 1, la cinquième de 2 etc.

4.3 Un déroulement possible :

- Rappel rapide du fonctionnement du décalage monoalphabétique.

- Faire comprendre aux élèves qu'il n'est pas dur de décoder un texte sans connaître au préalable le décalage utilisé (puisqu'il suffit de trouver le décalage utilisé pour une lettre comme e par exemple pour pouvoir décoder le message entier).

- Explication au tableau du chiffrement polyalphabétique avec par exemple la clef 1 2 3, qui consiste à décaler la première lettre de 1, la seconde lettre de 2, la troisième de 3, puis de nouveau de 1, puis 2, puis 3 etc.
Par exemple :

	Mot initial :	A	N	A	N	A	S	et	B	A	N	A	N	E
Clef :														
+1,+2,+3		B	P	D	O	C	V		C	C	Q	B	P	H
+2,-1		C	M	C	M	C	R		D	Z	P	Z	P	D
-1,+1,0		Z	O	A	M	B	S		A	B	N	Z	O	E

- Laisser les élèves expérimenter cette méthode par eux-mêmes, les faire se rendre compte qu'il devient bien plus dur de décoder un mot si l'on ne connaît pas la clef puisqu'elle résiste à l'analyse de fréquences.

5 Le lien avec l'informatique

Cette activité permet de faire découvrir aux élèves le concept de cryptographie en expérimentant par eux-mêmes le chiffrement par décalage monoalphabétique dans le cœur de l'activité et polyalphabétique dans une seconde séance.
Le chiffrement par décalage est une des premières méthodes utilisée en cryptographie, elle était notamment utilisée par Jules César (on peut pour cette raison souvent entendre parler de cette méthode sous le nom de "code de César" ou "chiffre de César").
Communiquer secrètement est bien sur encore utile aujourd'hui 2000 ans plus tard, mais pour faire face aux failles du chiffrement monoalphabétique, le chiffrement polyalphabétique a été mis en place. Il pu être utilisé notamment durant la Seconde Guerre mondiale par la machine allemande Enigma.