Atelier

« Secrets de cuisine »

Le but de cet atelier est de découvrir la **cryptographie**. Une brève introduction permet de découvrir l'étymologie du terme « cryptographie », d'en donner une rapide définition et de montrer deux exemples de codes (peu efficaces). Le **chiffrement de César** est introduit dans la première partie. Les élèves constatent, par la manipulation, qu'il est facile de chiffrer et de déchiffrer avec ce code mais qu'il est également facile de le décrypter. Le **chiffrement par substitution** est ensuite présenté dans la deuxième partie. De même, chiffrer et déchiffrer ce code ne pose pas de difficulté particulière. Le calcul du nombre de clefs permet de voir qu'il sera impossible d'utiliser la force brute pour décrypter. Les élèves réussiront tout de même à décrypter un texte à l'aide de l'analyse fréquentielle. Puis une explication très rapide de la **machine Enigma** peut être faite. La fin de l'atelier explique les attentes d'un chiffrement idéal.

Thématique : informatique, cryptographie
Nombre de participant·es : en demi-classe (jusqu'à 16 élèves)
Niveau scolaire : version 1 pour 5ème-4ème et version 2 pour 3ème-2nde
Durée : 1h15

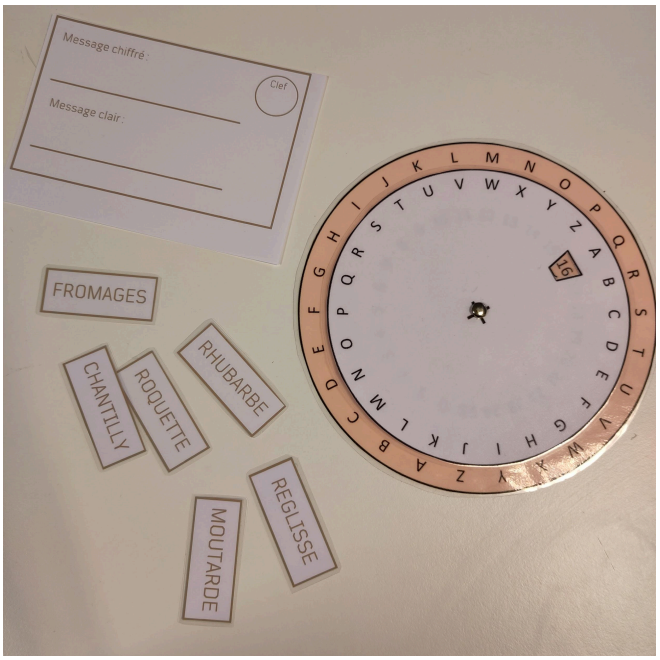
Sommaire

Matériel

Pour tout l'atelier :

- Le diaporama adapté au niveau (5ème-4ème[1] ou 3ème-2de[2]) ;
- Crayons et gommes.

Pour le chiffrement de César :



- Sept roues de chiffrement et de déchiffrement[3] ;
- Mots à chiffrer[4] ;
- Fiches « Message chiffré / Message clair »[5] sur lesquelles les élèves peuvent écrire.

- Messages à décrypter[6] ;
- Fiches « Message clair »[7] sur lesquelles les élèves peuvent écrire ;
- Rouleau de décryptage[8].

[1] Fichier .pdf : « Crypto 5ème-4ème »
[2] Fichier .pdf : « Crypto 3ème-2nde »
[3] Nous avons utilisé les roues de l'activité « Cryptographie débranchée » proposée par la Fondation La Main à la Pâte : https://fondation-lamap.org/sequence-d-activites/cryptographie-debranchee
[4] Fichier .pdf : « Documents à imprimer », page 1
[5] Fichier .pdf : « Documents à imprimer », page 2
[6] Fichier .pdf : « Documents à imprimer », pages 3 et 4
[7] Fichier .pdf : « Documents à imprimer », page 5
[8] Nous avons utilisé les rouleaux de l'activité « Cryptographie débranchée » proposée par la Fondation La Main à la Pâte : https://fondation-lamap.org/sequence-d-activites/cryptographie-debranchee

Pour le chiffrement par substitution :

- Six différents tableaux de substitutions[9] ;
- Fiches « Message chiffré / Message clair »[10] sur lesquelles les élèves peuvent écrire ;
- Mots à chiffrer[11].

- Texte à décrypter ;
- Récapitulatif des fréquences langue française/message.

[9] Fichier .pdf : « Documents à imprimer », pages 8 à 13
[10] Fichier .pdf : « Documents à imprimer », page 7
[11] Fichier .pdf : « Documents à imprimer », page 3

Déroulé de l'atelier

Cet atelier se décline en deux versions : une première pour des classes de 5ème et 4ème et une deuxième pour les classes de 3ème et seconde. Certaines parties de l'atelier sont communes aux deux versions et lorsqu'il y a une différence, cela est indiqué par un code couleur : 5ème-4ème et 3ème-2nde.

Avant de commencer, répartir les élèves en **6 groupes**.

1. Introduction (10 min)

Diapositives 1 à 12

Échanger avec les élèves pour introduire la notion de cryptographie. En fonction des connaissances ou des idées des élèves, donner les informations suivantes dans l'ordre qui semble le plus adapté :

- Étymologie du mot cryptographie : **crypto** (du grec ancien kruptos) signifie « caché » et **graphie** (du grec ancien graphein) signifie « écrire ».
- Un début de définition de la cryptographie : l'art de coder et décoder des messages pour avoir des communications secrètes et protégées entre deux personnes.
- La cryptographie existe depuis l'Antiquité. Le plus ancien document chiffré est une recette secrète de poterie datant du XVIe siècle av. J.-C. Remarque : l'écriture est née en -3000.
- Coder un message pour qu'il soit secret peut servir en temps de guerre (plus généralement, la cryptographie est très répandue dans le milieu militaire), à des communications entre politiques, à protéger des messages d'amour ou plus récemment à protéger toutes les communications privées dans la sphère numérique.

L'article Wikipédia sur la cryptographie donne des explications supplémentaires. En particulier, il est intéressant de comprendre la différence entre cryptographie, cryptologie et stéganographie.

Pour expliquer des concepts de cryptographie, on se place souvent dans le cadre suivant : « Alice veut envoyer un message à Bob ». Cela permet de donner des noms aux personnes qui envoient et reçoivent des messages. Il est intéressant de l'expliquer dès le début de l'atelier aux élèves pour bien différencier les rôles.

Illustrer toute cette introduction avec les deux exemples du diaporama (diapositives 3 à 12) :

- Le premier message est simplement écrit à l'envers et les espaces ont été supprimés ;
- Le deuxième message se chiffre en remplaçant chaque couple de chiffre par la lettre correspondant à la position dans l'alphabet (A correspond à 01, B à 02, etc.).

Il ne faut pas hésiter à utiliser les exemples très rapidement dans l'introduction, surtout si les élèves n'ont pas d'idées puisqu'ils permettent d'illustrer le propos.

Conclure l'introduction avec le fait qu'il existe en réalité énormément de techniques différentes et que certaines sont meilleures que d'autres (les deux exemples présentés ne

sont pas idéaux puisqu'ils ont été cassés en quelques secondes). Dans l'atelier, les élèves vont découvrir des chiffrements connus en s'initiant à la cryptographie et comprendre ce que l'on peut attendre d'un « bon » chiffrement.

2. Chiffrement de César (25 min)

a. Présentation du chiffrement

Diapositives 13 à 19

Le **chiffrement de César** (aussi appelé chiffre de César, code de César) est un classique en cryptographie. Il date du Ier siècle avant J.-C. et doit son nom à Jules César, qui ne l'a pas inventé mais qui utilisait ce chiffrement pour certaines de ses correspondances.

L'idée de ce chiffrement est d'utiliser une lettre pour en coder une autre en faisant un simple **décalage**. Les diapositives 14 à 19 permettent d'illustrer cela par un exemple où le décalage est de 2 lettres. Bien faire comprendre aux élèves que Y et Z sont envoyées sur A et B respectivement. Introduire la notion de **clef** à la diapositive 18 : ici la clef est de 2 puisque le décalage est de 2.

Diapositives 20 à 28

Présenter l'exemple d'utilisation du chiffrement de César. Reprendre le contexte introduit au départ : Alice souhaite envoyer un message à Bob, au départ ce message est dit clair (c'est-à-dire que tout le monde peut le comprendre), elle le chiffre à l'aide de son chiffrement et de la clef (qu'elle doit avoir choisi en amont avec Bob). Pour déchiffrer, Bob va faire l'opération inverse.

b. Chiffrer et déchiffrer

Diapositive 29

Les élèves vont jouer les rôles d'Alice (chiffrer) puis de Bob (déchiffrer). Pour cela, on explique ce qu'iels vont faire :

Pour le rôle d'Alice :

1. Chaque groupe va recevoir un mot (en clair) qu'il va falloir chiffrer avec le chiffrement de César et une fiche pour noter le message chiffré ;
2. Le groupe choisit sa clef et l'écrit sur sa fiche ;
3. Les élèves vont utiliser la roue de César pour chiffrer.

Expliquer le fonctionnement de la roue aux élèves :
Insister sur la différence entre les deux disques, un sert à lire l'alphabet en clair (à l'intérieur) et l'autre sert à lire celui en chiffré (à l'extérieur). Pour chiffrer un message, on lit donc de « l'intérieur vers l'extérieur ». Montrer où l'on lit la clef choisie. Profiter pour demander combien de clefs peuvent être utilisées (il y a 26 décalages possibles donc 26 clefs, mais le

décalage de 0 ne fait pas un message très secret). Préciser qu'une fois la clef choisie, il ne faut plus bouger les disques.

Pour le rôle de Bob :
Une fois que tous les groupes ont noté leur message chiffré, chaque groupe passe sa fiche à un autre pour qu'iels le déchiffrent. Iels utilisent également la roue pour déchiffrer et notent le message en clair sur la fiche.
Faire une vérification dès qu'un groupe a déchiffré.
Insister sur le fait que l'opération de déchiffrement est inverse de celle de chiffrement. Ici, Alice lisait le message clair sur une partie de la roue pour trouver le message chiffré sur une autre partie. Bob doit partir dans l'autre sens et lire son message chiffré sur la deuxième roue pour remonter à la première.

c. Décrypter

Diapositive 30

Les élèves vont maintenant jouer le rôle d'Oscar : celui qui intercepte un message qui ne lui est pas destiné, il cherche donc à le décrypter.

Ajouter un peu de narration :

- 5ème-4ème : « J'ai envoyé des messages chiffrés à votre enseignant·e, mais chaque groupe a réussi à intercepter un message. Évidemment vous avez envie de décrypter ce message ! »
- 3ème-2de : « J'ai envoyé un message chiffré à votre enseignant·e, mais chaque groupe a réussi à intercepter des bouts du message. Évidemment vous avez envie de décrypter ce message ! »

Distribuer à chaque groupe un message chiffré à décrypter et une fiche pour noter le message en clair et la clef. En fonction du niveau, ce ne sont pas les mêmes messages.

Laisser les élèves chercher à décrypter pendant quelques minutes. Certains groupes peuvent avoir de bonnes idées et réussir à décrypter avec la roue. La plupart auront des difficultés. Idéalement, faire verbaliser à un·e élève le fait « qu'il faut tout tester » et que cela est donc long et fastidieux.

Proposer de les aider en distribuant le rouleau à décrypter. En fonction du niveau et du temps, expliquer directement son fonctionnement ou laisser les élèves comprendre le fonctionnement du rouleau.

Fonctionnement du rouleau : aligner les anneaux de papier de sorte à « écrire le message » (nous avons ajouté une ligne noire sur laquelle les élèves mettent les lettres du message pour faciliter) puis, sans faire bouger les anneaux, tourner délicatement le rouleau. Sur chaque anneau se trouve l'alphabet dans l'ordre. À chaque fois que l'on regarde une ligne en dessous, on effectue un décalage de 1. Au final, tous les décalages sont réalisés : il y a forcément le message en clair sur le rouleau.

Vérifier les réponses avec tous les élèves, à adapter en fonction du niveau :

Diapositive 31

Montrer les mots décryptés.

Diapositives 31 et 32

Montrer les bouts de phrase décryptés et faire reconstituer la phrase par les élèves.

Diapositives 32 et 33 / 33 et 34

Faire un bilan sur le chiffrement de César. L'objectif est de conclure que :

- Il est simple d'utilisation pour chiffrer et déchiffrer, ce qui est un avantage ;
- Il n'était pas difficile de décrypter, surtout lorsqu'on a l'idée du rouleau à décrypter qui permet de tester tous les décalages.

Faire sentir aux élèves que la faiblesse du chiffrement de César vient du nombre de clefs qui est trop petit (26 clefs différentes dont une inintéressante avec un décalage de 0). Il faut donc imaginer un chiffrement avec plus de clefs.

3. Chiffrement par substitution (25 min)

a. Présentation du chiffrement

Diapositives 34 et 45 / 35 et 46

Présenter le chiffrement par substitution : on continue à remplacer une lettre par une autre mais on ne fait pas un simple décalage. Faire remarquer qu'une fois qu'une lettre est remplacée par une autre (par exemple A envoyé sur D), aucune autre lettre ne pourra être envoyée dessus (aucune autre lettre ne peut être envoyée sur D).

Utiliser l'exemple du chiffrement du message « casserole » pour expliquer le fonctionnement.

Demander ce qu'est une clef pour ce chiffrement : ce n'est plus un nombre comme pour le chiffrement de César, mais l'ensemble du tableau avec la correspondance entre les lettres.

b. Chiffrer et déchiffrer

Diapositives 46 / 47

De même que pour le chiffrement de César, les élèves vont jouer les rôles d'Alice puis de Bob. Distribuer une substitution à chaque groupe avec une fiche correspondante et un mot à chiffrer. Une fois que les groupes ont fini de chiffrer, faire circuler les fiches et les substitutions (nécessaires puisqu'elles représentent les clefs qu'il faut échanger avant de pouvoir chiffrer/déchiffrer, insister dessus).

Remarque : Dans la vraie vie, il ne faut pas faire circuler la clef avec le message chiffré puisque le décryptage serait trivial. Normalement, il faudrait se mettre d'accord autrement sur la clef (en amont par exemple en choisissant les clefs pour le mois suivant). Cela permet pour les plus grand·es de commencer à instiller la question du passage des clefs entre Alice et Bob.

Une fois le déchiffrage terminé, demander aux élèves si cela était difficile : normalement, il y a un consensus, c'était facile.

c. Le nombre de clefs

Diapositives 47 à 49 / 48 à 59

Rappeler que la faiblesse du chiffrement de César était le nombre de clefs. Indiquer que l'on va chercher le nombre de clefs possible.

- 5ème-4ème : Demander l'avis aux élèves par rapport au nombre de clefs. Avec la diapositive 48, expliquer qu'il y a 403 291 461 126 605 635 584 000 000 clefs pour le chiffrement par substitution (« 403 millions de milliards de milliards »). Expliquer que cela signifie que l'on peut imprimer 403 millions de milliards de milliards de petits tableaux comme ceux utilisés pour chiffrer/déchiffrer et que tous ces tableaux seront différents. Rappeler qu'il y avait 26 clefs pour le chiffrement de César. Il n'est évidemment pas possible de tester toutes les clefs à la main pour décrypter, les élèves imaginent souvent qu'un ordinateur peut tester toutes les clefs rapidement. Demander combien de temps un ordinateur prendrait pour tester toutes les clefs : environ 13 700 000 d'années (s'il est rapide) ! (Diapositive 49).
- 3ème-2de : Demander leur avis aux élèves par rapport au nombre de clefs. Expliquer que l'on va essayer de les compter. Rappeler qu'une clef est un tableau de correspondance entre les lettres.
    - *Diapositives 48 et 49 :* Combien y a-t-il de choix pour la lettre A ? Il y en a 26.
    - *Diapositives 50 à 52 :* Imaginons que l'on fixe A ↔ F, combien reste-t-il de choix pour la lettre B ? Il en reste 25, puisque F est interdit.
    - *Diapositive 53 :* Cette partie est la plus délicate. Il faut faire comprendre qu'il y a au total 26×25 choix pour A et B. Pour chaque A fixé, il y a 25 choix pour B. Puisqu'il y a 26 possibilités pour A, cela fait un total de 26×25.
    - *Diapositive 54 :* Et avec C ? $26 \times 25 \times 24$.
    - *Diapositive 55 :* On peut continuer et on obtient $26 \times 25 \times 24 \times \ldots \times 3 \times 2 \times 1$ choix.
    - *Diapositive 56 :* En mathématiques, $26 \times 25 \times 24 \times \ldots \times 3 \times 2 \times 1$ s'écrit aussi « $26!$ ». Cette notation est plus courte.
    - *Diapositive 57 :* $26! = 403\,291\,461\,126\,605\,635\,584\,000\,000$ de clefs possibles pour le chiffrement par substitution (« 403 millions de milliards de milliards »). Expliquer que cela signifie que l'on peut imprimer 403 millions de milliards de milliards de petits tableaux comme ceux utilisés pour chiffrer/déchiffrer et que tous ses tableaux seront différents. Rappeler qu'il y avait 26 clefs pour le chiffrement de César. Il n'est évidemment pas possible

de tester toutes les clefs à la main pour décrypter, les élèves imaginent souvent qu'un ordinateur peut tester toutes les clefs rapidement.

- *Diapositives 58 et 59 :* Expliquer qu'on peut estimer qu'un très bon ordinateur teste 1 000 000 000 000 clefs par seconde, cela correspond à 13 700 000 d'années.

Le chiffrement par substitution est donc incassable si l'on teste simplement toutes les clefs.

d. Décrypter

Diapositives 50 / 60

Le groupe entier d'élèves va à nouveau jouer le rôle d'Oscar qui intercepte un message, cette fois-ci chiffré avec le chiffrement par substitution. Montrer le texte chiffré et expliquer qu'il vient d'être intercepté. Rappeler qu'on ne peut pas tester toutes les clefs, il faut donc trouver une approche plus maline. Demander aux élèves s'iels ont des idées pour décrypter ce message. L'objectif est de les amener à voir que certaines lettres sont plus présentes que d'autres.

Diapositives 51 et 52 / 61 et 62

Demander si les élèves savent quelles lettres sont très fréquentes dans la langue française ou peu fréquentes. À l'aide de l'histogramme puis du tableau, on explique que la lettre la plus fréquente est le « e ».

Remarques :

- Le titre de cette diapositive possède déjà 8 fois la lettre « e ».
- Les élèves peuvent essayer de faire une phrase sans la lettre « e ». S'il s'agit de « Salut, ça va ? », proposer de faire une phrase intéressante.
- Georges Perec a écrit un livre en 1969, « La Disparition », de 300 pages sans la lettre « e ».
- Ce tableau de fréquence sera évidemment différent pour une autre langue : la lettre « h » par exemple est beaucoup plus fréquente en anglais.

Diapositives 53 et 54 / 63 et 64

Expliquer qu'il faut maintenant regarder les fréquences dans le message intercepté. Utiliser l'histogramme pour que les élèves constatent que la lettre la plus fréquente est le « g ».

Le tableau permet d'expliquer comment obtenir de telles fréquences. Il faut compter le nombre de lettres (488 au total), puis chaque lettre individuellement (par exemple, il y a 96 fois la lettre g). Il suffit ensuite de faire un calcul de pourcentage (ce calcul peut être expliqué si cela est pertinent).

Diapositives 55 à 57 / 65 à 67

Pour essayer de décrypter le message, on remplace les « g » du message par des « e ». Demander aux élèves s'iels voient des choses incohérentes : tout va bien. Le g et le e sont donc identifiés dans le tableau.

Correspondance « g » dans le message ⇔ « e » dans la langue française.

La lettre suivante la plus courante dans la langue française est le « a ». Les élèves supposent que c'est le « z » du message chiffré.

Diapositives 58 et 59 / 68 et 69

Lorsque l'on remplace les « z » par des « a », il y a énormément de mots qui semblent incohérents et inexistants dans la langue française. Utiliser l'exemple du titre.

Diapositives 60 à 64 / 70 à 74

La méthode utilisée s'appelle l'analyse fréquentielle : elle date du IXe siècle (Al-Kindi). Expliquer que les lettres ne sont pas simplement identifiées dans l'ordre décroissant des fréquences (puisqu'il n'y a pas de correspondance a-z). Il faut tester en utilisant ces fréquences comme indications, puis avoir un regard critique.

Expliquer que l'on cherche la lettre « a » : si ce n'est pas un z, c'est peut être un v. Montrer le texte avec ce remplacement. Demander aux élèves s'il y a quelque chose de bizarre ou à l'inverse de rassurant. Remarquer qu'il y a des mots d'une lettre qui sont devenus des « a ». Dans la langue française, en éliminant les lettres seules avant les apostrophes, il y a 3 mots d'une lettre : a, y et ô. Cela est donc un bon signe. On suppose que la lettre v de notre message est en réalité un a.

Correspondance « v » dans le message ⇔ « a » dans la langue française.

La lettre suivante la plus fréquente est le s, demander aux élèves s'iels ont une explication. Une des raisons est évidemment l'utilisation du S pour marquer le pluriel.

Diapositives 65 à 69 / 75 à 79

Le « s » du pluriel étant à la fin des mots, demander aux élèves de chercher une lettre qui revient fréquemment à la fin des mots. Indication : chercher uniquement dans les deux premières lignes. La lettre attendue est le « c ». Montrer de plus qu'il y a dans le titre le mot « pdgigc » que l'on retrouve dans le texte « pdgig » : cela semble à nouveau confirmer notre idée. Remplacer les « c » par des « s ».
Remarquer qu'ici nous avons également utilisé des caractéristiques de la langue française en plus de l'analyse fréquentielle.

Correspondance « c » dans le message ⇔ « s » dans la langue française.

En fonction du temps et de la motivation des élèves :

Si les bonnes conditions sont réunies, proposer aux élèves de continuer à chercher par groupe en distribuant un texte (où les e, a et s du message clair sont déjà décryptés) et les tableaux des fréquences. L'objectif ici n'est pas que les groupes aillent jusqu'au bout du décryptage. Les élèves peuvent explorer leurs idées et constater que le décryptage n'est pas systématiquement fluide.
Sinon, continuer avec le diaporama et le décryptage avec tous·tes les élèves. Dans la suite, cette option est expliquée.

Diapositives 70 à 73 / 80 à 83

Les élèves ont peut être remarqué qu'il y avait également des « d » à la fin des mots, sinon il faut le faire remarquer.

Remarque : si cette étape est trop forcée, il ne faut pas hésiter à expliquer que ce décryptage est guidé. Il serait évidemment possible de le faire autrement, que l'enchaînement n'est pas unique, mais qu'ici par contrainte d'atelier et/ou de diaporama, c'est cette option qui est choisie.

Faire apparaître les « d » à la fin des mots en rouge. En remarquant qu'ils sont toujours après des g donc des e, demander aux élèves quelles lettres sont possibles. L'option qui semble la plus probable est la lettre « r » qui supposerait qu'il s'agit de verbes du premier groupe à l'infinitif. En testant rien ne semble poser problème.

Correspondance « d » dans le message ⇔ « r » dans la langue française.

Il reste une lettre très fréquente dans notre message qui n'a toujours pas été décryptée : la lettre « z ». En utilisant notre tableau, on peut supposer qu'il s'agit soit d'un « i », d'un « n » ou d'un « t ».

Diapositives 74 à 79 / 84 à 89

Demander si la lettre « i » peut convenir. Remarquer qu'il y a « zz » dans le titre et qu'il n'y a pas de mot dans la langue française avec un double i.

Demander si la lettre « n » peut convenir. Puisqu'elle peut être doublée, il faut tester. Laisser les élèves chercher des indices. Le premier mot du texte « -ennre » pose déjà problème. Il ne s'agit pas d'un « n ».

Il reste à tester la lettre « t ». Cette fois-ci, le texte semble beaucoup plus cohérent. Les élèves vont probablement deviner des mots.

Correspondance « z » dans le message ⇔ « t » dans la langue française.

Diapositives 80 à 95 / 90 à 105

La dernière étape du décryptage se fait à l'aide du contexte : depuis le début de l'atelier les messages ont un lien avec la cuisine. Les élèves cherchent d'abord à deviner le titre, iels trouvent facilement : « Recette de crêpes ».

Montrer aux élèves la dernière ligne du texte. Le « — appet-t ! » semble correspondre à un « Bon appétit ! ». En remplaçant, cela est cohérent et permet d'identifier quatre lettres.

Les élèves sont capables de décrypter progressivement le reste du texte, une lettre à la fois. Passer rapidement les diapositives au fur et à mesure des propositions.

Finalement, le texte a été décrypté ! Pourtant, précédemment en calculant le nombre de clefs possibles cela semblait infaisable. En réalité, ce qui est infaisable est de tester toutes les clefs successivement (cela s'appelle de la force brute). Il est possible grâce à l'analyse fréquentielle de contourner ce problème et de décrypter un message.

Remarques :

- Ce message était particulièrement facile à décrypter : il restait les majuscules, la ponctuation, le titre clairement identifié. Sans ces indications, le décryptage est plus difficile.
- Cette méthode ne peut s'appliquer que sur un texte suffisamment long : calculer des fréquences de lettres sur un mot n'a aucun sens. Un message suffisamment court chiffré par substitution est donc (presque) indécryptable.

Diapositives 96 / 106

Le chiffrement par substitution est donc facile à chiffrer et à déchiffrer mais il est possible, avec certaines conditions réunies, de le décrypter.

4. Conclusion et ouverture (10 min)

En fonction du niveau, deux suites d'atelier sont envisagées :

- 5ème-4ème

Expliquer qu'il existe des façons d'utiliser le chiffrement par substitution et d'augmenter la sécurité du message. Puis passer directement à la conclusion.

- 3ème-2de

Demander aux élèves ce qui peut être fait pour éviter qu'Oscar puisse utiliser l'analyse fréquentielle pour décrypter le message. Rebondir sur les idées dans l'objectif d'arriver au fait de changer de substitution à chaque lettre.

Diapositive 107 à 110

Cette idée était utilisée dans la machine Enigma[12] utilisée par l'Allemagne nazie pendant la Seconde Guerre mondiale.

Expliquer brièvement le fonctionnement de la machine :

- Réglages à faire avant d'écrire un message (il s'agit de la clef) : il faut placer 3 *rotors* (qui correspondent chacun à une substitution) et un *reflector* dans la partie haute de la machine et les mettre dans une position précise. Il faut utiliser 10 fils pour relier des lettres deux à deux à l'avant de la machine.
- L'écriture d'un message : une fois les réglages faits, il suffit d'écrire à l'aide des touches le message lettre par lettre. À chaque fois qu'une touche est actionnée, une ampoule s'allume pour indiquer la lettre chiffrée, qu'il faut noter sur une feuille de papier.
- À chaque fois qu'une touche est activée le rotor le plus à droite tourne d'un cran, une fois qu'il a fait 26 crans, celui à sa gauche tourne d'un cran et une fois que celui-ci aura fait 26 crans, celui à sa gauche tourne d'un cran. En faisant ces changements, la substitution est modifiée : chaque lettre du message est chiffrée avec une substitution différente.
- Les réglages de la machine changeaient tous les jours. Pour savoir lesquels utiliser, il fallait avoir une feuille comme celle de la *Diapositive 108*. On peut voir sur chaque ligne : date du jour, numéro des rotors à utiliser et leur ordre, position de départ de chaque rotor et lettres à associer deux à deux.

Pour mieux comprendre le mécanisme d'Enigma, nous conseillons la vidéo de Jared Owen (en anglais). Pour avoir plus d'informations sur le calcul du nombre de clés, nous renvoyons à la vidéo de Numberphile (en anglais).

Puisque la substitution n'est jamais la même, une attaque par analyse fréquentielle est impossible. La machine Enigma a pourtant été décryptée par Alan Turing et son équipe. Iels ont utilisé deux failles : la machine Enigma ne permet pas de chiffrer une lettre par elle-même et l'Allemagne nazie était prévisible sur certains mots dans des messages. Pour mieux comprendre le décryptage de la machine, nous renvoyons à la deuxième vidéo de Numberphile (en anglais). L'équipe a construit une autre machine, appelée la Bombe, qui permet de connaître en une vingtaine de minutes les réglages du jour de la machine Enigma. Le film *Imitation game* explique cette histoire de façon romancée.

Diapositives 97 / 111

Les grandes lignes d'une conclusion :

Les deux méthodes de chiffrement que nous venons de découvrir sont des méthodes historiques qui nous ont permis de comprendre les différentes étapes dans la cryptographie : le chiffrement (Alice) à l'aide d'une clef, la transmission du message, le déchiffrement (Bob) à l'aide de la même clef et le décryptage (Oscar).

[12] Cette machine est inventée en 1919 et pouvait être achetée par toute personne souhaitant s'en procurer une.

Aujourd'hui la cryptographie est très présente dans notre quotidien, sans que l'on ne s'en rende compte : elle permet de sécuriser par exemple nos échanges sur nos ordinateurs ou nos téléphones. Les procédés de cryptographie utilisés sont évidemment plus complexes que ceux qu'on vient de voir et ils demandent des connaissances plus techniques de mathématiques et d'informatique. Et ce sont des méthodes de chiffrement et de déchiffrement qui sont réalisées par des ordinateurs, cela n'aurait pas de sens de le faire « à la main ».

Dans tous les cas, quelle que soit la méthode, on souhaite que le chiffrement soit à la fois facile à chiffrer/déchiffrer et difficile à décrypter, même lorsqu'on connaît le chiffrement utilisé. Par exemple, dans nos ordinateurs, on connaît certains algorithmes cryptographiques utilisés mais cela ne nous aide pas à les décrypter parce qu'on ne connaît pas la clef !

Si ce sujet plaît, il faut indiquer que la cryptographie est enseignée au lycée (Terminale, maths expertes) et peut même être une carrière professionnelle. En effet, la cryptographie est un vrai métier : il demande de faire des mathématiques et/ou de l'informatique à haut niveau.

Diapositives 112

Si les élèves ont posé des questions en ce sens ou si le temps le permet, une petite ouverture peut être faite sur la transmission de clef. Expliquer que tous les chiffrements découverts durant l'atelier sont des chiffrements symétriques : la même clef est utilisée pour chiffrer et déchiffrer. Pour utiliser un tel chiffrement, Alice et Bob doivent se mettre d'accord sur la clef : soit en personne, soit prendre le risque de se l'envoyer en clair. Depuis les années 70, il existe des chiffrements asymétriques qui utilisent des clés différentes : une paire composée d'une clé publique, servant au chiffrement, et d'une clé privée, servant à déchiffrer. Alice et Bob peuvent donc utiliser un chiffrement asymétrique pour s'échanger la clef !