LYCÉE JOACHIM DU BELLAY

Passeport Recherche

Sommaire

Page 1
Éditorial

Page 2
Messages codés chez les chauves-souris

Page 4
Message codé chez les fourmis

Page 5
Codage d'un message secret

Page 8
Construction d'une radio

Page 9
Interview

Page 12
Jeux mathématiques de cryptologie

Page 13
Remerciements

LYCÉE JOACHIM DU BELLAY

1, avenue Marie Talet
49100 Angers

Téléphone : 02 41 43 64 12
Télécopie : 02 41 34 88 47
Messagerie : ce.0490002l@ac-nantes.fr
Site Web : http://lyc-dubellay-49.ac-nantes.fr/

Qu'est-ce que le passeport recherche ?

Le passeport recherche a été mis en place par la structure fédérative de recherche François Bonamy. Le but est de permettre au lycéens de découvrir le monde de la recherche, par des visites de laboratoires et des rencontres avec des chercheurs. À la fin, les lycéens doivent synthétiser leurs recherches grâce à un journal(comme ici), une vidéo, une exposition etc.... qui sera présenté lors d'une journée collective de restitution.

Nous vous souhaitons une bonne lecture ☺

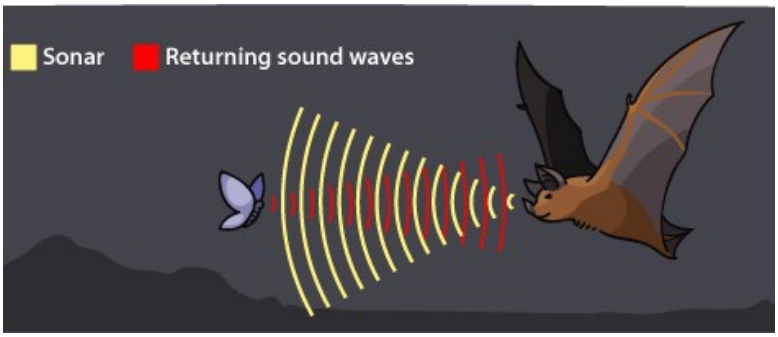
académie Nantes

Messages codés chez les chauves-souris

***INTRODUCTION**: les chauves souris produisent des ultrasons à l'aide du larynx et de la gorge . Elle peuvent aussi moduler la fréquence , l'intensité , les harmoniques de leur cris et la durée qui sépare deux cris . La fréquence des ultrasons peut atteindre 110 000 hertz et peuvent répéter leurs cris 200 fois par secondes .*

Les chauves souris produisent des ultrasons pour principalement se repérer dans l'espace, elles envoient leurs ultrasons et si les ultrasons se réfléchissent, elles le perçoivent. Cela veut dire qu'il y a un obstacle, elles peuvent donc le contourner . Elles envoient des ultrasons en continu.

Les échos de certaines feuilles peuvent perturber leurs perceptions pour chasser des insectes. Les chauves souris sont capables de se concentrer sur les échos de leurs proies en filtrant, en cessant d'écouter les échos renvoyés par les feuilles. Elles peuvent modifier les harmoniques de leurs cris, harmoniques qui leurs permettent de distinguer clairement l'écho de l'insecte de l'écho de la végétation. Certains insectes comme les papillons de nuit entendent les ultrasons et donc peuvent percevoir la chauve souris qui s'approche. Ils fuient de façon aléatoire, imprévisible… . Les papillons entendent jusqu'à 60 000 hertz donc les chauves souris augmentent l'intensité des ultrasons pour que le papillons ne perçoivent celle-ci.

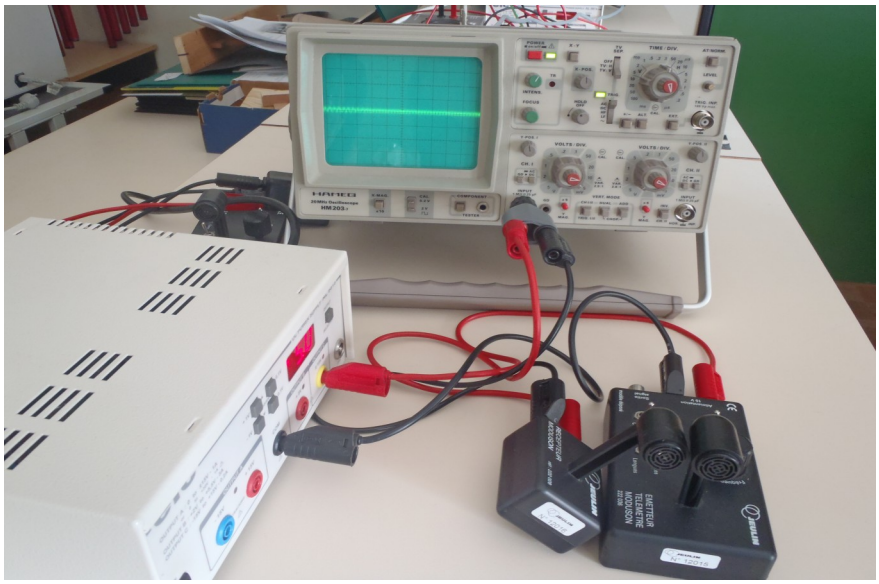


L'angle que fait le faisceau d'ultrasons est d'environ 40° dans le plan horizontale et de 45° dans le plan verticale : il ne balaye qu'une portion réduite de l'espace. La chauve souris peut élargir son angle lorsque un insecte ce déplace dans tous les sens de manière aléatoire. Le contrôle dynamique de l'amplitude de l'intensité et de la fréquence de ses faisceau d'ultrasons et de leurs échos donne aux chauves souris dans l'obscurité de la nuit une extraordinaire capacité de flexibilité et d'adaptabilité.

Les chauves souris possèdent d'autres moyens de perception. Elle ne possèdent pas de plumes mais une membrane, une peau. Les chauves souris ont au niveau de leurs ailes une sensibilité au touché aussi fine que celle de la pulpe de nos doigts. Les chauves souris perçoivent aussi les odeurs, elles voient, même si leur vue n'est pas très développée.Les chauves souris possèdent d'autres moyens de perception . Elle ne possèdent pas de plumes mais une membrane , une peau . Les chauves souris ont au niveau de leurs ailes une sensibilité au touché aussi fine que celle de la pulpe de nos doigts . Les chauves souris perçoivent aussi les odeurs , elles voient , même si leur vue n'est pas très développée .

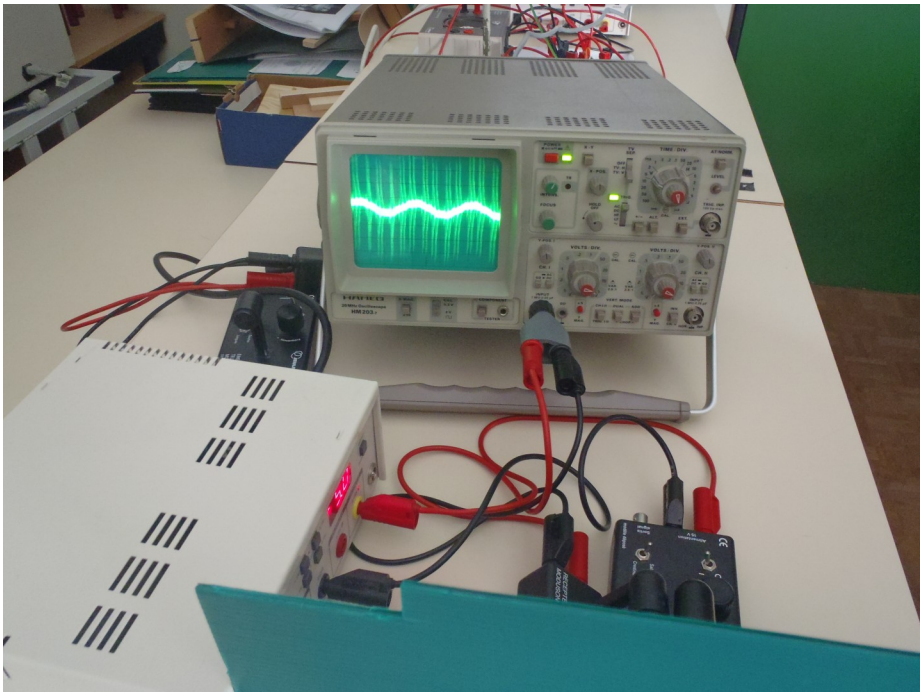
Par Mehdi Guennouni et Jean Hardouin

Messages codés chez les chauves-souris



Nous avons mis en marche un oscilloscope avec un émetteur et un récepteur à côté. Nous constatons que le récepteur ne reçoit aucun ultrason.

Nous avons mis un plastique en face de l'émetteur récepteur et nous constatons que le récepteur reçoit des ultrasons. Cela prouve que les ultrasons rebondissent sur les matières, les chauves souris font comme cela pour se repérer dans

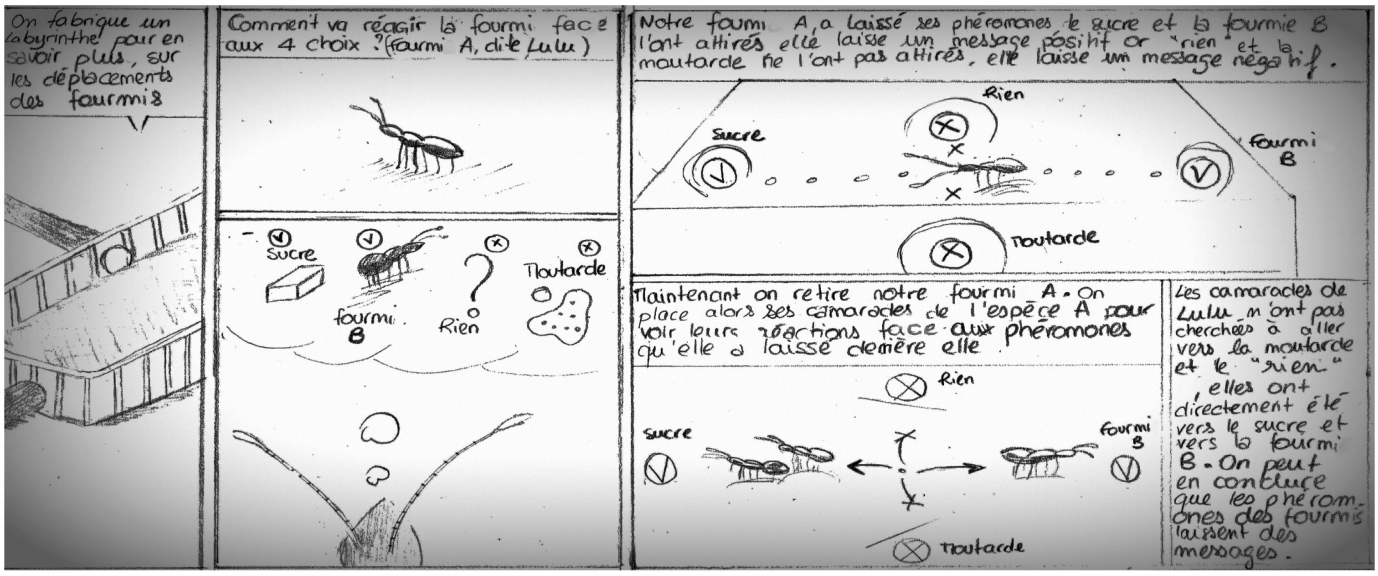


Messages codés chez les fourmis

Les fourmis, connues pour leur organisation fastidieuse, ont intéressé deux élèves de secondes, à Joachim Du Bellay. Elles ont créé un labyrinthe à plusieurs sorties où à chacune d'elles, y est déposées différentes substances. Elles ont déposé de la moutarde, du sucre, rien, ou une fourmi d'espèce B qui y déposera des phéromones. Les phéromones sont des substances chimiques déposées par les fourmis le long de leurs trajets. On peut décrypter ces phéromones à l'aide d'une équation trop complexe pour des élèves de seconde.

Par Louise Chabosseau et Camille Girardeau

Une fois la fourmi B retirée, les jeunes lycéennes ont déposé une fourmi de type À qui découvrira le labyrinthe. Celle-ci est répulsée par la moutard, et par la sortie où il ne s'y trouve rien. Mais elle est attirée par le sucre, et étrangement par les phéromones des fourmis étrangères. La fourmi A est alors retirée, et d'autres du même type entrent dans le labyrinthe. Les deux élèves ont alors remarqué que ces dernières sont allées presque instinctivement vers les sorties où se trouve le sucre, et les phéromones de la fourmi B, ou bien, elles ressortent très vite des tubes de moutarde, ou rien sans même allé jusqu'au bout du tunnel. Les jeunes élèves en ont alors conclu que les phéromones déposées par la première fourmi A jouent un très grand rôle pour les autres fourmis du même type. Ces phéromones seraient alors une sorte de code afin de communiquer des informations aux fourmis qui pourraient suivrent un même chemin.



La fourmi Lulu nous explique le déplacement des fourmis à l'aide de leurs phéromones

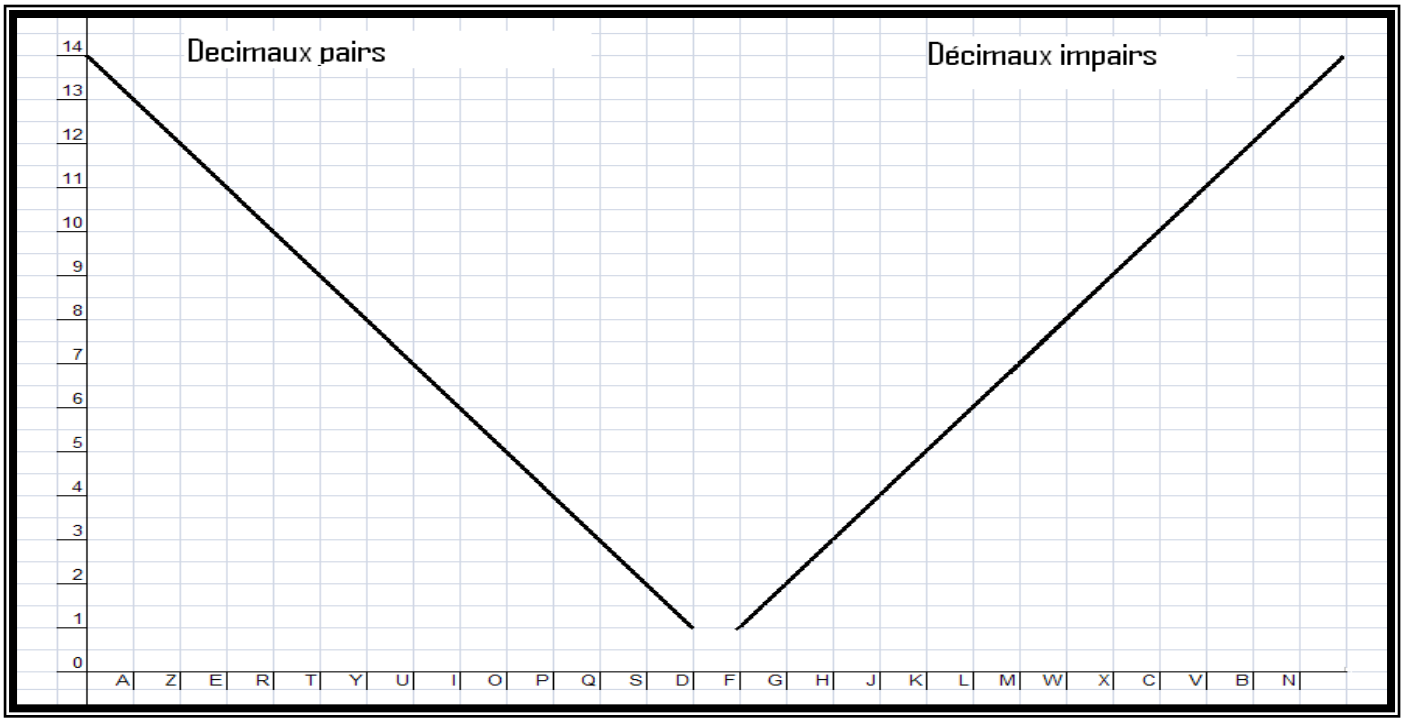
Codage d'un message secret

Nous avons travaillé sur le codage d'un message

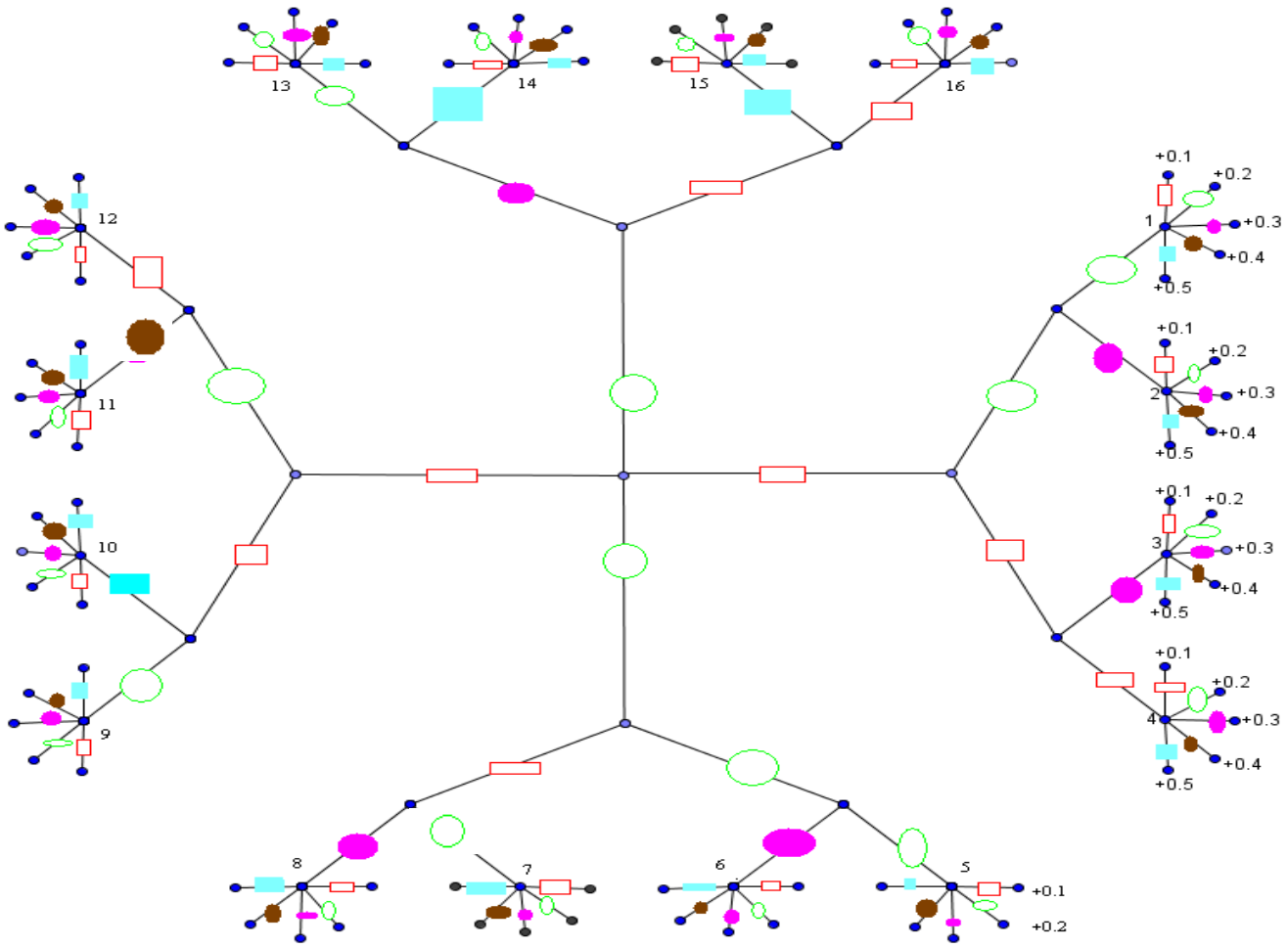
Explication:

Pour cela nous avons inventé clé pour coder notre message. Elle est composée de deux parties :

—> La première utilise une courbe pour transposer les lettres du message en nombres. Mais un nombre peut correspondre à 2 lettres, ce qui complique la tâche du décodeur. Mais pour ne pas avoir de confusion entre les lettres. On a rajouté a notre nombre une décimale comprise entre 1 et 5, si cette décimale est paire, on se servira de la première courbe, si celle-ci est impair, on utilisera la seconde.



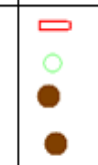
→La seconde partie du code est un morse modifié, qui transpose les nombres obtenus en une suite de symboles.

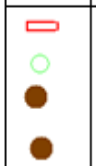
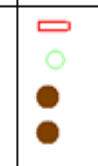


Exemple

Nous allons coder le message suivant : Crypter un message est un jeu d'enfant

Sur la première ligne, nous inscrivons le message a coder.
Sur la seconde, le nombre obtenu après le passage de ces lettres dans la courbe,
puis dans la dernière, le résultat obtenu, sous forme de symbole.

C	R	Y	P	T	E	R	U	N	M	E	S	S	A	G	E
10.3	10.2	8.2	4.4	9.2	11.4	10.4	7.2	13.3	7.5	11.2	2.2	2.4	13.2	2.3	11.2
															

E	S	T	U	N	J	E	U	D	E	N	F	A	N	T
11.4	2.2	9.2	7.4	13.3	4.1	11.2	7.2	1.4	11.4	13.1	1.1	13.2	13.5	9.2
														

C'est donc grâce à ces suites de symboles que le lecteur découvrira le message codé, et devra donc faire la démarche inverse, c'est-à-dire :

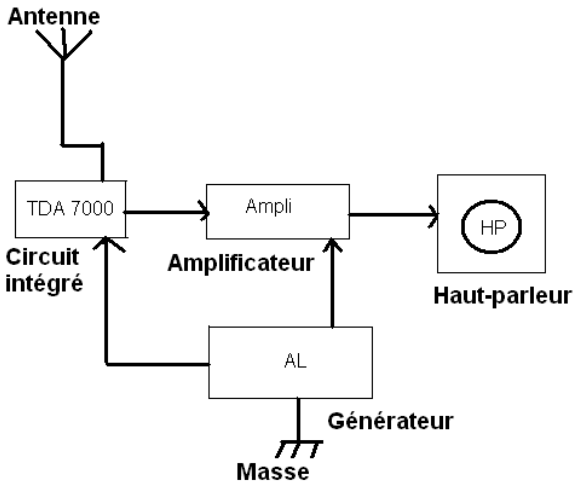
→ Découvrir un nombre grâce à ces symboles puis
→ Remplacer les nombres obtenus par des lettre grâce à la courbe (et à la décimale du nombre pour choisir la bonne courbe, pour sa lecture)

Construction d'une radio

Notre groupe et le technicien de laboratoire du lycée Joachim Du Bellay avons fabriqués une radio FM dans le but de décoder une fréquence radio. Pour la construire, nous avons sur une plaque labe*, crée un circuit constitué de deux résistances d'intensité différentes, plusieurs condensateurs différents, un circuit imprimeur,

un potentiomètre, qui sert à régler la fréquence réceptionnée et une bobine, c'est un fils de cuivre enroulé et une antenne. Le récepteur est relié a un amplificateur de fréquence qui est relié à un haut parleur qui sert à écouter la fréquence. Le principe de la radio est par un émetteur d'envoyer des ondes qui sont réceptionnées par le récepteur réglé sur la même fréquence.

Schéma synoptique



Par Anaïs Baudrier, Jeanne Bausière, Anaé Pipet et Marie Tijou

Lexique :

Plaque labe : C'est une plaque avec des circuits positifs et négatifs à relier

Interview avec une chercheuse

Zofia Denkowska est une experte en cryptologie. Elle travaille à l'université des sciences de Belle-Beille (Angers).
Nous l'avons interviewée.

- Bonjour, pouvez vous nous expliquer en quoi consiste votre travail s'il vous Zofia est professeur mais aussi chercheuse. Elle voulait être professeur car ses parents étaient professeurs des écoles.

Mais elle est aussi chercheuse car elle aime approfondir ce qu'elle enseigne et de temps en temps apprend.

- Que pouvez vous nous dire sur la cryptologie ? Quelles en sont les bases ?

La base principale de la cryptologie, c'est les nombres premiers. Pour calculer ces nombres premiers qui doivent être assez longs, on utilise des programmes, ce qui rend ces nombres, à 99,9% des nombres premiers. Donc la cryptologie concerne de nombreux domaines comme l'informatique, les mathématiques mais aussi beaucoup d'autres comme la robotique avec Riemann et ses ensembles de polynômes.

La cryptologie est plus connue pour les « codes secrets » comme le code RSA qui allie la factorisation avec des nombres premiers très grands.. Ce code est utilisé pour les achats en ligne par exemple. Le code RSA est le seul code sans clé cachée jusqu'à présent. Pour ce code : 2 nombres premiers P et Q qui sont obtenu avec un programme informatique, qu'on multiplie entre eux, on obtient alors le nombre N. On choisit un nombre E et on cherche D tel que : E*2 modulo 1[(P-1)(Q-1)]. Ensuite on détruit P et Q et on rend publique N et E et on protège D.

Mais le code le plus connu est le code Vigenère, c'est un tableau avec l'alphabet qu'on décale d'une lettre à chaque colonne. Ce code a été déchiffré par Charles Babbage.

- Pourquoi la cryptologie vous intéresse-t-elle ?

La cryptologie l'intéresse car on y utilise beaucoup les mathématiques pures qui n'ont rien à voir avec la réalité et qu'elle juge fascinantes. Elle est particulièrement intéressée par la probabilité, les équations différentielles. Zofia nous a parlé d'un chercheur en mathématiques comme elle qui dans un de ses livres, s'excusait de faire des « mathématiques inutiles » : Hardy.

- Quel est votre parcours professionnel ?

Son parcours est dû à une anecdote surprenante et touchante. Quand Zofia avait 6 ans, elle avait un ami et elle passait son temps avec lui. Mais un jour, ils ne se sont pas vu pendant les vacances et elle s'est ennuyée. Quand ils se sont revus, il lui a fait remarquer qu'elle aurait pu lire les livres de mathématiques de la classe suivante. C'est ce qu'elle fit quand il s'absenta de nouveau et ainsi elle devint excellente en cette matière.

Elle a été à l'université de Cracovie en Mathématiques, là bas elle a passé un doctorat puis elle a été invitée en France où un poste lui a été proposé. C'est comme cela qu'elle est devenue professeur à l'université de Belle-Beille à Angers.

- Vous avez écrit un livre ? Dans quel but ?

Comme presque tous les mathématiciens, elle a restitué ses thèses dans un livre pour « mettre de l'ordre ».

Interview avec une chercheuse

Voici les exercices proposés par Zofia Denkoska à notre classe :

1. Définition d'un nombre premier. Trouver le crible d'Eratosthène sur le net et l'utiliser pour trouver les nombres premiers entre 300 et 400.
2. On démontre qu'il y a une infinité des nombres premiers (selon Euclide) : Supposons que ceci n'est pas vrai et soit p_1, p_2,…, p_n la liste complète des nombres premiers. Prenez alors produit $p_1 x\ p_2 x \ldots x\ p_n + 1$ et montrez qu'il est forcément premier et qu'il n'est pas sur la liste.
3. On va admettre le théorème de Gauss : Si p est un nombre premier, a et b deux nombres naturels alors si p divise le produit axb, p divise soit a soit b (soit les deux, bien sûr)
4. Arithmétique de l'horloge. Il est 8 heures. Quelle heure sera-t-il dans a) 26h b) 49h c)80h
   Comment obtenez vous le résultat ?
5. Généralisation de l'arithmétique de l'horloge : congruences. Les congruences sont très utiles pour le cryptage et décryptage du code RSA à clé publique
6. Petit théorème de Fermat (aussi pour le code RSA) : Soit p un nombre naturel premier et a un autre nombre naturel quelconque. Alors a^p a (mod p). Cherchez le dans les manuels et sur le net. Formulez la réciproque de ce théorème et trouvez les exemples (livres, net) qui montrent qu'elle est fausse. Trouvez l'information sur le nombres « pseudo-premiers »
7. Il n'y a pas de formule qui permet de trouver tous les nombres premiers (lire Chapitre 5 du livre de Delahaye)

Remarque : Le livre de Singh est plus facile à lire que le livre de Delahaye. Commencez donc par Singh. Si vous pouvez le lire en anglais, c'est mieux, car il est assez mal traduit.
Il y a dedans beaucoup d'exemples. Apprenez à coder et décoder en code Vigenère (pas compliqué). En revanche, n'ayez pas l'ambition de lire le livre de Delahaye en détail (difficile), lisez le comme un livre historique qui montre comment les mathématiciens ne savent TOUJOURS PAS trouver les nombres premiers très très grands ou décomposer des très grands nombres en facteurs et quels efforts y étaient engagés, quelles erreurs déjà commises.
Bonne lecture !

Jeux mathématiques de cryptologie

Premier jeu :

Chaque chiffre ou signe d'opération correspond a une lettre. Le code correspond à un calcul qu'il faut ensuite effectuer

Le code : EUADWPZFBEFDZQVKFXHU

La clé :

0	1	2	3	4	5	6	7	8	9	-	+	*	/
Q	E	F	K	U	H	A	P	D	Z	V	W	X	B

La calcul : ……

La solution ……

Deuxième jeu :

Pour trouver une lettre, le plus signifie que le premier chiffre est celui de la verticale et le deuxième celui de l'horizontale, le moins signifie que le premier chiffre est celui de l'horizontal et le deuxième celui de la verticale. Ainsi vous trouver à chaque fois une lettre qui vous donne la solution.

\+ / −

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
0	Espace	L	P	U	S	T	N	D	K	N
1	H	G	N	B	E	Y	C	H	Q	D
2	L	N	A	T	I	W	A	M	O	A
3	T	P	W	L	H	U	F	S	T	Q
4	Q	C	X	B	Y	M	H	T	R	P
5	D	I	V	U	O	X	K	G	Z	S
6	C	S	M	Q	D	E	U	A	J	L
7	H	U	I	Z	P	Y	I	Z	N	P
8	R	O	Z	C	R	A	M	V	O	U
9	U	S	J	T	N	I	P	J	Espace	D

La Solution : ……

Les réponses : 1er jeu : 33896724,1
2ème jeu : Vive la cryptologie

Par Julien Ruiz et Anthony Suhard

Remerciements :

- Nos professeurs, Mme Renault, M. Le Meignen et M. Blondet
- M. Mulvé, technicien de laboratoire du lycée Joachim Du Bellay pour la radio
- M. Cossais, journaliste de Ouest France qui est venu nous aider
- Piotr Graczyk, chercheur à l'université d'Angers
- Zofia Denkowska, experte en cryptologie et chercheuse à l'université de Nantes
- Mme Nathalie Métais, documentaliste de Joachim du Bellay

Hommage à Roland Moreno, né le 11 juin 1945 au Caire et mort le 29 avril 2012 à Paris il est célèbre notamment pour avoir inventé la carte à puce en 1974.

Sources :

Message codé chez les chauves souris:
Emission de radioFrance Inter »sur les épaules du darwin » par Jean-Claude Ameisen le 25/02/2012 de 11h à 12h.

Message codé chez les fourmis:
Livre d'S.V.T niveau seconde édition Bordas
Wikipédia

Construction d'une radio FM:
Livre : Je construis ma première radio de Gérard Chevallier, édition Dunod, 2007 collection Planète sciences.