UN PROJET AUTOUR DE LA CRYPTOGRAPHIE EN SECTION EUROPEENNE MATHEMATIQUES-ANGLAIS

Emmanuelle PERNOT
LP2I à Jaunay Clan

Mickaël VEDRINE
Lycée Janot de Sens

Introduction

L'un des objectifs des sections européennes et de langues orientales (SELO) est la découverte culturelle des pays où la langue cible est parlée. La circulaire du 19 août 1992, texte fondateur du dispositif des SELO, cite trois éléments essentiels à la réussite d'un tel projet :

1. Un horaire d'enseignement linguistique très renforcé au cours des deux premières années, faisant place progressivement à partir de la troisième année à : [1]
2. L'enseignement, dans la langue de la section, de tout ou partie du programme d'une ou plusieurs disciplines non linguistiques ;
3. Enfin, dans le cadre du projet d'établissement, l'organisation d'activités culturelles et d'échanges, tendant à l'acquisition d'une connaissance approfondie de la civilisation du ou des pays où est parlée la langue de la section.

Dans cette optique, des échanges et voyages sont organisés dans la plupart des sections. Bien que l'intérêt de ces voyages ne soit pas remis en question, on peut regretter que la discipline non linguistique de la section ait souvent un rôle

1 Ce point concernait les années de 4ème et de 3ème, et il est tombé en désuétude dans beaucoup d'académies. En pratique, l'enseignement en langue est souvent renforcé pendant les trois années du lycée.

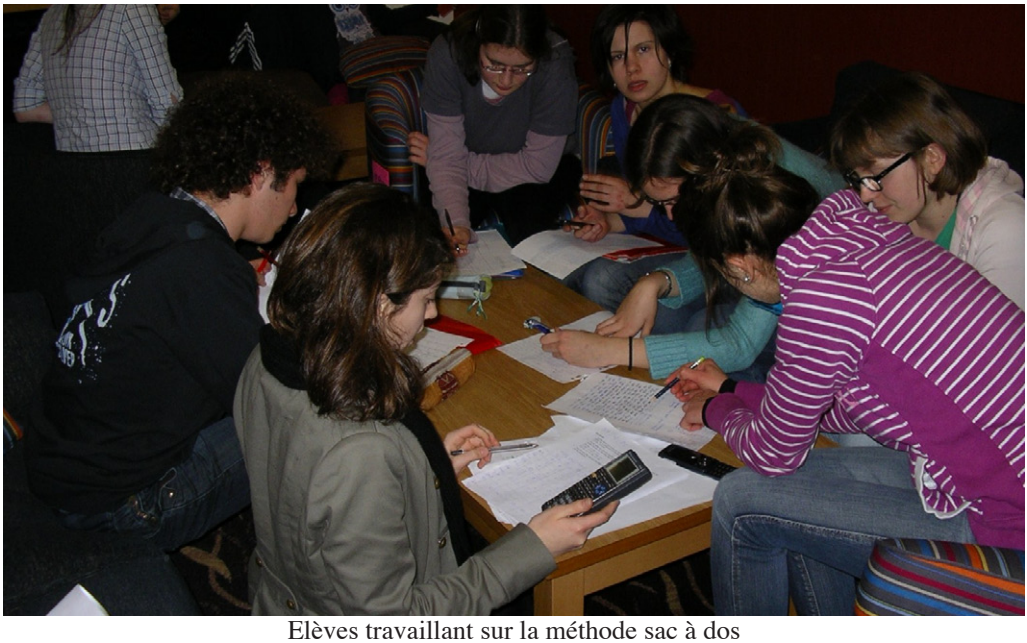
secondaire, en particulier quand il s'agit des mathématiques. C'est de ce constat qu'est née l'envie de construire un projet avec un réel contenu mathématique et aboutissant à un voyage dans un pays anglo-saxon.

Nous avons choisi de centrer ce projet sur le thème de la cryptographie. Cette notion n'est abordée actuellement qu'en spécialité mathématiques en terminale S, et pourtant cette notion n'est pas accessoire dans l'histoire des mathématiques, ni même dans l'histoire tout simplement. La cryptographie ayant été investie par les mathématiques lors du XIXe siècle, l'étude de certains codages met en jeu des compétences et des champs mathématiques divers, ainsi que des connaissances historiques et culturelles. Ce thème est de plus particulièrement propice à l'enseignement en SELO car il permet de nombreux échanges oraux entre élèves et professeurs, sur les fonctionnements des codes, leurs utilités, leurs efficacités, et il repose aussi largement sur la langue et donc des compétences linguistiques.

Nous avons décidé que le projet inclurait un travail préparatoire, des échanges virtuels entre élèves et un séjour en Angleterre, à Oxford. Nous avons choisi de travailler avec nos classes de terminales, ce qui représentaient en tout 62 élèves issus des séries L, ES et S. Nous avons débuté mi novembre 2009 pour clore le projet la première semaine de février 2010 en Angleterre.

Travail préparatoire

Avant de commencer les échanges, chaque professeur a introduit à sa manière les notions essentielles de cryptologie, avec le vocabulaire spécifique anglophone. Nous avons pu tout de suite constater l'intérêt et l'investissement des élèves pour ce sujet, qui allie les dimensions



Elèves travaillant sur la méthode sac à dos

scientifiques, culturelles, historiques et parfois un peu romanesques. Ils se sont ainsi rapidement familiarisé avec les concepts de codage et décodage, cryptographie et cryptanalyse, « plain text », « cipher text », « key »...

Blog

Les codes ne s'appréhendent réellement qu'en les utilisant aussi bien au codage qu'au décodage. Il nous a semblé alors important de mettre nos élèves en situation. L'élément central de la première partie du projet est un blog [2] mis en place sur le site du LP2I. Les élèves des deux lycées ont pu s'échanger des messages à travers ce site. Chaque classe a été divisée en une quinzaine de groupes de deux ou trois élèves. Chaque groupe a alors envoyé au groupe correspondant un texte de présentation crypté par un simple code César, dont la clé, c'est à dire le décalage, n'était connu que des expéditeurs. Les destinataires devaient alors décoder le message, et se rendre ainsi compte de la faiblesse du code de César pour sécuriser des communications.

Après ce premier échange, les approches des deux classes ont été différentes. Les groupes du LP2I ont envoyé des messages utilisant d'autres codes par substitution, comme par exemple le Carré de Polybe. Pour les décoder, les élèves du lycée Janot ont dû avoir recours à l'analyse des fréquences, et faire preuve d'initiative et d'inventivité, qualités essentielles en cryptanalyse. Cette méthode, qui au premier abord fonctionne très bien, nécessite en réalité un long travail de tests car les fréquences obtenues à partir du texte codé et les fréquences de la langue anglaise ne correspondent pas toujours exactement, surtout lorsque certains élèves ayant bien compris le système ont volontairement écrit des textes ne respectant pas du tout les fréquences habituelles.

En outre, les élèves de Sens ont réalisé des diaporamas sur des codes célèbres, tels que le code des Francs-Maçons, le code utilisé par Mary Queen of Scots et qui, cassé par un conseiller de la Reine d'Angleterre lui valu d'être condamnée à mort, ou encore les mystérieux codes de Beale. Ces diaporamas, publiés sur le blog [3], ont été présentés en classe à Sens par les auteurs eux-mêmes, mais également par les élèves du LP2I qui ont dû s'approprier les documents rédigés par leurs camarades.

Cet espace virtuel mis à disposition des élèves a occasionné de nombreux échanges tous codés de diverses manières permettant aux élèves de se rencontrer, de mutualiser leurs connaissances, ce qu'ils allaient être amenés à faire lors de leur séjour commun en Angleterre. Les élèves se sont agréablement pris au jeu, certains passant même de nombreuses heures à décoder les messages envoyés par tous les groupes.

Afin de compléter les connaissances des élèves, d'autres codes ont aussi été étudiés avant le voyage, en particulier le code de Vigenère qui résiste à la simple analyse des fréquences.

Voyage à Oxford

Comme point d'orgue de ce projet, nous avons organisé une semaine avec des activités toutes (ou presque) liées à la cryptographie. Nous avons choisi de nous installer dans la ville d'Oxford car il nous fallait une ville de taille suffisamment importante pour trouver un hébergement convenable pour 62 jeunes (en auberge de jeunesse), proche du musée Bletchley

2 Www.blogpeda.ac-poitiers.fr/cryptography

3 Www.blogpeda.ac-poitiers.fr/cryptography

Bletcley Park

Park et de Londres. Cette ville magnifique avec son université d'excellence, correspondait parfaitement à tous nos critères.

Notre projet, original pour un voyage scolaire, a séduit les institutions qui nous ont facilité certaines démarches et les intervenants que nous avons contacté. Nous avons ainsi eu le bonheur d'assister à des conférences de grande qualité et à des visites passionnantes dans des conditions appréciables.

Nous avons commencé notre séjour sur place avec Philip Bond, professeur à l'Université d'Oxford, spécialiste de cryptographie. Il nous a expliqué à quel point la cryptographie fait partie intégrante de notre monde actuel mais aussi et surtout de notre avenir, abordant aussi le thème des codes correcteurs d'erreurs. Il nous a fait l'honneur de venir avec un de ses élèves les plus prometteurs dans ce domaine, étudiant qui a su transmettre sa passion pour la cryptographie à son public tout en montrant à nos élèves un visage jeune et dynamique du monde de la recherche, notamment en mathématiques. Son exposé sur les courbes elliptiques, malgré la difficulté du sujet, a passionné élèves et professeurs.

Nos élèves ont ensuite découvert les charmes d'Oxford à travers un jeu de piste alliant messages codés, histoire de la ville, Lewis Caroll et son « Alice's adventures in Wonderland ». Pour donner un avant goût de la vie universitaire à nos futurs bacheliers, nous avons visité « Christ Church College » avec son impressionnante salle à manger ayant servi au tournage de Harry Potter.

Nous avons également décidé de consacrer une demi-journée à un travail détaillé sur la méthode « sac à dos » (« Knapsack method[4]» en anglais). Répartis en différents groupes composés d'élèves des deux établissements et de différentes séries (L-ES-S-spécialité maths), les élèves se sont vus attribués des rôles bien spécifiques. Chacun avait sa pierre à apporter à l'édifice : l'écriture d'un texte en anglais, le codage en binaire, la création d'une suite super croissante, le codage par congruences,... Des heures durant, les élèves ont écrit, codé et décodé leurs messages. Le temps imparti était trop court pour décoder les messages mais la motivation n'ayant pas faibli, l'atelier s'est poursuivi dans la soirée. Les codes correcteurs d'erreurs évoqués la veille par Philip Bond ont pris tout leur sens ici, car de nombreuses erreurs se sont glissées tout au long du processus et les messages une fois décryptés avaient parfois perdu tout leur sens !

Lors de notre journée à Londres, l'auteur à succès de vulgarisation scientifique Simon Singh (auteur du « Code Book », ouvrage de référence de cryptographie), a su nous captiver par son aisance et ses explications limpides. Venu avec une machine Enigma (machine de codage utilisée par les Allemands pendant la Seconde guerre), il a détaillé pas à pas et avec simplicité le fonctionnement de cet outil au mécanisme pourtant complexe. Il a également subjugué son public en démontrant qu'il fallait se méfier des soit-disant « messages cachés » dans les livres et des hallucinations auditives. En ouverture de sa conférence, Simon Singh nous a fait écouter un passage de la chanson *Stairway to Heaven* de Led Zepellin, qui quand on l'écoute à l'envers semble être un message adressé au diable. Il était intéressant de constater que personne n'avait remarqué quoi que ce soit de particulier avant que Simon Singh nous montre

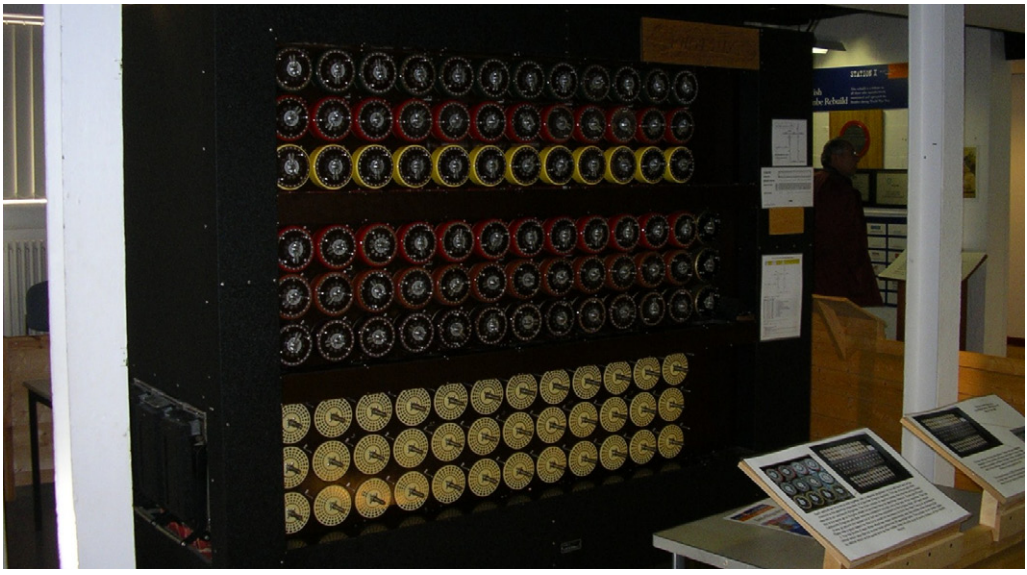
Présentation de la machine
Enigma par Simon Singh

le texte que nous étions censés reconnaître. Pour clore son exposé, il nous a parlé du fameux code de la Bible, qui cacherait des références à des événements comme le 9 septembre. Là encore, cette théorie est remise en question quand on apprend que l'on peut trouver, par la même méthode, des centaines de messages dans *Moby Dick*, dont une page entière qui ferait allusion à la mort de Lady Di.

Avant un temps libre bien mérité au cœur de Londres, les élèves ont visité le British Museum, en se concentrant sur les objets en lien avec la cryptographie et plus généralement les mathématiques, comme la Pierre de Rosette ou le papyrus de Rhynd.

Pour terminer notre semaine, nous nous sommes rendus à Bletchley Park, haut lieu

4 http://nrich.maths.org/2199



«The Turing Bomb» exposée à Bletchley PArk permettant de décoder
les messages des allemands cryptés par les machines Enigma.

incontournable de la cryptographie. Ce village situé en pleine campagne anglaise, s'est avéré être un lieu clé lors de la seconde guerre mondiale pour le décodage des messages de l'armée allemande notamment cryptés à l'aide des machines Enigma et de Lorene. Des milliers de personnes (le plus célèbre étant certainement le mathématicien Alan Turing,un des pionniers de l'informatique moderne) ont unis leurs connaissances pour construire d'impressionnantes machines de décodage dans le plus grand secret bien évidemment. Cette immersion dans le passé a permis de mieux comprendre le rôle vital des codeurs et casseurs de codes lors de ce moment fort de l'histoire.

Bilan

Ce projet a été réellement apprécié par les élèves comme par les professeurs. Notre but pédagogique de faire entrer les élèves dans le monde de la cryptographie en anglais a été atteint. Nombreux sont ceux qui se sont montrés curieux et ont cherché à aller au delà de nos cours, le monde de la cryptanalyse étant vaste. Bien sûr, le séjour à Oxford a apporté un réel plus pour la motivation des élèves. Un tel voyage permet certes de créer des liens avec ses élèves, de les voir sous un autre jour, de découvrir l'Angleterre mais surtout les connaissances et compétences acquises en cours par les élèves ont pris encore davantage de sens aussi bien en anglais qu'en mathématiques. Des liens ont aussi été noués entre les élèves des deux lycées, dont certains sont encore en contact plusieurs mois plus tard.

Le bonheur, pour nous professeurs, a été de réaliser que nos élèves ont fait des mathématiques toute une semaine avec une curiosité et un investissement remarquables. La langue

anglaise n'a jamais été un obstacle et les élèves eux-mêmes nous ont parfois rappelés à l'ordre lorsque nous parlions français. Les interlocuteurs, ont certes su se mettre à la portée de leur auditoire, mais nous avons surtout pu apprécier les progrès de nos élèves après trois ans en classe européenne. Cette expérience a également constitué un atout pour l'épreuve de baccalauréat qu'ils ont passée en fin d'année scolaire, offrant ainsi un point de discussion lors de l'entretien.

En mêlant des activités mathématiques d'un niveau élevé et des visites culturelles passionnantes, nous avons le sentiment d'avoir réussi à offrir à nos élèves un voyage riche et original, dont ils garderont longtemps le souvenir, comme nous.

Les élèves des deux lycées réunis une dernière fois devant l'auberge de jeunesse

Bibliographie

Simon Singh, *The Code Book the secret history of codes and code-breaking*, Fourth Estate, 2000 – traduit en français sous le titre *Histoire des codes secrets*

David Kahn, *The Codebreakers : The Comprehensive History of Secret Communication from Ancient Times to the Internet,* Simon & Schuster, 1997 – traduit en français sous le titre L*a guerre des codes secrets*

Lewis Caroll *Alice's Adventures in Wonderland,* Kindle Edition, 1997

Irem de Poitiers, *Enseigner l'arithmétique*, 2000

Sitographie

www.simonsingh.net

www.bletchleypark.org.uk

www.britishmuseum.org

http://nrich.maths.org/2199

http://www.lp2i-poitiers.fr/spip.php?article1169