PRÉFACE

KARIM BELABAS
Professeur à l'Université de Bordeaux

La cryptologie, science du secret, n'est plus l'apanage d'une petite élite de diplomates ou de militaires. Ses applications sont partout : dans les ordinateurs personnels, les téléphones portables, les terminaux de paiement, les bornes de validation des transports en commun, et nous les utilisons quotidiennement. La cryptographie asymétrique, à clé publique, inventée au cours des années 70, est en grande partie responsable de cette explosion : elle a permis de supprimer dans les protocoles l'échange initial sécurisé, coûteux, d'une clé secrète. Elle réalise avec une simplicité déconcertante l'idéal de la célèbre, et paradoxale, seconde loi de Kerckhoffs : la solidité du cryptosystème ne dépend en rien de l'obscurité de son fonctionnement. On peut supposer que l'adversaire en connaît tous les rouages, ainsi que l'ensemble des données échangées, sans que cela compromette en rien sa sécurité.

Les protocoles à clé publique utilisent tous des fonctions à sens unique f, souvent d'origine arithmétique. Ces fonctions – telles que $f(x)$ soit facile à calculer pour tout x, mais telles que trouver un antécédent x satisfaisant $f(x) = y$ ait un coût prohibitif, pour tout y «générique» – offrent depuis 40 ans de nouveaux terrains de jeux aux chercheurs en mathématiques et en informatique. Il peut s'agir par exemple de calculer $f(x)$ ou $f^{-1}(y)$ le plus rapidement possible, ou même de démontrer qu'un tel calcul implique la résolution d'un autre problème standard, donnant une sorte de borne inférieure pour sa difficulté. Sans parler du plaisir de construire et étudier de nouvelles fonctions de ce type, qui forment un zoo en constante évolution. Il y a aussi toute une ingénierie liée au développement de matériel informatique dédié (cartes à puces) ou à leur attaque par canaux auxiliaires, qui exploitent des failles dans l'implantation logicielle ou matérielle du protocole étudié par le mathématicien, sans remettre en cause sa sécurité intrinsèque.

Pour l'enseignant de mathématiques, ou d'informatique, la cryptographie est une mine. Le domaine a une riche et longue histoire et

fourmille d'anecdotes captivantes. Ses applications sont variées (chiffrement, authentification, intégrité des données, partage de secret, non-répudiation, preuve sans divulgation d'information, ...), immédiatement compréhensibles, et faciles à motiver. Finalement, en ce qui concerne les protocoles à clé publique (voire à clé privée si on les choisit suffisamment antiques), leur implantation concrète et leur étude utilise la plupart du temps des algorithmes très simples, ne nécessitant que des notions élémentaires d'arithmétique ou de combinatoire, sans trop s'éloigner des programmes officiels de mathématiques du collège ou du lycée. Sans oublier bien sûr un indéniable aspect ludique, à même de susciter l'enthousiasme pour les exercices !

Cette brochure à l'intention des enseignants de mathématiques, réalisée par le groupe «Découvertes Mathématiques» de l'IREM d'Aquitaine, en donne un aperçu convaincant, en présentant de nombreuses activités autour de ce thème, en lien avec les programmes.

Bonne lecture !

Sommaire

Introduction

Cette brochure est le fruit du travail du groupe Découvertes Mathématiques de l'IREM d'Aquitaine.

L'ambition du groupe est de construire des activités pour répondre à une question souvent posée par les élèves, ou même par la société : l'utilité de l'enseignement des mathématiques et plus précisément de la recherche en mathématiques. Conscients de la limite de temps dans nos classes, nous avons voulu que notre travail s'inscrive le plus possible dans les programmes et permette de réinvestir les notions vues dans le cadre du cours.

Le thème de la cryptographie nous a paru idéal pour répondre à ces deux exigences. Le monde moderne et les nouvelles technologies (ordinateurs, internet, téléphones, baladeurs, GPS, transactions bancaires, etc …) font une grande consommation de techniques cryptographiques. Nous sommes entourés, dans la vie de tous les jours, par des applications de la cryptographie. Les élèves le comprennent facilement même s'ils n'y pensent pas spontanément. De plus, la cryptographie peut être présentée à de très nombreux niveaux. Les rudiments sont accessibles à des élèves de collège, et présentent un caractère ludique (crypter, décrypter des messages) qui les intéresse facilement, tout en les confrontant à des notions mathématiques des programmes. Certaines, comme l'arithmétique ou les statistiques (congruences, permutations, calcul de fréquences) peuvent être assez complexes. Cela permet de réinvestir des notions comme la division euclidienne, dans un problème où son utilisation n'est pas guidée par l'intitulé du chapitre.

Concrètement notre travail a consisté à mettre au point un diaporama que nous avons exposé à plusieurs reprises dans des classes, que nous avons fait évoluer en tenant compte des réactions qu'il suscitait. Bien évidemment ce diaporama est adapté en fonction de la classe à laquelle il s'adresse. Nous avons également mis au point diverses activités autour de ce diaporama : codage et décodage de messages, jumelage de deux classes dans deux établissements avec échange de messages cryptés, construction de divers objets permettant de coder facilement (réglette de Saint Cyr), activités sur tableur pour programmer le codage ou le décryptage...
Ces activités ont été pratiquées notamment dans le cadre de l'enseignement d'exploration Méthodes et Pratiques Scientifiques en lycée, d'ateliers de mathématiques en collège et de devoirs maison.

Dans cette brochure, nous vous proposons quelques éléments théoriques et historiques autour de la cryptographie suivis par les activités de classe et le diaporama, accompagnés de commentaires sur les réactions des élèves et les difficultés qu'ils ont parfois rencontrées.
Le diaporama, en versions collège, seconde et terminale S, est disponible sur la page du groupe sur le site de l'IREM d'Aquitaine.

Pour la présentation des éléments de cryptographie en première partie, nous suivons le plan du diaporama, qui est essentiellement chronologique. Nous commençons par parler de la cryptographie 'antique' (avec les scytales), puis du chiffrement de César, du chiffrement affine, du chiffrement par substitution. Nous terminons l'exposé sur la cryptographie symétrique par le chiffrement de Vigenère. Tout ceci est ludique et accessible à des élèves de collège. Nous donnons les outils mathématiques sous-jacents, nous rappelons les propriétés mises en œuvre afin de guider les professeurs. Après un interlude autour de la machine Enigma (une belle histoire d'espionnage qui fascine toujours les jeunes), nous entrons dans le monde de la cryptographie asymétrique. En collège on peut simplement mentionner le chiffrement RSA, alors qu'au lycée, en seconde, on peut le présenter sur un exemple simple et en terminale S spécialité Mathématiques, on est dans le cadre du programme. Nous avons voulu également mentionner les courbes elliptiques (absentes du diaporama), outil plus sophistiqué de cryptographie contemporaine. Elles sont en tout cas un bel exemple d'utilisation de fonctions usuelles (cubiques).
Dans une deuxième partie nous présentons le diaporama commenté.
Nous terminons par les activités qui ont été réalisées en classe, de la $4^{ème}$ à la 2^{nde}. Ce sont parfois des activités très ludiques, avec éventuellement une grosse part de travail manuel, où nous avons essayé de donner quelques pistes pour limiter les difficultés d'ordre matériel. Vous trouverez aussi des exemples d'utilisation du tableur, avec là encore des conseils pratiques.
En annexe, vous trouverez des exemples de documents distribués en classe (en devoir en temps libre, en exercice, en séance de TP sur ordinateur...)
Les chiffrements proposés peuvent être présentés indépendamment les uns des autres (on peut parler du chiffrement de Vigenère sans parler du chiffrement affine ou parler du chiffrement affine seul, …). Nous vous conseillons quand même de commencer par le décalage afin d'habituer les élèves au principe de numérisation de l'alphabet.
Nous espérons que cette brochure vous donnera de nouvelles idées de situations à proposer à

vos élèves. Nous sommes en tout cas tous et toutes persuadés que la cryptographie est un excellent moyen de faire faire des mathématiques aux élèves de façon détendue, presque sans qu'ils s'en rendent compte : ils peuvent ainsi découvrir que les mathématiques peuvent être un jeu.

Au collège

La cryptologie est une source de problèmes de recherche, qui permettent de réinvestir des notions des programmes dans des situations motivantes. Ce thème est particulièrement adapté pour montrer l'utilité de la recherche en mathématiques et ses applications concrètes à la vie courante.

Les activités peuvent être proposées dans le cadre d'ateliers de mathématiques, hors de la classe avec des élèves volontaires.

Mais on peut aussi travailler ces questions en classe, ou dans des devoirs-maison.

	Contenus et capacités attendues	**Utilisation en cryptologie**
6ème	- tables de multiplication	Autres méthodes de cryptologie
6ème à 3ème	- division euclidienne, multiples et diviseurs	Chiffrement par décalage, Vigenère, affine
5ème à 3ème	- statistique (passer des effectifs aux fréquences), utiliser le tableur ou la calculatrice	Cryptanalyse
5ème à 3ème	- additions et soustractions de nombres relatifs	Chiffrement par décalage, affine, Vigenère
5ème à 3ème	- utilisation du tableur	Chiffrement par décalage, affine, substitution, Vigenère. cryptanalyse
3ème	- fonctions : déterminer les images et rechercher des antécédents. - exemples de fonctions définies sur un ensemble fini ou sur $\mathbb{N}$	Chiffrement par décalage, affine, substitution, Vigenère
	- fonctions affines	Chiffrement affine

Au lycée

Comme au collège, la cryptologie au lycée est l'occasion de problèmes de recherche, en lien avec une culture mathématique et des applications concrètes. Elle permet aussi d'utiliser le tableur dans un cadre où il est particulièrement rentable. De plus, les contenus suivants avec leurs capacités attendues sont directement inscrits dans les programmes.

En seconde, l'enseignement d'exploration Méthode et Pratiques Scientifiques contient le thème « sciences et investigation policière » avec un paragraphe « traitement de l'information » où apparaît la cryptologie.

En terminale, la spécialité mathématique prend appui sur la résolution de problème. Sur le thème de l'arithmétique, sont ainsi cités les problèmes de chiffrement et une sensibilisation au système RSA.

	Contenus et capacités attendues	**Utilisation en cryptologie**
2de	- fonctions : déterminer les images et rechercher des antécédents - quelques exemples de fonctions définies sur un ensemble fini ou sur $\mathbb{N}$ sont à donner (commentaire)	Chiffrement par décalage, affine, substitution, Vigenère
	- fonctions de référence : fonctions affines	Chiffrement affine
	- statistique (passer des effectifs aux fréquences), utiliser le tableur ou la calculatrice	Cryptanalyse
MPS	- cryptologie	Toute la brochure hormis Enigma, RSA et l'étude de courbes elliptiques
Term	- compléments sur les dérivées	Courbes elliptiques
Term spécialité	- problèmes de chiffrement (chiffrement affine, chiffrement de Vigenère, chiffrement de Hill)	Chiffrement affine, Vigenère
	- sensibilisation au système cryptographique RSA	RSA

Partie 1
Eléments mathématiques et historiques

1- La scytale :

On a trouvé en Irak des tablettes d'argile datant de 1600 avant Jésus Christ avec des recettes écrites de manière codée (probablement pour raison commerciale).
Mais les premières utilisations de la cryptographie furent essentiellement à but militaire ou diplomatique.

La scytale par exemple fut utilisée par Sparte au 5ème siècle avant Jésus Christ. Elle consiste en un cylindre autour duquel on enroule une bandelette de papier (du parchemin à l'époque). On écrit le message sur le parchemin, sur toute la longueur de la scytale. Lorsqu'on déroule le parchemin, les lettres du message sont « mélangées », et il faut un cylindre du même diamètre que l'original pour déchiffrer le message en enroulant de nouveau la bande autour de ce cylindre (voir photo partie 2).

Plutarque mentionne cette utilisation (Vies des hommes illustres) :
« Voici, du reste, ce que c'est que la scytale. Quand un général part pour une expédition de terre ou de mer, les éphores prennent deux bâtons ronds, parfaitement égaux en longueur et en grosseur, de façon à se correspondre exactement l'un à l'autre, dans toutes les dimensions. Ils gardent l'un de ces bâtons, et donnent l'autre au général: ils appellent ces bâtons scytales. Lorsqu'ils veulent mander au général quelque secret d'importance, ils taillent une bande de parchemin, longue et étroite comme une courroie, la roulent autour de la scytale qu'ils ont gardée, sans laisser le moindre intervalle entre les bords de la bande, de telle sorte que le parchemin couvre entièrement la surface du bâton. Sur ce parchemin ainsi roulé autour de la scytale, ils écrivent ce qu'ils veulent; et, quand ils ont écrit, ils enlèvent la bande, et l'envoient au général sans le bâton. Le général qui l'a reçue n'y saurait rien lire d'ailleurs, parce que les mots, tout dérangés et épars, ne forment aucune suite ; mais il prend la scytale qu'il a emportée, et il roule alentour la bande de parchemin, dont les différents tours, se trouvant alors réunis, remettent les mots dans l'ordre dans lequel ils ont été écrits, et présentent toute la suite de la lettre. On appelle cette lettre scytale, du nom même du bâton, comme ce qui est mesuré prend le nom de ce qui lui sert de mesure. »

Commandant de la flotte spartiate durant la guerre du Péloponnèse (-400), Lysandre réussit par la ruse à attirer les Athéniens à terre où la supériorité spartiate lui donna victoire. Mais il exerça son pouvoir dans les villes conquises avec brutalité, cruauté et injustice. Il fut accusé de brigandage dans les provinces sous sa tutelle et les Éphores qui gouvernaient Sparte lui envoyèrent la scytale de son rappel (ce point peut donner lieu à une recherche historique avec les élèves).

2- Chiffrement par décalage :

César est réputé pour avoir utilisé ce chiffrement (après traduction de son texte en grec, ce qui suffisait certainement déjà à se protéger contre les Gaulois) avec un décalage de 3 lettres.
Il y a 26 (ou 25 si on ne compte pas l'identité) chiffrements par décalage différents en français.

Le décalage de 13 lettres, ou ROT13, est un système effectivement utilisé sur internet : certains forums proposent une touche « ROT13 » pour coder un message (par exemple lorsqu'on veut commenter la fin d'un film sans que ceux qui ne l'ont pas vu soient gênés). La même touche permet alors de décoder le message, puisque 2 × 13 = 26.
Cela peut être l'occasion de voir ce qui se passe lorsqu'on itère des chiffrements par décalage. Pour un alphabet de 26 lettres, en itérant 13 fois un décalage de 2 on retombe sur l'identité, il en est de même pour tout décalage d'un multiple de 2. Pour les autres décalages, il faut les répéter 26 fois pour retrouver l'alphabet d'origine.
On peut aussi se poser la question de ce qui se passe avec un alphabet de 36 lettres (même en restant au français, en effet, 26 signes ne suffisent pas pour écrire un texte avec une accentuation et une ponctuation correctes).
Avec un alphabet de N lettres, chercher au bout de combien d'itérations n un décalage de d redonne le message initial revient à chercher le plus petit entier n tel que $n \times d$ est multiple de N.

$n \times d$ doit donc être le plus petit multiple commun de N et d : $n = \frac{ppcm(N,d)}{d}$ or

$ppcm(N,d) = \frac{Nd}{pgcd(N,d)}$ donc $n = \frac{ppcm(N,d)}{d} = \frac{N}{pgcd(N,d)}$

Exemple : Supposons un alphabet de 36 lettres (N = 36) et un décalage de 20 (d = 20)

Pour trouver le nombre d'itérations nécessaires il y a donc deux méthodes

Soit on calcule *ppcm* (36, 20) = 180 et donc $n = \frac{180}{20} = 9$

Soit on calcule *pgcd* (36, 20) = 4 et donc $n = \frac{36}{4} = 9$

3- Chiffrement affine.

On doit numéroter les lettres de l'alphabet de 0 à 25 (A = 0, B = 1, etc.).
Le principe du chiffrement affine de clé (a,b) est qu'une lettre de numéro x est codée par la lettre de numéro y qui est le reste de la division euclidienne de x par 26. On dit que $ax + b$ et y sont congrus modulo 26, $y \equiv ax + b$ [26].
Mais cette fonction n'est en général pas injective… Il est assez immédiat que $a = 0$ ne conduit pas à un code satisfaisant, et que lorsque $a = 1$, on retrouve un chiffrement par décalage.

Il peut sembler à première vue qu'il existe une infinité de clés possibles (puisqu'il y a une infinité de paires d'entiers). Mais on voit assez facilement (et les élèves aussi!), comme pour le décalage, que le codage par le couple (a , b) est le même que le codage par le couple (a , b +26).
Mais il en est de même avec le codage par le couple (a + 26 , b) : en effet, pour tout entier x,
$(a + 26)x + b \equiv ax + b + 26x \equiv ax + b$ [26]
Cette démonstration n'est telle quelle pas accessible en collège ; mais ils peuvent comprendre l'argument essentiel, qui est qu'on ne change pas le reste de la division euclidienne d'un nombre par 26 en ajoutant un multiple de 26.

La recherche des valeurs de a et b (entiers naturels entre 0 et 25) qui donnent un codage satisfaisant peut s'énoncer ainsi :
a et b sont de mauvais choix si et seulement s'il existe x et x' différents dans Z/26Z tels que $ax' + b \equiv ax + b$ [26], c'est-à-dire $a(x' - x) \equiv 0$ [26].
On sait qu'un tel couple (x ; x') existe si et seulement si a n'est pas premier avec 26 puisque le produit $a(x' - x)$ doit être un multiple de 26.
Comme $a \leq 25$, les mauvaises valeurs de a sont donc 13 et les multiples de 2 inférieurs à 25.
Finalement 12 valeurs de a, et 26 valeurs de b, conviennent. Il y a donc 12×26 chiffrements affines différents.

On peut également, au lycée, s'intéresser au décodage connaissant a et b : en utilisant a^{-1} l'inverse de a modulo 26, le décodage est un chiffrement affine de clé (a^{-1} ; $-ba^{-1}$).
Pour trouver a^{-1} le plus simple est de tester les multiples de a jusqu'à en trouver un congru à 1 modulo 26. Cela peut aussi être une application du théorème de Bézout en spécialité maths de terminale S.

Exemples :

1) si $a = 3$ et $b = 1$ on a $y = 3x + 1$ [26] de sorte que l'image de $x = 10$ est $y = 5$

Cherchons l'image de 5 par la fonction réciproque :

$3 \times 9 = 27$ et $27 = 1$ [26]

donc $a^{-1} = 9$; on retrouve bien que l'image de 5 par la fonction réciproque est $9 \times 5 - 9 = 36$ et $36 = 10$ [26]

2) si $a = 7$ et $b = 2$ on a $y = 7x + 2$ [26] de sorte que l'image de $x = 6$ est $y = 18$

Cherchons l'image de 18 par la fonction réciproque :

$7 \times 15 = 105$ et $105 = 1$ [26]

donc $a^{-1} = 15$ d'où l'image de 18 par la fonction réciproque est

$15 \times 18 - 2 \times 15 = 240 = 26 \times 9 + 6$ et $240 = 6$ [26]

On peut s'interroger sur l'intérêt de ce chiffrement, puisqu'il n'est après tout qu'un chiffrement par substitution particulier. Il présente cependant l'intérêt d'avoir une clé courte (2 entiers), différente de la clé de décodage. Il est de plus l'occasion de se poser des questions mathématiques intéressantes et abordables (quoique difficiles au niveau collège), et d'introduire (sans forcément prononcer le mot) le concept de fonction non injective.

4- Chiffrement par substitution

Il s'agit ici d'une transformation « générale » de l'alphabet, l'unique contrainte étant que chaque lettre doit être codée par une lettre différente (injectivité de la transformation). Ici un codage correspond donc à une permutation de l'ensemble des lettres de l'alphabet : la clé consiste en la donnée de cette permutation, c'est-à-dire du tableau comportant les codages des 26 lettres de l'alphabet (les 25 premières pourraient suffire). De tels codages se trouvent dans certains recueils de jeux, et les élèves y sont souvent familiarisés.

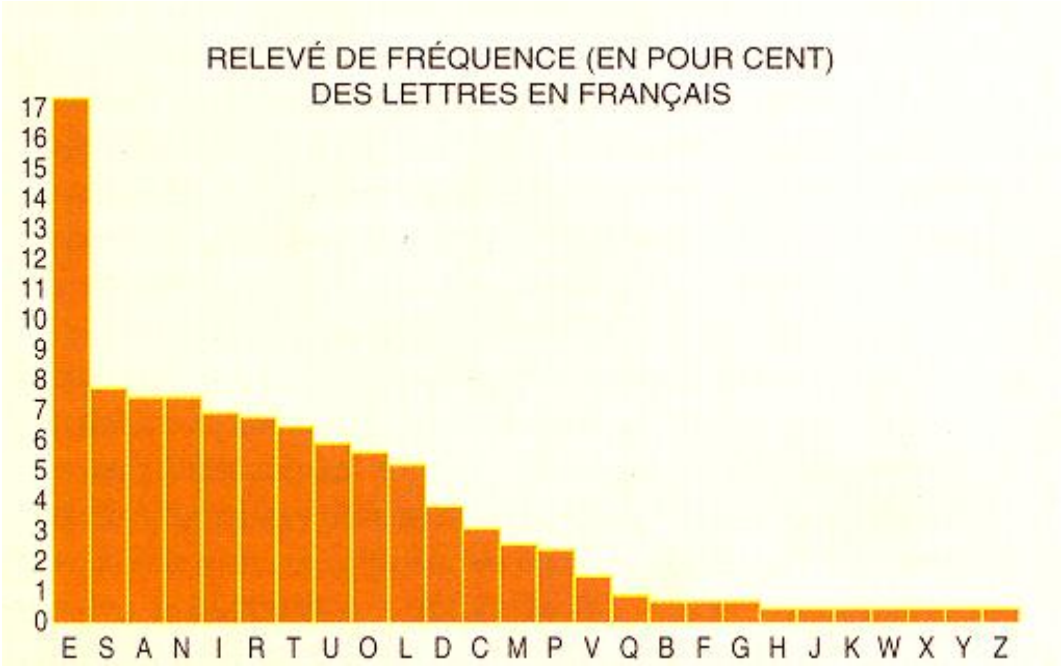
Exemple de code par substitution :

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

On peut pour se familiariser avec ces permutations se poser la question de savoir si en itérant un tel codage on retombe encore sur l'identité. La permutation étant donnée, cela revient en fait à la décomposer en cycles, puis à chercher le *ppcm* de toutes les longueurs de cycle. On peut chercher

des permutations qui itérées deux fois donnent l'identité, des permutations pour lesquelles il faudrait 3 (ou 4 ou…) itérations pour donner l'identité. Ces problèmes tout à fait intéressants mathématiquement s'éloignent cependant du contexte de la cryptographie.

La cryptanalyse d'un tel chiffrement se fait par tâtonnement, en s'aidant d'une analyse de fréquences : on classe les lettres par ordre décroissant de fréquence d'apparition, et on essaye de faire une correspondance avec les fréquences d'apparition des lettres dans la langue du texte : en français, les lettres les plus courantes (on peut faire référence au scrabble) sont, dans l'ordre, E-S-...
Évidemment cet ordre n'est pas *a priori* strictement respecté et il faut être prêt à procéder par essais.
De plus si le texte chiffré est donné en respectant les séparations entre les mots, le travail est grandement facilité. Un texte chiffré est donc généralement donné sans cette structuration en mots, et une analyse de fréquences assez poussée est nécessaire. On peut également utiliser, en plus des fréquences des lettres, les fréquences des lettres répétées (par exemple en français *ss* , *ll* ou *nn*). On y pense assez naturellement lorsqu'on voit des lettres qui se répètent dans le message chiffré.
De manière générale, la cryptanalyse d'un texte chiffré par substitution est assez pénible sans l'aide d'un ordinateur, mais ne pose pas de réel problème.



Cette méthode de cryptanalyse fréquentielle fut publiée pour la première fois par Al Kindi au IX^{ème} siècle, dans son "*Manuscrit sur le déchiffrement des messages cryptographiques*", manuscrit retrouvé en 1987 dans les archives ottomanes d'Istanbul. Né à Bagdad à la période de l'âge d'or des sciences arabes, Al Kindi travailla entre autre à la "Maison de la sagesse" et y acquit une grande renommée. Considéré comme l'un des plus grands philosophes arabes, il a contribué de manière originale à de nombreux autres domaines : mathématiques, physique, médecine, astronomie,

musique …. Savant complet et écrivain prolifique, il publia environ trois cents ouvrages dont certains furent traduits en latin au Moyen Age et dont l'influence fut importante pendant des siècles (ce point peut faire l'objet d'une recherche historique avec les élèves).

5- Chiffrement de Vigenère

Le chiffrement de Vigenère est un système de chiffrement élaboré par Blaise de Vigenère (1523-1596), diplomate français. Au début, son intérêt pour la cryptographie était purement pratique et lié à son activité diplomatique. Par la suite, ayant abandonné sa carrière de diplomate, il se consacra à l'étude de la cryptographie. C'est à ce moment-là qu'il étudia les idées de certains de ses prédécesseurs. Il imagina ainsi un nouveau système de chiffrement qui porte actuellement son nom. Ce chiffrement est une amélioration décisive de celui de César. L'idée principale réside dans l'utilisation non pas d'un, mais de 26 alphabets décalés pour chiffrer un message. Pour son application on utilise souvent une table appelée carré de Vigenère (mais ce n'est pas obligatoire). Ce chiffrement utilise une clef (un mot ou une phrase) qui définit le décalage pour chaque lettre du message (A: décalage de 0, B: décalage de 1, C: décalage de 2, ..., Z: décalage de 25). Comme pour le chiffrement affine, on considère que les lettres de l'alphabet sont numérotées de 0 à 25 (A=0, B=1, etc.). La transformation lettre par lettre se formalise alors simplement par :

Chiffré = (Texte + Clef) modulo 26.

Ceci correspond au « reste de la division euclidienne de (Texte + Clef) par 26 » En fait il suffit d'ajouter les valeurs des deux caractères puis de réduire modulo 26. (Le modulo nous assure que notre résultat sera compris entre 0 et 25). On cherche ensuite la lettre associée au résultat.

Comme la somme Texte + Clef est toujours inférieure à 52, une autre manière est d'écrire bout à bout deux alphabets. Cette méthode permet d'éviter les divisions par 26.

Pour déchiffrer, on retranche la clé au lieu de l'ajouter. En cas de résultat négatif, il suffit d'ajouter 26 pour obtenir le résultat entre 0 et 25, ou, là encore d'écrire un autre alphabet à gauche.

Exemple : Déchiffrage de « DEJUPCVSUJFWJCZME», sachant qu'il a été obtenu avec un chiffrement de Vigenère de clef BAR.

	D	E	J	U	P	C	V	S	U	J	F	W	J	C	Z	M	E
X	**3**	**4**	**9**	**20**	**15**	**2**	**21**	**18**	**20**	**9**	**5**	**22**	**9**	**2**	**25**	**12**	**4**
	B	A	R	B	A	R	B	A	R	B	A	R	B	A	R	B	A
Y	**1**	**0**	**17**	**1**	**0**	**17**	**1**	**0**	**17**	**1**	**0**	**17**	**1**	**0**	**17**	**1**	**0**
X – Y	**2**	**4**	**-8**	**19**	**15**	**-15**	**20**	**18**	**3**	**8**	**5**	**5**	**8**	**2**	**8**	**11**	**4**
modulo26	**2**	**4**	**18**	**19**	**15**	**11**	**20**	**18**	**3**	**8**	**5**	**5**	**8**	**2**	**8**	**11**	**4**
	C	E	S	T	P	L	U	S	D	I	F	F	I	C	I	L	E

La grande force du chiffrement de Vigenère est que la même lettre sera chiffrée de différentes manières (on parle de chiffrement polyalphabétique) suivant sa position dans le message. Ceci rend inutilisable l'analyse des fréquences. Ce chiffrement a résisté trois siècles aux cryptanalystes.

Pourtant il est relativement facile à casser, grâce à une méthode mise au point indépendamment par Babbage et Kasiski (une autre méthode complètement différente a été mise au point plus tard par le commandant Bazeries). Ces méthodes reposent sur le fait que si l'on connaît la longueur de la clef, le problème n'est pas si compliqué : on est ramené à faire un, ou plutôt plusieurs déchiffrements de chiffrements par décalage, la valeur du décalage dépendant de la position dans le texte. Connaissant la longueur L de la clef, on peut séparer le message codé en L paquets (le premier comportant les lettres numéro 1, $1 + L$, $1 + 2L$, etc. du message, le deuxième, les lettres 2, $2 + L$, $2 + 2L$, ...et ainsi de suite) ; chaque paquet a été codé par un même chiffrement par décalage, différent pour chaque paquet. On cherche alors, sur chacun des L sous-messages, la lettre la plus fréquente, qu'on supposera correspondre au E. On détermine ainsi, si le message est assez long, le décalage utilisé sur chaque sous-message, et donc on peut déchiffrer tout le message.

Par exemple, pour une clé de longueur 3, on sépare en groupes de 3 lettres puis on regroupe toutes les premières lettres, toutes les deuxièmes, toutes les troisièmes. On obtient 3 paquets de lettres qu'on décode séparément.

C'est ce principe qu'ont utilisé Babbage et Kasiski, en commençant par déterminer la longueur de la clef, ce qui est la difficulté essentielle. Pour cela, l'idée est de dire qu'une répétition dans un cryptogramme (assez long) n'est pas due au hasard mais provient d'un même groupement de lettres

dans le message en clair, et dans la clef. Par conséquent la distance (en nombre de lettres) entre ces répétitions est un multiple de la longueur de la clef. En analysant ainsi les différentes répétitions que l'on peut trouver dans un cryptogramme, la longueur de la clef sera nécessairement un diviseur du plus grand commun diviseur des distances obtenues. Il reste alors à tester les différences possibilités.

6- La machine Enigma

C'est un ingénieur allemand, Arthur Scherbius qui met au point à des fins commerciales, en 1918, la machine Enigma, servant à encoder des messages. Elle devait servir à sécuriser les transactions bancaires mais sa commercialisation est un échec.

Cependant, la marine allemande s'intéresse à la machine et adopte le modèle D d'Enigma en 1926. L'appareil est ensuite repris par l'armée allemande en 1929. À partir de ce moment, son usage est étendu à toute l'organisation militaire allemande et à une grande partie de la hiérarchie nazie.

Les Allemands pensent que leur système est tellement complexe, que même si une puissance ennemie parvenait à voler une machine Enigma et à comprendre son fonctionnement, ils ne pourraient pas déchiffrer les messages : il y a plusieurs milliards de séquences d'encryptage possibles !

Cependant, un des défauts de la machine est qu'une lettre ne peut jamais être encodée par elle-même, ce qui permet d'éliminer des possibilités. De plus les messages envoyés, notamment par la météo allemande comportent souvent les mêmes mots, ou commencent de la même façon.

Ce que les Allemands ignorent, c'est que les services de contre-espionnage polonais travaillent depuis 1930 sur une méthode de déchiffrage. Avant la guerre, les Polonais ont accumulé un grand nombre d'informations, au point de pouvoir construire une réplique de la machine Enigma. Aidés de moyens électromécaniques (surnommés « bombes de Rejewski »), ils ont déchiffré le code. A ce moment-là, les Allemands encodent leurs messages avec une machine Enigma comportant trois rotors qui permutent les lettres plusieurs fois, mais ils ne changent la clé qu'une fois par mois.

Ainsi, au début de la seconde guerre mondiale, la Pologne peut clairement lire les messages allemands. Lorsque les troupes allemandes envahissent la Pologne, en 1939, les Polonais partagent leurs connaissances avec les services de renseignements britanniques et français.

Dès 1940, les services du code et du chiffre, installés à Bletchley Park peuvent déchiffrer les messages de l'armée allemande. Les alliés récupèrent une véritable machine Enigma, et surtout le manuel de ses instructions, lors du naufrage d'un sous-marin allemand.

En 1942, un nouveau modèle Enigma est mis en service par les Allemands. Pendant onze mois, les alliés ne parviennent plus à déchiffrer les nouveaux messages. Mais alors qu'au début de la guerre, 120 personnes travaillaient à Bletchley Park, en 1944 plusieurs milliers y travaillent. Ce programme Enigma est baptisé "Alan Turing Spearhead Ultra" (Fer de Lance Alan Turing). C'est en effet sous la houlette de ce grand mathématicien (un des inventeurs de l'informatique) que les services secrets alliés réussissent finalement à percer Enigma. Ils perfectionnent le système mis au point par les Polonais, la « Bombe », constituée de plusieurs machines Enigma.

Cette découverte influencera énormément le cours de la Seconde Guerre mondiale et permettra de libérer la voie pour l'Opération Overlord et pour le débarquement en France.

Il est remarquable de noter que jamais les Allemands ne se doutèrent de ce qui se passait car les alliés se sont toujours montrés extrêmement prudents. Ils se sont toujours gardés d'intervenir, au risque de sacrifier du matériel, des militaires ou même des civils, lorsque l'information ne pouvait avoir été obtenue qu'en déchiffrant un message codé avec Enigma. Ce n'est qu'une fois que les archives des armées anglaises ont été rendues publiques que ces faits ont été connus, y compris par les Allemands !

<u>Intéressons nous maintenant au fonctionnement de la machine.</u>

Lorsqu'on regarde une machine Enigma on croirait que c'est une machine à écrire. Son utilisation est particulièrement simple : l'objet est équipé d'un clavier pour la saisie du message, de différentes roues pour le codage, et enfin d'un tableau lumineux pour le résultat. A chaque pression d'une touche du clavier, une lettre du panneau lumineux s'illumine.

La machine est constituée de plusieurs éléments en chaîne :

- le tableau de connexion : il permet d'échanger 12 lettres de l'alphabet, deux à deux, au moyen de fiches.

- les rotors : Ils permettent également d'effectuer des permutations (à chaque lettre entrée, correspond une autre lettre).

Les rotors sont composés, c'est-à-dire mis les uns à la suite des autres. La machine Enigma dispose, au gré de ses évolutions successives, de 3 à 6 rotors différents. Parmi ces rotors, seuls 3 sont utilisés pour le codage, et on a le choix de les placer dans l'ordre que l'on souhaite. De plus ces rotors sont cylindriques et peuvent tourner autour de leur axe. Ils possèdent chacun 26 positions. Ainsi, à chaque fois qu'on a tapé une lettre, le premier rotor tourne d'un cran et la permutation qu'il engendre est changée. Après 26 lettres, il revient à sa position initiale et le second rotor tourne alors d'un cran. On recommence à tourner le premier rotor, et ainsi de suite... Quand le second rotor a retrouvé sa position initiale, c'est le troisième rotor qui tourne d'un cran.

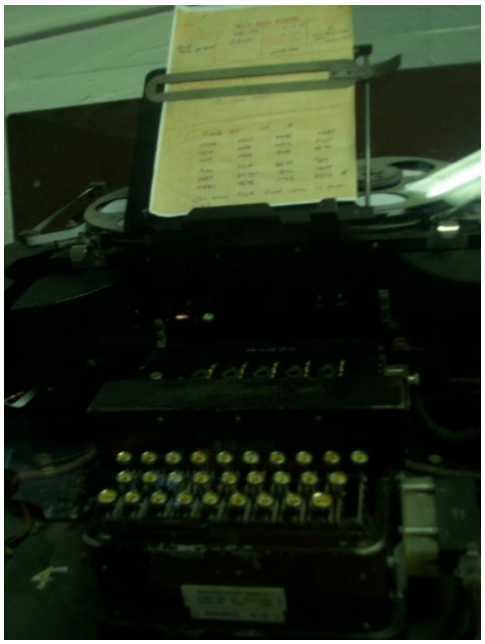
- le réflecteur : Il se situe après les 3 rotors. Il permute une dernière fois les lettres 2 par 2, et les renvoie par le chemin inverse sur les rotors et le tableau de connexion.

Plus précisément, lorsqu'on regarde le nombre de clefs on obtient :

Pour le tableau de connexion, on commence par choisir 12 lettres parmi 26. Le nombre de choix possibles est le coefficient binomial égal à $\frac{26!}{12!14!}$.

Il faut ensuite grouper ces 12 lettres en 6 couples : pour le couple comportant la première lettre, il y a 11 choix possibles. Pour le couple suivant (il comporte la première lettre qui n'a pas encore été choisie), il y a 9 choix possibles. Et ainsi de suite, on obtient : $11 \times 9 \times 7 \times 5 \times 3$. Finalement en tout il y a 100 391 791 500 branchements possibles.

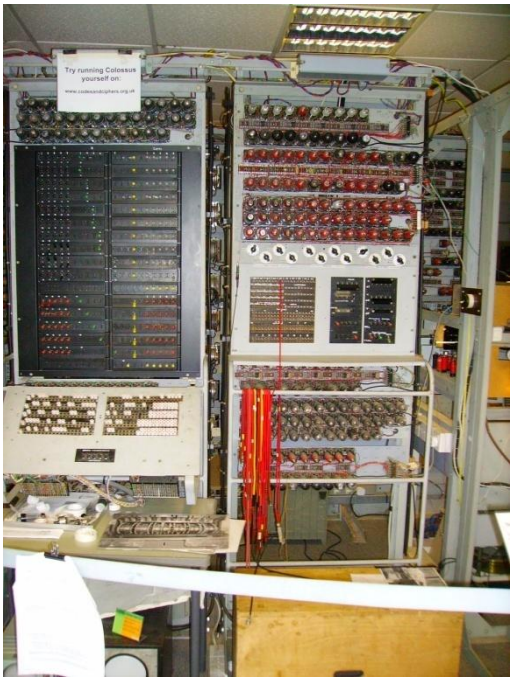
Pour les rotors il y a 17 576 combinaisons : $(26 \times 26 \times 26)$ liées à l'orientation de chacun des trois rotors, ainsi que 6 combinaisons possibles liées à l'ordre dans lequel sont disposés les rotors.



Au total on obtient plus de 10^{16} possibilités avant d'arriver au réflecteur.

Pour terminer il faut noter que le déchiffrage se fait avec la même clef que le codage. C'est-à-dire que pour décoder un message il faut placer Enigma dans la même position initiale que pour le cryptage et taper le message codé. C'est l'une des faiblesses de ce système.

La machine Lorenz est une machine de chiffrement encore plus complexe qu'Énigma. Pendant la seconde guerre mondiale, elle est utilisée exclusivement pour les messages les plus importants à passer entre les maréchaux allemands et le Haut Commandement Central à Berlin. Sa taille implique que ce n'est pas un dispositif portable comme Énigma. Les cryptanalystes l'appellent « le Thon » et les messages codés « les Poissons ». John Tiltman réussit à casser les « Poissons » à Bletchley en 1941 en utilisant des méthodes manuelles qui reposent sur l'analyse statistique. Mais en 1944, les Allemands complexifient le système, le rendant pratiquement impossible à déchiffrer à la main. Une première machine conçue pour casser le code Lorenz, est construite au département de recherche de la Poste par Max Newman, mais elle est lente et peu fiable. Tommy Flowers, un brillant ingénieur électronicien des Postes conçoit et construit « Colossus », une machine beaucoup plus rapide qui utilise 1 500 tubes à vide. La première machine « Colossus » parvient à Bletchley en décembre 1943. C'est la première machine d'informatique numérique électronique au monde, un ancêtre des ordinateurs d'aujourd'hui. « Colossus »[1] peut lire 5 000 caractères par seconde sur une bande de papier qui circule dans la machine à 30 miles par heure (environ 50 km/h). La somme énorme de travail mathématique qui aurait nécessité des semaines ne prend plus que quelques heures.



7- Principe du chiffrement asymétrique à clé publique et exemple du RSA

Dans la cryptographie symétrique, la donnée de la clé de chiffrement permet de trouver facilement la clé de déchiffrement. Il faut échanger la clé avant de communiquer.

Les systèmes que l'on a étudiés précédemment rentraient dans ce cadre ; comme on l'a vu, ils ne sont pas très sûrs : le plus difficile à « casser » est le chiffrement par Vigenère. Pourtant, si le message est beaucoup plus long que la clef, même ce chiffrement ne résiste pas à une attaque par un expert disposant d'un ordinateur. De plus, ces systèmes nécessitent l'échange de la clé par les deux participants : un codage par Vigenère avec une longue clé peut donc être adapté à des communications entre deux chefs d'états, entre deux généraux, mais on voit bien que les besoins modernes de cryptographie (chaîne cryptée, commerce en ligne,...) à beaucoup plus grande échelle

[1] La photo ci-contre représente une réplique de la machine Colossus qui est actuellement exposée à Bletchley Park en Angleterre et qui fonctionne.

vont nécessiter la mise au point d'autres protocoles, plus sûrs mais aussi simplement plus praticables !

Dans la cryptographie asymétrique, il y a une clé pour chiffrer dite clé publique et une clé pour déchiffrer dite clé secrète ou clé privée. La donnée de la clé publique seule ne permet pas de trouver la clé de déchiffrement.
Par exemple, dans le cadre du paiement en ligne, le vendeur fournit une clé publique : tout acheteur peut donc coder son numéro de carte bleue (l'acheteur ne se rend compte de rien, l'ordinateur le fait pour lui à l'aide de cette clé publique) et c'est ce numéro chiffré qui est transmis par le réseau et est récupéré par le vendeur. Lui seul détient la clé privée permettant de déchiffrer. Ainsi tout le monde peut coder, mais une seule personne sait déchiffrer. Comme on le verra dans la section suivante, ce système permet aussi d'authentifier la personne qui envoie un message.

Un exemple de cryptographie asymétrique est le chiffrement RSA qui fut inventé par Rivest, Shamir et Adleman en 1977. Il permet de coder des nombres. Pour coder un texte, il suffit de le transformer en nombres.

Le principe de RSA :
On multiplie deux nombres premiers, leur produit donne la clé publique (celle qui permet de coder). Pour décoder, il faut connaître ces deux nombres premiers. Ainsi pour « casser le code », il faudrait pouvoir retrouver les deux nombres premiers de départ à partir de leur produit. Or si les nombres premiers sont grands cela prend très longtemps ; bien qu'il soit très facile d'écrire un algorithme (il suffit d'essayer les nombres les uns après les autres), c'est impraticable pour de grands nombres (grand signifiant plusieurs centaines de chiffres !). On dit donc que ce problème est « difficile » d'un point de vue informatique.

Comment ça marche ?
Détaillons le principe sur un exemple simple : on prend deux nombres premiers $p = 5$ et $q = 11$.
Bien évidemment ces exemples ne sont pas réalistes car les nombres choisis sont faciles à factoriser !
Pour déterminer la clé publique :
On considère leur produit $n = 55$.
On cherche un nombre qui soit premier avec $(p - 1)(q - 1)$ donc avec 40, nombre que l'on désignera par la lettre e, initiale du mot « exposant ». Le plus petit est 3.
$n = 55$ et $e = 3$ vont constituer la clé publique

Pour déterminer la clé privée, on cherche un inverse de e modulo $(p-1)(q-1)$: ici, on ajoute 1 aux multiples successifs de 40, soit 41, 81, 121, 161, 201, …, et on cherche parmi eux le premier multiple de $e = 3$. C'est $81 = 3 \times 27$. On garde le quotient 27 que l'on désigne par la lettre d, initiale du mot « déchiffrement ».

$d = 27$ sera la clé privée : on a $ed = 1[40]$.

Chiffrement d'un nombre m avec n et e :

On travaille dans l'ensemble des classes modulo n, on ne peut donc coder que les nombres m inférieurs à $n = 55$ par un autre nombre qui sera lui aussi inférieur à 55.

Par exemple, pour coder $m = 18$ on calcule $18^e = 18^3 = 5832$ qu'on divise par 55,

soit $5832 = 55 \times 18 + 2$. Le code est le reste de cette division.

Le code de 18 sera donc 2.

Déchiffrement avec n et d :

On veut déchiffrer 2. On calcule $2^d = 2^{27} = 134\,217\,728$ qu'on divise par 55.

$134\,217\,728 = 55 \times 2\,440\,322 + 18$

Le décodage de 2 est le reste de cette division. On retrouve bien le message initial :18.

Si les nombres p et q sont grands, avec la seule donnée de leur produit n, il est difficile de les trouver. Donc on ne peut pas calculer $(p-1)(q-1)$ donc on ne peut pas trouver d.

Pourquoi ça marche ?

Cela va découler de résultats classiques d'arithmétique que l'on rappelle ci-dessous.

Définition (Congruence) : a est congru à b modulo l'entier n si n divise $a - b$

Ceci revient à dire que a et b donnent le même reste quand on les divise par n, de sorte que la différence est un multiple de n. On le note $a \equiv b\ [n]$ ou encore $a = b$ modulo n

L'ensemble des classes modulo n (de 0 à $n-1$) forme un groupe pour l'addition noté $\mathbb{Z}/n\mathbb{Z}$.

De plus la multiplication des classes est possible : si $a \equiv b\ [n]$ et $c \equiv d\ [n]$ alors $ac \equiv bd\ [n]$

Égalité de Bezout : Soit $d = \text{PGCD}(a,b)$ alors il existe deux entiers relatifs u et v tels que $au + bv = d$.

Preuve : On effectue l'algorithme d'Euclide pour trouver le PGCD d de a et b. Si $a>b$, on obtient ainsi une suite d'égalités $a = bq_1 + r_1$, $b = r_1q_2 + r_2$,..., $r_{n-2} = r_{n-1}q_n + d$.

On obtient une égalité de Bezout entre r_{n-2} et r_{n-1} : $d = r_{n-2} - q_n r_{n-1}$. On utilise alors l'avant-dernière égalité pour écrire r_{n-1} en fonction de r_{n-2}et r_{n-3} , ce qui donne alors une égalité de Bézout entre r_{n-3} et r_{n-2}. Par une récurrence montante, on arrive bien ainsi à une égalité de Bézout entre *a* et *b*.

Théorème de Bézout : Deux nombres *a* et *b* sont premiers entre eux *si et seulement si* il existe deux nombres entiers *u* et *v* tels que $au + bv = 1$.

En effet d'après l'égalité de Bézout, si *a* et *b* sont premiers entre eux il existe deux nombres entiers *u* et *v* tels que $au + bv = 1$; réciproquement on suppose qu'il existe deux nombres *u* et *v* tels que $au + bv = 1$. Soit *d* un diviseur de *a* et *b,* alors *d* divise $au + bv$, donc *d* divise 1 : on en déduit $d = 1$. Donc *a* et *b* sont bien premiers entre eux.

Corollaire : L'ensemble des inversibles pour la multiplication dans $\mathbb{Z}/b\mathbb{Z}$ est l'ensemble des nombres premiers avec *b*.

Preuve : si *a* et *b* sont premiers entre eux alors d'après le théorème de Bezout il existe *u* et *v* tels que $au + bv = 1$; donc le nombre $(au - 1)$ est divisible par *b* ce qui signifie que au est congru à 1 modulo *b* autrement dit la classe de au est la classe de 1 modulo *b*.

Par définition, cela signifie que *a* est inversible dans $\mathbb{Z}/b\mathbb{Z}$ et son inverse est la classe de *u.*

Donc *a* premier avec *b* implique que *a* est inversible dans $\mathbb{Z}/b\mathbb{Z}$.

Réciproquement, si *a* est inversible dans $\mathbb{Z}/b\mathbb{Z}$, il existe *u* tel que la classe de au est la classe de 1.

Donc $au - 1$ est divisible par *b,* c'est-à-dire qu'il existe *v* tels que $au - 1 = bv$. On peut appliquer le théorème de Bezout, et on en déduit que *a* et *b* sont premiers entre eux.

Définition de l'indicatrice d'Euler : $\varphi(n)$ est le nombre d'entiers inversibles dans $\mathbb{Z}/n\mathbb{Z}$.

Ce sont des entiers plus petits que *n*. D'après le résultat précédent, ce sont exactement tous les entiers entre 1 et $n - 1$ premiers avec *n* (0 n'est jamais inversible).

L'ensemble des inversibles dans $\mathbb{Z}/n\mathbb{Z}$ forme un groupe pour la multiplication ; $\varphi(n)$ est l'ordre de ce groupe, c'est à dire son cardinal.

Théorème 2 : Si *p* est premier alors $\varphi(p) = p - 1$.

Preuve : Il s'agit de montrer que tous les éléments de $\mathbb{Z}/p\mathbb{Z}$ sont inversibles sauf 0. Or tous les nombres entre 1 et $p - 1$ sont premiers avec *p,* ils sont donc tous inversibles. 0 n'est pas inversible ; il y a donc $p - 1$ inversibles dans $\mathbb{Z}/p\mathbb{Z}$.

Théorème : Si $n = pq$ avec p et q premiers alors $\varphi(n) = (p-1)(q-1)$

Preuve : Les non inversibles dans $\mathbb{Z}/n\mathbb{Z}$ sont les multiples de p ($0, p, 2p, \ldots, (q-1)p$) et les multiples de q ($0, q, 2q, \ldots, (p-1)q$). Il y en a $q + p - 1$ distincts. Attention à ne pas compter 0 deux fois ! On a donc $\varphi(n) = pq - q + p - 1 = p-1\ q-1$.

En fait ce théorème est un cas particulier de la propriété suivante (qui se démontre avec le lemme des restes chinois) : Si a et b sont premiers entre eux alors $\varphi(ab) = \varphi(a)\varphi(b)$.

Théorème d'Euler Fermat :

Si a et n sont premiers entre eux (autrement dit a est inversible dans $\mathbb{Z}/n\mathbb{Z}$) alors $a^{\varphi(n)}$ est congru à 1 modulo n.

Preuve : L'ensemble des inversibles dans $\mathbb{Z}/n\mathbb{Z}$ est un groupe fini pour la multiplication, donc il existe un entier k (appelé ordre de a) tel que a^k est congru à 1 modulo n. Or l'ordre d'un élément d'un groupe divise toujours l'ordre du groupe : on en déduit qu'il existe un entier m tel que $\varphi(n) = mk$.

Par conséquent, $a^{\varphi(n)} = a^{mk} = 1^m = 1$.

Exemple $n = 10 = 2 \times 5$ $\varphi(10) = (2-1)(5-1) = 4$

$\mathbb{Z}/10\mathbb{Z} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$.

Les inversibles sont les classes des nombres premiers avec 10 soit {1, 3, 7, 9}

Vérification : $1 \times 1 = 1$; $3 \times 7 = 21$; $9 \times 9 = 81$; le reste est bien 1 dans la division par 10,

Ainsi 1 et 9 sont leurs propres inverses et 3 et 7 sont inverses.

Vérification de l'égalité de Bézout :

$$1 \times 11 + 10 \times -1 = 13 \times 7 + 10 \times -2 = 19 \times 9 + 10 \times -8 = 1$$

Enfin calculons les nombres $a^{\varphi(n)}$: $1^4 = 1$ et $3^4 = 81$ etc. Ils sont tous congrus à 1 modulo 10.

Corollaire : Si p est un nombre premier alors quel que soit l'entier a, a^p est congru à a modulo p.

Preuve : $\varphi(p) = p - 1$ donc si a est premier avec p, a^{p-1} est congru à 1 modulo p donc a^p est congru à a modulo p. Si a n'est pas premier avec p, a et a^p sont des multiples de p donc sont congrus tous les deux à zéro.

Reprenons l'exemple du codage RSA avec $p = 5$ et $q = 11$ (et leur produit $n = 55$).

On peut coder un nombre m (par exemple $m = 18$) dans l'ensemble $\{0,1,2,...,54\} = \mathbb{Z}/55\mathbb{Z}$

$\varphi(n) = (p-1)(q-1) = 40$. Donc l'ensemble $\mathbb{Z}/55\mathbb{Z}$ a 40 éléments inversibles.

On cherche un nombre e premier avec $\varphi(n)$c'est à dire avec 40, pour qu'il soit inversible modulo $\varphi(n)$, donc inversible dans $\mathbb{Z}/40\mathbb{Z} = \{0, 1, 2, 3, 4, 5, 6..... 39\}$. Par exemple $e = 3$.

Comme e et $\varphi(n)$ sont premiers entre eux, il existe u et v tels que $eu + \varphi(n)v = 1$.

On trouve, par exemple avec l'algorithme d'Euclide que $3 \times 27 + 40 \times -2 = 1$.

Donc $3 \times 27 \equiv 1$ [40]. Ainsi $e = 3$ est inversible dans $\mathbb{Z}/40\mathbb{Z}$, et son inverse est $u = 27$.

Précédemment cet inverse a été appelé la clé privée notée d au lieu de u.

Maintenant, abordons la démonstration.

On veut coder le message m.

Soit $n = pq$ avec p et q premiers. Soient e un inversible modulo $\varphi(n)$ et d son inverse. Il existe donc un entier k tel que $ed = 1+\varphi(n)k$

Soit r, le code de m, c'est à dire le reste de la division de m^e par n. Pour montrer que le décodage fonctionne, il faut vérifier que le reste de la division de r^d par n est m. Pour cela on va montrer d'abord que le reste des divisions de $(m^e)^d$ par p et par q est m.

$(m^e)^d = m^{ed} = m^{1+\varphi(n)k} = m^{k(q-1)p+1-k(q-1)}$

D'après le corollaire du théorème de Fermat, $m^{k(q-1)p}$ est congru à $m^{k(q-1)}$ modulo p

donc $m^{k(q-1)p+1-k(q-1)}$ est congru à $m^{k(q-1)+1-k(q-1)}$ modulo p. Finalement, on a bien $(m^e)^d$ congru à m modulo p. De même, on montre que $(m^e)^d$ congru à m modulo q.

$(m^e)^d - m$ est donc multiple de p et de q. Comme p et q sont premiers entre eux, on en déduit que $(m^e)^d - m$ est multiple de n. Donc $(m^e)^d$ est congru à m modulo n.

Or r est congru à m^e modulo n donc r^d est bien congru à m modulo n.

Interlude sur l'exponentiation rapide

Dans le système RSA, on se retrouve assez vite pour chiffrer et déchiffrer à devoir calculer des expressions du type x^y [N] où y peut être assez grand. Or si on calcule d'abord x^y puis qu'on fait la division euclidienne, il est fort possible qu'on dépasse la capacité d'un ordinateur, et ce n'est pas nécessaire.

On peut en fait utiliser le fait que si $x_1 = a$ [N] et si $x_2 = b$ [N] alors $x_1x_2 = ab$ [N].

Exemple : pour calculer 5^{100} modulo 18

5^{100} est un nombre gigantesque.

Mais $5^2 = 25 = 7[18]$

Donc $5^4 = (5^2)^2 = 49$ [18], et finalement $5^4 = 13$ [18]

De même $5^8 = 13^2$ [18] donc $5^8 = 7$ [18]

$5^{16} = 13$ [18]

$5^{32} = 7$ [18]

et enfin $5^{64} = 13$ [18]

Finalement $5^{100} = 5^{(64+32+4)} = 13\times7\times13$ [18], donc $5^{100} = 13$ [18]

Le principe de manière générale est d'écrire l'exposant *y* en base 2 (ici 100 = 64 + 32 + 4) et de calculer les puissances x^2, x^4 etc , en élevant au carré à chaque fois et en calculant le reste de la division euclidienne par *N* à chaque étape. Les nombres qu'on manipule ainsi restent petits.

8- Deux autres interludes.

Partage d'un secret

Si on ne peut pas partager de clé publique, on peut imaginer un système où Alice et Bob ont chacun une clé privée. On peut concevoir concrètement un tel système avec un coffre dans lequel Alice met son message et ferme avec son cadenas. Bob récupère alors le coffre, le ferme à l'aide de son propre cadenas et le renvoie à Alice qui enlève alors son cadenas et renvoie une dernière fois le coffre à Bob. Il peut alors l'ouvrir et découvrir le message.

Le message n'est jamais accessible à quelqu'un d'autre qu'Alice ou Bob puisque le coffre circule toujours fermé.

Le message dans le coffre peut par exemple être une troisième clé privée, qui sera alors commune à Alice et Bob, et pourra ensuite leur servir pour chiffrer par une méthode de cryptographie symétrique (avec Vigenère par exemple).

Malheureusement il n'est pas toujours matériellement possible de s'échanger des coffres...

Une autre méthode, plus mathématique, permet aussi, à l'aide de deux clés privées, de se mettre d'accord sur une troisième clé en faisant en sorte qu'elle ne soit jamais transmise en clair. Il s'agit du partage de secret de Diffie Hellman. A la différence du système précédent à base de cadenas, ici ni Alice ni Bob ne connaissent la troisième clé à l'avance.

Alice et Bob commencent par se mettre d'accord (cela peut être par des messages publics) sur un nombre *N*, et sur un nombre *p* premier avec *N*. Ils choisissent ensuite secrètement chacun un nombre (*a* et *b*), sans le dire à personne. Alice transmet le reste r_A de la division euclidienne de p^a

par N à Bob. Bob transmet le reste r_B de la division euclidienne de p^b par N à Alice.

Alice peut maintenant calculer le reste de la division euclidienne de $(r_B)^a$ par N, et Bob peut lui aussi calculer le reste de la division euclidienne de $(r_A)^b$ par N. L'intérêt est que ces deux nombres sont égaux. En effet, $(r_A)^b = (p^a)^b = (p^b)^a = (r_B)^a$ modulo N (On utilise ici la commutativité de l'opération de multiplication dans $\mathbb{Z}/N\mathbb{Z}$). Ce nombre commun peut donc ensuite servir de clé privée commune c, pour un chiffrage (symétrique), à l'aide de Vigenère par exemple. En effet, même si p est connu de tout le monde, la connaissance des restes de la division euclidienne de p^a par N et de p^b par N ne permet pas (si les nombres sont grands) de trouver a et b. Seuls Alice et Bob peuvent donc déterminer la clé c.

Exemple : $N = 31$, $m = 8$. Alice choisit $a = 3$, Bob choisit $b = 4$.

Alice envoie alors $r_A = 16$ et Bob envoie $r_B = 4$.

Alice calcule alors $(r_B)^3 = 4^3 = 2$ modulo 31

Bob calcule de son côté $(r_A)^4 = 16^4 = 2$ modulo 31

Alice et Bob se sont donc finalement mis d'accord sur la clé 2. Aucun des deux ne le savait à l'avance.

Remarque : si on ne prend pas m premier avec N, on pourrait obtenir 0 comme clé, ce qui pourrait poser problème. Mais si on choisit pour N un nombre premier, il suffit de choisir m plus petit que N pour que cela n'arrive pas.

Méthode de chiffrement El-Gamal

Il y a bien d'autres protocoles de chiffrement asymétrique que RSA. La méthode d'El-Gamal est encore plus simple que RSA, et elle fournit de plus une bonne introduction à la cryptographie à l'aide de courbes elliptiques qu'on verra plus loin.

Bob choisit un nombre premier p (assez grand) et un nombre d strictement plus petit que p, qui seront publics. Il choisit aussi un entier s qui sera secret, et il calcule $h=d^s$ modulo p. La clé publique sera alors (p, d, h) et la clé secrète s.

Si Alice souhaite envoyer un nombre m inférieur à p à *Bob*, elle commence par choisir un entier a, comme elle veut, puis elle calcule $r = m\, h^a$ modulo p, ainsi que $t = d^a$ modulo p. Elle transmet alors ces deux nombres (r,t) à Bob.

Puisque Bob connaît s, il peut alors calculer t^s. Comme p est premier, le théorème de Bézout nous assure que ce nombre a un inverse u dans $\mathbb{Z}/p\mathbb{Z}$ (il existe deux entiers u et v tels que $u\, t^s + v\, p = 1$, et cette égalité nous garantit bien que le reste de la division euclidienne de $u\, t^s$ par p est 1). Par construction $t^s = d^{(sa)} = h^a$ modulo p. Donc toujours modulo p, on a $r\, u = m\, h^a\, u = m\, t^s\, u = m$. Ainsi, en calculant le reste de la division euclidienne de $r\, u$ par p, Bob retrouve m. C'est là encore

la commutativité de la multiplication dans $\mathbb{Z}/p\mathbb{Z}$ qui intervient.

Exemple :

Bob choisit $p = 23$, $d = 18$, $s = 3$; alors $h = 13$.

Alice souhaite envoyer le nombre $m = 12$. Elle choisit $a = 5$.

Elle transmet alors $r = 2$ et $t = 3$.

Bob calcule alors $t^s = 27$. Il trouve par l'algorithme d'Euclide $1 = -7\times23 + 6\times27$ et il en déduit donc $u=6$.

Le reste de la division euclidienne de $r\,u = 12$ par p est alors 12 et Bob retrouve bien le message m.

Fondamentalement, ce système cryptographique très simple est basé sur le fait que $(\mathbb{Z}/p\mathbb{Z})^*$ munie de la multiplication constitue un groupe commutatif. La cryptographie à l'aide de courbes elliptiques qui sera abordée plus tard est basée sur la même idée, mais le groupe sur lequel on travaille est alors plus abstrait.

9- Quelques mots sur l'authentification et la signature électronique.

Jusqu'à présent nous nous sommes focalisés sur le problème de la confidentialité : comment transmettre un message de sorte qu'un espion éventuel ne puisse pas lire le message. La cryptographie asymétrique permet de répondre également facilement à un problème voisin, celui de l'authentification : ce qui est ici important est que celui (Bob) qui reçoit et déchiffre le message soit certain qu'il a bien été envoyé par la bonne personne (Alice), et pas par Ariane qui prétendrait être Alice.

On va dans un premier temps oublier le problème de la confidentialité et s'intéresser uniquement à l'authentification. Il faut alors considérer que c'est l'envoyeur (Alice) qui dispose de deux clés : une clé secrète, et une clé publique. La clé secrète lui permet de coder le message, la clé publique permettra à Bob de déchiffrer (le rôle des deux clés est inverse par rapport au problème de confidentialité). Alice va envoyer le message en clair M (rappelons qu'ici la confidentialité n'est pas le problème), ainsi que le même message codé à l'aide de sa clé secrète, C. Bob peut alors décoder C à l'aide de la clé publique et vérifier qu'il retrouve bien M (qu'Alice lui a aussi envoyé) : cela prouve que c'est bien Alice qui a envoyé les deux, puisqu'elle seule pouvait effectuer le codage.

Exemple avec RSA : on suppose que la clé publique de Alice est ($N_A = 91$, $e_A = 5$) et sa clé secrète $d_A = 29$, obtenue à l'aide de la décomposition $91 = 13 \times 7$. Elle souhaite envoyer le message M = 18 à Bob et lui certifier que le message vient d'elle.

Elle chiffre M à l'aide de sa clé secrète et obtient C = 18^{29}[91] = 44

Elle envoie (18,44) à Bob.

Celui-ci sait donc que M=18, et vérifie que c'est bien Alice qui a envoyé le message en calculant 44^5[91] = 18.

Pour avoir un système avec confidentialité et authentification, Alice et Bob doivent avoir chacun une clé publique et une clé secrète, et Alice doit appliquer la méthode précédente, mais en chiffrant tous ses envois avec la clé publique de Bob.

Par exemple, dans le cas de RSA, les rôles des deux clés publiques (*e*) et secrètes (*d*) sont symétriques, les deux opérations (chiffrage et déchiffrage) consistant toutes deux à élever à une certaine puissance. Ainsi, imaginons qu'Alice ait une clé publique (N_A,e_A) et une clé secrète d_A, et Bob une clé publique (N_B, e_B) et une clé secrète d_B. Alice souhaite envoyer le message M et elle veut prouver à Bob que le message vient bien d'elle.

Elle calcule $c_B = M^{e_B}$ [N_B] (message chiffré par la méthode de Bob), puis utilise sa clé secrète pour calculer $c_{BA} = {c_B}^{d_A}$[N_A] (message chiffré par les deux méthodes successivement).

Elle envoie alors (c_B,c_{BA}). Bob peut alors déchiffrer c_{BA} à l'aide de la clé publique d'Alice : il calcule ${c_{BA}}^{e_A}$[N_A] et il peut vérifier que c'est bien égal à c_B : c'est donc bien Alice qui a envoyé le message.

Il peut finalement déchiffrer c_B à l'aide de sa clé secrète en calculant ${c_B}^{d_B}$[N_B], et il obtient M.

Exemple : (N_A = 91, e_A = 5, d_A = 29) et (N_B = 55, e_B = 3, d_B = 27) ; M = 18.

Alice chiffre 18 avec la clé publique de Bob : elle obtient $c_B = 18^3$ [55] = 2.

Elle rechiffre alors c_B avec sa clé secrète : elle obtient $c_{BA} = 2^{29}$ [91] = 32.

Elle envoie le couple (2;32) à Bob.

Bob déchiffre 32 avec la clé publique d'Alice et obtient 32^5 [91] = 2 : il retrouve bien ce que lui a envoyé Alice : le message est authentifié.

Il peut alors enfin décoder à l'aide de sa clé secrète d_B et obtenir le message 2^{27} [55] = 18.

10- Quelques mots sur les courbes elliptiques

Le principe à la base de la cryptographie asymétrique est la notion de fonction à sens unique. C'est à dire une fonction

- facile à calculer
- difficile à inverser, au sens où on ne dispose pas d'algorithme permettant le calcul de l'antécédent d'un nombre en un temps raisonnable.

C'est le cas en particulier pour RSA : le calcul à une certaine puissance modulo un entier n est facile mais pour décoder il faut trouver p et q tels que $n = pq$, ce qui est très long, même pour un ordinateur puissant, si n est très grand. Ceci explique que de gros moyens en cryptographie sont mis sur la recherche d'algorithmes de factorisation les plus rapides possibles.

On peut trouver d'autres fonctions difficiles à inverser dans le cadre de l'arithmétique dans $\mathbb{Z}/n\mathbb{Z}$, elles permettent alors de construire d'autres systèmes que le système RSA.

Mais pour compliquer un peu plus, on peut travailler sur des objets plus sophistiqués que les entiers : des points sur des courbes elliptiques. Cela donne une méthode de cryptographie plus sûre encore que RSA.

Une courbe elliptique (affine) est l'ensemble des points de coordonnées réelles (x , y) où x et y vérifient :

$y^2 = x^3 + ax + b$ avec $4a^3 + 27b^2 \neq 0$

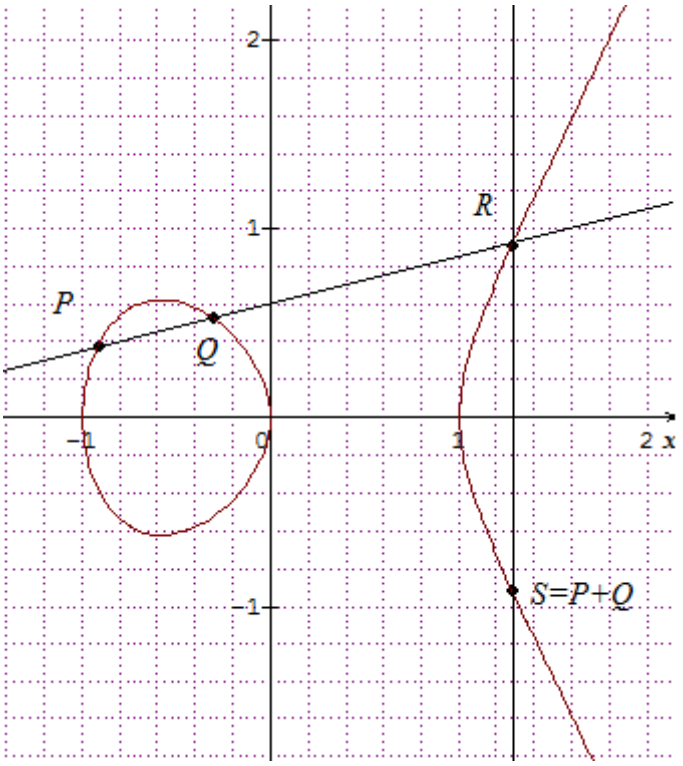
Comme leur nom l'indique, il y a un lien entre les courbes elliptiques et l'ellipse. On obtient une représentation paramétrique des courbes elliptiques avec des fonctions elliptiques, elles-mêmes liées aux intégrales elliptiques qui servent à calculer la longueur de l'ellipse. Weierstrass (1815-1897) a exhibé les courbes elliptiques en poursuivant les travaux menés par Abel (1802-1829) sur les intégrales elliptiques.

Cette courbe est bien évidemment toujours symétrique par rapport à l'axe des abscisses.
Les solutions de l'équation $x^3 + ax + b = 0$ sont les abscisses des points d'intersection de cette courbe avec l'axe des abscisses.

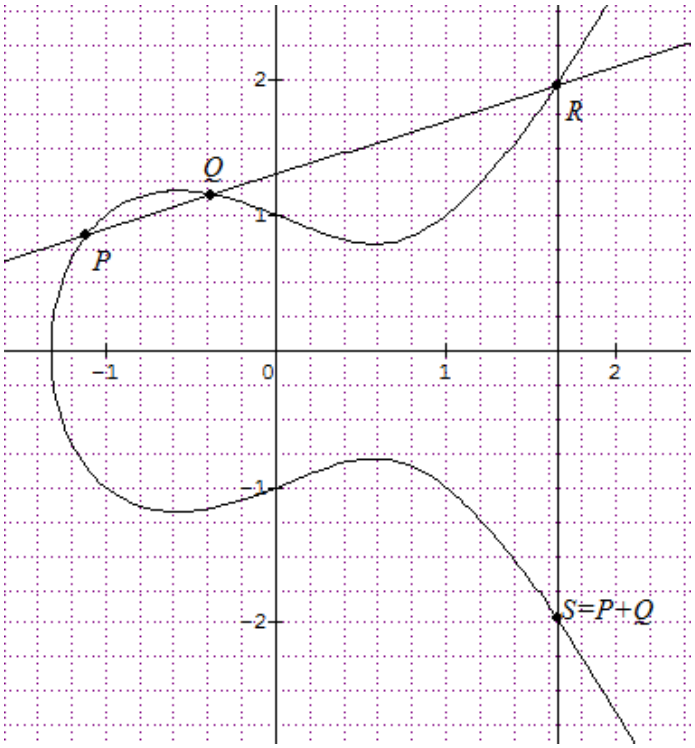
$\Delta = 4a^3 + 27b^2$ est le discriminant de l'équation du troisième degré $x^3 + ax + b = 0$.
Si $\Delta = 0$ le polynôme $x^3 + ax + b$ possède trois racines réelles (avec multiplicité), non toutes distinctes. S'il n'est pas nul il n'y pas de racine multiple. Cette condition garantit que la courbe elliptique dans $\mathbb{R}^2$ est lisse (elle n'a pas de point de rebroussement).

Une courbe elliptique ($\Delta \neq 0$) a l'une des deux allures suivantes[2] :

a- si $\Delta < 0$ le polynôme $x^3 + ax + b$ a alors trois racines réelles distinctes, donc la courbe possède trois intersections avec l'axe des abscisses.



b- si $\Delta > 0$ le polynôme a alors une unique racine réelle.



La représentation graphique d'une courbe elliptique peut se faire en terminale, par exemple pour les courbes d'équation $y^2 = x^3 - x$ (C_1) et $y^2 = x^3 - x + 1$ (C_2), en commençant par l'étude du signe du polynôme.

[2] La définition de la somme et la construction du point S = P + Q sont introduites dans la suite du texte.

Les élèves peuvent étudier les variations et tracer la courbe représentative des fonctions f_1 et f_2 telles que $f_1(x) = \sqrt{x^3 - x}$ et $f_2(x) = \sqrt{x^3 - x + 1}$.
On obtient les deux courbes complètes par une symétrie par rapport à l'axe des abscisses. On peut faire remarquer alors que ces courbes ne sont plus la représentation graphique de fonctions.
On trouvera en annexe 1 une étude mathématique détaillée qui permet de comprendre à quoi ressemblent les courbes elliptiques à l'aide d'étude de fonctions. Ce travail peut être mené en terminale S lors de l'heure d'accompagnement personnalisé en approfondissement.

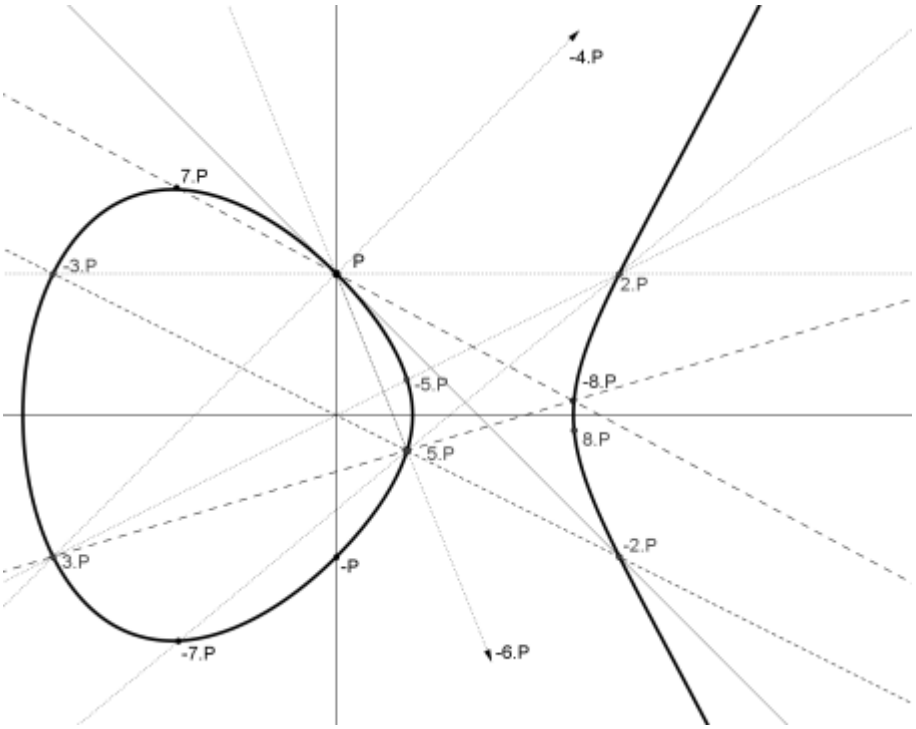
On rajoute par convention à cette courbe elliptique un « point à l'infini » qu'on notera ici P_0 (il faut imaginer qu'il correspond à une ordonnée *y* infinie).

On définit alors une loi de groupe notée + sur cet ensemble de points, de la façon suivante :

- Cas général : Soient P et Q deux points sur la courbe. On trace la droite (PQ). Elle intersecte la courbe en un troisième point R. On note alors S le symétrique de R par rapport à l'axe des abscisses, et on définit P+Q = S.

- Cas particuliers :
  - Si P = Q, on prend pour droite (PQ) la tangente à la courbe en P. On notera P + P=2.P
  - $P+P_0 = P_0$ (P_0 est l'élément neutre)
  - Si P et Q sont symétriques par rapport à (O*x*), c'est à dire P(*x*,*y*) et Q(*x*,–*y*), la droite (PQ) intersecte la courbe « à l'infini » : on définit alors $P + Q=P_0$. P et Q sont opposés.

Pour montrer que c'est une loi de groupe, il faudrait démontrer qu'elle est associative, ce qui est bien le cas mais n'est pas évident du tout. On peut simplement le constater sur l'exemple suivant avec $y^2 = x^3 - x + \frac{1}{4}$.



On choisit un point P sur la courbe : ici on a pris P (0 ; 1). On trace la tangente à la courbe en P pour obtenir – 2.P puis son symétrique 2.P. On construit ensuite 3.P = 2.P + P ; 4.P n'est pas visible sur le dessin donc pour 5.P on peut utiliser 5.P = (2.P + 3.P) ; en joignant (-2.P) et (-3.P) on peut aussi directement obtenir (-(-5.P)). On continue ainsi pour 6.P = 5.P + P mais il sort de la figure ; 7.P = 5.P + 2.P et 8.P = 7.P + P. Ici, on peut vérifier l'associativité de l'addition : 5.P + 3.P = 8.P.

Il existe des formules explicites pour trouver les coordonnées de P + Q en fonction des coordonnées de P et de Q. On peut les utiliser pour montrer en particulier que lorsque les coefficients de la courbe elliptique sont des entiers et en choisissant un point P de coordonnées rationnelles, tous les multiples *n*.P auront aussi des coordonnées rationnelles mais cela dépasse largement le cadre de cette brochure.

On peut alors concevoir un système cryptographique analogue au système El-Gamal vu en **8-** :
On choisit un entier *q* premier (dans la pratique, on le choisit très grand). Au lieu de travailler dans le corps des réels, on travaillera dans le corps $\mathbb{Z}/q\mathbb{Z}$. On choisit ensuite *a* et *b* des entiers inférieurs à *q* tels que $4a^3 + 27b^2 \neq 0$ modulo *q*. On considère alors l'ensemble des points dont les coordonnées (*x* ;*y*) dans $\mathbb{Z}/q\mathbb{Z}$ vérifient $y^2 = x^3 + ax + b$ modulo *q*. On continuera de l'appeler « courbe elliptique ». On définit la même opération sur ces points en utilisant les formules explicites mentionnées dans le paragraphe précédent et on obtient aussi un groupe.
Grâce à ces formules, un ordinateur peut « facilement» calculer le point (P + P +...+ P) = *n*.P lorsqu'on lui donne l'entier *n* et le point P (et ce de façon exacte).

Le calcul « difficile » consiste à calculer n lorsqu'on connaît les points $n.P$ et P.

Pour obtenir ces deux dernières propriétés, qui permettent d'avoir un système cryptographique sûr, il était nécessaire de se placer dans $\mathbb{Z}/q\mathbb{Z}$.

Dans ce système cryptographique :

- la clé publique de Bob est le triplet (une courbe elliptique, un point P sur la courbe, le point $Q = n.P$),
- sa clé privée est l'entier n.

Pour comprendre le principe, on peut faire fonctionner un exemple en utilisant en fait la courbe elliptique à coordonnées réelles.

On suppose que le message qu'Alice souhaite envoyer est un point M sur la courbe. Alice choisit alors un entier $k > 1$, calcule le point $k.P$ et transmet à Bob les deux points $(k.P, M+k.Q)$.

Bob connaît n : il peut donc déterminer $n.k.P = k.Q$. Il peut alors calculer $-k.Q$, et finalement il trouve $(M+k.Q) + (-k.Q) = M$.

Remarque : Alice doit garder k secret : si un espion connaît k, il peut retrouver M. Mais comme Bob connaît n, il n'a pas besoin de k.

Exemple : avec $n = 3$ et $k = 2$. (Pour que le système soit sûr n et k doivent être beaucoup plus grands)

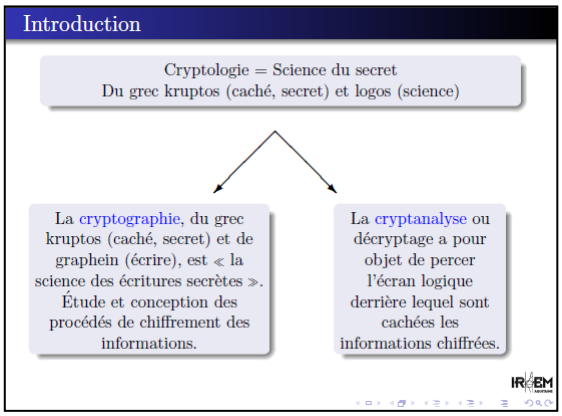
Alice récupère la clé publique et connaît donc P et Q

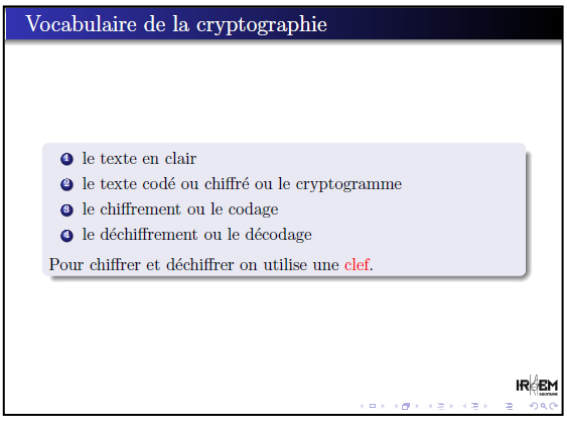
Elle calcule alors $U = 2.P$ et $V = M + 2.Q$, et transmet à Bob le couple (U, V). Bob calcule alors $3.U$, puis $V - 3.U$. Or $Q = 3.P$ donc $3.U = 3.2.P = 2.3.P = 2.Q$

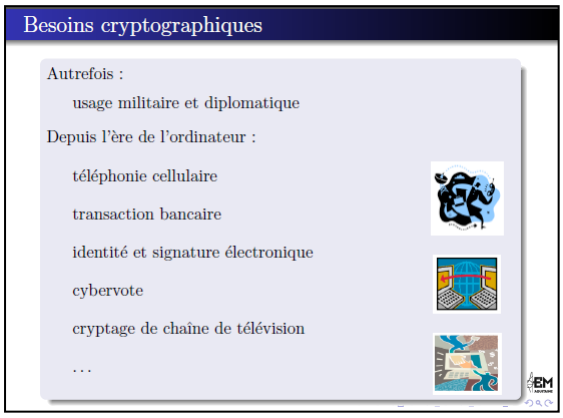
Finalement Bob a calculé $V - 3.U = (M + 2.Q) - 2.Q = M$

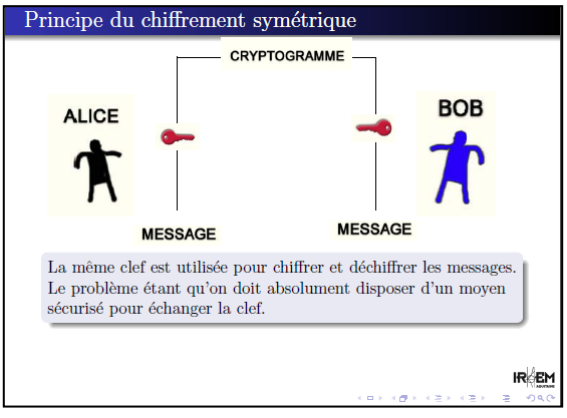
Partie 2
Diaporama commenté

Nous avons présenté ce diaporama devant des classes de la quatrième à la terminale. Deux versions, une pour le collège et une pour le lycée sont disponibles sur le site de l'IREM d'Aquitaine (Université de Bordeaux) à la page du groupe « Découvertes mathématiques ». Le diaporama lycée est accessible en seconde, à l'exception des dernières diapositives, concernant RSA, qui s'adressent aux élèves de terminale. Dans cette partie nous vous en présentons l'intégralité assortie de commentaires. Ces derniers concernent aussi la version collège car les diaporamas sont en grande partie identiques. Vous trouverez également en annexe 4 des petits problèmes qui ont été posés aux élèves après le diaporama.

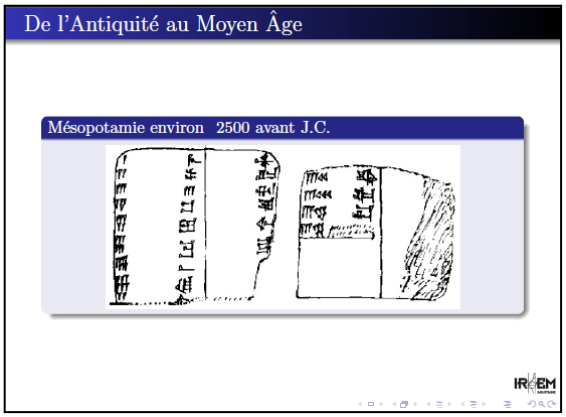


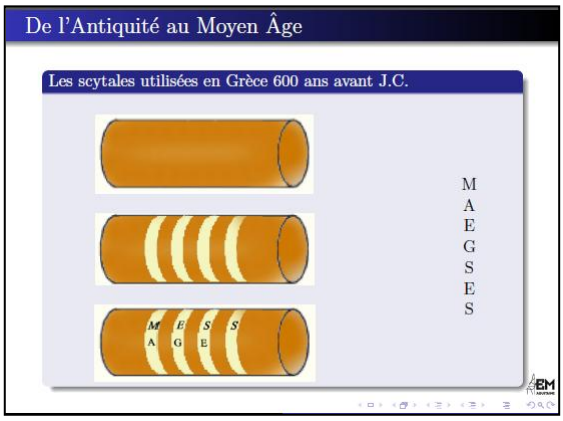


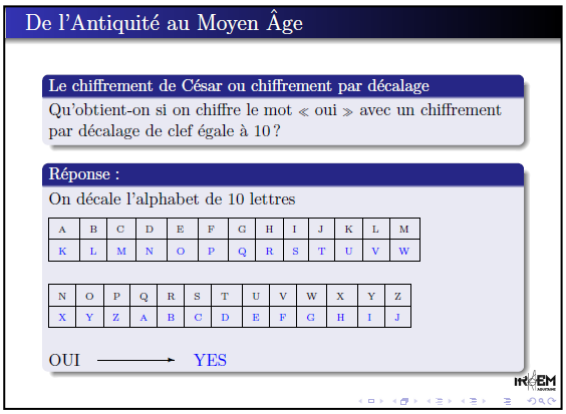




Historiquement le chiffrement symétrique est resté longtemps le seul système utilisé, il ne l'est pratiquement plus aujourd'hui : il n'est pas sûr. La nécessité de l'échange de clé entre les correspondants rend impossible son usage avec de très nombreux interlocuteurs (paiement en ligne, …).

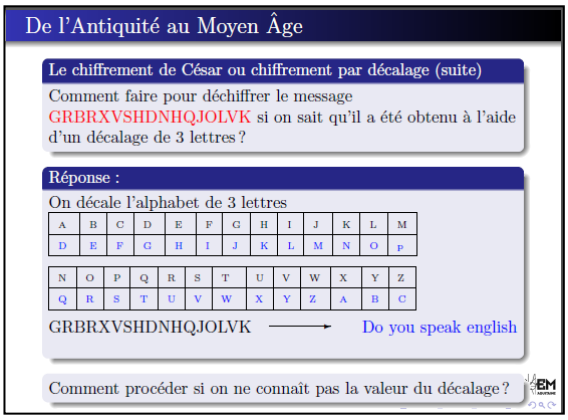






Le principe du chiffrement par décalage est expliqué oralement. On montre le tableau aux élèves pour qu'ils comprennent à partir de cet exemple comment fonctionne ce chiffrement. Cette méthode est accessible à tous les niveaux de classe car elle ne nécessite pas de numériser l'alphabet.

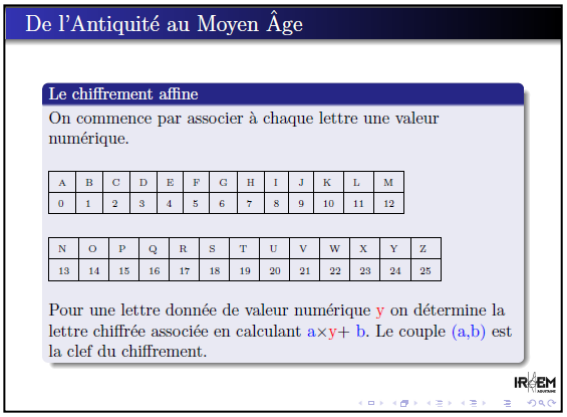
On laisse les élèves trouver la réponse. La transformation de « oui » en « yes » est amusante, on peut préciser que bien sûr il ne s'agit pas d'une méthode de traduction du français en anglais !



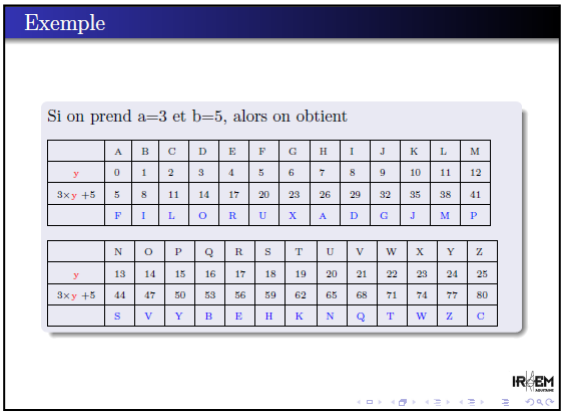
La réponse est orale. Les élèves pensent spontanément à essayer tous les décalages possibles et se rendent compte qu'il n'y a pas beaucoup de possibilités : ils se rendent compte de la faiblesse de la protection que ce chiffrement procure.

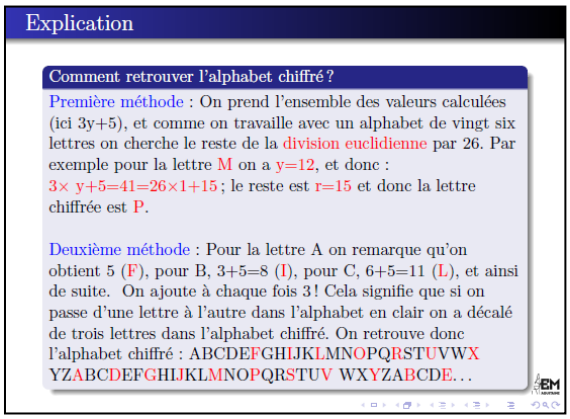
Plusieurs fois, des élèves (qui visiblement s'étaient déjà intéressés à la cryptographie) ont suggéré spontanément l'étude des fréquences dans le cas du décalage "pour trouver le E" et éviter de faire 25 essais successifs.

Mais curieusement ceux à qui cette idée vient naturellement ne verront pas toujours comment la généraliser lorsqu'il s'agira d'un chiffrement par substitution quelconque.



Le chiffrement affine est accessible à partir de la troisième. C'est une activité intéressante pour utiliser les notions d'images, antécédents. On retrouve visuellement la proportionnalité des accroissements.

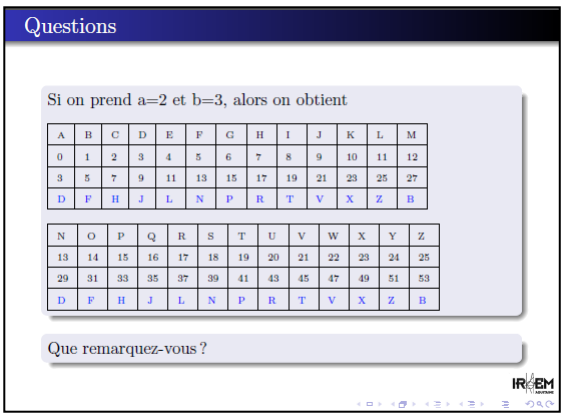




On demande aux élèves de réfléchir à des méthodes pour retrouver la lettre de l'alphabet qui correspond à une image supérieure à 26.

Les élèves remarquent vite qu'une même lettre peut être codée par deux nombres différents. Le fait que cela entraine que ce codage n'est pas utilisable est plus difficile à comprendre : on pourra coder mais pas décoder.

La recherche des clés qui ne conviennent pas peut donner lieu à un prolongement en classe au lycée.



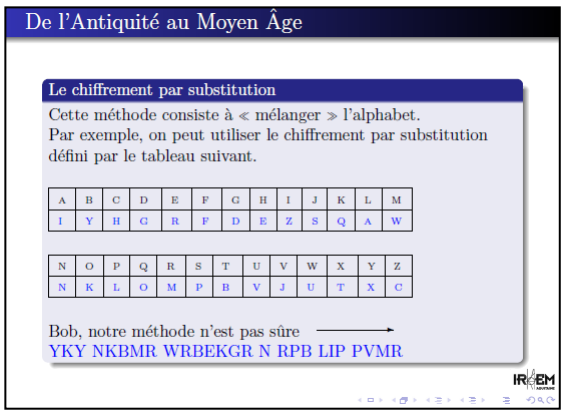
Questions

Si on prend a=2 et b=3, alors on obtient

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
3	5	7	9	11	13	15	17	19	21	23	25	27
D	F	H	J	L	N	P	R	T	V	X	Z	B

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25
29	31	33	35	37	39	41	43	45	47	49	51	53
D	F	H	J	L	N	P	R	T	V	X	Z	B

Que remarquez-vous ?



De l'Antiquité au Moyen Âge

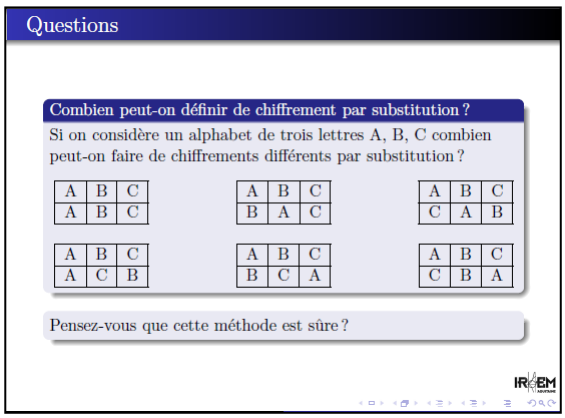
Le chiffrement par substitution

Cette méthode consiste à « mélanger » l'alphabet.
Par exemple, on peut utiliser le chiffrement par substitution défini par le tableau suivant.

A	B	C	D	E	F	G	H	I	J	K	L	M
I	Y	H	G	R	F	D	E	Z	S	Q	A	W

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
N	K	L	O	M	P	B	V	J	U	T	X	C

Bob, notre méthode n'est pas sûre ⟶
YKY NKBMR WRBEKGR N RPB LIP PVMR



Questions

Combien peut-on définir de chiffrement par substitution ?

Si on considère un alphabet de trois lettres A, B, C combien peut-on faire de chiffrements différents par substitution ?

A	B	C
A	B	C

A	B	C
B	A	C

A	B	C
C	A	B

A	B	C
A	C	B

A	B	C
B	C	A

A	B	C
C	B	A

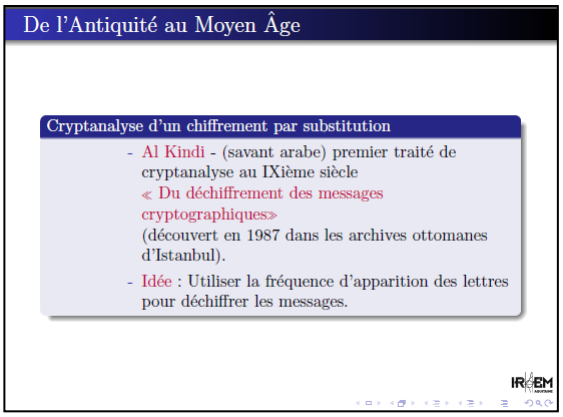
Pensez-vous que cette méthode est sûre ?

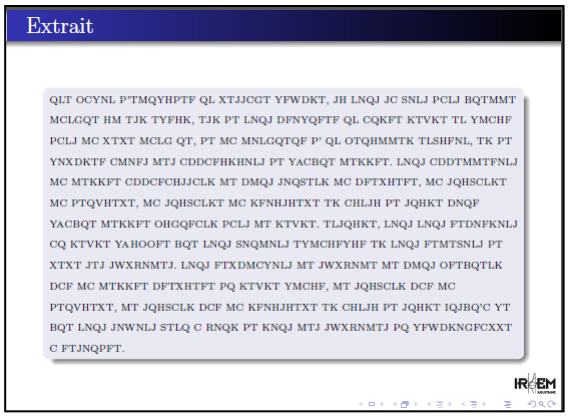
Lorsqu'on pose la question du nombre de substitutions possibles pour un alphabet à trois lettres, les élèves proposent :

- 9 = 3 + 3 + 3 car ils pensent à 3 possibilités pour l'image de chaque lettre et ils les ajoutent.
- 8 = 2 × 2 × 2 (?) Probablement parce qu'ils pensent qu'une lettre ne peut pas être sa propre image.
- Certains trouvent bien 6 possibilités mais ils le justifient par la somme 2 + 2 + 2.
- D'autres trouvent 5 possibilités car ils ne comptent pas l'identité. Ils n'ont pas tort de ne pas la considérer comme un chiffrement utile.

On peut ultérieurement, proposer de trouver le nombre de possibilités pour un alphabet à 4 lettres (abordable en troisième), 5 lettres pour les plus ingénieux.

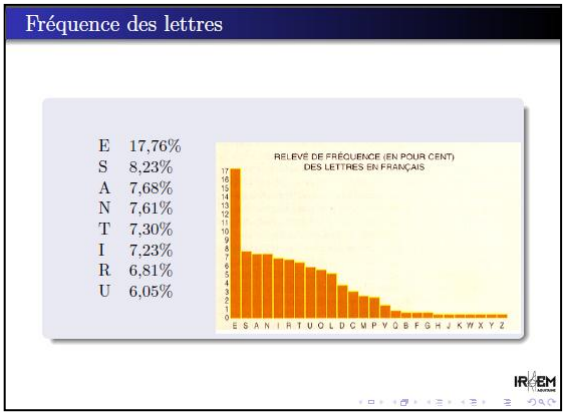
Le nombre total de possibilités pour un alphabet à 26 lettres est difficile à trouver, même en lycée. Le calcul de la factorielle n'est plus explicitement au programme mais s'effectue avec un algorithme simple abordable dès la seconde. Les élèves, même en collège, comprennent que c'est un grand nombre, ils en déduisent à tort, comme on va le voir ensuite, que la méthode est sûre car la recherche exhaustive n'est pas possible.





Le texte proposé est un extrait du livre d'Al Khindi. A priori, même ceux qui avaient pensé à chercher l'image de la lettre « E » pour le décalage, se disent que trouver une lettre n'est pas suffisant, et donc que cela ne sert à rien. Ils ne pensent pas à analyser les fréquences de toutes les lettres. De plus, ils n'ont pas conscience que quelques lettres très fréquentes suffisent souvent pour donner une bonne idée du contenu du message à décoder.

Quand on leur dit qu'on va utiliser les fréquences, ils trouvent assez facilement le « E ». Le fait qu'on ait gardé les espaces les aide à trouver d'autres lettres en utilisant les mots les plus courts. Ils sont ainsi rapidement convaincus que la méthode n'est pas si sûre qu'ils le pensaient.



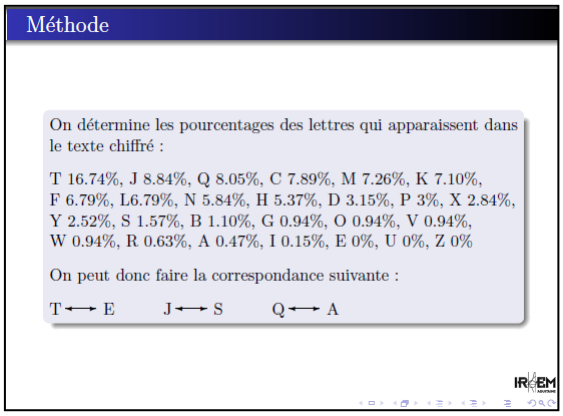
On peut faire remarquer que certaines fréquences sont très proches, donc il sera difficile de distinguer, par ce moyen, certaines lettres dans un texte donné. Il faudra éventuellement faire plusieurs essais.

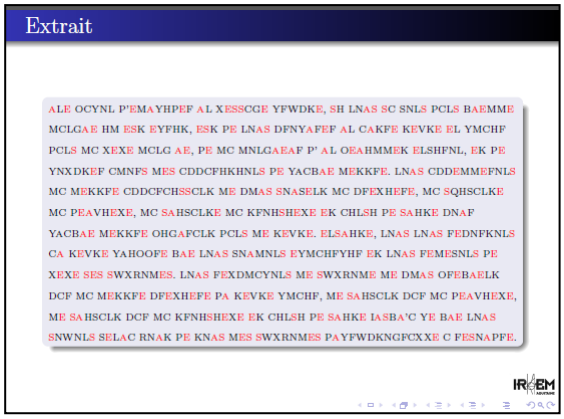
Les élèves se demandent comment ces fréquences ont été déterminées. On peut leur dire qu'elles diffèrent légèrement selon le type de texte choisi comme échantillon de référence. On peut évoquer l'exemple du livre de Georges PEREC, *La disparition*, dans lequel il n'y a pas une seule fois la lettre « E ». Par ailleurs, ces fréquences dépendent évidemment de la langue choisie.

De plus, pour que les fréquences soient significatives, il faut qu'il y ait suffisamment de lettres dans le texte à déchiffrer.

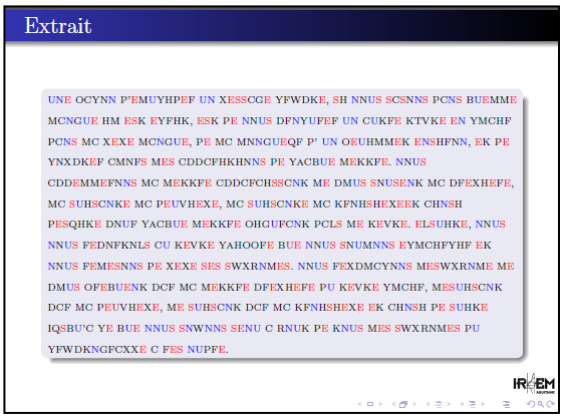
Le déchiffrement d'un texte codé par substitution est une bonne illustration de l'intérêt des statistiques, accessible dès la cinquième.

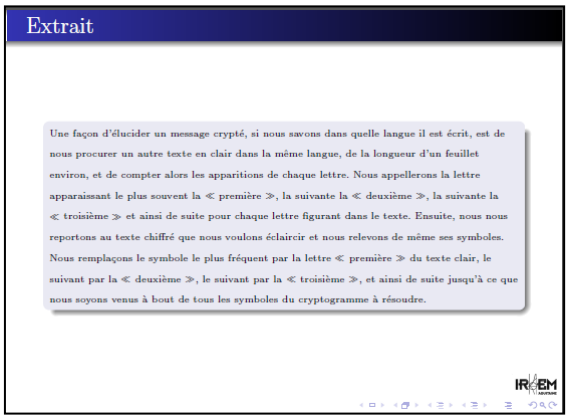
Pour gagner du temps et permettre des vérifications, on peut partager le travail de comptage des lettres entre les élèves.



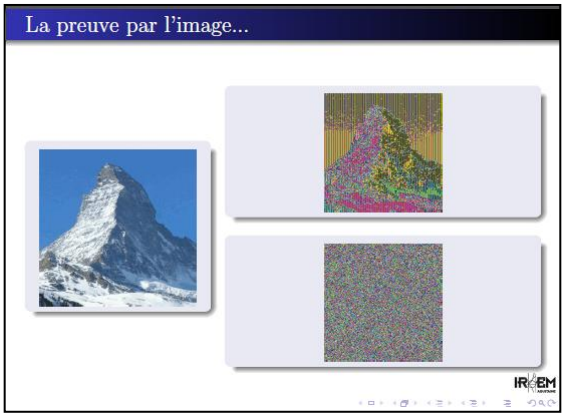


Le premier mot « A _ E » ne correspond pas à un mot qui débuterait une phrase en français. De plus la succession des deux lettres AE, extrêmement rare en français apparait plusieurs fois dans le texte. Les élèves en déduisent que la lettre A n'est pas bien décodée, certains pensent au mot « UNE » pour débuter le texte.





Les élèves sont convaincus que, de proche en proche, on va pouvoir déchiffrer le texte.



Dans les méthodes précédentes, une lettre donnée est toujours transformée en une même lettre : la structure du texte est conservée. Cela permet le déchiffrement par l'étude des fréquences. Sur cette diapo, la photo en haut à droite est obtenue en faisant une transformation par substitution des couleurs de la photo d'origine (à gauche). On peut toujours distinguer les contours de l'image (la structure). Par contre, l'image en bas à droite est obtenue par une transformation qui dépend de la position du pixel. Une couleur donnée n'est pas toujours remplacée par la même couleur, cette fois, l'image est totalement brouillée.

Cela permet d'introduire le chiffrement de Vigenère qui fonctionne selon ce principe.

Du Moyen Âge à la seconde guerre mondiale

Le chiffrement de Vigenère au XVI ème

Méthode

On fait du décalage, mais qui change suivant la position des lettres dans le message.

On choisit un mot de passe (la clef du chiffrement), qui n'est pas obligé d'être un mot qui a un sens, par exemple VIGENERE. Si on souhaite alors chiffrer le message « Bob, j'ai trouvé mieux » on procède de la manière suivante

Méthode

B	O	B	J	A	I	T	R	O	U	V	E
1	14	1	9	0	8	19	17	14	20	21	4
V	I	G	E	N	E	R	E	V	I	G	E
21	8	6	4	13	4	17	4	21	8	6	4
22	22	7	13	13	12	36	21	35	28	27	8
W	W	H	N	N	M	K	V	J	C	B	I

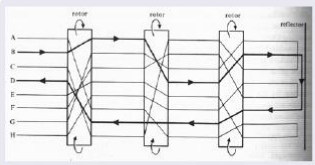
M	I	E	U	X
12	8	4	20	23
N	E	R	E	V
13	4	17	4	21
25	12	21	24	44
Z	M	V	Y	S

Les élèves voient tout de suite que les deux premières lettres B et O sont toutes les deux codées par W. Donc la méthode des fréquences sera inopérante.

Dans cette méthode, le décodage pose des difficultés. Les élèves comprennent bien qu'ils vont devoir faire des soustractions, mais ne savent pas qui soustraire à qui, d'autant plus qu'ils peuvent trouver des nombres négatifs qu'ils ne savent pas trop interpréter. (voir partie 3)

Enigma vers 1920

Enigma vers 1920



On a plus de possibilités de chiffrer un message que de secondes écoulées depuis la naissance de l'univers !

Enigma vers 1920

On peut remarquer que les permutations employées dans les rotors et les réflecteurs ne peuvent pas être considérées comme faisant partie du secret. En effet, toutes les machines utilisent les mêmes, et il suffit donc d'en avoir une à disposition. Les Anglais, par exemple, en ont récupéré une pendant la guerre dans un sous-marin coulé. Ceci est une illustration d'un principe général en cryptographie, principe dit de Kerckhoffs, qui veut que tout le secret doit résider dans la clef secrète de chiffrement et de déchiffrement, et pas dans une quelconque confidentialité de l'algorithme (ici de la machine) qui ne peut être raisonnablement garantie.

Alan Turing (1912 - 1954)

Mathématicien de génie, l'un des cerveaux travaillant pendant la guerre au château de Bletchley Park.

Concepteur de machines ayant permis la cryptanalyse d'ENIGMA et du COLOSSUS ancêtre de nos ordinateurs.

Voir partie 1 pour le fonctionnement de la machine et un historique.

On peut décrire brièvement le fonctionnement de la machine aux élèves. C'est le même principe que le chiffrement de Vigenère, mais c'est une substitution qui change à chaque lettre. La partie historique intéresse les élèves.

Buts de la cryptographie moderne

CONFIDENTIALITÉ
information disponible aux seules personnes autorisées

INTÉGRITÉ
information exempte de toute modification

AUTHENTIFICATION
identification de l'émetteur et du récepteur de l'information

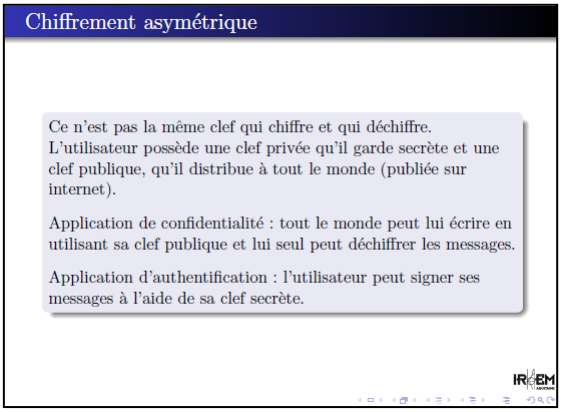
NON-RÉPUDIATION
impossibilité de nier a posteriori l'envoi de l'information

Le concept de confidentialité est le but premier de la cryptologie. C'est celui qu'on a étudié jusqu'à présent dans ce diaporama.

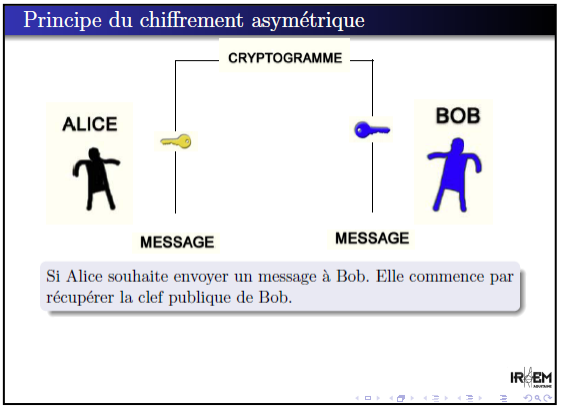
L'intégrité consiste à être sûr que le message reçu est bien celui qui a été envoyé et qu'il n'a pas été modifié lors de l'envoi, par erreur ou malveillance.

L'authentification consiste à être sûr que l'expéditeur est bien celui qu'il prétend être.

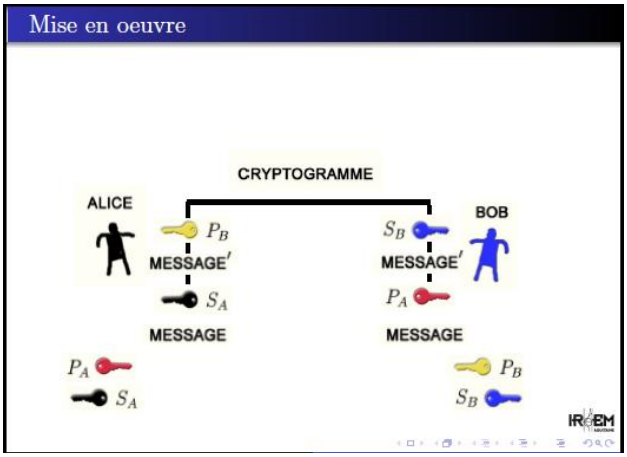
La non-répudiation consiste à rendre impossible à l'expéditeur de nier qu'il a envoyé le message. (Très important pour le paiement en ligne)



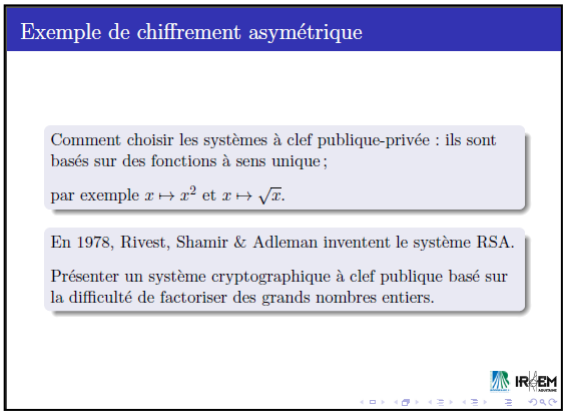
Ce principe évite les problèmes liés à l'échange des clés.



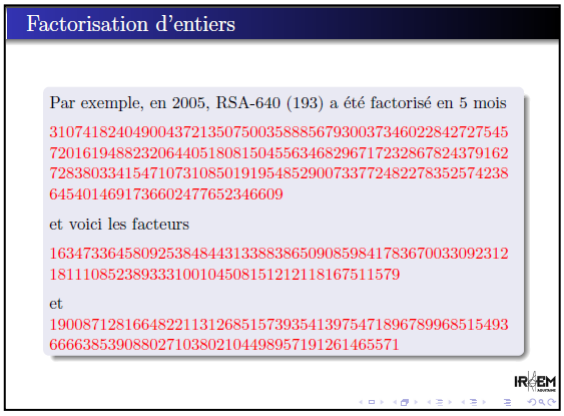
La clé jaune est la clé publique de Bob et la clé bleue, sa clé secrète.

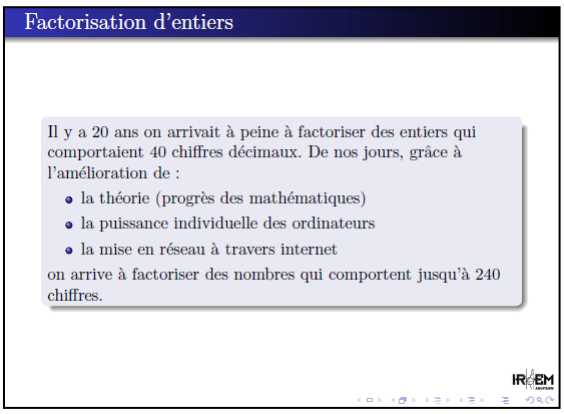


La clé rouge est la clé publique d'Alice et la clé noire sa clé secrète. Le principe d'authentification illustré ici est un peu plus compliqué à comprendre pour les élèves.
Pour envoyer un message à Bob, Alice chiffre son message à l'aide de sa clé secrète (noire) puis le rechiffre à l'aide de la clé publique de Bob. Bob déchiffre alors le message à l'aide de sa clé secrète puis déchiffre le message obtenu à l'aide de la clé publique d'Alice. Le fait que le message ait alors un sens prouve qu'il a bien été chiffré au début par la clé secrète d'Alice, ce qui prouve que c'est bien Alice qui l'a envoyé.

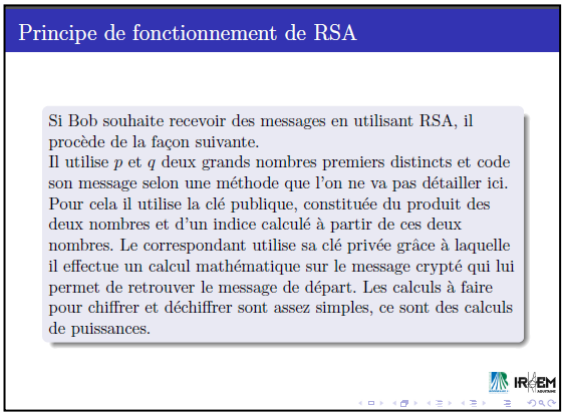


Un élève peut comprendre que calculer le carré d'un nombre est assez facile et rapide même si le nombre est grand. Retrouver la racine carrée lui semblera plus difficile surtout quand le nombre est très grand.
De même, multiplier deux nombres premiers est facile, par contre, même pour un ordinateur, retrouver les facteurs est très difficile et peut être très long si les nombres sont très grands. C'est sur ce principe que repose la sécurité du codage RSA.

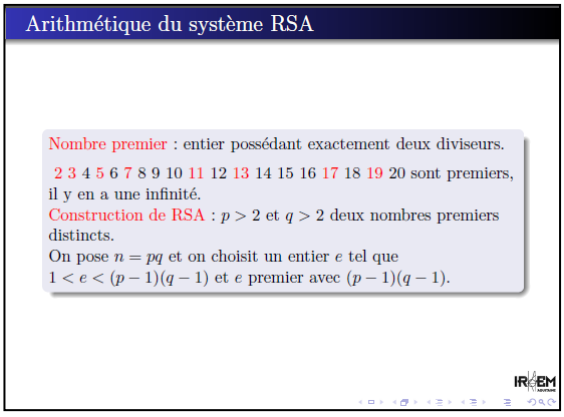




Cela peut être l'occasion de parler du métier de chercheur en mathématiques, même s'il faut préciser que le travail de chercheur ne consiste pas uniquement à faire de grosses multiplications !



En collège, on explique brièvement le principe sans donner d'exemple chiffré, trop difficile à suivre.



On peut détailler l'explication jusqu'au bout pour les terminales, par contre on peut passer rapidement sur l'obtention de 29 avec les secondes. (voir diapo suivante)

Exemple non réaliste

Bob prend $p = 7$ et $q = 13$, calcule

$$n = pq = 91 \text{ et } (p-1)(q-1) = 72.$$

Il choisit ensuite e premier avec $(p-1)(q-1)$, par exemple $e = 5$ (e ne doit pas avoir de diviseur comun avec $(p-1)(q-1)$).
Il en déduit, par l'algorithme d'Euclide étendu, un entier d tel que le reste de la division euclidienne de $e.d$ par $(p-1)(q-1)$ vaut 1 .
Il trouve par exemple $d = 29$, qui vérifie bien

$$e.d = 5.29 = 145 = 72.2 + 1$$

Exemple non réaliste

La clef publique de Bob est alors $(n, e) = (91, 5)$ et sa clef privée $(p, q, d) = (7, 13, 29)$.
Si Alice veut envoyer le code $M = 18$ elle calcule le reste de la division de $M^e = 18^5$ par n=91, et envoie le résultat à Bob

$$M^e = 18^5 = 1889568 = 91 \times 2067 + 44.$$

Elle envoie $C = 44$ à Bob, qui calcule à son tour le reste de la division de $C^d = 44^{29}$ par $n = 91$ et retrouve $M = 18$

On signalera, en terminale, que l'égalité peut se noter à l'aide d'une congruence.

$91 \times 2067 + 44 \equiv 44\ [91]$.

Pourquoi ça marche

Bob applique le petit théorème de Fermat qui dit que : si a est un nombre premier avec $p \times q$ alors

$$a^{(p-1)(q-1)} \equiv 1\ (pq)$$

Bob effectue donc le calcul suivant :

$$C^d = 44^{29} \equiv 18^{5.29}\ (91) \equiv 18^{72.2+1}\ (91) \equiv (18^{72})^2.18^1\ (91)$$

Par le petit théorème on a $18^{72} \equiv 1\ (91)$. Bob trouve donc

$$C^d \equiv 18\ (91).$$

Cette diapositive est réservée aux terminales.

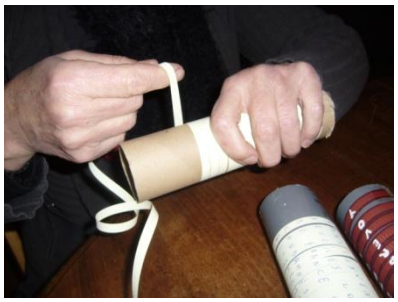
Partie 3
Compte-rendu d'activités et observations

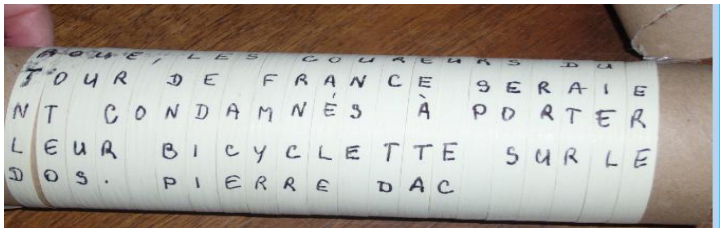
1- Codage ludique

Nous avons expérimenté dans nos classes de collège la réalisation d'une scytale ainsi que d'autres jeux de codage et décodage.

a- La scytale

Voici par exemple une réalisation de nos élèves :





1. On enroule une bande de papier autour d'un cylindre. On scotche le début de la bande et la fin sur le cylindre pour la fixer.

2. On écrit le message, une lettre par spire sur chaque ligne.

3. On déroule la bande et le message devient illisible.

4. Pour retrouver le message, on enroule à nouveau la bande sur un cylindre de **même diamètre** que celui qui a servi à coder.

Dans la partie 1 nous avons donné un texte de Plutarque à propos de la scytale.
Ce texte peut être commenté soit par le professeur de mathématiques seul, soit, si cela est possible, dans le cadre d'un travail interdisciplinaire avec un professeur d'histoire ou de lettres classiques.

<u>Quelques pistes de questions à poser aux élèves :</u>

Le professeur d'histoire ou de grec peut poser des questions sur Sparte.
Le professeur de mathématiques peut poser des questions dont les élèves trouveront la réponse dans un dictionnaire, dans le texte lui-même, ou ... dans leur tête.

- Qui était Plutarque ? Qui était Lysandre ?
- Qui étaient les éphores ? (réponse : 5 magistrats élus annuellement pour exercer un contrôle sur tous y compris les rois).
- Plutarque nous dit que le mot scytale désigne deux objets, lesquels ?
- Plutarque nous dit « ... comme ce qui est mesuré prend le nom de ce qui lui sert de mesure »

Voyez-vous un exemple pour illustrer cela ? (Réponse possible : On dit : « la surface de la table est lisse » et aussi « la surface de la table est 1 m^2 ». Le langage courant emploie le même mot pour l'objet qui est la surface et sa mesure qui est un nombre avec une unité. Les mathématiciens distinguent pour être précis trois concepts : l'objet (la surface), la grandeur que l'on mesure (l'aire qui ne dépend pas de l'unité) et le nombre qui est la mesure elle-même et qui dépend de l'unité. Il

en est de même pour la grandeur longueur (colorier la longueur du rectangle, la longueur est 3 cm). Mais quand il n'y a pas risque de confusion, on emploie le même mot pour ne pas surcharger le langage).

b- <u>Le carré de Polybe et les tables de multiplication</u>

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I	J
3	K	L	M	N	O
4	P	Q	R	S	T
5	U	V W	X	Y	Z

Chaque lettre est codée par un couple formé de deux chiffres : le chiffre de sa ligne puis celui de sa colonne. Pour obtenir un carré, on a fondu les lettres V et W. Ainsi on écrira VAGON à la place de WAGON.

<u>Questions, éventuellement en relation avec le professeur d'histoire ou de lettres classiques :</u>

- Chercher qui était Polybe (un simple dictionnaire suffit)

Réponse : Polybe était un historien grec né vers 200 avant J.C. Déporté comme otage à Rome en 168, il se lia d'amitié avec Scipion Emilien qu'il accompagna dans ses campagnes contre Carthage et Numance. Il nous reste quelques exemplaires de ses œuvres.

- Qui étaient Scipion Emilien, Scipion l'Africain (grand-père du précédent) ?
- Où se trouvaient Carthage et Numance ?

<u>Une façon amusante d'utiliser les tables de multiplication :</u>

En collège, de la 6ème à la 3ème, une révision des tables de multiplication n'est pas inutile, même si théoriquement elles sont connues depuis l'école élémentaire. Autant organiser cette révision en jouant en même temps à déchiffrer un message.

Voici par exemple ce que nous avons proposé à nos élèves :

1) Dans le message secret ci-dessous, on voit des nombres soulignés par des traits. Le nombre qui se trouve au-dessus de chaque trait est le résultat d'une multiplication. A chaque trait correspond une lettre ou un signe de ponctuation. Grâce à la connaissance des tables de multiplication et à la grille ci-dessous, il est possible de décoder ce message.

Message à décoder :

2548 / 3056 / 1225 / 166340494810101863 / 4042 / 24422525121542 / 4264 / 2436486425 / 1642 / 1648 2 / 24486456304225 / 7 / 3056 / 25124825 / 304225 / 301228204225 / 1642 / 24562030485420484012304836664 / 50 / 2548643664 / 186372482542 / 204225 / 100

×	1	2	3	4	5	6	7	8	9	10
1	–	x	ç	w	j	è	,	k	'	f
2	x	w	è	k	f	a	:	d	r	l
3	ç	è	'	a	g	r	û	m	ï	t
4	w	k	a	d	l	m	b	q	o	c
5	j	f	g	l	s	t	à	c	ê	.
6	è	a	r	m	t	o	e	i	p	z
7	,	:	û	b	à	e	h	u	é	y
8	k	d	m	q	c	i	u	n	v	î
9	'	r	ï	o	ê	p	é	v	?	â
10	f	l	t	c	.	z	y	î	â	!

Message en clair : Si tu as déchiffré ce message en moins de dix minutes, tu sais tes tables de multiplication. Sinon révise-les !

Remarques : Dans le message codé nous avons séparé les mots.

Les élèves comprennent vite qu'une même lettre est codée de la même façon quelle que soit sa place dans le message. Ils s'en servent pour deviner certains mots en partant de quelques lettres et

en s’aidant du contexte. Ce qui leur permet de compléter d’autres lettres sans se préoccuper des tables de multiplication.
Il peut donc être intéressant de proposer des mots qu'ils ne connaissent pas afin qu'ils soient obligés de les décoder lettre par lettre (par exemple PYTHAGORE en sixième).
Des élèves s’inquiètent car le nombre 18 par exemple peut être 2 × 9 ou 3 × 6. Le professeur leur fait vérifier que la table est bien construite et que toutes les possibilités pour faire 18 correspondent bien à la même lettre R.
Bien évidemment la table est symétrique par commutativité de la multiplication. Cette table de 10 par 10 permet de coder 43 symboles.
Certaines lettres accentuées n'apparaissent pas, mais la table choisie permet de coder la plupart des messages.

2) De la même façon, écris ci-dessous un message de ton choix et code-le à l’aide de la grille. Puis demande à ton voisin de le déchiffrer.

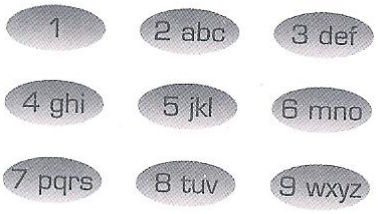
Intérêt de ce jeu : Au moment du décodage, les élèves doivent savoir par exemple que 25 est 5 × 5 donc représente la lettre S, ou que 30 est 6 × 5 ou 3 × 10 et donc représente donc la lettre T. Au moment du codage de leur message ils travaillent les tables dans l’autre sens. Par exemple pour coder la lettre A qu’ils trouvent dans la case (6 ; 2) ou dans la case (4 ; 3), ils doivent savoir que le produit est 12.

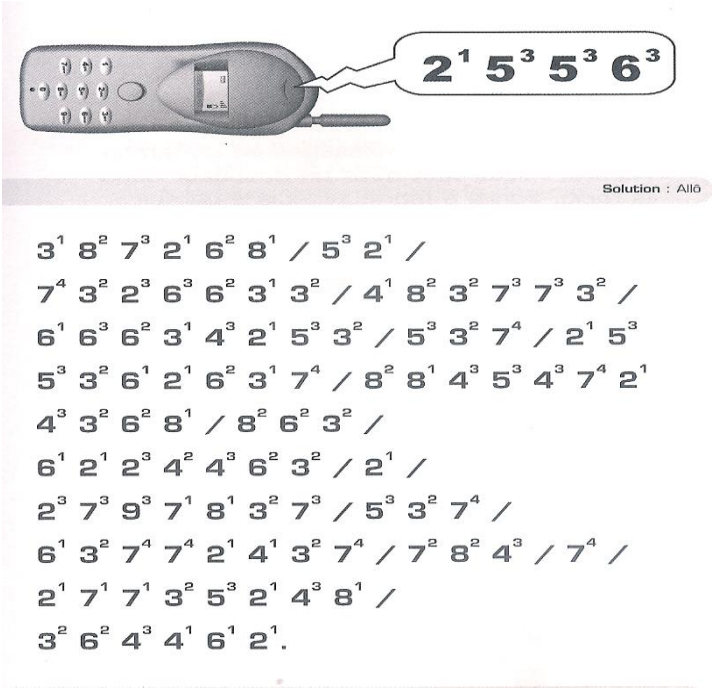
Des élèves qui ont été assez astucieux dans la première partie du travail, mais qui ne savent pas leurs tables de multiplication font beaucoup d’erreurs. Les camarades qui décodent leurs messages le leur font remarquer.
Les élèves sont très motivés par ce travail et même ceux qui rechignent à étudier les tables de multiplication d’habitude veulent réussir.
Pour certains élèves de sixième en grande difficulté, le professeur peut proposer une table de Pythagore dans laquelle les élèves pourront trouver les résultats qu’ils ne connaissent pas. A force de fréquenter les tables, on peut espérer qu’ils finiront par les mémoriser !

On peut donner aux élèves une grille (différente de celle proposée ci-dessus) en partie vide, par exemple en sixième, contenant une fois chaque caractère et leur demander de la compléter.

c- SMS

Pour distraire les élèves :





<u>Correction :</u> Durant la seconde guerre mondiale les Allemands utilisaient une machine à chiffrer les messages qui s'appelait Enigma.

Ce texte peut être l'occasion de proposer aux élèves de faire des recherches historiques sur la seconde guerre mondiale, selon leur niveau.

<u>Remarques sur la saisie intuitive ou T9 :</u>

Les premiers téléphones possédaient une correspondance chiffre/lettre qui permettait de donner l'indicatif du central téléphonique en région parisienne avec les trois premières lettres du nom. Ainsi l'indicatif de OBServatoire était 027. Il est intéressant de noter que certaines lettres « rares » étaient situées sur une touche à part au lieu du simple ordre alphabétique.

Rendue inutile avec l'utilisation de standards automatiques, ces lettres servent aujourd'hui à écrire des messages sur un clavier en utilisant 9 touches. Le principe est simple mais devient rapidement fastidieux : il faut appuyer entre une et trois fois sur une touche pour écrire la lettre voulue. Pour écrire "crypto", il faut presser trois fois la touche 2 puis trois fois la touche 7, trois fois la touche 9, une fois la touche 7, une fois la touche 8 et trois fois la touche 6 soit 14 pressions pour un mot de 6 lettres. Un brevet a été déposé en 1985 pour améliorer la communication avec les sourds en permettant une "saisie intuitive". Le principe est de ne saisir qu'une seule fois la touche où apparaît la lettre voulue, quelle que soit la position de la lettre sur la touche. Aujourd'hui le "T9" ("text on 9 keys") est intégré à la plupart des téléphones. Le problème de la pluralité des combinaisons est

résolu grâce à un dictionnaire. Par exemple, l'entrée 279786 correspond à 576 suites de lettres possibles, dont une seule correspond à un mot reconnu par le dictionnaire : "crypto". Le système est d'autant plus efficace que les mots sont longs. Si la majorité des combinaisons de touches donnent un mot unique, certaines peuvent prêter à confusion comme l'entrée 7273 qui peut correspondre à RARE, RAPE, SAPE, PARE... C'est à l'utilisateur de sélectionner le bon mot. Un algorithme mémorise alors la fréquence de choix de certains mots et les proposera en premier.

2- Le chiffrement par décalage

Exemple : décalage de 5 :

	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
X	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**
X + 5	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
reste	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**	**0**	**1**	**2**	**3**	**4**
	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E

Le chiffrement par décalage peut se comprendre sans formalisme mathématique ; il s'agit bien évidemment d'une addition « modulo 26 ». Les élèves comprennent assez bien l'intérêt de la représentation des lettres par des chiffres, ainsi que la nécessité d'enlever 26 lorsque le résultat est trop grand. Il n'est pas forcément nécessaire de parler de reste de division euclidienne dans ce contexte.

Au collège :

Certains élèves ne comprennent pas la méthode du décalage. Pour un décalage de 3 par exemple, ils pensent que A devient C et non D car ils comptent A, B, C (3 lettres) et ne comprennent pas qu'un décalage de 3 correspond à trois décalages successifs de 1 : A donne B, B donne C et C donne D. On retrouve ce phénomène dans de nombreuses situations de comptage des pas d'une graduation (mesure de longueur, usage du rapporteur, comptage du nombre de termes d'une suite…)

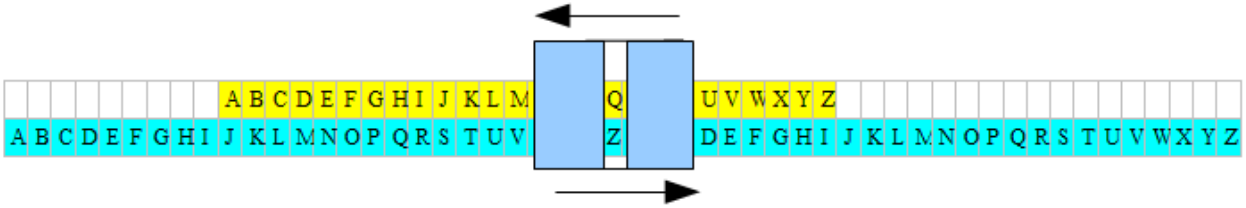
Le fait de présenter ce décalage comme une fonction en associant les nombres aux lettres dans un tableau de valeurs, facilite la mise en œuvre de cette méthode de codage.

Par ailleurs les élèves ont du mal à ne pas lire « intuitivement » le tableau dans les deux sens : si A donne F alors F donne A…. Il est judicieux de bien distinguer les tableaux de codage et de décodage (quitte à leur faire remplir séparément les deux) et d'être rigoureux sur l'en-tête des lignes.

Ces activités de codage ou décodage sont l'occasion de montrer l'efficacité d'un tableur pour des opérations répétitives (voir 6°). Le chiffrage par décalage, simple à appréhender, permet d'introduire les fonctions nécessaires à la manipulation du tableur.

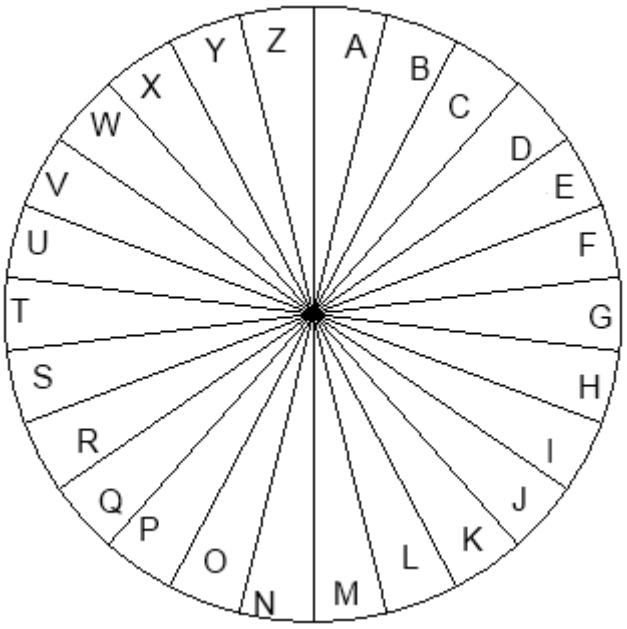
Pour réaliser les décalages, on peut proposer aux élèves de construire et de manipuler des objets, par exemple :

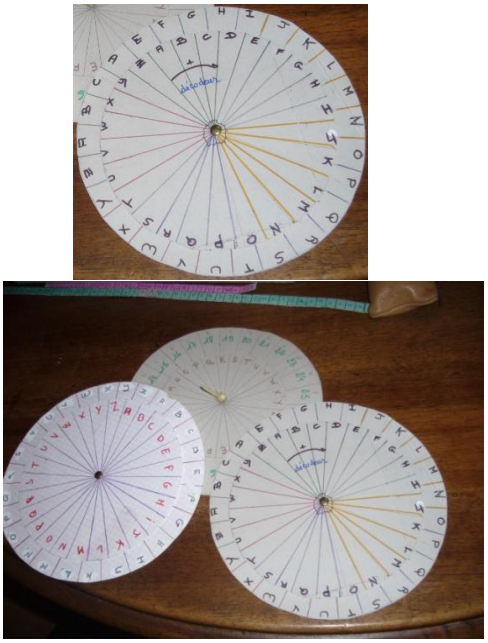
-une réglette de Saint Cyr munie d'un cache



-un codeur ou décodeur circulaire

Le professeur peut demander aux élèves de réaliser les deux disques. Cela se révèle en pratique difficile avec le rapporteur, d'autant plus que les élèves ne graduent pas spontanément le demi-cercle en laissant le rapporteur fixe et en ajoutant le pas à chaque étape, comme l'on gradue un axe en se servant d'une règle graduée : ils dessinent en général un des secteurs avec le rapporteur, puis déplacent le rapporteur pour dessiner le suivant, etc. De la sorte les erreurs se cumulent.



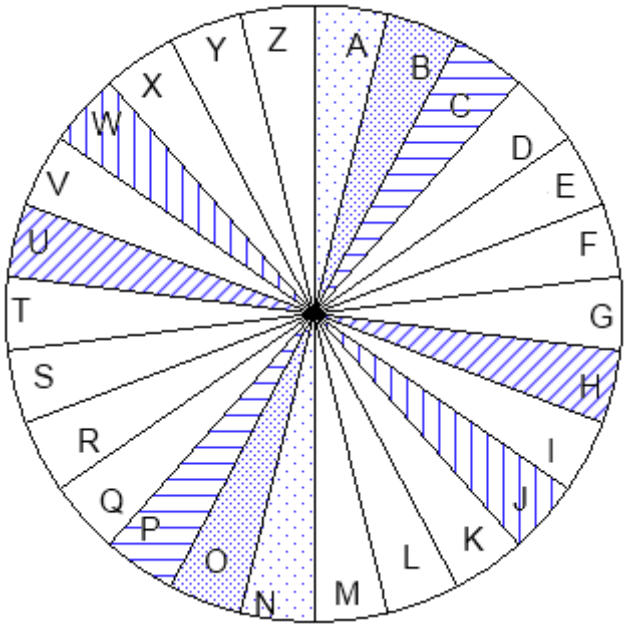


Le professeur peut leur montrer comment utiliser un logiciel pour dessiner un « camembert » divisé en 26 parties égales. Il ne restera plus qu'à écrire les lettres dans les secteurs et faire une réduction

de la taille pour obtenir le second disque. On peut par exemple, sur un tableur, remplir une ligne avec 26 cellules contenant le nombre 1 et créer le diagramme circulaire correspondant.

Il serait dommage de ne pas rattacher ces méthodes de cryptographie (décalage, substitution, chiffrement affine, ….) à la notion de fonction, particulièrement en $3^{ème}$.
Dans la classe de $5^{ème}$ et $4^{ème}$ le mot fonction est employé chaque fois que nécessaire en situation et sans définition formelle. Le professeur peut utiliser des tableaux ou des schémas fléchés.
Dans le cours classique de mathématique à partir de la $3^{ème,}$ les manuels mettent souvent l'accent sur des fonctions de $\mathbb{R}$ dans $\mathbb{R}$, parfois de $\mathbb{N}$ dans $\mathbb{N}$. On y rencontre rarement des fonctions d'un ensemble fini dans un autre ensemble fini et qui ne sont pas définies par une expression algébrique. C'est ici l'occasion de voir de telles fonctions dans un contexte où elles sont utiles.

Le ROT 13 (décalage de 13 lettres) a la particularité d'être involutif : si on applique deux fois ce décalage, on retrouve le message de départ. On peut demander aussi aux élèves s'ils n'ont pas vu en géométrie des transformations qui, quand on les fait deux fois à la suite, donnent l'identité (les symétries).
Il y a par exemple la symétrie centrale (on fait un demi-tour). Pour visualiser le lien avec le ROT 13, on écrit les 26 lettres régulièrement espacées sur deux cercles concentriques. Avec un demi-tour on a la correspondance, et avec deux demi-tours on retombe sur les lettres de départ d'où le lien avec la symétrie centrale. Ou bien, on écrit l'alphabet sur un seul cercle et on associe les lettres diamétralement opposées.



Lorsque la clé est un nombre assez grand, le calcul du décodage par soustraction peut donner des nombres négatifs. Certains élèves sont désemparés et pensent qu'ils se sont trompés. Pour résoudre ce problème, ils proposent de compléter la grille de décodage avec un autre alphabet placé à gauche.

						…	X	Y	Z	A	B	C	D	…					

Ils pensent rarement à ajouter 26 pour revenir dans les positifs. Parfois ils ne savent pas faire

l'addition : certains écrivent – 15 + 26 = – 41.

Cette difficulté va réapparaitre dans les chiffrements affines ou de Vigenère, lorsque le décalage est grand. Il est intéressant de donner un problème avec un grand décalage pour confronter les élèves à cette situation avant qu'il n'y ait d'autres difficultés.

Au lycée :

La difficulté liée au codage par involution (A donne F donc F donne A) est encore présente au lycée.

Une fois le mécanisme compris, les démarches mises en œuvre pour réduire le temps de déchiffrement face à un texte quand le décalage n'est pas connu, sont multiples. Ainsi, les élèves ont eu à déchiffrer la phrase « Xy ew higshi gi qiwweki, fvezs ! », en temps libre. (*Réponse : Tu as décodé ce message, bravo !*) On leur a demandé d'écrire leur démarche et le nombre de décalages qu'ils ont testés pour déchiffrer (au maximum 25). Leur technique la plus rapide a été de chercher à déchiffrer « xy » (le début du message). Pour cela, ils ont cherché les mots de deux lettres de la langue française, constitués de deux lettres consécutives de l'alphabet. Cette démarche est très efficace pour un message en français, codé en conservant les espaces avec un simple décalage…

3- Le chiffrement affine

L'utilisation d'un tableau de valeurs pour calculer les nombres correspondant aux codes du message chiffré rappelle le travail fait en classe sur les fonctions, dans un autre contexte plus motivant.

	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
X	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**
3x+5	**5**	**8**	**11**	**14**	**17**	**20**	**23**	**26**	**29**	**32**	**35**	**38**	**41**	**44**	**47**	**50**	**53**	**56**	**59**	**62**	**65**	**68**	**72**	**75**	**78**	**81**
Reste	**5**	**8**	**11**	**14**	**17**	**20**	**23**	**0**	**3**	**6**	**9**	**12**	**15**	**18**	**21**	**24**	**1**	**4**	**7**	**10**	**13**	**16**	**19**	**22**	**25**	**2**
	F	I	L	O	R	U	X	A	D	G	J	M	P	S	V	Y	B	E	H	K	N	Q	T	W	Z	C

Pour des petites valeurs de *a*, les élèves trouvent des astuces pour remplir le tableau de valeurs à la main, plus rapidement, sans faire tous les calculs : ils pensent aux écarts. Pour 3*x* + 5, A devient 5, B devient 8, C devient 11, …. Les nombres vont de 3 en 3. On découvre une propriété des fonctions affines (ou retrouve si le thème des fonctions affines a déjà été travaillé en classe).

Les cases grisées du tableau représentent les images des lettres de l'alphabet dans l'ordre : A donne F (décalage de 5), les autres se trouvent en décalant de 3 cases à chaque lettre.

B donne I, C donne L, etc.....

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

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

Cette activité, une fois le principe de chiffrement affine assimilé, est l'occasion de poursuivre l'utilisation du tableur qui permet par exemple de rechercher empiriquement les bons et mauvais couples de codage (voir 6- Utilisation du tableur).

Pour remplir tout le tableau :

La notion de modulo prend plus de sens que dans le chiffrement par décalage parce qu'on obtient des nombres assez grands. Les élèves voient qu'ils peuvent trouver l'image d'une lettre en écrivant l'alphabet plusieurs fois à la suite. Certains comprennent qu'il faut enlever plusieurs fois 26, ce qui peut leur faire penser à la division. Il y a une étape supplémentaire à franchir pour passer à l'utilisation du reste de la division euclidienne qui donne le résultat directement. Tous se rendent compte de l'intérêt de formaliser ainsi pour trouver le résultat plus rapidement (pour de « grandes » valeurs de a).

« De mauvais codes »

Lors de l'obtention d'une table de codage avec $a = 2$, les élèves voient vite qu'il y a un problème : deux lettres différentes peuvent être codées de la même façon. La recherche des coefficients a et b qui donnent un « bon code » est difficile au collège. Mais, on peut leur expliquer par l'exemple que si une valeur de a ne convient pas, tous les chiffrements de la forme $ax+b$, quel que soit b, ne conviennent pas non plus.

Combien de codes différents ?

Le fait qu'on peut se limiter à des valeurs de b inférieures à 26 est abordable même à un niveau collège.

La même remarque pour a, plus difficile, peut se faire, au collège, sur des exemples, en comparant les codages obtenus avec a et $a + 26$. Au lycée, la démonstration peut être faite par les élèves dans le cadre du programme. (Voir partie 1)

Questions possibles en seconde sous forme d'un travail de recherche à la maison par exemple :
Attention, la correction du dernier point peut être lourde à gérer en classe entière.

* Quel chiffrement obtient-on pour $a = 1$?
Réponse : si l'on prend $a = 1$ on obtient le chiffrement par décalage de b.

* Si a est donné, combien de chiffrements différents existe-t-il ?
Réponse : si $b \geq 26$ alors il existe p entier naturel et b' entier naturel entre 0 et 25 tel que $b = 26 \times p + b'$ alors la clé $(a ; b)$ mène au même chiffrement que la clé $(a ; b')$. Donc il en existe 26.

* On veut obtenir un chiffrement avec lequel 2 lettres différentes sont codées par 2 lettres différentes. Quelles valeurs de a (b étant choisi) sont impossibles ?
Réponse :
1) $a = 0$ est impossible, car alors toutes les lettres seraient codées par b.
2) a est un multiple de 2 est impossible car alors 0 et 13 sont codés par b. En effet 0 est codé par b. De plus, 13 est codé par b car il existe un entier p tel que $a = 2p$ donc $a \times 13 + b = 26\,p + b$.
3) a est un multiple de 13 est impossible car alors 0 et 2 sont codés par b. En effet 0 est codé par b. De plus 2 est codé par b car il existe un entier p tel que $a = 13p$ donc $a \times 2 + b = 26\,p + b$.
4) Enfin … les valeurs de a précédemment déterminées sont-elles les seules impossibles ?
Raisonnons par l'absurde : supposons que a n'est pas un multiple de 2 ni de 13 et qu'il existe x_1 et x_2 deux lettres distinctes codées par le même nombre, alors il existe n entier naturel tel que $a \times x_1 + b = a \times x_2 + b + 26 \times n$. D'où $a \times (x_1 - x_2) = 26 \times n$, or a n'est pas un multiple de 2 ni de 13, donc a n'est pas un multiple de 26. L'égalité précédente implique que $(x_1 - x_2)$ est un multiple de 26, ce qui est absurde puisque x_1 et x_2 sont deux entiers naturels compris entre 0 et 25.

4- Le chiffrement par substitution

Même en collège, les élèves voient vite qu'il y a beaucoup plus de chiffrements par substitution que de chiffrements par décalage. Avec un alphabet de 3 lettres, leurs conjectures sont très souvent 9, et parfois 8. Le résultat 9 s'explique par le calcul 3 + 3 + 3. Et même ceux qui trouvent 6, n'ont pas nécessairement fait le bon calcul $(3 \times 2 \times 1)$ car le résultat 6 peut provenir du calcul $3 + 2 + 1 = 6$. Cependant si on leur demande d'écrire tous les cas, ils arrivent à dénombrer les 6 possibilités (5 s'ils ne comptent pas l'identité).
Le professeur peut demander alors le nombre de possibilités avec 4 lettres, ce qui permet de voir

comment trouver le résultat par le calcul. Ceux qui font 4 + 3 + 2 + 1 trouvent 10 et non pas 24.
La généralisation à 26 est difficile, surtout parce que le nombre factorielle 26 leur paraît trop grand. Ils ont du mal à se le représenter, et à le considérer comme un nombre. En lycée, la notion de factorielle est beaucoup plus accessible. En terminale, cela peut être l'occasion également d'essayer de déterminer le nombre de chiffres de l'écriture décimale de 26! à l'aide du logarithme.

Pour la cryptanalyse, on propose d'abord un texte chiffré dans lequel les séparations entre les mots sont respectées, le travail est grandement facilité. Les élèves s'en rendent très facilement compte : ils commencent en général par les mots d'une lettre, puis de deux lettres, et en tirent beaucoup d'informations. Ainsi le texte proposé ne leur résiste en général que peu de temps : en moins d'une dizaine de minutes ils ont deviné un assez grand nombre de lettres pour que le message devienne lisible.

Dans la réalité les mots ne sont pas séparés, on calcule la fréquence de chaque lettre dans le texte. En classe, on peut demander aux élèves de se partager le travail, la fonction « rechercher » du traitement de texte rend la tâche moins fastidieuse et évite les erreurs de comptage. On compare les fréquences calculées avec les fréquences usuelles pour établir des correspondances. (Voir partie 1)
Selon le texte, la lettre la plus fréquente n'est pas le E ! Cette question peut se poser pour toutes les lettres. Mais connaître les fréquences usuelles d'apparition des différentes lettres permet tout de même de conclure.
Ce travail est une bonne illustration de l'intérêt des statistiques : elles sont vraiment utiles pour résoudre un problème motivant.

En devoir en temps libre en seconde, on peut poser le problème de la façon suivante :
Anna décide, plutôt que de décaler, de mélanger les lettres de l'alphabet.

1) Si l'alphabet n'avait que 3 lettres A, B, C, un mélange possible est « A est transformé en B, B est transformé en A et C reste C. Pouvez-vous écrire tous les « mélanges » possibles différents ?
2) Si l'alphabet n'avait que 4 lettres, pourriez-vous compter tous les « mélanges » possibles différents ?
3) L'alphabet compte 26 lettres : Avec ce principe de « mélange », pouvez-vous compter le nombre de manières différentes de coder le mot « codage » ? Donner un ordre de grandeur de ce nombre (*par exemple douze millions)* ».

Un intérêt de ce devoir est dans les démarches mises en œuvre, les notations ou illustrations utilisées. Ainsi, une partie des élèves gardent « ...est transformé en ... », ce qui les pousse à abandonner l'énoncé des mélanges possibles de 4 lettres, car c'est trop long à écrire, et donc ils sont conduits à expliciter la façon dont ils dénombrent.
Dans certaines classes, beaucoup d'élèves pensent que le nombre de mélanges est 4 + 3 + 2 + 1, ce qui est faux. Certains écrivent tous les mélanges sans chercher de formule.
De plus, à cause de recherches via internet, une partie des élèves est convaincue qu'il faut avoir étudié les probabilités pour répondre, ce qui donne, dans quelques devoirs, des références aux mots arrangement, combinaison, permutation ou factoriel.

La correction du devoir donne lieu à des échanges en classe :
Beaucoup choisissent une notation, dont l'interprétation peut être discutée : ABC est-il différent de BAC ? Que dire de la notation « A=B et B=C et C=B » ? Et de l'utilisation de flèches « $A \rightarrow B$ », d'un tableau... Comment écrire un triplet ?
Pour 4 lettres, ceux qui n'ont pas traité la question disent « on ne peut pas écrire tous les mélanges, il y en a beaucoup trop, on s'y perd ». Ceux qui les ont écrits en se référant à la question précédente répondent « il suffit de s'organiser » Et de leur organisation nait leur calcul. Soit « je choisis la transformée de A, puis je mélange les 3 autres d'où le calcul 4×6 ». Soit ils ne font pas référence à la question précédente et dénombrent 4 × 3 × 2 × 1, ce qui justifie le résultat 4 ! de certains, trouvé sans comprendre, sur Internet. Il est à noter qu'à aucun moment un arbre n'a été utilisé !
La substitution est très lourde à gérer avec un tableur.

5- Le chiffrement de Vigenère

a) Exemple d'exercice proposé aux élèves de collège à la suite du diaporama

Décoder le message suivant, qui a été codé avec la méthode de Vigenère et la clé ZIP

Texte en clair													
Texte en clair numérisé													
Clé	Z	I	P	Z	I	P	Z	I	P	Z	I	P	Z
Clé numérisée	25	8	15										
Texte codé numérisé	11	8											
Texte codé	L	I	I	G	M	B	Z	B	X	P	C	T	R

Réponse : MATHEMATIQUES

b) Difficultés rencontrées lors du codage et décodage

Certaines difficultés apparaissent plus spécifiquement lors du codage et décodage de Vigenère.
Le décalage de Vigenère peut induire un grand décalage dans les lettres et certains élèves qui ne sont pas à l'aise avec leur table d'addition sont fragilisés même lors de l'opération de codage.
Ensuite, les élèves ont du mal à comprendre que pour déchiffrer un message, il faut soustraire les valeurs correspondantes aux lettres de la clé puisque lorsqu'on code, on les ajoute.
On revient sur la relation addition-soustraction qui n'est pas encore évidente pour tous, alors qu'elle est essentielle si on veut comprendre la technique de résolution des équations par exemple.
Enfin, lors de la soustraction, le résultat peut être négatif. Si les élèves n'ont pas de soucis à considérer que 38 renvoie sur 12 ils ont naturellement plus de mal à associer -14 et 12. Certains se contentent d'enlever le signe et associent -14 à la lettre n°14. Cet obstacle peut être préparé lors de la numérisation de l'alphabet pour un chiffrement avec un grand décalage.

Le codage de Vigenère permet encore d'utiliser efficacement un tableur notamment lors de la mise en place d'échange sans communication de clé (voir 6° utilisation d'un tableur)

c) Une activité utilisant le codage de Vigenère sans communication de clé

« Faire deux équipes. Chaque équipe choisit une clé de Vigenère qu'elle ne transmet pas à l'autre. L'équipe 1 choisit un message qu'elle code avec sa clé 1, et l'envoie à l'autre groupe, qui code à nouveau le message à l'aide de sa clé 2, et renvoie le message (qui est maintenant doublement codé). Le message est décodé (clé 1) par la première équipe, puis envoyé et décodé (clé 2) par la $2^{ème}$ équipe…

Pourquoi ça marche ? C'est grâce à la **commutativité** de l'addition.
Une explication efficace a été celle d'un élève : armé de « post-it » (de deux couleurs) il code en couvrant d'un post-it –pour chaque code– et décode en enlevant un post-it (les post-it sont collés indépendamment les uns des autres, l'**ordre** du collage n'influe pas !).
En effet, à chaque codage par Vigenère on effectue une addition, suivie d'un modulo 26. On peut vérifier que l'opération de codage est commutative. En effet :
$((x + b)\ [26] + b'\ )\ [26] = (x + b + b')\ [26] = ((x + b')\ [26] + b)[26]$
Le message codé par les deux équipes aurait pu directement être codé par la somme des deux clés.
Il en est de même avec l'opération de décodage.

Il est à noter qu'on peut faire la même activité avec un codage par décalage, mais pas par un codage affine, ni par un codage par substitution. En effet, pour le codage affine,

$(a'(a\,x + b\,[26]) + b')\,[26] = a'a\,x + a'b + b'\,[26] \neq a'ax + ab' + b\,[26]$ (en général)

Pour la substitution, le codage consiste à appliquer une permutation ; en général si σ et τ sont deux permutations, $\sigma\tau \neq \tau\sigma$ et $\sigma^{-1}\tau^{-1} \neq \tau^{-1}\sigma^{-1}$

On peut penser que cette méthode est très sûre car les clés n'ont pas été communiquées. Mais bien que les messages voyagent chiffrés, les clés peuvent être connues par les transmetteurs et récepteurs. En effet, à la fin, les deux groupes possèdent le message en clair et le message chiffré uniquement avec la clé de l'autre. Ils peuvent donc calculer le décalage de chaque position. De même, quelqu'un qui aurait suivi toutes les étapes de l'échange est capable de retrouver les deux clés en comparant le message doublement codé avec chacun des messages codés une seule fois, donc il peut aussi retrouver le message en clair. Finalement le principe du double codage n'est pas sûr du tout !

Exemple d'échanges :

le groupe 1 a pour CLE	**M**	**A**	**T**	**H**	**S**														
soit :	12	0	19	7	18														
La phrase à envoyer est :	**L**	**E**	**W**	**I**	**S**	**H**	**A**	**M**	**I**	**L**	**T**	**O**	**N**	**E**	**S**	**T**	**N**	**U**	**L**
soit :	11	4	22	8	18	7	0	12	8	11	19	14	13	4	18	19	13	20	11
CLE 1	12	0	19	7	18	12	0	19	7	18	12	0	19	7	18	12	0	19	7
LA PHRASE CODEE EST	23	4	41	15	36	19	0	31	15	29	31	14	32	11	36	31	13	39	18
	23	4	15	15	10	19	0	5	15	3	5	14	6	11	10	5	13	13	18
soit :	X	E	P	P	K	T	A	F	P	D	F	O	G	L	K	F	N	N	S

Le groupe 2 code ce message avec

SA CLE	**H**	**O**	**M**	**E**	**R**														
soit :	7	14	12	4	17	7	14	12	4	17	7	14	12	4	17	7	14	12	4
il obtient :	30	18	27	19	27	26	14	17	19	20	12	28	18	15	27	12	27	25	22
modulo 26 :	4	18	1	19	1	0	14	17	19	20	12	2	18	15	1	12	1	25	22
	E	S	B	T	B	A	O	R	T	U	M	C	S	P	B	M	B	Z	W

Le groupe 1 décode ce message doublement codé avec

SA CLE	12	0	19	7	18	12	0	19	7	18	12	0	19	7	18	12	0	19	7
Il obtient	-8	18	-18	12	-17	-12	14	-2	12	2	0	2	-1	8	-17	0	1	6	15
modulo 26 :	18	18	8	12	9	14	14	24	12	2	0	2	25	8	9	0	1	6	15
soit :	S	S	I	M	J	O	O	Y	M	C	A	C	Z	I	J	A	B	G	P

Le groupe 2 décode ce message avec

SA CLE	7	14	12	4	17	7	14	12	4	17	7	14	12	4	17	7	14	12	4
il obtient	11	4	-4	8	-8	7	0	12	8	-15	-7	-12	13	4	-8	-7	-13	-6	11
modulo 26	11	4	22	8	18	7	0	12	8	11	19	14	13	4	18	19	13	20	11
soit :	**L**	**E**	**W**	**I**	**S**	**H**	**A**	**M**	**I**	**L**	**T**	**O**	**N**	**E**	**S**	**T**	**N**	**U**	**L**

6- Utilisation du tableur

Les tableurs possèdent des fonctions qui permettent un codage/décodage rapide d'une chaine de caractères (sans les espaces). Les formules se rentrent en commençant par un signe = et une fois la première case/colonne remplie, la poignée de recopie adapte la formule aux cellules adjacentes (on peut aussi utiliser le copier/coller)

Numérisation de l'alphabet :

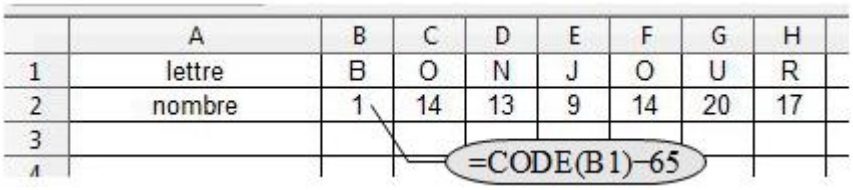
Dans un ordinateur, chaque lettre est associée à un nombre qu'on appellera 'code informatique', et cela facilite les codages et encodages à l'aide du tableur.

Les trois fonctions principales qui vont servir sont : CODE(), CAR() et MOD().

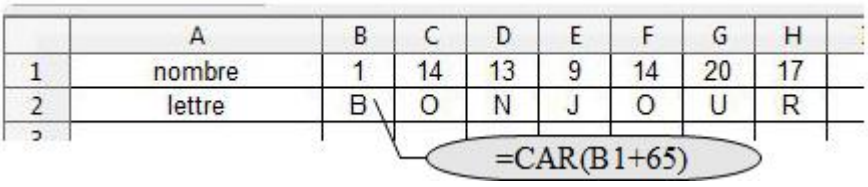
CODE renvoie le code informatique d'une lettre et réciproquement CAR renvoie la lettre correspondant au code informatique. Ces deux fonctions permettent donc de remplir une grille contenant l'alphabet à coder ou de numériser un texte entré case par case. Attention, le A correspond au numéro 65, le Z à 90 et non pas respectivement à 0 et 25. De plus, les majuscules et minuscules et les lettres accentuées portent un numéro différent, et à partir du numéro 92 apparaissent les autres caractères tels que [, / ^ etc …

Il est conseillé de travailler uniquement avec des majuscules et sans espace (dont le code informatique est loin de celui des autres lettres de l'alphabet).

Concrètement, en utilisant la poignée de recopiage des cellules du tableur, on obtient rapidement la numérisation de l'alphabet entre 0 et 25 ou d'un texte. Il est plus clair pour les élèves de ne pas afficher le code informatique pur entre 65 et 90. Ainsi pour BONJOUR on obtient :



Pour transformer une suite numérique en texte (après l'opération de décodage ou d'encodage), on utilise la fonction CAR sans oublier d'ajouter 65 à la valeur avant transformation.



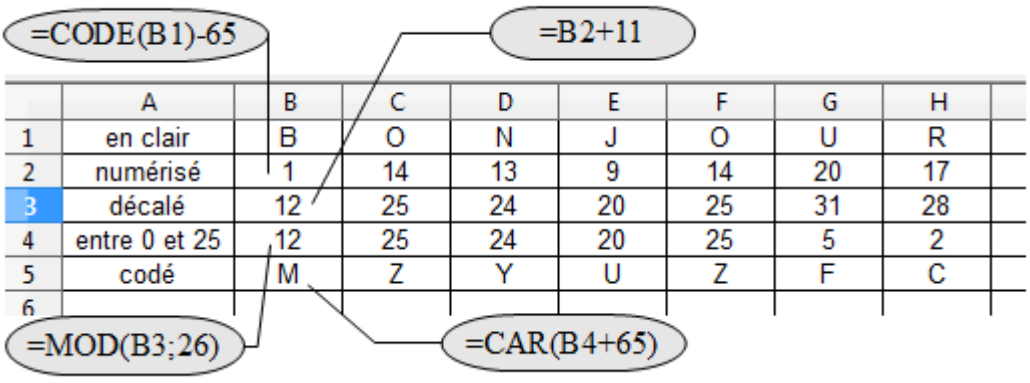
Lors des opérations d'encodage/décodage, le nombre pourra éventuellement dépasser 25 donc il faudra alors avant l'opération CAR utiliser la commande MOD(dividende, diviseur) qui renvoie le reste dans la division euclidienne du dividende par le diviseur. On peut le faire en utilisant une ligne dédiée à rapporter le nombre entre 0 et 25 à la fin de l'encodage. L'utiliser à l'intérieur de la fonction CAR est assez lourd et nécessite une bonne compréhension du tableur : =CAR(mod(B1;26)+65)

Encodage ou décodage :

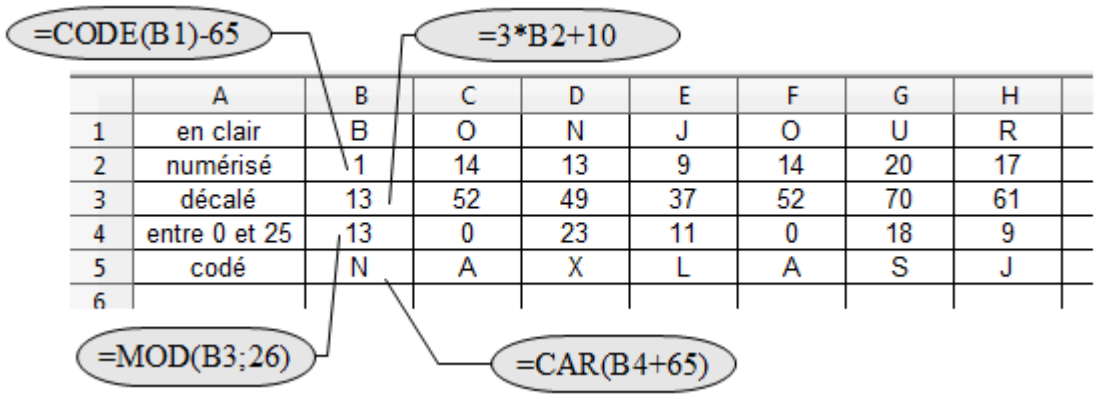
Pour une meilleure compréhension, il est conseillé de ne pas chercher à optimiser le nombre de lignes mais de différencier toutes les étapes. On aura ainsi une ligne avec le message en clair, puis sa numérisation (directement entre 0 et 25), une ou des lignes avec la transformation numérique et une ligne pour le retour à 0-25 puis enfin une ligne pour le message codé. De même on reprendra toutes ces étapes lors du décodage.

Pour encoder un décalage, il faut ajouter le décalage au code de la lettre, que ce soit un nombre fixe ou une lettre comme dans le codage Vigenère.

Exemple d'encodage par décalage fixe de 11 :

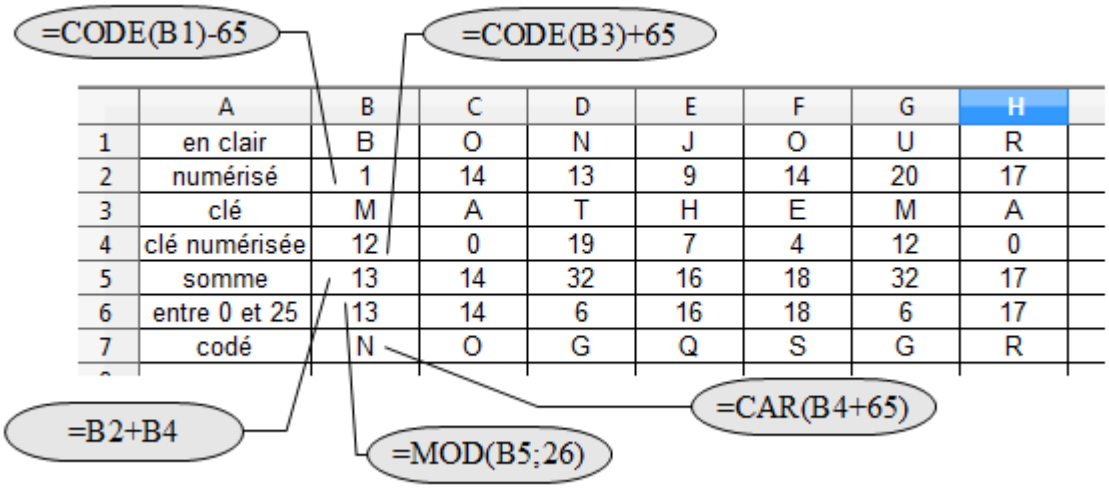


Exemple d'encodage par la fonction affine f(x)=3x+10 :



	A	B	C	D	E	F	G	H
1	en clair	B	O	N	J	O	U	R
2	numérisé	1	14	13	9	14	20	17
3	décalé	13	52	49	37	52	70	61
4	entre 0 et 25	13	0	23	11	0	18	9
5	codé	N	A	X	L	A	S	J
6								

Exemple d'encodage par méthode Vigenère avec le mot MATHEMATIQUES :

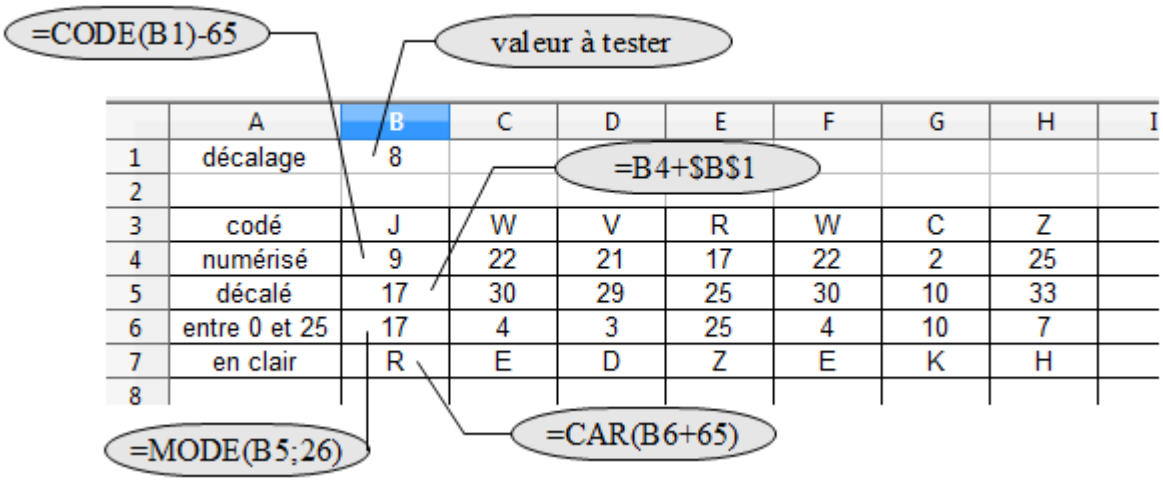


	A	B	C	D	E	F	G	H
1	en clair	B	O	N	J	O	U	R
2	numérisé	1	14	13	9	14	20	17
3	clé	M	A	T	H	E	M	A
4	clé numérisée	12	0	19	7	4	12	0
5	somme	13	14	32	16	18	32	17
6	entre 0 et 25	13	14	6	16	18	6	17
7	codé	N	O	G	Q	S	G	R

<u>Quelques remarques:</u>

1) Le tableur permet aussi de déchiffrer 'rapidement' en testant toutes les clés possibles d'un chiffrement par décalage jusqu'à obtenir un texte compréhensible en français. Les valeurs de la clé à tester sont inscrites successivement dans une cellule et les formules devront utiliser la référence absolue de cette cellule ($).

   Si on n'utilise pas la référence absolue, on peut créer un grand tableau de 26 lignes avec toutes les clés possibles. On prendra la ligne contenant un message compréhensible (voir annexe)

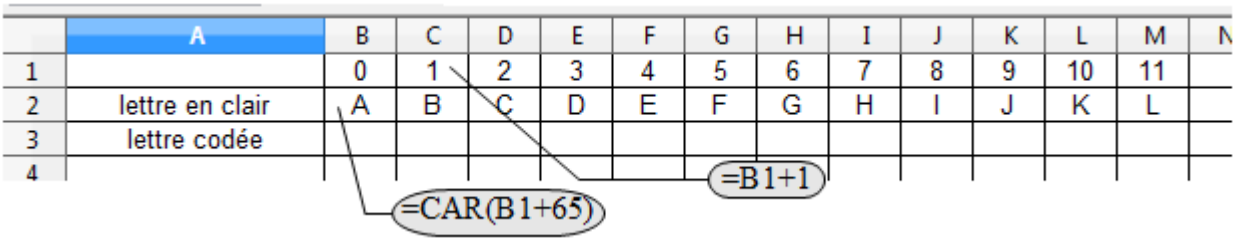


	A	B	C	D	E	F	G	H	I
1	décalage	8							
2									
3	codé	J	W	V	R	W	C	Z	
4	numérisé	9	22	21	17	22	2	25	
5	décalé	17	30	29	25	30	10	33	
6	entre 0 et 25	17	4	3	25	4	10	7	
7	en clair	R	E	D	Z	E	K	H	
8									

On teste les valeurs jusqu'à pouvoir lire un texte en clair :

	A	B	C	D	E	F	G	H
1	décalage	18						
2								
3	codé	J	W	V	R	W	C	Z
4	numérisé	9	22	21	17	22	2	25
5	décalé	27	40	39	35	40	20	43
6	entre 0 et 25	1	14	13	9	14	20	17
7	en clair	B	O	N	J	O	U	R
8								

2) Ces fonctions permettent d'écrire un alphabet de codage ou décodage à faire remplir aux élèves (pour rendre invisible la 1ere ligne, il suffit de choisir comme couleur de caractère le blanc). Des grilles photocopiables sont en annexe.

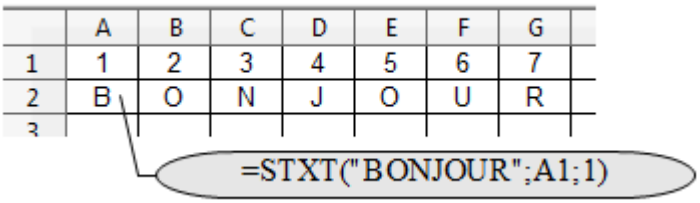


	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1		0	1	2	3	4	5	6	7	8	9	10	11	
2	lettre en clair	A	B	C	D	E	F	G	H	I	J	K	L	
3	lettre codée													
4														

L'utilisation du tableur pour remplir ces grilles permet de rechercher expérimentalement les couples (*a* , *b*) qui ne donnent pas un codage affine correct. Là encore on utilise le référencement absolu sur les paramètres (il peut être judicieux d'amener les élèves à réfléchir au rôle de *b*)

4) Le professeur peut lors de la préparation de ses activités utiliser la fonction STXT ("texte"; *début* ; *nombre*) qui extrait les lettres du texte situées à la position donnée par *début, nombre* étant le nombre de lettres à extraire, ici 1. Cela évite de retaper le texte lettre par lettre dans les

cases : il suffit de créer une ligne d'entiers successifs puis de recopier la cellule A2 vers la droite.



4) Le site internet http://www.dcode.fr/ permet un gain remarquable pour préparer les fiches élèves. Le professeur y trouvera des logiciels permettant de coder un texte tapé normalement.

Les feuilles distribuées aux élèves sont présentées avec leur corrigé en annexe.

Partie 4

Cubiques et cubiques elliptiques en 1ère et terminale

Nous proposons ici quelques idées aux enseignants de lycée pour faire étudier des fonctions à leurs élèves tout en faisant un lien avec la cryptologie.

Nous avons vu dans la **Partie 1** la définition d'une courbe elliptique. C'est l'ensemble des points de coordonnées (x,y) où x et y vérifient
$y^2 = x^3 + px + q$ les paramètres p et q étant choisis tels que $4p^3 + 27q^2 \neq 0$

Nous avons dit que dans ce cas la courbe n'a pas de points de rebroussement et que l'allure des courbes dépend du signe de $4p^3 + 27q^2$.

Les élèves de 1ère ou de terminale peuvent comprendre un peu de quoi il s'agit en procédant par étapes. Nous suggérons que le professeur dise d'abord ce qu'est une cubique.
C'est une courbe dans le plan dont l'équation générale est de la forme
$Ax^3 + By^3 + Cx^2y + Dxy^2 + Ex^2 + Fy^2 + Gxy + Hx + Iy + J = 0$ avec au moins un des quatre paramètres A, B, C ou D non nuls.

La courbe d'équation $y = x^3$ (qu'ils connaissent peut-être déjà) est une cubique (sinon leur demander de la tracer rapidement). C'est la représentation graphique d'une fonction.
La courbe d'équation $y^2 = x^3 + 1$ est aussi une cubique mais n'est pas la représentation graphique d'une fonction.

Nous allons commencer par quelques remarques sur la résolution de l'équation du 3ème degré et les fonctions polynômes de 3ème degré.

a) Forme réduite pour résoudre l'équation $x^3 + ax^2 + bx + c = 0$ et pour représenter la fonction f telle que $f(x) = x^3 + ax^2 + bx + c$

Nous prenons le coefficient du terme en x^3 égal à 1 car même si ce n'est pas le cas c'est un nombre non nul. Nous pouvons donc supposer que nous avons divisé les deux membres de l'équation par ce nombre. Pour la fonction ceci revient à transformer la courbe représentative par une affinité (multiplication des ordonnées) comme lorsqu'on remplace la parabole d'équation

$y = ax^2$ par celle d'équation $y = x^2$

Par un changement d'inconnue pour l'équation ou une translation des axes pour la courbe, on peut ensuite éliminer le terme en x^2.

On pose $x = X + \alpha$ et l'équation devient

$$(X + \alpha)^3 + a(X + \alpha)^2 + b(X + \alpha) + c = 0$$

$$X^3 + X^2(3\alpha + a) + X(3\alpha^2 + 2a\alpha + b) + \alpha^3 + a\alpha^2 + b\alpha + c = 0$$

Pour éliminer le coefficient de X^2 il suffit de choisir $\alpha = -\frac{a}{3}$

L'équation se ramène alors à $x^3 + px + q = 0$ et il suffit d'étudier les fonctions f telles que $f(x) = x^3 + px + q$

Il nous paraît intéressant de faire remarquer aux élèves que le même procédé permet de réduire l'équation du second degré $ax^2 + bx + c = 0$

Ils connaissent peut être la forme canonique pour réduire l'équation, mais un autre procédé consiste à écrire: $(X + \alpha)^2 + b(X + \alpha) + c = 0$ et à chercher α pour annuler le coefficient de X.

$$X^2 + X(2\alpha + b) + \alpha^2 + b\alpha + c = 0$$

Pour annuler le coefficient de X, on choisit $\alpha = -\frac{b}{2}$ et alors $\alpha^2 + b\alpha + c = \frac{4c - b^2}{4}$

L'équation devient $x^2 + k = 0$ et il suffit d'étudier les fonctions f telles que $f(x) = x^2 + k$ avec $k = \frac{4c - b^2}{4}$ Ceci revient évidemment à effectuer le même changement d'inconnue pour l'équation et la même translation des axes pour la courbe qu'avec la forme canonique.

Si $k < 0$ soit $b^2 - 4c > 0$, l'équation a deux racines réelles et la courbe coupe l'axe des abscisses en deux points.

<u>b- Nombre de racines réelles de l'équation $x^3 + px + q = 0$ et variations de la fonction</u>

Le professeur pourra éventuellement parler du procédé de résolution des équations de degré 3, en donnant (ou démontrant) la formule de Cardan (Ars Magna-1545) découverte par Tartaglia

(vers 1530) et en parlant du travail de Bombelli à partir de ces formules (en 1572), ce qui a motivé l'introduction de l'écriture de nombre sous la forme $a + b\sqrt{-1}$.

La notation $\sqrt{-1} = i$ a été introduite par Euler en 1777.

L'étude de la fonction f telle que $f(x) = x^3 + px + q$ va nous donner les résultats dont nous avons besoin.

On a: $f\,'(x) = 3x^2 + p$

1er cas : $p \geq 0$: La dérivée est positive donc la fonction f croit de façon monotone dans P. Elle s'annule une seule fois et donc le polynôme a une seule racine réelle.

2ème cas : $p<0$: la dérivée change deux fois de signe pour $x_1 = -\sqrt{\frac{-p}{3}}$ et $x_2 = \sqrt{\frac{-p}{3}}$

ce qui donne le tableau de variation suivant :

x	$-\infty$ $\quad -\sqrt{\frac{-p}{3}} \quad\quad \sqrt{\frac{-p}{3}} \quad +\infty$
f	$-\infty$ ↗ $f(x_1)$ ↘ $f(x_2)$ ↗ $+\infty$

Si $f(x_1)$ et $f(x_2)$ sont de signe contraire, c'est-à-dire $f(x_1) \times f(x_2) < 0$, la fonction s'annule trois fois, donc l'équation a trois racines réelles.

Si $f(x_1)$ et $f(x_2)$ sont de même signe (positif ou négatif), c'est-à-dire $f(x_1) \times f(x_2) > 0$, la fonction s'annule une seule fois, donc l'équation a une seule racine réelle.

Si $f(x_1) \times f(x_2) = 0$, ceci veut dire que $f(x_1)$ ou $f(x_2)$ est nul, donc x_1 ou x_2 est racine double de l'équation et que la courbe est tangente à l'axe des abscisses en ce point.

Si c'est $f(x_1)$ qui est nul alors $f(x_2) <0$ et la fonction s'annule en un autre point.

Si c'est $f(x_2)$ qui est nul alors $f(x_1) > 0$ et la fonction s'annule en un autre point.

Dans tous les cas : $f\,''(x) = 6\,x$

La courbe a un point d'inflexion pour $x = 0$. La concavité de la courbe est tournée vers le bas sur $]-\infty, 0]$ et elle est tournée vers le haut sur $[0, +\infty[$.

On peut calculer $f(x_1) \times f(x_2)$ en fonction de p et q :

$$\left[\left(\sqrt{\frac{-p}{3}}\right)^3 + p\sqrt{\frac{-p}{3}} + q\right]\left[\left(-\sqrt{\frac{-p}{3}}\right)^3 - p\sqrt{\frac{-p}{3}} + q\right] = \left(-\frac{p}{3}\sqrt{\frac{-p}{3}} + p\sqrt{\frac{-p}{3}} + q\right)$$

$$\left(\frac{p}{3}\sqrt{\frac{-p}{3}} - p\sqrt{\frac{-p}{3}} + q\right) = \left(q + \frac{2p}{3}\sqrt{\frac{-p}{3}}\right)\left(q - \frac{2p}{3}\sqrt{\frac{-p}{3}}\right) =$$

$$q^2 - \left[\left(\sqrt{\frac{-p}{3}}\right)\frac{2p}{3}\right]^2 = q^2 + \frac{4p^3}{27} = \frac{4p^3 + 27q^2}{27}$$

Il y a donc trois racines réelles distinctes si $4p^3 + 27\,q^2 < 0$.

<u>En résumé :</u> Dans le cas où $p \geq 0$ on a $4p^3 + 27\,q^2 \geq 0$ et, comme nous l'avons vu, une seule racine réelle.

$4p^3 + 27\,q^2 < 0$ est bien la condition générale pour avoir trois racines réelles distinctes. (quel que soit p) = 1

<u>Remarque sur la notion de discriminant</u> :

Pour le second degré, on a vu que l'équation $ax^2 + bx + c = 0$ peut devenir $x^2 + k = 0$ avec $k = \dfrac{4c - b^2}{4}$.

On a alors $f(x) = x^2 + k$ donc $f'(x) = 2x$ qui s'annule en 0 et $f(0) = k$

C'est bien le signe de k qui donne le nombre de racines de l'équation.

En effet, si $k < 0$ soit $b^2 - 4c > 0$, l'équation a deux racines réelles et la courbe coupe l'axe des abscisses en deux points.

Dans le cas de la fonction $f(x) = ax^2 + bx + c$ alors $f'(x) = 2ax + b$ qui s'annule en x_1 et on a :

$f(x_1) = f\left(\frac{-b}{2a}\right) = \frac{-b^2+4ac}{4a^2}$

On reconnait, au numérateur de $f(x_1)$, l'opposé du discriminant usuel.

Pour la fonction polynôme de degré 3, on a été amené à considérer $f(x_1) \times f(x_2)$ qui est le produit des valeurs prises par la fonction quand sa dérivée s'annule.
le signe de ce produit indique le nombre de racines réelles de l'équation $f(x)= 0$.

Ceci conduit, en généralisant la notion de discriminant d'une équation, à appeler $4p^3 + 27q^2$ le discriminant de l'équation $x^3 + px + q = 0$.

c- Exemples de courbe d'équation $y = x^3 + px + q$

Exemple 1 : $y = x^3 - x = x(x^2 - 1)$

On considère la fonction $f(x) = x^3 - x$.

L'équation $f(x) = 0$ a trois racines réelles évidentes : 0 ; 1 et –1.

On a bien $4p^3 + 27q^2 = -4$ négatif.

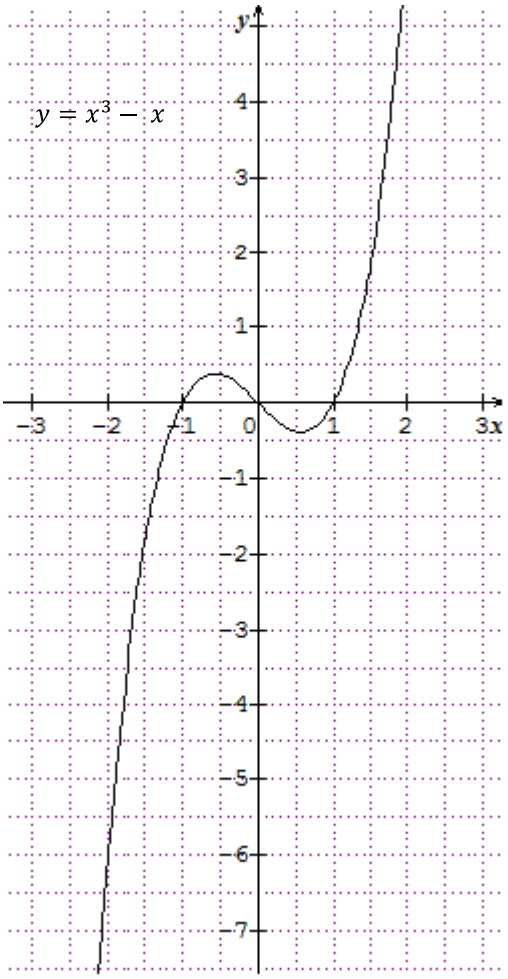
$f'(x) = 3x^2 - 1$ d'où deux changements de signe de la dérivée.

$f''(x) = 6x$ d'où un point d'inflexion à l'origine.

La fonction est impaire donc il y a une symétrie de la courbe par rapport à l'origine.

x	$-\infty$ $\quad -\frac{\sqrt{3}}{3} \quad \frac{\sqrt{3}}{3} \quad +\infty$
$f(x)$	$-\infty$ ↗ $\frac{2\sqrt{3}}{9}$ ↘ $-\frac{2\sqrt{3}}{9}$ ↗ $+\infty$

On vérifie que le produit $f(x_1) \times f(x_2)$ est bien égal à $\frac{4p^3 + 27q^2}{27} = \frac{-4}{27}$



Exemple 2 : On considère $y = x^3 - 1 = (x - 1)(x^2 + x + 1)$

$$y = (x-1)\left[(x+\frac{1}{2})^2 - \frac{1}{4} + 1\right]$$

$$y = (x-1)\left[(x+\frac{1}{2})^2 + \frac{3}{4}\right]$$

On considère $f(x) = x^3 - 1$, l'équation $f(x) = 0$ a une seule racine réelle : 1 .

On a bien $4p^3 + 27\,q^2 = 1$ positif.

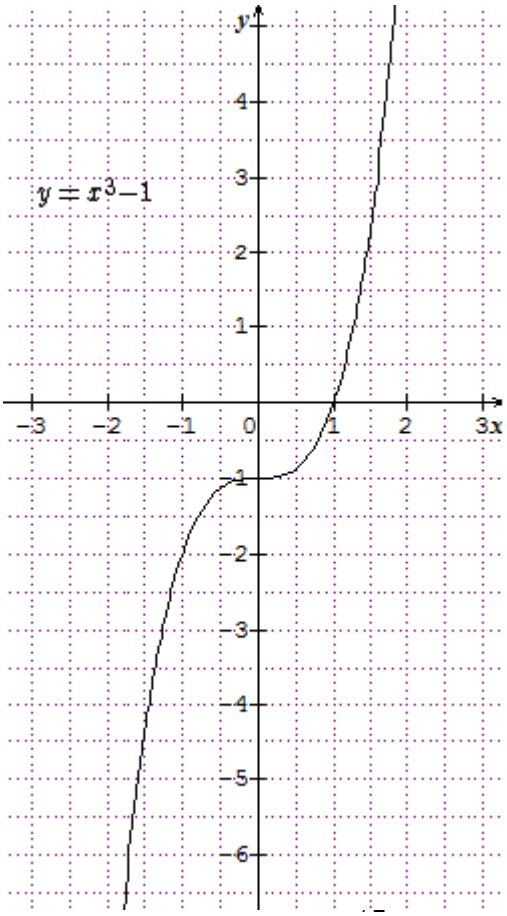
$f'(x) = 3x^2$ est toujours positive ou nulle, la fonction est croissante.

$f''(x) = 6x$ s'annule en 0 en changeant de signe, d'où un point d'inflexion au point (0, −1).

En ce point la tangente est horizontale.

De plus ce point est centre de symétrie pour la courbe car

$f(x) + 1 = x^3$ change de signe si x change de signe.



Exemple 3 : $y = x^3 - 3x + 2 = (x-1)^2 (x+2)$

On considère la fonction $f(x) = x^3 - 3x + 2$.

L'équation $f(x) = 0$ a une racine réelle simple (–2) et 1 est une racine réelle double.

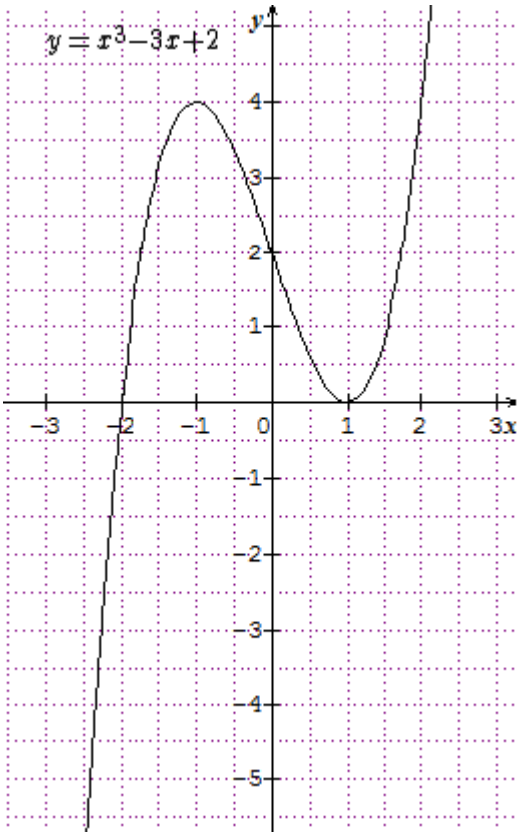
On a bien $4p^3 + 27q^2 = 0$

$f'(x) = 3x^2 - 3 = 3(x+1)(x-1)$ change deux fois de signe.

Au point d'abscisse 1, la courbe est tangente à l'axe des abscisses (point double)

$f''(x) = 6x$ d'où un point d'inflexion au point (0 ; 2).

De plus, ce point est centre de symétrie pour la courbe car $f(x) + 2 = x^3 - 3x$ change de signe si x change de signe.



d- Courbes d'équation $y^2 = x^3 + px + q$

Ces courbes se placeront dans des domaines où $x^3 + px + q$ est positif ou nul.

On pourra les décomposer en deux branches.

$y = \sqrt{x^3 + px + q}$ et $y = -\sqrt{x^3 + px + q}$

Ces branches seront symétriques par rapport à l'axe des abscisses.

Exemple 1 : Courbe d'équation $y^2 = x^3 - x$

Il s'agit donc de tracer la courbe représentant la fonction $f(x) = \sqrt{x^3 - x}$

Domaine de définition : $[-1, 0] \cup [1, +\infty[$

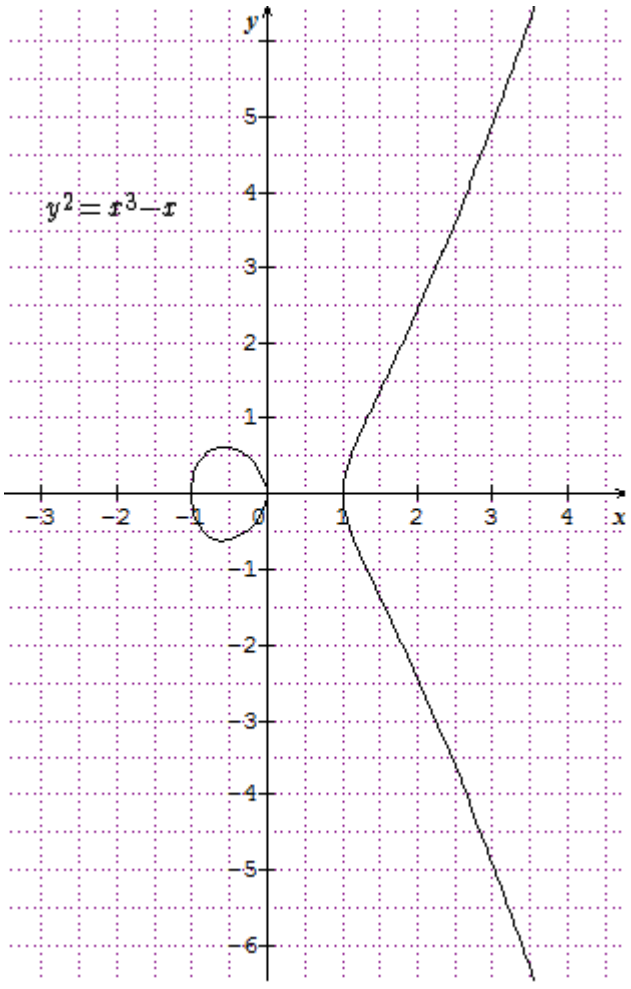
$f'(x) = \dfrac{3x^2 - 1}{2\sqrt{x^3 - x}}$ qui change une fois de signe dans le domaine de définition.

On remarque que la tangente à la courbe sera verticale pour $x = -1$, $x = 0$ et $x = 1$

On peut dresser le tableau de variations :

x	$-\infty$	-1	$-\frac{\sqrt{3}}{3}$	0	$\frac{\sqrt{3}}{3}$	1	$+\infty$
$f'(x)$		$+$	0	$-$		$+$	
$f(x)$		0 ↗		↘ 0		0 ↗	$+\infty$

Après symétrie par rapport à l'axe des abscisses on obtient la courbe complète, type de celles utilisées en cryptologie



Exemple 2 : Courbe d'équation $y^2 = x^3 - 1$

Il s'agit donc de tracer la courbe représentant la fonction $f(x) = \sqrt{x^3 - 1}$.

Domaine de définition : $[1,+\infty[$.

$f'(x) = \dfrac{3x^2}{2\sqrt{x^3-1}}$ La dérivée est toujours positive dans le domaine de définition.

Au point d'abscisse $x = 1$, la tangente est verticale.

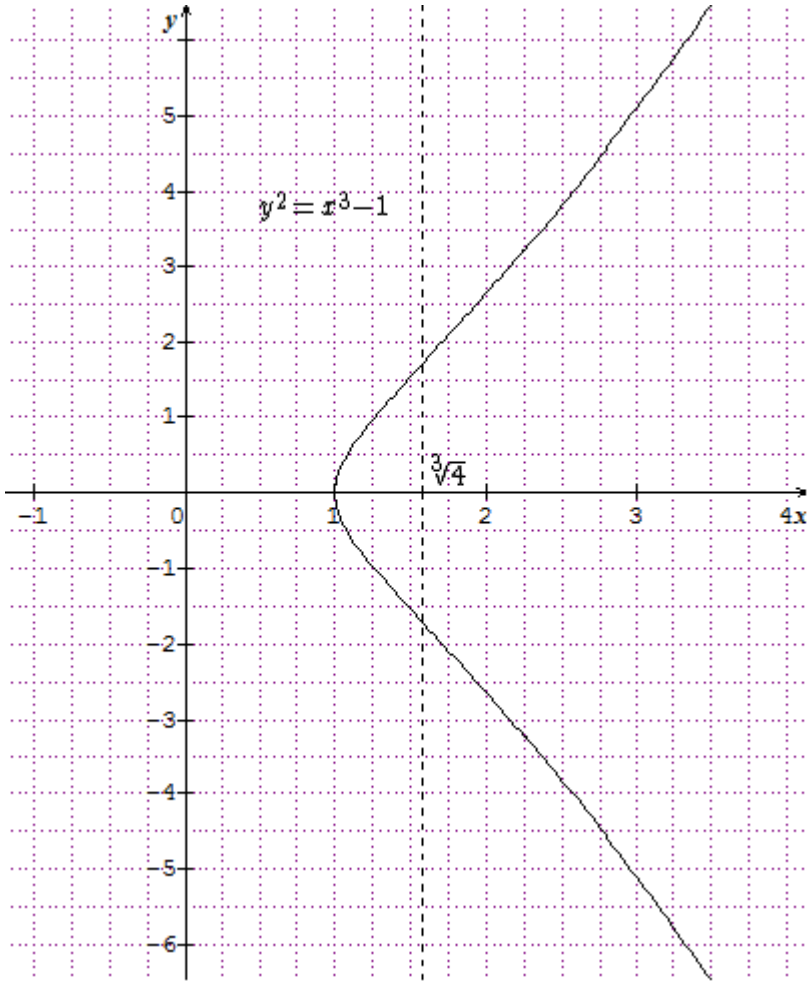
$$f''(x) = \frac{3}{2} \times \frac{2x\sqrt{x^3-1} - x^2 \times \dfrac{3x^2}{2\sqrt{x^3-1}}}{x^3-1} = \frac{3}{2} \times \frac{4x(x^3-1) - 3x^4}{2(x^3-1)\sqrt{x^3-1}} = \frac{3}{4} \times \frac{x(x^3-4)}{(x^3-1)\sqrt{x^3-1}}$$

Il y a un point d'inflexion d'abscisse $\sqrt[3]{4}$.

$f''(x) < 0$ si $x < \sqrt[3]{4}$ (concavité vers le bas),

$f''(x) > 0$ si $x > \sqrt[3]{4}$ (concavité vers le haut).

En complétant par la symétrie par rapport à l'axe des abscisses on obtient la courbe complète.



Exemple 3 : Courbe d'équation $y^2 = x^3 - 3x + 2 = (x - 1)^2(x + 2)$

Il s'agit donc de tracer la courbe représentant la fonction $f(x) = \sqrt{x^3 - 3x + 2}$.

Domaine de définition : $[-2, +\infty[$.

$f'(x) = \dfrac{3x^2 - 3}{2\sqrt{x^3 - 3x + 2}}$ qui change deux fois de signe dans le domaine de définition.

La tangente est horizontale au point de coordonnées (–1, 2).

La tangente est verticale au point de coordonnées (–2, 0).

On peut chercher la pente de la tangente au point de coordonnées (1, 0)

Si x tend vers 1 par valeurs supérieures la pente de la tangente sera donnée par

$f'(x) = \dfrac{3(x-1)(x+1)}{2(x-1)\sqrt{x+2}} = \dfrac{3}{2} \times \dfrac{x+1}{\sqrt{x+2}}$ soit $\sqrt{3}$

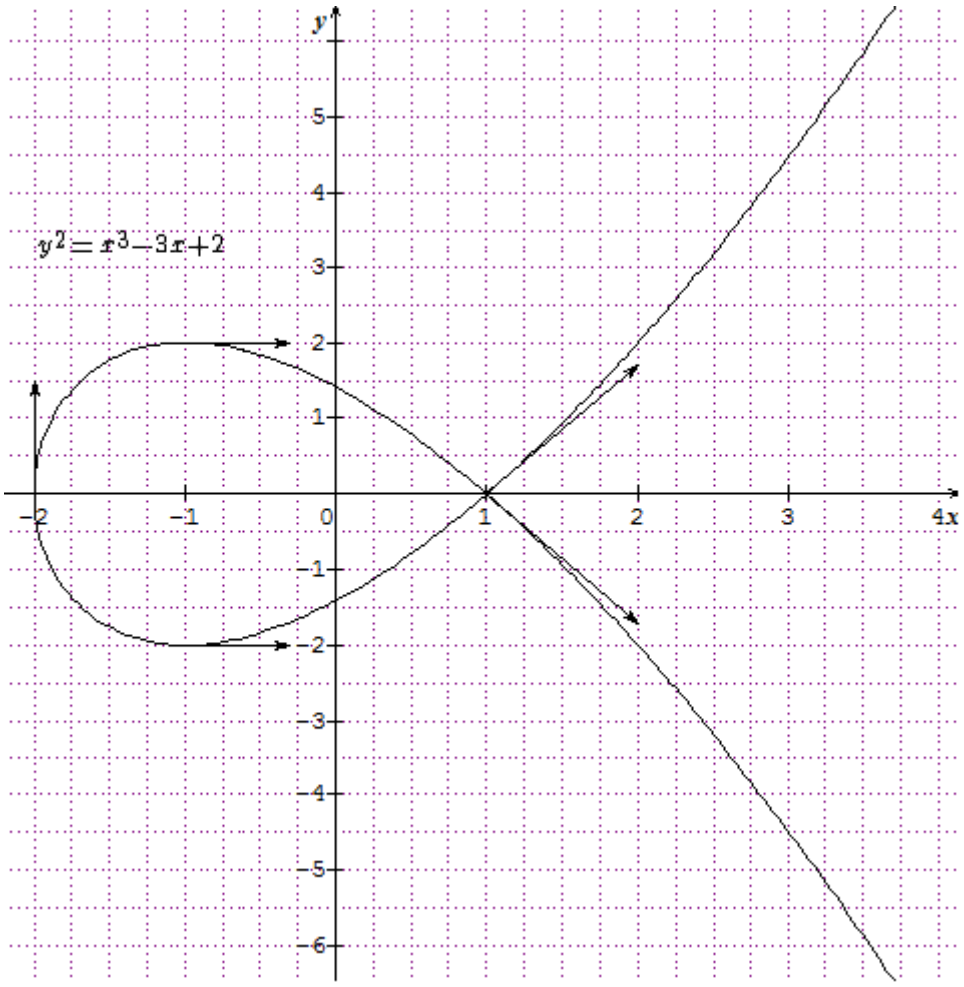
Si x tend vers 1 par valeurs inférieures la pente de la tangente sera donnée par

$f'(x) = \dfrac{3(x-1)(x+1)}{-2(x-1)\sqrt{x+2}} = -\dfrac{3}{2} \times \dfrac{x+1}{\sqrt{x+2}}$ soit $-\sqrt{3}$

D'où le point de rebroussement : nous sommes dans le cas $4p^3 + 27\,q^2 = 0$.

On peut dresser le tableau de variations :

x	$-\infty$	-2	-1	1	$+\infty$
$f'(x)$		+	0 –		+
$f(x)$		0 ↗	2 ↘	0 ↗	$+\infty$



Remarques sur la forme des courbes :

La relative ressemblance dans la forme entre les courbes d'équation $y = x^3 + px + q$ et celles d'équation $y = \sqrt{x^3 + px + q}$ et cela dans les trois cas, s'explique par la composition avec la fonction racine carrée, croissante, donc le sens de variation est le même.

Dans le troisième exemple, la racine double $x = 1$, de la courbe d'équation $y = x^3 - 3x + 2$ induit un point de rebroussement pour la courbe d'équation $y^2 = x^3 - 3x + 2$.

Une telle courbe ne peut pas servir en cryptologie. Le codage consiste à calculer pour les points P, la somme P + P + …. + P = n.P. Pour cela on utilise la tangente à la courbe (voir partie 1 p 22). En P(1 ; 0), le point de rebroussement, il y a deux tangentes, la somme P + P n'est pas définie.

Sommaire des annexes

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

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

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

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

	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
x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
f(x)																										
mod(26)																										
code																										

	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
x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
f(x)																										
mod(26)																										
code																										

	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
x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
f(x)																										
mod(26)																										
code																										

	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
x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
f(x)																										
mod(26)																										
code																										

Vigenère

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**
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Phrase à coder																									
X																									
clé																									
Y																									
X+Y																									
modulo26																									
Phrase codée																									

Phrase à décoder																									
X																									
clé																									
Y																									
X-Y																									
modulo26																									
Phrase décodée																									

Devoir maison seconde

Ce travail est à rédiger, votre recherche sera évaluée, mais non notée.

La réglette de Saint Cyr : Un instrument simple pour faire du chiffrement par décalage.

Anna souhaite envoyer un message codé à Nicolas …

Partie A : Elle utilise la réglette ci-dessus pour décaler chaque lettre de l'alphabet. Elle obtient le message suivant : « Xy ew higshi gi qiwweki, fvezs ! Xy gsrremw fmir xsr eptlefix ! » .

1) Combien de tests au maximum doit-on faire pour déchiffrer ce message ?
2) Décrypter ce message (écrivez votre démarche, le nombre de tests, la technique pour réduire le nombre de tests…)

Partie B : Le déchiffrement de son message étant trop « facile », Anna décide, plutôt que de décaler, de mélanger les lettres de l'alphabet (Par exemple : A→B, B→E, C→A, D→C, E→D, etc.)

1) Si l'alphabet n'avait que 3 lettres A, B, C… Pouvez-vous écrire tous les « mélanges » possibles différents ?
2) Si l'alphabet n'avait que 5 lettres… Pouvez-vous compter tous les « mélanges » possibles différents ?
3) L'alphabet compte 26 lettres… Avec ce principe de « mélange », pouvez-vous compter le nombre de manières différentes de coder le mot « codage » ? Donner un ordre de grandeur de ce nombre (*par exemple douze millions).*
4) Un texte suffisamment long étant donné, pouvez-vous trouver le nombre de tests au maximum qu'il faut faire pour décoder l'alphabet *(donner un ordre de grandeur de ce nombre, énoncez le comme au 3°)* ?

Partie C : Le codage précédent pouvant difficilement être déchiffré sans en connaître la « clé », Anna (qui a de la suite dans les idées) décide de revenir au décalage, en utilisant plusieurs décalages différents. Elle envoie pour cela à Nicolas une « clé » pour décoder le message.

Le message qu'elle envoie à Nicolas (celui que vous avez déchiffré au A] 2)) avec ce nouveau codage est : '' « Vv du ehepgg dh ofvubjg, cucwr ! Vv fqoqcjv djhp urp boriddfw ! » . La clé est 213. Anna. ''

Devinez le principe du codage d'Anna.

Partie D : Quelques jours plus tard, Nicolas donne à Anna « 25 48 30 56 12 25 16 63 40 49 48 10 10 18 63 40 42 24 42 25 25 12 15 42 42 64 24 36 48 64 25 16 42 16 48 2 24 48 64 56 30 42 25 7 30 56 25 12 48 25 30 42 25 30 12 28 20 42 25 16 42 24 56 20 30 48 54 20 48 40 12 30 48 36 64 100 25 48 64 36 64 18 63 72 48 25 42 20 42 25 100 » avec ce tableau :

Décodez le message de Nicolas.

×	1	2	3	4	5	6	7	8	9	10
1	–	x	ç	w	j	è	,	k	ô	f
2	x	w	è	k	f	a	:	d	r	l
3	ç	è	ô	a	g	r	û	m	ï	t
4	w	k	a	d	l	m	b	q	o	c
5	j	f	g	l	s	t	à	c	ê	.
6	è	a	r	m	t	o	e	i	p	z
7	,	:	û	b	à	e	h	u	é	y
8	k	d	m	q	c	i	u	n	v	î
9	ô	r	ï	o	ê	p	é	v	?	â
10	f	l	t	c	.	z	y	î	â	!

Utilisation du tableur pour tester tous les décodages d'un chiffrement par décalage (méthode exhaustive)

1. Ecrire une seule lettre par cellule et en majuscule

2. Traduire la lettre en nombre
=CODE(A2)-65
Formule à étirer vers la droite

	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	AA	AB	AC	AD
1																														
2	T	X	L	S	R	X	U	U	D	G	H	F	K	L	I	I	U	H	U	Q	R	V	P	H	V	V	D	J	H	V
3	U	Y	M	T	S	Y	V	V	E	H	I	G	L	M	J	J	V	I	V	R	S	W	Q	I	W	W	E	K	I	W
4	V	Z	N	U	T	Z	W	W	F	I	J	H	M	N	K	K	W	J	W	S	T	X	R	J	X	X	F	L	J	X
5	W	A	O	V	U	A	X	X	G	J	K	I	N	O	L	L	X	K	X	T	U	Y	S	K	Y	Y	G	M	K	Y
6	X	B	P	W	V	B	Y	Y	H	K	L	J	O	P	M	M	Y	L	Y	U	V	Z	T	L	Z	Z	H	N	L	Z
7	Y	C	Q	X	W	C	Z	Z	I	L	M	K	P	Q	N	N	Z	M	Z	V	W	A	U	M	A	A	I	O	M	A
8	Z	D	R	Y	X	D	A	A	J	M	N	L	Q	R	O	O	A	N	A	W	X	B	V	N	B	B	J	P	N	B
9	A	E	S	Z	Y	E	B	B	K	N	O	M	R	S	P	P	B	O	B	X	Y	C	W	O	C	C	K	Q	O	C
10	B	F	T	A	Z	F	C	C	L	O	P	N	S	T	Q	Q	C	P	C	Y	Z	D	X	P	D	D	L	R	P	D
11	C	G	U	B	A	G	D	D	M	P	Q	O	T	U	R	R	D	Q	D	Z	A	E	Y	Q	E	E	M	S	Q	E
12	D	H	V	C	B	H	E	E	N	Q	R	P	U	V	S	S	E	R	E	A	B	F	Z	R	F	F	N	T	R	F
13	E	I	W	D	C	I	F	F	O	R	S	Q	V	W	T	T	F	S	F	B	C	G	A	S	G	G	O	U	S	G
14	F	J	X	E	D	J	G	G	P	S	T	R	W	X	U	U	G	T	G	C	D	H	B	T	H	H	P	V	T	H
15	G	K	Y	F	E	K	H	H	Q	T	U	S	X	Y	V	V	H	U	H	D	E	I	C	U	I	I	Q	W	U	I
16	H	L	Z	G	F	L	I	I	R	U	V	T	Y	Z	W	W	I	V	I	E	F	J	D	V	J	J	R	X	V	J
17	I	M	A	H	G	M	J	J	S	V	W	U	Z	A	X	X	J	W	J	F	G	K	E	W	K	K	S	Y	W	K
18	J	N	B	I	H	N	K	K	T	W	X	V	A	B	Y	Y	K	X	K	G	H	L	F	X	L	L	T	Z	X	L
19	K	O	C	J	I	O	L	L	U	X	Y	W	B	C	Z	Z	L	Y	L	H	I	M	G	Y	M	M	U	A	Y	M
20	L	P	D	K	J	P	M	M	V	Y	Z	X	C	D	A	A	M	Z	M	I	J	N	H	Z	N	N	V	B	Z	N
21	M	Q	E	L	K	Q	N	N	W	Z	A	Y	D	E	B	B	N	A	N	J	K	O	I	A	O	O	W	C	A	O
22	N	R	F	M	L	R	O	O	X	A	B	Z	E	F	C	C	O	B	O	K	L	P	J	B	P	P	X	D	B	P
23	O	S	G	N	M	S	P	P	Y	B	C	A	F	G	D	D	P	C	P	L	M	Q	K	C	Q	Q	Y	E	C	Q
24	P	T	H	O	N	T	Q	Q	Z	C	D	B	G	H	E	E	Q	D	Q	M	N	R	L	D	R	R	Z	F	D	R
25	Q	U	I	P	O	U	R	R	A	D	E	C	H	I	F	F	R	E	R	N	O	S	M	E	S	S	A	G	E	S
26	R	V	J	Q	P	V	S	S	B	E	F	D	I	J	G	G	S	F	S	O	P	T	N	F	T	T	B	H	F	T
27	S	W	K	R	Q	W	T	T	C	F	G	E	J	K	H	H	T	G	T	P	Q	U	O	G	U	U	C	I	G	U

AE AF

AG	AH	AI	AJ	AK	AL	AM	AN	AO	AP	AQ	AR	AS	AT	AU	AV	AW	AX	AY	AZ	BA	BB	BC	BD	BE	BF	BG	BH	BI	BJ
19	23	11	18	17	23	20	20	3	6	7	5	10	11	8	8	20	7	20	16	17	21	15	7	21	21	3	9	7	21
20	24	12	19	18	24	21	21	4	7	8	6	11	12	9	9	21	8	21	17	18	22	16	8	22	22	4	10	8	22
21	25	13	20	19	25	22	22	5	8	9	7	12	13	10	10	22	9	22	18	19	23	17	9	23	23	5	11	9	23
22	0	14	21	20	0	23	23	6	9	10	8	13	14	11	11	23	10	23	19	20	24	18	10	24	24	6	12	10	24
23	1	15	22	21	1	24	24	7	10	11	9	14	15	12	12	24	11	24	20	21	25	19	11	25	25	7	13	11	25
24	2	16	23	22	2	25	25	8	11	12	10	15	16	13	13	25	12	25	21	22	0	20	12	0	0	8	14	12	0
25	3	17	24	23	3	0	0	9	12	13	11	16	17	14	14	0	13	0	22	23	1	21	13	1	1	9	15	13	1
0	4	18	25	24	4	1	1	10	13	14	12	17	18	15	15	1	14	1	23	24	2	22	14	2	2	10	16	14	2
1	5	19	0	25	5	2	2	11	14	15	13	18	19	16	16	2	15	2	24	25	3	23	15	3	3	11	17	15	3
2	6	20	1	0	6	3	3	12	15	16	14	19	20	17	17	3	16	3	25	0	4	24	16	4	4	12	18	16	4
3	7	21	2	1	7	4	4	13	16	17	15	20	21	18	18	4	17	4	0	1	5	25	17	5	5	13	19	17	5
4	8	22	3	2	8	5	5	14	17	18	16	21	22	19	19	5	18	5	1	2	6	0	18	6	6	14	20	18	6
5	9	23	4	3	9	6	6	15	18	19	17	22	23	20	20	6	19	6	2	3	7	1	19	7	7	15	21	19	7
6	10	24	5	4	10	7	7	16	19	20	18	23	24	21	21	7	20	7	3	4	8	2	20	8	8	16	22	20	8
7	11	25	6	5	11	8	8	17	20	21	19	24	25	22	22	8	21	8	4	5	9	3	21	9	9	17	23	21	9
8	12	0	7	6	12	9	9	18	21	22	20	25	0	23	23	9	22	9	5	6	10	4	22	10	10	18	24	22	10
9	13	1	8	7	13	10	10	19	22	23	21	0	1	24	24	10	23	10	6	7	11	5	23	11	11	19	25	23	11
10	14	2	9	8	14	11	11	20	23	24	22	1	2	25	25	11	24	11	7	8	12	6	24	12	12	20	0	24	12
11	15	3	10	9	15	12	12	21	24	25	23	2	3	0	0	12	25	12	8	9	13	7	25	13	13	21	1	25	13
12	16	4	11	10	16	13	13	22	25	0	24	3	4	1	1	13	0	13	9	10	14	8	0	14	14	22	2	0	14
13	17	5	12	11	17	14	14	23	0	1	25	4	5	2	2	14	1	14	10	11	15	9	1	15	15	23	3	1	15
14	18	6	13	12	18	15	15	24	1	2	0	5	6	3	3	15	2	15	11	12	16	10	2	16	16	24	4	2	16
15	19	7	14	13	19	16	16	25	2	3	1	6	7	4	4	16	3	16	12	13	17	11	3	17	17	25	5	3	17
16	20	8	15	14	20	17	17	0	3	4	2	7	8	5	5	17	4	17	13	14	18	12	4	18	18	0	6	4	18
17	21	9	16	15	21	18	18	1	4	5	3	8	9	6	6	18	5	18	14	15	19	13	5	19	19	1	7	5	19
18	22	10	17	16	22	19	19	2	5	6	4	9	10	7	7	19	6	19	15	16	20	14	6	20	20	2	8	6	20

4. Traduire la lettre obtenue après décalage
=CAR(AG3+65)
Formule à étirer vers la droite et vers le bas

3. Ajouter 1 à la case au-dessus puis calculer le reste de la division euclidienne par 26
=MOD(AG3+1)
Formule à étirer vers le bas (avec 26 lignes on testera tous les décodages possibles) et vers la droite (pour décoder tout le message)

5. Trouver la ligne où le texte a une signification

Méthodes et Pratiques Scientifiques

1. Le chiffrement par décalage

Le principe est un décalage de l'alphabet de plusieurs lettres . Dans le cas du décalage de César, on dit que la clé est 3. Que devient le A ? le B ?
Compléter la grille ci-dessous :

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
codé																										

codé	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
clair																										

Que remarquez-vous ?

✂---

Encoder le message suivant avec le décalage de César :_
JULES CESAR A VECU AU PREMIER SIECLE AVANT JESUS CHRIST

✂---

Comment pouvez vous décoder le message (les espaces entre les mots ont été conservés)
DWCA DMVMH LM LMKPQNNZMZ DWBZM XZMUQMZ UMAAIOM KZGXBM JZIDW

✂---

Si les espaces entre les mots sont supprimés, pouvez vous toujours décrypter ce message ?
NQJXYYWTUKFHNQJIJIJHWDUYJWZSRJXXFLJJSHTIJUFWIJHFQFLJ

Quel est le point important qui vous a permis de déchiffrer rapidement ? Combien y a t il de cryptages différents ?

✂---

2. Utilisation d'un tableur pour coder et décoder des messages

Un tableur permet d'effectuer des opérations répétitives. Les cellules (cases) contiennent les lettres à coder et/ou à décoder. Le tableur a des fonctions prédéfinies pour chiffrer les lettres. Il utilise un code informatique qui à chaque lettre majuscule attribue un nombre à partir de 65. Ainsi A correspond à 65, B à 66 etc....Attention au delà de 90, d'autres caractères comme [, ^ etc sont codés.
La formule CAR(nombre) permet de récupérer la lettre correspondant au nombre donné entre 65 et 90 et CODE("lettre") permet de récupérer le code entre 65 et 90 de la lettre choisie.
ATTENTION pour être reconnue comme une formule, le texte doit commencer par "="
Pour des questions pratiques, nous numéroterons les lettres de 0 à 25. Nous utiliserons la fonction MOD(dividende, diviseur) permet de récupérer le reste dans la division euclidienne du 1er nombre par le 2d).
tableau de numérisation :

lettre	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
nombre	0																									

a) Utiliser les formules pour reconstruire le tableau du chiffrement de César puis celui du décodage.

b) Entrer sans espace, en majuscule et une lettre par cellule le texte JULES CESAR A VECU AU PREMIER SIECLE AVANT JESUS CHRIST puis programmer le tableur pour qu'il l'encode (en utilisant la poignée de recopie)

✂---

3. Le chiffrement affine

Un des problèmes du codage par décalage est qu'il conserve l'ordre des lettres de l'alphabet. Si une lettre est décodée alors toutes les autres le sont très facilement. Le codage affine permet une mélange des lettres qui ne soit pas "évident". On utilise une fonction affine *(f(x)=ax + b)* pour coder (transformer) le chiffre associée à la lettre en clair et on retransforme ensuite le nombre obtenu en lettre à l'aide du tableau de numérisation.

Le couple (*a* ;*b*) est la clef de chiffrement.

Par exemple, si on prend $a = 7$ et $b = 11$, on obtient pour le code de A : $7 \times 0+11=11$ donc la lettre L:

lettre en 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
x	0	1																								
7x + 11	11																									
entre 0-25	11																									
lettre codée	L																									

Compléter le tableau et traduire le message ci-dessous ?

LVYNVCPNRNHPNZKNVYRLOINRLOPZPNYNOMIPKFHFMINLALSNLKDPYGPLOAFVCN

ZF RRNYOGNZIPUUANAZNHRNHHLBNHBALZNL KLYLKXHNUANTVNYOPNKKN

Combien y a t il a priori de couple de nombres qui donnent un cryptage différent ?

Dans la pratique, certains couples ne permettent pas de crypter comme le couple (13,11). Essayer et expliquer pourquoi :

A l'aide de la notation absolue ($) pouvez vous trouver d'autres couples de nombres qui ne permettent pas décrypter ? Combien y en a t il au total ?

✂---

Utilisation du tableur pour coder ou décoder un message

c) Utiliser les formules trouvées précédemment pour reconstruire rapidement le tableau correspondant au chiffrement affine (7,11)

d) Il n'est pas compliqué si deux lettres sont connues de trouver la clé de décodage mais cela dépasse le niveau d'un élève de seconde.

Pour le code (7,11) la fonction affine de décodage est (15;17)

Modifier votre tableau pour traduire le texte suivant en utilisant une lettre par case :

KLZAXMOLYLKXHNNHOKLHZPNYZNTVPMNARNOGNGNZIPUUANAKNHRNHHLBNHZFGNH NONHOLVHHPPRMFAOL YONTVNKLZAXMOFBALMIPN

✂---

4. Le codage Vigenere

Blaise de Vigenère était un diplomate né en 1523. Le principe de son codage est qu'une lettre ne remplace pas toujours la même lettre. Pour cela, on utilise un tableau et une clé constituée d'un mot ou d'une phrase (facile à retenir ou à transmettre). Plus la clé est longue, meilleur est le codage. Il faut savoir qu'il y a eu une période où des passages entiers de livre étaient utilisés pour chiffrer les plus grands secrets. Il faut attendre

la fin du XIXe siècle pour qu'un système de décryptage soit mis en place.

Le principe est d'additionner la lettre à coder avec la lettre de la clé : sous le message en clair, on écrit la clé, quitte à la recopier si elle est trop courte puis on additionne dans les valeurs numériques et on trouve ainsi la valeur numérique de la lettre codée et ainsi la lettre correspondante. Ainsi avec la clé "sciences", le début de la phrase "Vigenere n est pas " devient "PV...."
A vous de programmer le tableur grâce aux formules précédentes (CODE et CAR sans oublier que le code informatique de A est 65 et pas 0) pour compléter le tableau ci dessous.

en clair	V	I	G	E	N	E	R	E	N	E	S	T	P	A	S	L	E	V	R	A	I	I	N	V	E	N	T	E	U	R
valeur																														
clé	S	C	I	E	N	C	E	S	S	C	I	E	N	C	E	S	S	C	I	E	N	C	E	S	S	C	I	E	N	C
valeur																														
somme																														
0-25																														
codé																														

✂---

Comment programmer le tableur pour décoder lorsque la clé est connue ?
Décode le message suivant avec toujours le code "sciences" :
DCVEY AWWXT MUHGR LAGTP RPIHW TUIGR EKVGL IPQHW JWVGU KJXJG UIAVH WNKOI AGVW

✂---

5. Le problème d'échange de la clé et du décryptage
Formez des équipes de deux ou trois. Chaque équipe choisit un code Vigenere puis crée le tableau d'encodage et le tableau de décodage dans le tableur. Vous commencez par inventer un message à me transmettre, vous l'encodez et vous venez l'écrire au tableau. Je vais moi meme l'encoder avec ma propre clé et vous rendre un message sur lequel vous appliquerez votre décodage avant de me donner le résultat (toujours incompréhensible) ….

✂---

Tous les messages transmis sont incompréhensibles mais après deux échanges, j'ai pu lire vos message transmis. Comment cela est il possible ? Que s'est il passé ?
Si quelqu'un intercepte tout nos messages, a-t-il la possibilité de trouver les clés de codages et donc de décoder le message initial ?

Méthodes et Pratiques Scientifiques
Corrigé pour le professeur

1. Le chiffrement par décalage

le A devient D et le B devient E

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

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

… l'ordre est conservé... mais attention ce n'est pas symétrique A devient D qui ne redevient pas A ...

Encoder le message suivant avec le décalage de César :_
JULES CESAR A VECU AU PREMIER SIECLE AVANT JESUS CHRIST
MXOHV FHVDU D YHFX DX SUHPLHU VLHFOH DYDQW MHVXV FKULVW

DWCA DMVMH LM LMKPQNNZMZ DWBZM XZMUQMZ UMAAIOM KZGXBM JZIDW
Vous venez de déchiffrer votre premier message Bravo (décalage de 8)

NQJXYYWTUKFHNQJIJIJHWDUYJWZSRJXXFLJJSHTIJUFWIJHFQFLJ
Il est trop facile de décrypter un message encode par décalage.

Le fait que l'ordre des lettres soit conservée et que le E revienne beaucoup plus souvent en francais a permis de décoder rapidement. Il y a 25 cryptages différents et l'identité.

2. Utilisation d'un tableur pour coder et décoder des messages

lettre	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
nombre	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

a)		A	B	C	D	E	F	G
1	lettre	A	B	C	D			
2	en nombre	"=code(A1)-65"	"=code(B1)-65"	etc ...				
3	decalé	"=mod(A2+3;26)"	"=B2+3"					
4	lettre codé	"=car(A3+65)	"=car(B3+65)					

		A	B	C	D	E	F	G
1	lettre codé	A	B	C	D			
2	en nombre	"=code(A1)-65"	"=code(B1)-65"	etc ...				
3	enleve le décalage	"=mod(A2-3;26)"	"=B2+3"					
4	lettre codé	"=car(A3+65)	"=car(B3+65)					

b)		A	B	C	D	E	F	G	H	I	J
1	lettre	J	U	L	E	S	C	E	S	A	R
2	en nombre	"=code(A1)-65"	20	11	4	19	2	4	18	0	17
3	decalé	"=mod(A2+3;26)"	23	14	7	21	5	7	21	3	20
4	lettre codé	"=car(A3+65)	X	O	H	V	F	H	V	D	U

3. Le chiffrement affine

lettre	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
x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
7x+11	11	18	25	32	39	46	53	60	67	74	81	88	95	102	109	116	123	130	137	144	151	158	165	172	179	186
0-25	11	18	25	6	13	20	1	8	15	22	3	10	17	24	5	12	19	0	7	14	21	2	9	16	23	4
lettre	L	S	Z	G	N	U	B	I	P	W	D	K	R	Y	F	M	T	A	H	O	V	C	J	Q	X	E

Compléter le tableau et traduire le message ci-dessous ?
LVYNVCPNRNHPNZKNVYRLOINRLOPZPNYNOMIPKFHFMINLALSNLKDPYGPLOAFVCN
AUNEUVIEMESIECLEUNMATHEMATICIENETPHILOSOPHEARABEALKINDIATROUVE
ZF RRNYOGNZIPUUANAZNHRNHHLBNHBALZNL KLYLKXHNUANTVNYOPNKKN
COMMENTDECHIFFRERCESMESSAGESGRACEALANALYSEFREQUENTIELLE

Combien y a t il a priori de couple de nombres qui donnent un cryptage différent ? 26*26-1=675
on remarque que les couples (1,b) correspondent à un simple décalage.

Dans la pratique, certains couples ne permettent pas de crypter comme le couple (13,11). Essayer et expliquer pourquoi ? toutes les lettres sont transformée en L ou Y …

Pouvez vous trouver d'autres couples de nombres qui ne permettent pas décrypter ?
b correspond au décalage donc ne pose pas de problème mais si a n'est pas premier avec 26 alors les lettres seront répétées. Il faut enlever les couples correspondants à a pair et a=13 Il reste 12 possibilités pour a et 26 pour b donc 312 auquel il faut enlever l'identité (1,0) donc 311 possibilités....

Utilisation du tableur pour coder ou décoder un message
c)

lettre	A	B	C	D	E	F	G	H	I
x	0	1	2	3	4	5	6	7	8
7x+11	"=B2*7+11"	18	25	32	39	46	53	60	67
0-25	"=MOD(B3;26)"	18	25	6	13	20	1	8	15
lettre	"=CAR(B4+65)"	S	Z	G	N	U	B	I	P

d)

lettre	K	L	Z	A	X	M	L	Y	L
x	"=CODE(B1)-65"	11	25	0	23	12	11	24	11
15x+17	"=B2*15+17"	182	392	17	362	197	182	377	182
0-25	"=MOD(B3;26)"	0	2	17	24	15	0	13	0
lettre	"=CAR(B4+65)"	A	C	R	Y	P	A	N	A

KLZAXMOLYLKXHNNHOKLHZPNYZNTVPMNARNOGNGNZIPUUANAKNHRNHHLBNH
LACRYPTANALYSEESTLASCIENCEQUIPERMETDEDECHIFFRERLESMESSAGES

ZFGNHNONHOLVHHPPRMFAOL YONTVNKLZAXMOFBALMIPN
CODESETESTAUSSIIMPORTA NTEQUELACRYPTOGRAPHIE

4. Le codage Vigenere

CODAGE

en clair	V	I	G	E	N	E	R	E	N	E	
valeur	"=CODE(B1)-65"	8	6	4	13	4	17	4	13	4	
clé	S	C	I	E	N	C	E	S	S	C	
valeur	"=CODE(B3)-65"	2	8	4	13	2	4	18	18	2	
somme	"=B4+B2"	10	14	8	26	6	21	22	31	6	
0-25	"=MOD(B5;26)"	10	14	8	0	6	21	22	5	6	
codé	"=CAR(B6+65)"	K	O	I	A	G	V	W	F	G	

Vigenere n'est pas le vrai inventeur, codé avec le mot sciences :
NKOIAGVWFGAXCCWDWXZEVKRNWPBIHT

DÉCODAGE :

codé	D	C	V	E	Y	A	W	W	X	T	
valeur	"=CODE(B1)-65"	2	21	4	24	0	22	22	23	19	
clé	S	C	I	E	N	C	E	S	S	C	
valeur	"=CODE(B3)-65"	2	8	4	13	2	4	18	18	2	
soustraction	"=B4-B2"	0	13	0	11	-2	18	4	5	17	
0-25	"=MOD(B5;26)"	0	13	0	11	24	18	4	5	17	
en clair	"=CAR(B6+65)"	A	N	A	L	Y	S	E	F	R	

D CVEYAWW XTMUHGRLAGTPR PI HWTUIG REK VG LIPQHWJ WV GUKJXJGUIAV HW NKOIAGVW
L ANALYSE FRÉQUENTIELLE NE PERMET PAS DE DECODER UN CHIFFREMENT DE VIGENERE

5. Le problème d'échange de la clé et du décryptage

On peut imaginer un système de cadenas sur une boite avec deux fermetures ; Au départ le message est mis dans la boite et l'équipe d'élève mets son cadenas, en codant ce qui transmis, le professeur rajoute à coté son cadenas et redonne la boite aux élèves. Ils enlèvent alors leur cadenas et lui rendent la boite puis le prof enlève son cadenas et ouvrir la boite pour lire le message (on peut utiliser une chemise avec les deux rabats élastiques.

En fait, si quelqu'un intercepte tous les messages, il peut grâce aux deux messages envoyés par les élèves trouver leur clé (il a un texte encodé puis décodé avec leur clé). De plus, il pourra alors deviner la clé du professeur...

Quelques petites questions de cryptographie

Ces questions, assez difficiles, ont été parfois distribuées aux élèves après le diaporama.

1. Le ROT 13 (décalage de 13) est un chiffrement particulier : quand on le répète, on retrouve le message non crypté. Y a-t-il d'autres chiffrements par décalage qui vérifient ceci ?
   Et en répétant éventuellement plusieurs fois (3 fois, 4 fois,...) ?

2. Combien y a-t-il de chiffrements par substitution différents, pour notre alphabet de 26 lettres ?

3. Faire deux équipes. Chaque équipe choisit une clé de Vigenère, qu'elle ne donne pas à l'autre équipe. La première équipe choisit un message qu'elle veut transmettre à l'autre équipe. Elle le chiffre à l'aide de sa clé, et envoie ce message codé. L'autre équipe recode ce message à l'aide de sa clé, (Le message a donc été crypté 2 fois), et renvoie ce nouveau message à l'équipe 1. L'équipe 1 décrypte le message à l'aide de sa clé, et renvoie encore. L'équipe 2 décrypte enfin... Vérifier qu'elle a bien le message initial.
   Intérêt : les deux équipes n'ont pas eu à se transmettre la clé...
   Inconvénient : quelqu'un qui écoute toutes les transmissions peut trouver la clé et le message...

4. Le message suivant a été codé avec Vigenère en utilisant la clé CBD.
   Vv du ehepgg dh ofvubjg, cucwr! Vv fqoqcjv djhp urp boriddfw!
   Saurez-vous le déchiffrer ?

5. (Très difficile !) Comment feriez-vous pour déchiffrer le message suivant, sachant qu'il a été obtenu à l'aide d'un chiffrement de Vigenère et d'une clé de longueur 3 ?

   QYK WYA HOV AYA GUO SKC WUM HYK CXM OFI WXM RYD WAM BYZ SYB RYT OWT SIC WWW AGM WFM GNI GMM NFW BAD COA RYD FCM NUZ FCD SLI ZYZ SNZ COD SLQ ZMC TZQ HXC BJM IXM DUB WYV QYM HXI GNC QYR SMX SLM EOM JIC GHI JYH DUA HLW IPM QYT ONZ CJL WZN WWQ ZYM HKC SWM ZUV OJI GYB SNZ CJT CHO GCD COA OPM NLM IMA WVZ OPW SPQ RYU AYV HWM GNX ZOA QIU DFQ EOM ZIZ GKC CHV SWW BHI WNX OMT ONI WFT SXM ZUK ZYK SMB DIC FWM ZUY IYK SWP WZN FYU SHB OYB SYN TCK OWM DYV RUV HFW BAB SGX G

6. Quelle sorte de chiffrement obtient-on avec $a = 1$ dans le chiffrement affine $ax + b$?

   Pouvez-vous trouver quelle(s) valeur(s) de a sont interdites si on veut que deux lettres différentes soient codées par deux lettres différentes ? Et si on n'avait pas 26 lettres, mais 36, les valeurs interdites seraient-elles les mêmes ?

   Si on suppose que a est donné, combien de choix a-t-on pour b ? Combien y a-t-il de chiffrements affines différents ?

Le carré de Polybe

L'historien grec Polype a inventé un code simple dont voici la grille :

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I	J
3	K	L	M	N	O
4	P	Q	R	S	T
5	U	VW	X	Y	Z

Décode le message.
251124 11241415 44132441243534
15332432241534 11 4311441543
1311434523112215

Le carré de Polybe à clé

On peut introduire une variante en utilisant une clé : INVITATION

	1	2	3	4	5
1	I	N	VW	T	A
2	O	B	C	D	E
3	F	G	H	J	K
4	L	M	P	Q	R
5	S	U	X	Y	Z

Décode le message.
412244 231121 451112 454111 211144
323111 412223 511144 4411

La clé du carré est : « espionnage »

Décode le message.
211541 212232 352331 311521 221314
224115 212115 441253 451223 15

La clé du carré est : « Michel-ange »

À toi de jouer

	1	2	3	4	5
1					
2					
3					
4					
5					

Ton message :

…….

…….

…….

Chiffrement de Vigenère

Le chiffrement de Vigenère est une amélioration d'un chiffrement de César.

Un mot clé détermine les décalages successifs.

Exemple : mot clé de **trois lettres** : « BUT »

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

Le texte est découpé en groupes de **trois lettres**.

La ***première lettre*** de chaque groupe est codée
avec le décalage indiqué par la première lettre de la clé,

la ***deuxième*** par le décalage indiqué par la deuxième lettre

et la ***troisième*** par le décalage indiqué par la troisième lettre de la clé.

On peut bien sûr utiliser une clé avec davantage de lettres.

Déchiffre le message suivant :

WIBDCNOYQFGIMYWFGXTMTHYVSSIUYTWY VMYFPNUVN

Remarque : une lettre n'étant pas toujours remplacée par la même, on ne peut se servir des fréquences qu'après avoir listé les premières puis les deuxièmes puis les troisièmes lettres de chaque groupe.

Utilise cette grille pour coder un message à l'aide de Vigenère

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**

Clé de trois lettres.

Chiffrement affine

On associe à chaque lettre, une valeur numérique.
Complète ce tableau :

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
0	1									10															25

Soit f la fonction affine définie par : $f(x) = \mathbf{5}\,x + \mathbf{1}$
Calcule les images des 26 nombres de ce tableau.

	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
x	0	1									10															25
f(x)	1										51															
	1										25															
	B										**Z**															

$f(0) = 5 \times 0 + 1$

$f(0) = 1$

Calcule le reste de la division euclidienne de f(x) par 26, puis, en utilisant le premier tableau retrouve la lettre.

$f(10) = 5 \times 10 + 1$

$f(10) = 51$

$51 = 26 \times 1 + 25$

Reste de la division euclidienne par 26

fonction « mod » : = mod(f(x) ; 26)

Vérifie les résultats du tableau
en utilisant un tableur (OpenOffice classeur)

Ce tableau te permet de coder ou de décoder un message par chiffrement affine (5 ; 1)

Vérifie ton codage sur http://www.dcode.fr/chiffre-affine

Chiffrement affine

On associe à chaque lettre, une valeur numérique.
Complète ce tableau :

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
0	1									10															25

Soit f la fonction affine définie par : $f(x) = \mathbf{3}\,x + \mathbf{4}$
Calcule les images des 26 nombres de ce tableau.

	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
x	0	1									10															25
f(x)	1										34															
	4										8															
	E										**I**															

$f(0) = 3 \times 0 + 4$

$f(0) = 4$

Calcule le reste de la division euclidienne de f(x) par 26, puis, en utilisant le premier tableau retrouve la lettre.

$f(10) = 3 \times 10 + 4$

$f(10) = 34$

$34 = 26 \times 1 + 8$

Reste de la division euclidienne par 26

fonction « mod » : = mod(f(x) ; 26)

Vérifie les résultats du tableau
en utilisant un tableur (OpenOffice classeur)

Ce tableau te permet de coder ou de décoder un message par chiffrement affine (3 ; 4)

Vérifie ton codage sur http://www.dcode.fr/chiffre-affine

Bibliographie non exhaustive

Vulgarisation

Simon Singh : *Histoire des codes secrets* (Livre de Poche)

Joan Gomez : *Codage et cryptographie* (Série Le monde est mathématique, publié par le journal Le Monde)

Hors-série Tangente n°26 : *Cryptographie et codes secrets*

Hypercube n°49-50 : *Cryptographie*

Roman

Didier Muller : *Les 9 couronnes* (*Petit cours de cryptographie sous forme de roman policier)* (Société Jurassienne d'émulation, peut se commander en ligne)

Un site à connaître

www.dcode.fr *:* codage et décodage faciles...