GROUPE DE RÉFLEXION SUR L'ENSEIGNEMENT DES MATHÉMATIQUES
AU COLLÈGE DE L'ACADÉMIE DE NICE
Avril 2020

Cryptographie : tâche à prise d'initiative en groupe en 4ème ou 3ème

Sylvain ETIENNE
Professeur de Mathématiques
Collège Sidney BECHET
Antibes (Alpes-Maritimes)

Résumé

Cette activité consiste à déchiffrer des messages codés à l'aide de l'analyse fréquentielle.
Le fichier en annexe permet d'avoir les fréquences d'apparition des lettres dans quelques langues.
Un extrait de vidéo est à visionner (entre le début et 3 min 20 s) :
https://www.youtube.com/watch?v=8BM9LPDjOw0
Une fois le texte traduit, une recherche du texte dans un moteur de recherche permet de retrouver l'extrait.
Il y a deux extraits de deux livres différents, le deuxième extrait se décline en anglais, italien et espagnol.
Un scénario de classe à la maison est disponible en annexe.

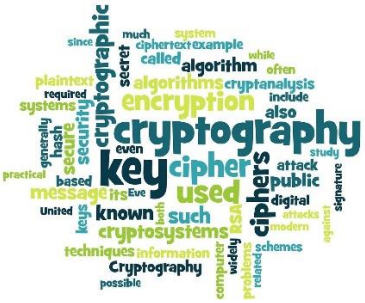

Image d'après Pixabay

Description du travail de groupe

Les élèves sont en groupe de quatre élèves, voire trois.
Chaque élève se voit attribuer un rôle : gardien, rédacteur, ambassadeur et rapporteur.
Les élèves sont évalués selon les 6 compétences de l'activité mathématique dont chercher, modéliser, représenter, raisonner et calculer sont des compétences communes au groupe et seront évaluées tant dans les discussions avec l'ambassadeur, que la présentation du rapporteur ou de l'écrit du rédacteur. Seule la compétence communiquer est personnelle et liée au rôle de l'élève.

Le référentiel des compétences est personnel et devra être adapté.

D'une durée de deux heures distantes d'une semaine environ selon le schéma :

- une séance d'une heure avec présentation du problème, passage dans tous les groupes interroger l'ambassadeur pour s'assurer de l'appropriation et de guider les premières pistes ;
- un travail hors classe afin que les groupes finalisent entre eux l'activité ;
- une séance pour s'assurer de l'avancée de chaque groupe, donner des conseils pour la présentation notamment et faire passer les rapporteurs à l'oral.

Tableau des compétences aidant à l'évaluation

Les 6 compétences de l'activité mathématique		😢	😐	😃	😎
CHERCHER	CH01 : Décomposer un problème en sous-problèmes. CH02 : Extraire les informations utiles, les reformuler, les organiser, les confronter à ses connaissances. CH06 : Tester, essayer plusieurs pistes de résolution.				
MODELISER	MO16 : Traduire en langage mathématique une situation réelle à l'aide d'outils statistiques. MO17 : Utiliser des outils numériques pour réaliser une production.				
REPRESENTER	RE04 : Choisir et mettre en relation un cadre numérique adapté pour traiter un problème. RE06 : Représenter des données sous forme d'une série statistique. RE07 : Utiliser plusieurs représentations des nombres.				
RAISONNER	RA02 : Justifier, argumenter. RA03 : Mener collectivement une investigation en sachant prendre en compte le point de vue d'autrui. RA04 : Raisonner en utilisant des outils de dispersion ou de position.				
CALCULER	CA01 : Calculer avec des nombres. CA03 : Contrôler la vraisemblance de ses résultats.				
COMMUNIQUER	CO02 : Avoir une tenue correcte lors d'un oral.	Evaluée directement dans les rôles			
	CO05 : Définir et respecter une organisation et un partage des tâches dans le cadre d'un travail de groupe.				
	CO08 : Expliquer à l'écrit sa démarche, son raisonnement.				
	CO09 : Rendre un travail clair et propre.				
	CO10 : Savoir s'exprimer, présenter sa recherche et ses résultats à l'oral.				

Tableau d'évaluation des rôles

Liste des membres du groupe		Evaluation du rôle			
		😢	😐	😃	😎
N° de groupe :	Le gardien :				
	Le rédacteur :				
	L'ambassadeur :				
	Le rapporteur :				

Tableau des responsabilités

Responsabilités	
Le gardien	• **Gardien du temps :** il veille à indiquer le temps qu'il reste de temps à autre pour la réalisation des différentes tâches. • **Gardien du bruit :** il veille à ce que le groupe ne dérange pas les autres groupes. • **Gardien des documents :** il doit s'assurer que les documents sont bien remis au professeur, notamment ceux, **numériques**, sur le **bon groupe de travail**. • **Compétence de l'activité mathématiques :** Il s'assure (avec l'ambassadeur) que les productions écrite et numérique **prennent bien en compte** les différentes compétences mathématiques attendues pour l'activité.
Le rédacteur	• **Idées développées :** il **rédige la production** et présente à l'écrit les idées de **TOUS** les membres. • **Trace écrite :** il doit rédiger à l'écrit la (ou les) réponse(s) finale(s). Les autres membres peuvent l'aider oralement.
L'ambassadeur	• **Professeur :** il est le **SEUL** interlocuteur avec les professeurs. • **Matériel :** il est le **SEUL** à pouvoir utiliser le matériel. Les autres membres peuvent l'aider oralement. • **Compétence de l'activité mathématiques :** Il s'assure (avec le gardien) que les productions écrite et numérique **prennent bien en compte** les différentes compétences mathématiques attendues pour l'activité.
Le rapporteur	• **Restitution :** il **présente** à l'oral le travail de son groupe au reste de la classe. L'utilisation de la tablette par vidéo projection est **obligatoire**. • **Production numérique :** il est **responsable** de la production numérique du groupe.

Remarques importantes à dire aux élèves :

- ce travail est une **production de groupe** et l'ensemble des élèves doivent participer à l'élaboration de la trace écrite et de la production numérique ;
- tous les membres du groupe doivent **proposer / argumenter** leurs idées et **écouter** celles des autres… ;
- **le brouillon de chacun** compte dans la notation ;
- les fichiers numériques et diaporama, au nom du groupe, seront à **envoyer** sur l'ENT.

Le problème

Cédric demande à sa tante Maryam une idée de romans à lire. Elle lui envoie alors les textes suivants en lui disant qu'il s'agit d'un chiffrement par substitution, différent à chaque fois. Chacun des textes est une partie d'un livre, différent lui aussi entre l'extrait N°1 et l'extrait N°2.

Extrait N°1 : en français

TI ZTITRWE JE I S W PWG H WQYRT CKSTI XQT H TGGWSTR GQNNTGGJBTCTIY TI GT HJRJZTWIY GQJBWIY ETG PRKMWMJEJYTG YKQYTG ETG EWIZQTG XQJ BKQG GKIY NKIIQTG LQGXQ W NT XQT BKQG WSTV YRKQBT EW MKIIT CWJG HWIG ET NFJUURT XQJ IKQG KNNQPT YKQYT HJUUJNQEYT W NTY TZWRH TYWJY RTGKEQT PWR EW GJZIWYQRT ET RTMQG GQR ET CKY AJHH I TGY PKGGJMET XQT HWIG EW EWIZQT WIZEWJGT GWIG NTYYT NJRNKIGYWINT L WQRWJG NKCCTINT CTG TGGWJG PWR E TGPWZIKE TY ET URWINWJG NKCCT TYWIY ETG EWIZQTG HWIG ETGXQTEETG QI PJRWYT HTG CTRG TGPWZIKETG WQRWJY HQ ET PEQG IWYQRTEETCTIY TIUTRCTR QI GTNRTY HT NTYYT IWYQRT

Extrait N°2 A : en italien

EO XBBETO XJVGGO XWWX AXBMV AED GMBXYX JVW QEO BXSSOYMO SEBSX DYX GVMMEQXYX HX EW QXBMVJE JVWWX GVMMEQXYX

GSOBGX RO GSOAVBMO GDW COBJO JE DYX HEYVGMBX DYX GVBEV JE GMBXYV AESSOWV GXFOQV JXYIXYME SOQV PDVWWV GDWWX SXBMX VBXYO GSXBXCOSSREXMV X QXMEMX RO SBVJDMO SRV VBX EW FXBIOYV JE GSDJVBEX SRV WV XTVTX JEGVFYXMV QX EW BXFXIIO QE RX FEDBXMO SRV YOY SE VYMBXTX AVB YDWWX SOGX SRV GEX GOYO XAAXBGV JDBXYMV WX YOMMV EO WE RO HXMMO MOFWEVBV V YOY RO QVYIEOYXMO W EYSEJVYMV X QEX QOFWEV SRV AED MXBJE X QEX GOBABVGX VWWX W RX ABVGO QOWMO GDW GVBEO QE RX EQAWOBXMO GV XWMBE JEGVFYE XAAXBETXYO JE WXGSEXBFWEVWE TVJVBV YOY AXGGO DYX GVMMEQXYX V AOE EVBE QXMMEYO RO GSOAVBMO PDVGMO SXBMOYSEYO XCCXYJOYXMO GDW PDXJBXYMV GOWXBV JVW FEXBJEYO EO W RO QOGMBXMO X VWGEV V VWWX V GTVYDMX

Extrait N°2 B : en espagnol

N IZMJF QLFJQ IZ SQ GQJMI IKMJQZQ UI PR JISQMF LQJQ VZQ OIPQZQ IS PQJMIO UI SQ GQOQUQ UIOEVDJR IZ SFO QZMIGIELFO UI SQO AIZMQZQO VZQ EQZMRUQU UI QDOVJUFO URDVBFO UI DQRSQJRZIO GQJIERUFO Q SFO UI IOI GQGIS IOMQDQZ LIELFO EFZ MRHQ GIZOI YVI LQDJRQ ORUF IS PFHF UI EVQUJQ YVRIZ SFO LQDRQ URDVBQUF GIJF PI BVJF YVI IS ZF OQDRQ ZQUQ TVIOI EFPF TVIOI SFO GRZMQJFZ UVJQZMI SQ ZFELI LREI YVI SFO DFJJQOIZ N ZQUQ LQDSI UIS QOVZMF Q PR PVBIJ LQOMQ UIOGVIO EFZ WJQZ OFJGJIOQ PRQ ISSQ MFPF SQ EFOQ PVN IZ OIJRF N PI OVGSREF YVI OR AFSARQZ Q QGQJIEIJ SI

GIJPRMRIOI AIJSFO ZQUQ FEVJJRF GFJ IOGQERF UI VZQ OIPQZQ GIJF QNIJ GFJ SQ PQZQZQ PI IZEFZMJI IOI GQGIS IZERPQ UIS JISFB UI QJIZQ UIS BQJURZ OI SF PFOMJI Q ISORI N ISSQ OVTJRF VZ EFSQGOF

Extrait N°2 C : en anglais

XJVV DAX U ZAHJ PA PEJ CSJJO MKOP AY HB NPAOB KRASP K XJJI KFA UP XKN PEJ PSJNWKB AY VKNP XJJI U YASDW AD ADJ AY PEJ XUDWAX NUVVN K DSHRJO AY KRNSOW VUPPVJ WKDZUDF YUFSOJN VUIJ PEJNJ SMAD PEJ MKMJO PEJB XJOJ NZOKXVJW XUPE ZEKVI U PEASFEP PEKP UP XKN PEJ NPKRVJ RAB XEA EKW WOKXD PEJH RSP PEJ VKW NXAOJ EJ IDJX DAPEUDF KRASP UP KDBEAX PEJB EKW ZAHJ PEJOJ WSOUDF PEJ DUFEP U EKW PEJH XKNEJW ASP KDW U ADVB HJDPUADJW PEJ HKPPJO PA HB XUYJ KYPJOXKOWN PA HB NSOMOUNJ NEJ PAAI UP GJOB NJOUASNVB KDW RJFFJW HJ UY KDB HAOJ ZKHJ PA VJP EJO NJJ PEJH DADJ WUW ZAHJ YAO K XJJI KDW PEJD BJNPJOWKB HAODUDF U YASDW PEUN MKMJO VBUDF AD PEJ NSD WUKV UD PEJ FKOWJD

Cédric commence par regarder un extrait vidéo sur le Web (début à 3 min 20 s) :

https://www.youtube.com/watch?v=8BM9LPDjOw0

Il faut cependant aider Cédric à retrouver de quels livres il s'agit afin qu'il puisse les lire.

A noter que ces livres sont libres de droits et peuvent donc être lus intégralement gratuitement (40 pages environ, chaque histoire).

Eléments de correction :

L'extrait N°1 est tiré de : POE, Allan Edgar. *Le scarabée d'or*. 1 843.
L'extrait N°2 est tiré de : DOYLE, Arthur Conan. *Les Hommes dansants.* 1 903.

Extrait N°1 : en français

En général, il n'y a pas d'autre moyen que d'essayer successivement, en se dirigeant suivant les probabilités, toutes les langues qui vous sont connues jusqu'à ce que vous ayez trouvé la bonne. Mais, dans le chiffre qui nous occupe, toute difficulté à cet égard était résolue par la signature. Le rébus sur le mot Kidd n'est possible que dans la langue anglaise. Sans cette circonstance, j'aurais commencé mes essais par l'espagnol et le français, comme étant les langues dans lesquelles un pirate des mers espagnoles aurait dû le plus naturellement enfermer un secret de cette nature.

Extrait N°2 A : en italien

Io arrivo adesso alla parte più strana del mio racconto. Circa una settimana fa, il martedì della settimana scorsa, ho scoperto sul bordo di una finestra una serie di strane piccole sagome danzanti come quelle sulla carta. Erano scarabocchiate a matita. Ho creduto che era il garzone di scuderia che le aveva disegnate ma il ragazzo mi ha giurato che non ci entrava per nulla. Cosa che sia, sono apparse durante la notte. Io li ho fatto togliere e non ho menzionato l'incidente a mia moglie che più tardi. A mia sorpresa, ella l'ha preso molto sul serio, mi ha implorato, se altri disegni apparivano, di lasciarglieli vedere Non passò una settimana e poi, ieri mattino, ho scoperto questo cartoncino abbandonato sul quadrante solare del giardino. Io l'ho mostrato a Elsie e ella è svenuta.

Extrait N°2 B : en espagnol

Y entro ahora en la parte extraña de mi relato. Harà una semana (el martes de la pasada) descubri en los antepechos de las ventanas una cantidad de absurdos dibujos de bailarines, parecidos a los de ese papel. Estaban hechos con tiza. Pensé que habrîa sido el mozo de cuadra quien los habia dibujado, pero me juro que él no sabia nada. Fuese como fuese, los pintaron durante la noche. Hice que los borrasen, y nada hablé del asunto a mi mujer hasta después. Con gran sorpresa mia, ella tomo la cosa muy en serio, y me suplico que si volvian a aparecer, le permitiese verlos. Nada ocurrio por espacio de una semana; pero ayer por la manana, me encontré ese papel encima del reloj de arena del jardin. Se lo mostré a Elsie, y ella sufrio un colapso.

Extrait N°2 C : en anglais

Well, now I come to the queer part of my story. About a week ago—it was the Tuesday of last week—I found on one of the window-sills a number of absurd little dancing figures like these upon the paper. They were scrawled with chalk. I thought that it was the stable-boy who had drawn them, but the lad swore he knew nothing about it. Anyhow, they had come there during the night. I had them washed out, and I only mentioned the matter to my wife afterwards. To my surprise, she took it very seriously, and begged me if any more came to let her see them. None did come for a week, and then yesterday morning I found this paper lying on the sun-dial in the garden.

Annexe : scénario de classe à la maison

En amont

Idéalement, on peut mettre les élèves par binôme, les élèves ayant leurs propres moyens de communication ou en utilisant des salles de groupes dans une classe virtuelle.
Si le professeur souhaite utiliser les rôles, alors les élèves doivent se les répartir comme suit : gardien et rapporteur pour l'un et rédacteur et ambassadeur pour l'autre.
On leur demande alors de regarder l'extrait vidéo, directement sur le site proposé, soit en découpant la vidéo et en la plaçant sur un espace académique de dépôt en mode privé (par exemple sur Moodle).
Les élèves renvoient au professeur par mail ou lors d'un questionnaire en ligne ce qu'ils ont compris en deux à trois phrases maxima.
Le professeur doit alors faire une synthèse qui sera affichée lors de la première séance si elle s'effectue en classe virtuelle ou envoyée par mail sinon.

La première séance

Lors de la première séance, le professeur affiche / envoie la synthèse avec ses commentaires.
Il donne alors le travail en ne sélectionnant qu'un extrait (attention à l'extrait N°2 qui se décline en trois langues étrangères différentes) et répond aux premières questions.
Il place ensuite les élèves par groupe et navigue de groupe en groupe afin de répondre aux questions des élèves, donne des pistes de réflexion.
Une fois l'ensemble des groupes sur une bonne piste, on peut les laisser finaliser seuls.

La deuxième séance

Chaque élève-rédacteur doit construire la trace écrite du groupe avec toutes les pistes de réflexion, peu importe qu'elles soient fructueuses ou non, tandis que l'élève-rapporteur prépare son oral.
La trace écrite est envoyée par mail.
Dans le cas d'une classe virtuelle, l'élève-rapporteur est mis en présentateur par le professeur et doit expliquer à la communauté la démarche, si possible avec quelques photos ou un diaporama.
Dans le cas où la classe virtuelle n'est pas possible, l'élève peut s'enregistrer sur son téléphone, tablette, ordinateur et envoyer son travail au professeur.
Dans ce dernier cas, le professeur devra veiller à ce que lui seul puisse avoir accès au fichier et de mander au préalable une autorisation (qui est souvent demandée dans les établissements en début d'année, se renseigner auprès de la direction).
Le document modèle d'autorisation d'enregistrement image/voix est disponible sur Eduscol : https://eduscol.education.fr/cid149770/protection-des-donnees-personnelles.html#lien1