CRYPTOGRAPHIE :

des activités adaptables de la 6e à la 3e

Jean-Baptiste MAYENSON
Professeur au collège Roger Martin du Gard
Épinay-sur-Seine

Christelle SERRA
Professeure au collège Liberté
Chevilly Larue

Niveau concerné

Sixième, quatrième et troisième

Modalité

– En sixième, tout ce qui est présenté a été abordé dans l'ordre annoncé. Le travail même des élèves en classe ou à la maison dépend des activités. Les activités peuvent cependant se traiter séparément, sans lien effectif entre elles.
Ces séances ont été menées, en sixième, dans le cadre d'un projet d'écriture de conte mathématique, lien interdisciplinaire mathématiques-français réalisé tout le long de l'année scolaire. Les élèves bénéficiaient donc pour cela d'une heure supplémentaire de mathématiques (et de français) inscrite dans leur emploi du temps.
– En quatrième, de même qu'en sixième, les activités ont été abordées dans l'ordre annoncé. Elles ont été traitées en classe entière, sur trois fins de séances successives de 10/15 minutes, puis sur deux heures en salle informatique en alternant l'utilisation individuelle des ordinateurs. La mise en commun et la synthèse ont nécessité une séance supplémentaire.
– En troisième, les activités ont été testées sur quatre séances en classe entière en salle informatique (deux fois deux heures) avec une utilisation alternée des ordinateurs.

Pré-requis

– Activités sixième : aucun pré-requis mathématique important n'est nécessaire. La compréhension de consignes est le principal pré-requis.
Toutefois, avant de lancer les activités présentées, la notion de cryptographie a été rapidement présentée à la classe pour qu'il n'y ait pas d'ambiguïté sur ce que l'on entend par *texte codé* et *texte clair*.
– Activités quatrième : compréhension de consignes, notions de statistique de cinquième.
– Activités troisième : compréhension de consignes, notion de fonction (TP1), fonction affine et arithmétique (TP2)

Objectifs

Ces activités permettent de travailler certaines méthodes de cryptographie (compréhension par les élèves des procédures à utiliser) et sont adaptables à différents niveaux du collège, selon les objectifs que l'on veut se fixer.
En 6e, ces activités sont un support pertinent pour la compréhension des consignes à travers l'appropriation des méthodes de cryptage. Elles abordent les connaissances et compétences mathématiques suivantes : lire, utiliser et interpréter des données à partir de tableaux ou de représentations graphiques. Elles obligent enfin les élèves à s'organiser dans la gestion des données qui sont à leur disposition.
Le prolongement sur tableur en 4e peut être traité indépendamment des autres méthodes de cryptographie. Ces activités permettent d'asseoir les acquis de 5e, d'utiliser le tableur, de présenter une démarche statistique et d'étudier la limite de la méthode par analyse de fréquence.
Le prolongement en 3e sur le chiffrement linéaire permet de s'initier au raisonnement algorithmique, de revoir les notions de fonction et fonction affine, ainsi que d'utiliser le tableur à bon escient. Ces activités sont aussi développées en lycée.

Interdisciplinarité

Ces activités sont un prétexte intéressant pour faire un lien avec le français : reprise de textes étudiés en cours de français (travail interdisciplinaire avec la collègue de lettres) et notamment pour travailler autour de littérature et mathématique avec des textes évoquant les mathématiques (voir les exemples donnés dans la fiche professeur).
En effet, l'extrait de *Marius* de Marcel Pagnol (document 1) est particulièrement riche lorsque l'on travaille sur les fractions (partie importante du programme pour la classe de sixième) ; il permet également, de façon générale, de montrer la différence entre l'usage rigoureux d'un outil et son usage « sauvage » dans la vie de tous les jours.
Dans le document 2, le poème de « géométrie » est extrait du recueil d'Eugène Guillevic. Il constitue une manière originale d'aborder cette partie des mathématiques. Il peut être complété avec d'autres poèmes : la discussion évoque alors la compatibilité avec les définitions apprises en géométrie. On peut aussi espérer que les élèves s'approprient mieux les notions, grâce au jeu et à la création.
Dans le document 3, la chanson de Boris Vian est un exemple permettant de travailler, tout en « s'amusant », sur la polysémie des mots» et on sait à quel point, en classe de sixième, il est nécessaire de s'y attarder.

En quatrième le thème sur la poésie, a été choisi avec les professeurs de français. Les poèmes utilisés pour l'étude des fréquences d'apparitions des voyelles ont été étudiés en cours. Dans l'une des deux classes, cette étude a permis de préparer un travail en français sur les contraintes d'écriture.

CRYPTOGRAPHIE – Fiche professeur

Durée : 6 séances **Classe de 6e**

Situation

Code de César : coder et décoder un texte à partir de la méthode décrite.
Variante du code de César : décoder un texte à partir d'un diagramme en bâtons qui indique la fréquence d'apparition de chaque lettre dans le texte clair.
Carré de Polybe : coder un texte grâce aux coordonnées des lettres lisibles dans tableau double-entrée.
Substitution mono-alphabétique : décoder un texte à partir d'un diagramme en bâtons qui indique la fréquence d'apparition de chaque lettre dans le texte clair.

Supports et ressources de travail (fournis pages suivantes)

Document 1 : principe de la méthode, extrait du poème « C'est les Mathématiques » de Tom Lehrer à décoder et extrait de la pièce de théâtre « Marius »de Marcel Pagnol (acte 2) à décoder.
Document 2 : principe de la méthode, poème extrait des « Euclidiennes » de Eugène Guillvec à décoder et diagramme en bâtons qui indique le nombre de fois où apparaît chaque lettre dans le texte clair.
Document 3 : principe de la méthode (un tableau double entrée) et chanson « Racine Carrée » de Boris Vian à coder.
Document 4 : extrait des « Contes » de Charles Perrault à décoder grâce à un diagramme.

Compétences

Pratiquer une démarche scientifique ou technologique	Capacités susceptibles d'être évaluées en situation	Exemples d'indicateurs de réussite
Rechercher, extraire et organiser l'information utile	Extraire d'un document papier les informations utiles Organiser les informations pour les utiliser	Entreprendre le comptage de chaque lettre Présenter les nombres d'apparition pour les comparer
Réaliser, manipuler, mesurer, calculer, appliquer des consignes	Suivre un protocole	Compter chaque lettre sans oubli
Raisonner, argumenter, pratiquer une démarche expérimentale ou technologique, démontrer	Proposer une procédure	Mettre en œuvre une stratégie pour associer les lettres du texte codé à celles du texte clair
Présenter la démarche suivie, les résultats obtenus, communiquer à l'aide d'un langage adapté	Rendre compte de la démarche de résolution	Expliquer les choix pour remplacer les lettres. Reconstituer les textes sans erreur

Savoir utiliser des connaissances et compétences mathématiques	Capacités susceptibles d'être évaluées en situation	Exemples d'indicateurs de réussite
Organisation et gestion de données	Lire des données présentées sous forme de graphiques	Reconnaître que le nombre d'apparition de chaque lettre du texte codé est lié au nombre d'apparition des lettres du graphique (texte clair)

Niveaux	Connaissances	Capacités
6e	Représentations usuelles des données	Lire, utiliser et interpréter des informations à partir d'une représentation graphique simple Organiser des données en choisissant un mode de représentation adapté : tableau à deux ou plusieurs colonnes

CRYPTOGRAPHIE – Fiche élève

Durée : 6 séances **Classe de 6e**

Document 1

Principe de la méthode du code de César

Le texte codé s'obtient en remplaçant chaque lettre du texte clair par la lettre qui est située trois rangs plus loin dans l'alphabet.
La longueur du décalage constitue la clé du chiffrement

Extrait du poème « C'est les Mathématiques », de Tom Lehrer

Compter les moutons
Quand tu essayes de dormir,
Etre juste
Quand il y a quelque chose à partager,
Etre soigneux
Quand tu plies une feuille,
C'est les mathématiques !
Quand une balle
Rebondit contre un mur,
Quand tu cuisines
Avec un livre de recettes,
Quand tu sais
Combien d'argent tu dois,
C'est les mathématiques !
Quelle quantité d'or tient dans l'oreille d'un éléphant ?
A midi sur la lune, quelle heure est-il sur terre ?
Si tu pouvais compter pendant toute une année, arriverais-tu à l'infini,
Ou quelque part, dans les environs ?
Quand tu décides
Combien de timbres utiliser,
Quand tu sais
Quelles sont les chances qu'il neige,
Quand tu paries
Et finis par t'endetter,
Oh tu peux toujours essayer,
Tu ne pourras jamais échapper
Aux mathématiques !
[…]

En choisissant une clé de 3, coder le poème ci-dessus et expliquer la méthode.

Extrait de la pièce de théâtre « Marius », de Marcel Pagnol (acte II)

FHVDU
HK ELHQ, SRXU OD GLALHPH IRLV,MH YDLVWH O'HASOLTXHU, OH SLFRQ-FLWURQFXUDC¸ DR. DSSURFKH-WRL ! WX PHWV G'DERUG XQ WLHUV GH FXUDC¸DR. IDLV
DWWHQWLRQ : XQ WRXW SHWLW WLHUV. ERQ. PDLQWHQDQW, XQ WLHUV GH
FLWURQ. XQ SHX SOXV JURV. ERQ. HQVXLWH, XQ ERQ WLHUV GH SLFRQ. UHJDUGH
OD FRXOHXU. UHJDUGH FRPPH F'HVW MROL. HW D OD ILQ, XQ JUDQG WLHUV G'HDX. YRLOD.

PDULXV
HW C¸D IDLW TXDWUH WLHUV.

FHVDU
HADFWHPHQW. M'HVSHUH TXH FHWWH IRLV, WX DV FRPSULV.

PDULXV
GDQV XQ YHUUH, LO Q'B D TXH WURLV WLHUV.

FHVDU
PDLV, LPEHFLOH, C¸D GHSHQG GH OD JURVVHXU GHV WLHUV!...

PDULXV
HK QRQ, C¸D QH GHSHQG SDV. PHPH GDQV XQ DUURVRLU, RQ QH SHXW PHWWUH
TXH WURLV WLHUV.

FHVDU
DORUV, HASOLTXH-PRL FRPPHQW M'HQ DL PLV TXDWUH GDQV FH YHUUH!

En choisissant une clé de 3, décoder l'extrait ci-dessus et expliquer la méthode.

Document 2

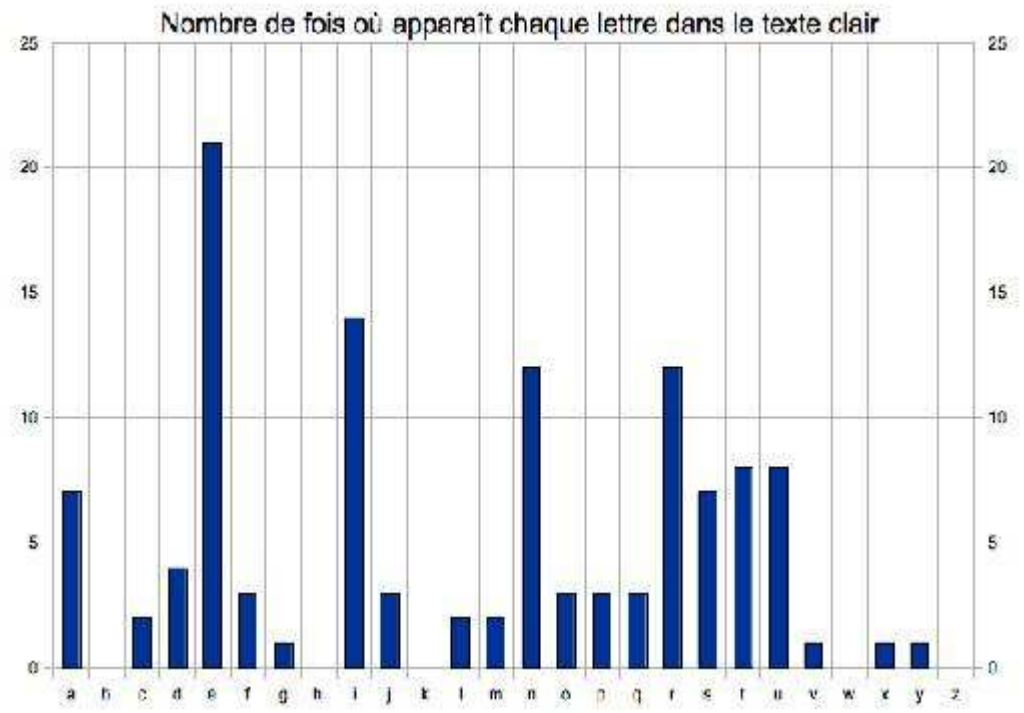
Principe de la méthode du code de César

Le texte codé s'obtient en remplaçant chaque lettre du texte clair par la lettre qui est située trois rangs plus loin.
La longueur du décalage constitue la clé du chiffrement.

Poème extrait des « Euclidiennes », de Eugène Guillvec

YT CT HJXH FJT AT UGJXI ETJI-TIGT
ST STJM AXVCTH FJX HT GTCRDCIGTCI.
YT C'PX GXTC
DC SXI : EPGIXG SJ EDXCI,
N PGGXKTG.
YT C'TC HPXH GXTC.
BPXH FJX
B'TUUPRTGP?

Diagramme en bâtons



Le professeur a crypté, avec le code de César, le poème donné ci-dessus. Il a oublié la clé pour le décoder. Avec le diagramme en bâtons, aider le professeur à décoder le poème et expliquer la méthode.

Document 3

Principe de la méthode du Carré de Polybe

Polybe est à l'origine d'une méthode très originale pour coder. Pour cela, il dispose les lettres dans un tableau 5×5 (on identifier le I et le J) :

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

On remplace alors chaque lettre par ses coordonnées dans le tableau, en écrivant d'abord la ligne, puis la colonne.

Chanson « Racine carrée » de Boris Vian

II y a des racines de tout'les formes
Des pointues, des rond' et des difformes
Cell'de la guimauve est angélique
II y a un Racin' qui est classique
Et la mandragore est diabolique
Mêm's'il nous bassin' on n'y peut plus rien
Mais la racine que j'adore
Et qu'on extrait sans effort-eu
La racin' carrée c'est ma préfé-rée
Une racine qu'a un aspect louche
C'est cell'de l'arbre de couche
Le drogué vend son âme
Pour cell' de l'arbre à cames
Si la racine du manioc a
De quoi fair'du tapioca
Evitons tout'not' vie (de bouffer)
Celle du pissenlit
II y a des racin' qui s' vend'en bottes
Le radis, l'navet ou la carotte
Vous connaissez celle de la bruyère
Dans laquell' on taille des pip' en terre
II y a la racin' de canne à pêche
Cultivez-la donc, qu'est-c'qui vous empêche ?
Mais la racine que j'adore
Donnez m'en-z-encore, encore
La racin' carrée c'est ma préfé-rée.

Coder la chanson ci-dessus et expliquer la méthode.

Document 4

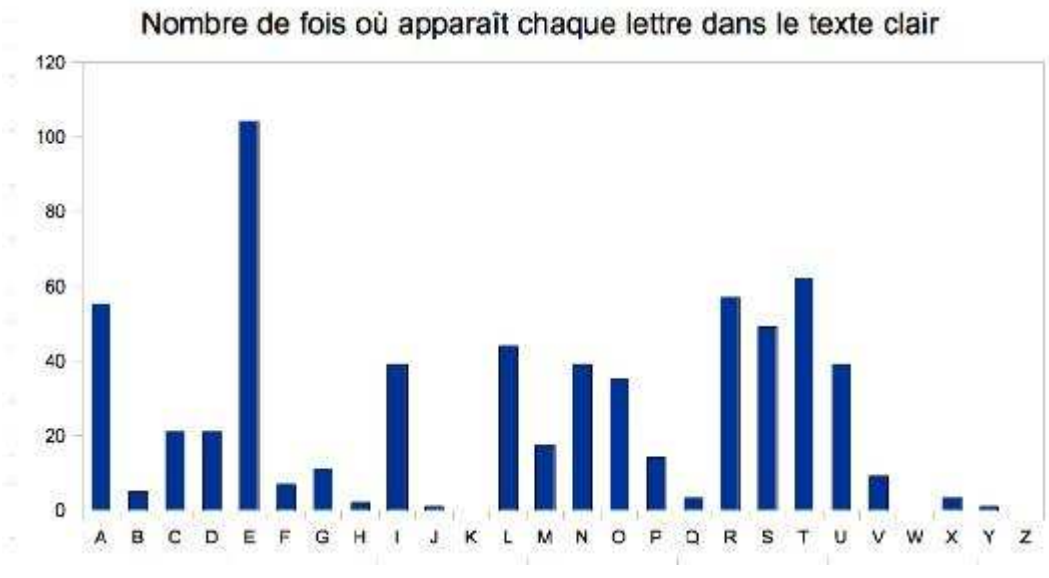
Principe de la méthode de substitution mono-alphabétique

On définit une substitution mono-alphabétique en indiquant de quelle façon remplacer chaque lettre de l'alphabet par une autre différente. Pour qu'une telle substitution puisse servir au cryptage d'un texte, il faut respecter les deux conditions suivantes : deux lettres différentes sont codées de façons différentes et la même lettre est toujours codée de la même façon.

Extrait des « Contes » de Charles Perrault

GN OLZXFQ CGLHVNSD QN HNINVGGN NP QSHQFSE,
NZS UN ONEEN ISN NE U'SP NQXLVH QV JFSE.
VG HNPU CHFON FS QLGNVG, NE ANHZN OLZZN SP FVCGN
GN HNCFHUN NE Q'NP IF : XSVQ HNPOLPEHN GF HNCGN;
UHLVEN, U'SP CHFIN XLHE, XGNVPN UN ZFBNQEN,
VPAGNDVWGN NE QSHELSE LWQNHIFPE G'NMSVEN (...)
ELSENALVQ PLQ FZLSHQ, HNXGVMSF GN OLZXFQ,
XHLUSVHLPE UNQ NPAFPEQ MSV IFVPOHLPE GN EHNXFQ.
UN PLSQ UNSD QLHEVHF GF WNGGN FHOJVENOESHN,
NE ZVGGN PLWGNQ FHEQ XLSH XLGVH GF PFESHN, (...)
GN OLZXFQ FSQQVELE QSH SP XVNU QN UHNQQF,
NE UN G'FSEHN, NP ELSHPFPE SP CHFPU ONHOGN EHFOF,
GF HNCGN NP ASE HFIVN, NE QLSUFVP QN IVPE ZNEEHN
UFPQ GN ZVGVNS US ONHOGN, NE AVE GN UVFZNEHN.
QLP FZFPE G'NZWHFQQF, G'FRFPE F QF ZNHOV,
EFPELE Q'NGFHCVQQFPE NE EFPELE HFOOLSHOV,
NE G'LP IVE PFVEHN FGLHQ UN GNSHQ ULOENQ XLQESHNQ
EHVFPCGNQ NE OFHHNQ, NE ZVGGN FSEHNQ AVCSHNQ.

Diagramme en bâtons



Avec le diagramme en bâtons, décoder le texte ci-dessus et expliquer la méthode.

CRYPTOGRAPHIE – Fiche professeur

Durée : 3 fins de séances (doc 1 à 3) + 3 séances (doc 4 à 6) Classe de 4e

Situation

Code de César : coder et décoder un texte à partir de la méthode décrite.
Variante du code de César : décoder un texte à partir d'un diagramme en bâtons qui indique la fréquence d'apparition de chaque lettre dans le texte clair.
Carré de Polybe : coder un texte grâce aux coordonnées des lettres lisibles dans le tableau à double-entrée.
Substitution mono-alphabétique : décoder un texte à partir d'un diagramme en bâtons qui indique la fréquence d'apparition de chaque lettre dans le texte clair.
Fréquence d'apparition des voyelles : (trois documents par groupe) utilisation du tableur.

Supports et ressources de travail (fournis pages suivantes)

Document 1 : principe de la méthode, mots à coder ou décoder, poèmes à coder.
Document 2 : principe de la méthode, poème extrait des « Euclidiennes » de Eugène Guillvec à décoder et diagramme en bâtons qui indique le nombre de fois où apparaît chaque lettre dans le texte clair.
Document 3 : principe de la méthode (un tableau à double entrée), chanson « Racine Carrée » de Boris Vian à coder, citations à décoder.
Document 4 : principe de la méthode (tableau des fréquences), analyse et étude de fréquence d'apparition des lettres dans un poème.
Document 5 : TP tableur, fréquence d'apparition des voyelles dans des poèmes.
Document 6 : recueil des données, calcul de pourcentage.

Compétences (Prolongement)

RÉSOLUTION D'UN PROBLÈME	**Organisation et gestion de données**	
C3. Observer, rechercher, organiser les informations.	Traduire des symboles, des consignes, coder, décoder…	Exploiter des données statistiques
C3. Réaliser, manipuler, mesurer, calculer, appliquer des consignes.	Utiliser un tableur-grapheur pour : • Présenter des données ; • Calculer des effectifs, des fréquences ; • Créer un graphique ou un diagramme à partir des données d'une feuille de calcul • Calculer, utiliser une formule • Créer, analyser, utiliser une formule	• Utiliser et construire des tableaux, diagrammes et graphiques • Calculer une fréquence • Calculer le pourcentage relatif à plusieurs groupes Compétence 4 domaine 3
C3. Raisonner, argumenter et démontrer.	Confronter le résultat au résultat attendu	Choisir la bonne représentation statistique ; Porter un regard critique sur des résultats.
C3. Communiquer à l'aide de langages adaptés.	Compte rendu : rédiger la réponse avec les critères de rigueur mathématiques	

CRYPTOGRAPHIE – Fiche élève

Durée : 3 + 3 séances **Classe de 4e**

Document 1

Principe de la méthode du code de César :
Le texte codé s'obtient en remplaçant chaque lettre du texte clair par la lettre qui est située trois rangs plus loin dans l'alphabet.
La longueur du décalage constitue la clé du chiffrement

Pour chaque codage et décodage, expliquer la méthode.

Exercice 1 :
Décoder le message *ERQ GHEXW* a été crypté avec la méthode de codage de Jules César.

Exercice 2 : Maintenant, on utilise la **clé 17**.

1°) Coder le message : *CRYPTAGE* .

2°) Décoder le message : *JKRZJKZHLVL* .

3°) Décoder le message : *MIRZDVEK WRTZCV R UVTIPGKVI.*

Exercice 3 : Décoder le message *KWLIOM BZWX AQUXTM* sachant qu'il a été crypté avec la méthode de chiffrement de César et que la lettre *H* est codée par la lettre *P*.
Quelle est la clé ?

Aide pour le cryptage et le décryptage par la méthode de César……

Pour faciliter le cryptage et le décryptage, on utilise un tableau de chiffrage. Voici comment. :

- On numérote les lettres de l'alphabet de 0 à 25 :

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

- Il suffit d'ajouter la clé au numéro de la lettre à crypter et de chercher à quelle lettre correspond le nombre obtenu.

Aide pour l'exercice 2 …….

Compléter le tableau de chiffrage avec la clé 17

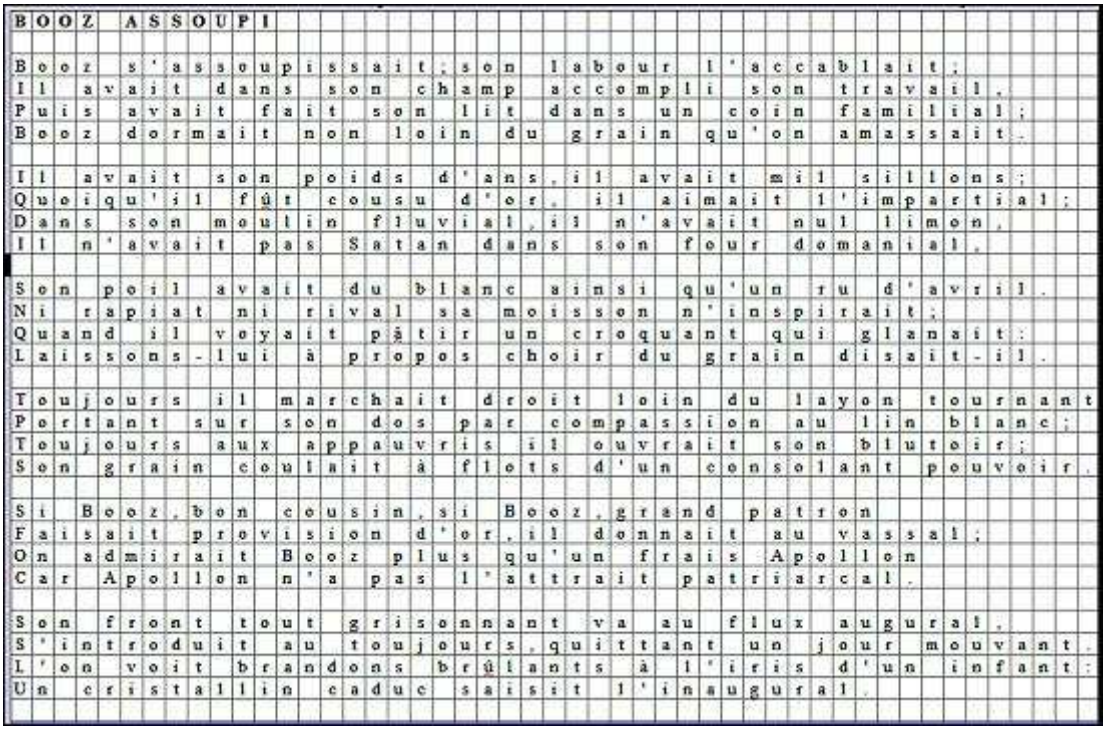
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
		20										4													
		T										D													

Exercice 4 :
Crypter un message pour le donner à un groupe qui devra le décrypter sans lui donner la clé.
Facultatif :

En choisissant une clé de votre choix, coder un des deux poèmes suivant et expliquer la méthode

Extrait du poème « C'est les Mathématiques », de Tom Lehrer

Compter les moutons
Quand tu essayes de dormir,
Etre juste
Quand il y a quelque chose à partager,
Etre soigneux
Quand tu plies une feuille,
C'est les mathématiques !
Quand une balle
Rebondit contre un mur,
Quand tu cuisines
Avec un livre de recettes,
Quand tu sais
Combien d'argent tu dois,
C'est les mathématiques !
Quelle quantité d'or tient dans l'oreille d'un éléphant ?
A midi sur la lune, quelle heure est-il sur terre ?
Si tu pouvais compter pendant toute une année, arriverais-tu à l'infini,
Ou quelque part, dans les environs ?
Quand tu décides
Combien de timbres utiliser,
Quand tu sais
Quelles sont les chances qu'il neige,
Quand tu paries
Et finis par t'endetter,
Oh tu peux toujours essayer,
Tu ne pourras jamais échapper
Aux mathématiques ![…]



BOOZ ASSOUPI

Booz s'assoupissait, son labour l'accablait ;
Il avait dans son champ accompli son travail,
Puis avait fait son lit dans un coin familial ;
Booz dormait non loin du grain qu'on amassait.

Il avait son poids d'ans, il avait mille sillons ;
Quoiqu'il fût cousu d'or, il aimait l'impartial ;
Dans son moulin fluvial, il n'avait nul limon,
Il n'avait pas Satan dans son four domanial,

Son poil avait du blanc ainsi qu'un ru d'avril.
Ni rapiat ni rival sa moisson n'inspirait ;
Quand il voyait pâtir un croquant qui glanait :
Laissons-lui à propos choir du grain disait-il.

Toujours il marchait droit loin du layon tournant
Portant sur son dos par compassion au lin blanc ;
Toujours aux appauvris il ouvrait son blutoir ;
Son grain coulait à flots d'un consolant pouvoir.

Si Booz, bon cousin, si Booz, grand patron
Faisait provision d'or, il donnait au vassal ;
On admirait Booz plus qu'un frais Apollon
Car Apollon n'a pas l'attrait patriarcal.

Son front tout grisonnant va au flux augural,
S'introduit au toujours, quittant un jour mouvant.
L'on voit brandons brûlants à l'iris d'un infant :
Un cristallin caduc saisit l'inaugural.

Document 2

Principe de la méthode du code de César

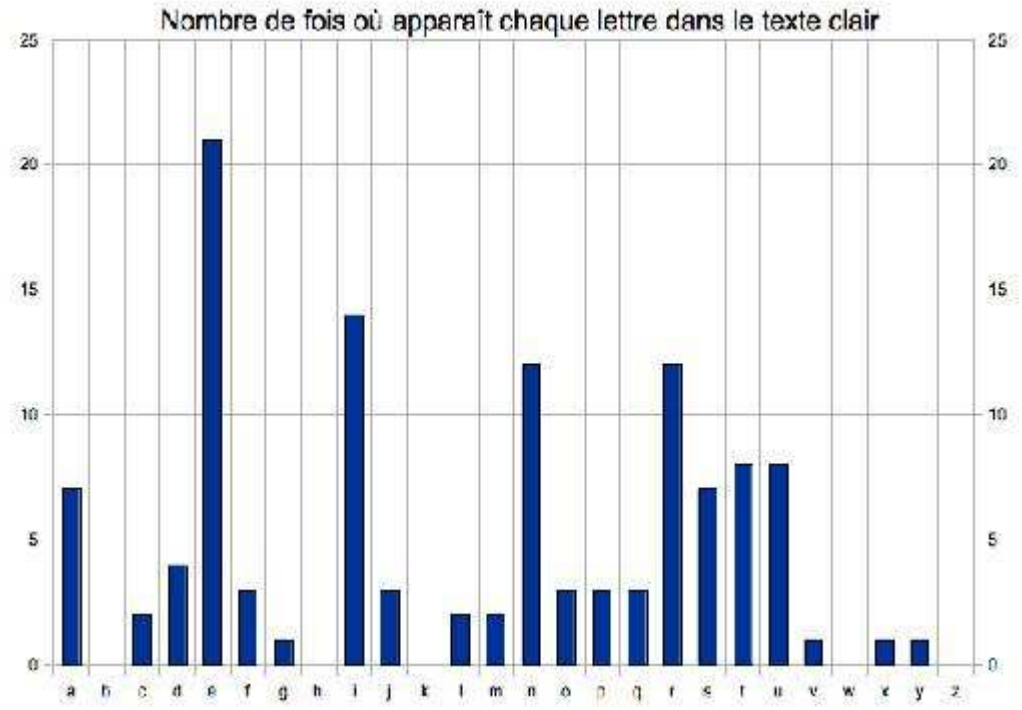
Le texte codé s'obtient en remplaçant chaque lettre du texte clair par la lettre qui est située trois rangs plus loin.
La longueur du décalage constitue la clé du chiffrement

Exercice 5

Poème extrait des « Euclidiennes », de Eugène Guillvec.

YT CT HJXH FJT AT UGJXI ETJI-TIGT
ST STJM AXVCTH FJX HT GTCRDCIGTCI.
YT C'PX GXTC
DC SXI : EPGIXG SJ EDXCI,
N PGGXKTG.
YT C'TC HPXH GXTC.
BPXH FJX
B'TUUPRTGP?

Diagramme en bâtons



Le professeur a crypté, avec le code de César, le poème donné ci-dessus. Il a oublié la clé pour le décoder.
1°) Avec le diagramme en bâtons, aider le professeur à décoder le poème et expliquer la méthode.
2°) Calculer les fréquences en pourcentages

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

Document 3

Principe de la méthode du Carré de Polybe

Polybe est à l'origine d'une méthode très originale pour coder. Pour cela, il dispose les lettres dans un tableau 5×5 (nous sommes ici obligés d'identifier le I et le J) :

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

On remplace alors chaque lettre par ses coordonnées dans le tableau, en écrivant d'abord la ligne, puis la colonne. Par exemple, le mot EVASION, se code avec le carré de Polybe en 15511143243433.

Exercice 6 : **Décoder les deux citations suivantes**

« 3115 3534154415 154344 453315 2111124224414515 14'243211221543 »
Pierre Reverdy (1889-1930)

« 3111 353415432415 42153314 3111 512415 434542 4415424215 35314543 1215313115, 3234243343 1535231532154215, 3234243343 322443154211123115 »
Adonis (né en 1930)

Exercice 7 : **Créer votre propre carré de Polybe et coder le texte de votre choix.**

Document 4

Principe de la méthode de substitution mono-alphabétique :
On définit une substitution mono-alphabétique en indiquant de quelle façon remplacer chaque lettre de l'alphabet par une autre différente. Pour qu'une telle substitution puisse servir au cryptage d'un texte, il faut respecter les deux conditions suivantes : deux lettres différentes sont codées de façons différentes et la même lettre est toujours codée de la même façon.
C'est Al Kindi qui découvrit une méthode pour déchiffrer les messages chiffrés par toute substitution mono-alphabétique sans la connaissance de la clef du chiffrement, ni même du type exact du chiffrement.
Le procédé mis au point par Al-Kindi est basé sur l'analyse des fréquences des lettres. Il observa que la fréquence des lettres d'une langue pour un long texte est toujours sensiblement la même. En conséquence, pour déchiffrer un texte chiffré, Al-Kindi propose de calculer les fréquences des lettres que l'on trouve dans ce texte afin de les comparer aux fréquences constatées dans la langue qui a servi à l'écrire : il devient alors possible, non sans difficultés, de déchiffrer un texte chiffré par substitution mono-alphabétique.
Il y a autant de langues que de fréquences d'apparitions des lettres. Le tableau suivant montre les fréquences moyennes des lettres utilisées dans les textes écrits en français (les valeurs sont données en %).

A	B	C	D	E	F	G	H	I	J	K	L	M
9.42	1.02	2.64	3.39	15.87	0.95	1.04	0.77	8.41	0.89	0.00	5.34	3.24

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
7.15	5.14	2.86	1.06	6.46	7.90	6.26	6.24	2.15	0.00	0.30	0.24	0.32

Exercice 1 :
1°) Dans un texte chiffré, que représente donc la lettre qui apparaît le plus fréquemment ?
2°) Dans un texte chiffré, que représentent donc les lettres qui apparaissent le moyennement fréquemment ?
3°) Dans un texte chiffré, que représentent donc les lettres qui apparaissent le moins fréquemment ?

Exercice 2 : (**à faire à la maison**) **Faire une petite étude statistique des fréquences des lettres dans le poème ci-dessous. Retrouvez son auteur et son titre.**

Je m'en allais, les poings dans mes poches crevées;
Mon paletot soudain devenait idéal;
J'allais sous le ciel, Muse, et j'étais ton féal;
Oh! là là! que d'amours splendides j'ai rêvées!

Mon unique culotte avait un large trou.
Petit-Poucet rêveur, j'égrenais dans ma course
Des rimes. Mon auberge était à la Grande-Ourse.
Mes étoiles au ciel avaient un doux frou-frou

Et je les écoutais, assis au bord des routes,
Ces bons soirs de septembre où je sentais des gouttes
De rosée à mon front, comme un vin de vigueur;

Où, rimant au milieu des ombres fantastiques,
Comme des lyres, je tirais les élastiques
De mes souliers blessés, un pied près de mon cœur!

Les pourcentages correspondent-ils au tableau proposé ?

Document 5

FRÉQUENCE D'APPARITION DES VOYELLES (1) - groupe 4

Étude de la fréquence d'apparition des voyelles dans le poème classique *Booz endormi*

Tableur de Open Office
Nous allons travailler sur le tableur de Open Office, qui est un logiciel gratuit que l'on peut télécharger, si c'est possible, à la maison.

a. Ouvrir le fichier *Voyelles-élèves* qui est composé de six feuilles de tableur.

b. L'enregistrer sous *MES DOCUMENTS* : *Nom.prénom*.

c. Dans l'onglet « Exercice 4 », lire le poème *Booz endormi*.

d. Dans la cellule BF2, compter le nombre total de « a », dans le poème, en utilisant la formule suivante : =NB.SI(A1:BD32;"a")+NB.SI(A1:BD32;"à")+NB.SI(A1:BD32;"â").
Comment comprenez-vous cette formule ? ……
……..
……..

e. Recommencer le travail dans les cellules BG2, BH2 jusqu'à BK2 pour les lettres E, I, O, U et Y.
(Penser aux différentes variantes de chacune de ses lettres)
E : "e";"é""è";"ê";"ë" I : "i";"î";"ï" O : "o""ô" U : "u" ;"ù";"û" et Y : "y"
BG2 : .....
BH2 : .....
BI2 : .....
BJ2 :.....
BK2 :.....

f. Dans la cellule BL2, faire compter le nombre total de voyelles du poème.
Entrer la formule suivante : =BF2+BG2+BH2+BI2+BJ2+BK2

Quelle autre formule peut-on entrer ? .....

g. Dans la cellule BF3, faire compter le pourcentage de « a » par rapport au nombre total de voyelles dans le poème.
Quelle formule doit-on entrer ? ……

h. Recommencer le travail dans les cellules BG3, BH3 jusqu'à BK3.
BG3 : ..... BH3 : .....
BI3 : ..... BJ3 : .....
BK3 : .....

Quelle formule pour BL3 ? .....

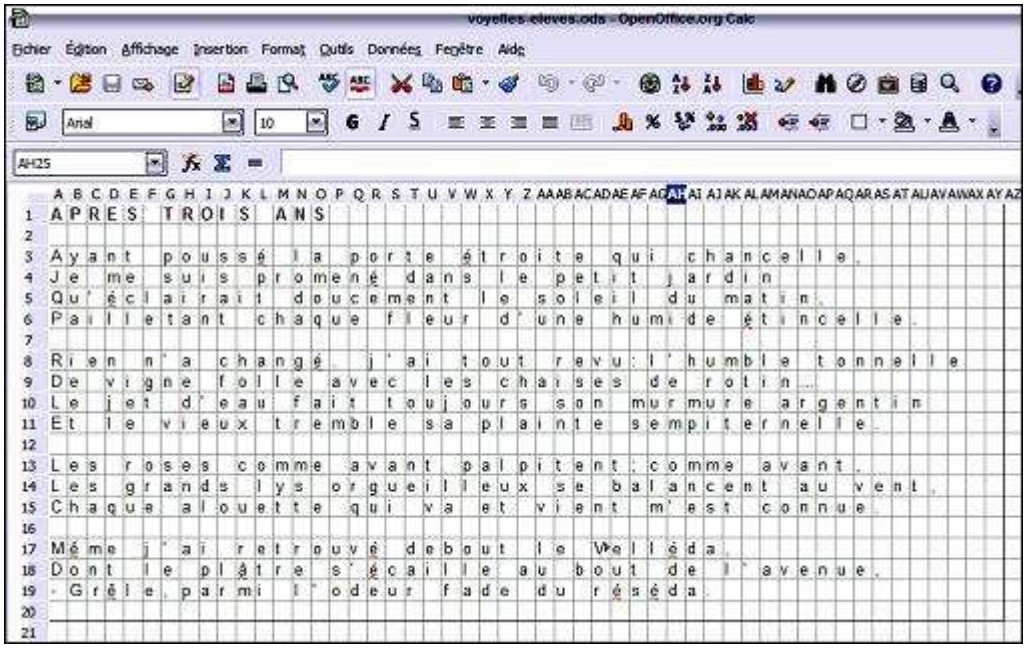
i. **Représenter graphiquement, par un diagramme en bâtons**, les pourcentages d'apparition des voyelles dans *Booz endormi*.

j. Citer les voyelles dans l'ordre décroissant de leur fréquence d'apparition.
.....

k. Cliquer sur Fichier puis enregistrer le travail.

D'après la fiche 35 © SCÉRÉN/CRDP Nord – Pas de Calais – *Mathématiques et Socle commun au collège*

Aides : texte édité et comment insérer un graphique



	BE	BF	BG	BH	BI	BJ	BK	BL
	Voyelles	A	E	I	O	U	Y	Total
	Effectifs							
	Pourcentages							

Graphique

Pour insérer un graphique ……..

- Sélectionner les cellules BE1 à BK1 Ctrl puis sélectionner les cellules BE3 à BK3
- Sélectionner l'icône 'insérer un graphique'
- Choisir 'colonne' comme type de graphique suivant
- Plage de données sélectionner : séries de données en ligne ; 1ère ligne et 1ère colonne en étiquette suivant
- Séries de données suivant
- Éléments du diagramme : choisir un titre, un nom pour chaque axe et sélectionner 'afficher légende' terminer

……

Recherche en temps libre

FRÉQUENCE D'APPARITION DES VOYELLES (2) – Groupe 4

1°) Effectuer une recherche internet pour répondre aux questions suivantes.

a. Quel est l'auteur de *Booz endormi* ?

.....

b. Durant quel siècle a-t-il vécu ?

.....

c. De quel recueil ce poème fait-il partie ?

.....

2°) Étudier la fréquence d'apparition des voyelles dans le poème *Booz assoupi* (Exercices 5 du fichier *Voyelles-élèves.*)
Comparer les fréquences avec celles de *Booz endormi.*
En quoi cet extrait fournit-il un exemple de limite de la méthode d'Al-Kindi ?

Document 6

FREQUENCE D'APPARITION DES VOYELLES (3)

Recueil et comparaison des résultats

1°) Fréquence en %

	Texte 1	Texte 2	Texte 3	Texte 4	Texte 5	Texte 6	Texte 7
A							
E							
I							
O							
U							
Y							

2°) Effectifs

	Texte 1	Texte 2	Texte 3	Texte 4	Texte 5	Texte 6	Texte 7
A							
E							
I							
O							
U							
Y							
Nombre Total de lettres							

3°) Calculer les fréquences d'apparition de voyelles relatives au nombre total de lettres du texte.
4°) Comparer les résultats obtenus aux valeurs données dans la situation 4 de cryptographie.
5°) En quoi ces extraits fournissent-ils des exemples de limite de la méthode d'Al-Kindi ?

CRYPTOGRAPHIE – Fiche professeur

Durée : 4 séances **Classe de 3e**

Situation

Code de César : coder et décoder un texte à partir de la méthode décrite. Utilisation du tableur.
Code affine : coder et décoder un texte à partir de la méthode décrite. Utilisation du tableur.

Supports et ressources de travail (fournis pages suivantes)

Document 1 : principe de la méthode, mots à coder et décoder. Créer un outil de codage à l'aide du tableur.
Document 2 : principe de la méthode, mots à coder et décoder. Créer un outil de codage à l'aide du tableur. Vérifier ses résultats.
Documents 2 et 3 de 4e donnés aux plus rapides. *Variante du code de César*: principe de la méthode, poème extrait des « Euclidiennes » de Eugène Guillvec à décoder et diagramme en bâtons qui indique le nombre de fois où apparaît chaque lettre dans le texte clair.
On peut évoquer la faiblesse du code de césar, connaissance la fréquence d'occurrence des lettres dans la langue cryptée.
Carré de Polybe : principe de la méthode (un tableau à double entrée), une chanson « Racine Carrée » de Boris Vian à coder, des citations à décoder.

Compétences

<table>
<tr><th>RESOLUTION D'UN PROBLEME</th><th colspan="2">Organisation et gestion de données</th></tr>
<tr><td>C3. Observer, rechercher, organiser les informations.</td><td colspan="2">• Utiliser un tableur pour recueillir, mettre en forme les informations afin de les traiter.
• Modéliser un problème</td></tr>
<tr><td>C3. Réaliser, manipuler, mesurer, calculer, appliquer des consignes.</td><td>• Créer, analyser, utiliser une formule.
• Compétence 4 domaine 3 : créer, modifier une feuille de calcul, insérer une formule.</td><td>• Mener à bien un calcul instrumenté.
• Conduire un calcul littéral simple.</td></tr>
<tr><td>C3. Raisonner, argumenter et démontrer.</td><td colspan="2">• Participer à l'écriture d'un algorithme simple et mettre en œuvre le programme correspondant.
• Évaluer la pertinence d'un algorithme, d'un programme simple.
• Confronter le résultat au résultat attendu.</td></tr>
<tr><td>C3. Communiquer à l'aide de langages adaptés.</td><td colspan="2">Compte rendu : rédiger la réponse avec les critères de rigueur mathématiques.</td></tr>
</table>

CRYPTOGRAPHIE – Fiche élève

Durée : 4 séances **Classe de 3e**

Document 1 : idem doc 4e

Document 2 : **Le chiffrement de César**

Exercice 5

But : utiliser le tableur pour effectuer ces tâches plus rapidement.

1°) Réfléchir comment construire un tableau similaire à celui de l'exercice 2.

2°) Ouvrir le fichier *code de César* (sous serveur commun/travail/maths/3ème)

Voici des formules utilisées dans ce fichier ; observe et explique leur utilisation.

CAR

Convertit un nombre en caractère en fonction du tableau de code actif. Il peut s'agir d'un nombre entier à deux ou trois chiffres.

Syntaxe

CAR(nombre)

nombre est un nombre entre 1 et 255 représentant la valeur de code du caractère.

Exemple

=CAR(100) renvoie le caractère d.

……
……
……

MOD

Renvoie la différence après la division d'un nombre.

Syntaxe

MOD(dividende;diviseur)

Pour les arguments de nombres entiers, cette fonction renvoie le dividende modulo le diviseur, c'est à dire le reste quand le **dividende** est divisé par le **diviseur**.

Exemple

=MOD(22;3) renvoie 1, le reste quand 22 est divisé par 3.

=MOD(11,25;2,5) renvoie 1,25.

……
……
……
……

Que permet de faire la fonction **RECHERCHE utilisée dans ce fichier ?**

……
……
……
……
……

3°) A l'aide du 1°) et 2°) créer votre propre outil de cryptage (et décodage si temps)

Enregistrer votre travail sous *MES DOCUMENTS* : *Nom.prénom. crypto1*.

Document 3 : Le codage affine

Principe de la méthode

Le texte chiffré s'obtient en remplaçant chaque lettre du texte clair par la lettre correspondant à la valeur numérique obtenue par le calcul du reste par 26 de l'expression affine ($ax + b$) où x est la valeur numérique de la lettre du texte clair.

Exemple avec la clé (7, 5) qui est associée à la fonction affine définie par $f(x) = 7x + 5$

Pour faciliter le cryptage et le décryptage, on utilise un tableau de chiffrage. Voici comment. :

- On remplace chaque lettre de l'alphabet par son chiffre correspondant de 0 à 25 :

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

- Chaque lettre claire est d'abord remplacée par son équivalent numérique x puis chiffrée par le calcul du reste par 26 de $f(x)=7x + 5$.

Si on veut crypter la lettre C,
- le nombre correspondant à C est 2
- $f(2) = a \times 2 + b = 7 \times 2 + 5 = 14 + 5 = 19$
- la lettre correspondant à 19 est T
- C est codé par la lettre T

Si on veut crypter la lettre M,
- le nombre correspondant à M est 12
- $f(12) = 12 \times 7 + 5 = 84 + 5 = 89$
- le problème est que 89 est supérieur à 26 et ne correspond à aucune lettre mais $89 = 3 \times 26 + 11$ donc le nombre qui code M est 11(reste de la division euclidienne de 89 par 26)
- la lettre correspondant à 11 est L
- M est codé par la lettre L

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
		19										11													
		T										L													

Exercice 1 :

1°) Compéter le tableau ci-dessus et **expliquer vos calculs**
ATTENTION : on ne peut pas faire un simple décalage des lettres comme dans le code de César qui est un cas particulier de ce chiffrement, il faut faire le calcul pour chaque lettre de l'alphabet.

2°) Coder le texte suivant : *Le début du codage* ……
3°) Décoder les mots suivants : *OZSTIJZS FOOJSH* ……

Exercice 2 :
1°) Quelle fonction affine est associée au code de César ? ……...

2°) **Des contraintes ….**

a. L'expression affine $2x + 3$ permet-elle de définir une fonction de codage ? (Deux lettres distinctes sont-elles codées de façons différentes ?)

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	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
$f(x)$																										
Reste de $f(x) \div 26$																										
Chiffré																										

b. Les nombres 2 et 26 sont-ils premiers entre eux (justifier) ?

c. En fait, les seules valeurs de *a* permettant de décoder clairement un message sont les 12 valeurs suivantes : **1; 3; 5; 7; 9; 11; 15; 17; 19; 21; 23; 25**.
Dans toute la suite, dès que l'on parlera d'une fonction affine de codage il sera sous-entendu que son coefficient a est un de ces 12 nombres.
Quelle condition vérifient ces nombres ? ……..
……
d. Combien de fonctions affines de codage différentes peut –on faire ? ……

3°) Quelle fonction affine permet de crypter le mot « CODE » par le mot « LHCT » ?

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

Exercice 3

But : utiliser le tableur pour effectuer le codage plus rapidement

1°) Réfléchir comment construire un tableau similaire à celui de l'exercice 2. Choisir une clé et un message à coder.

2°) A l'aide du 1°) et du TP sur le code de César (cf. fichier *code de César* sous serveur commun/travail/maths/3ème + *Nom.prénom crypto1*), créer votre propre outil de cryptage dans une nouvelle feuille de travail.
Quelle est la formule pour obtenir les 26 lettres de l'alphabet ? .....
Quelle est la formule pour obtenir la valeur numérique correspondante ? .....
Comment réduire les lignes 3 et 4 à une seule ligne ? ……

3°) Enregistrer votre travail sous *MES DOCUMENTS* .

COMPTE-RENDU DE L'ACTIVITÉ « CRYPTOGRAPHIE »

En sixième

Code de César : une séance + discussion autour du texte

Les élèves ont travaillé seul en début de séance afin de s'approprier au mieux la situation proposée. Le principe de la méthode a été globalement compris par l'ensemble de la classe.
Pour commencer le codage, les élèves ont tous pris la première lettre à laquelle ils ont appliqué la méthode de cryptage puis ils ont réitéré l'expérience pour chaque lettre du mot, et ceci pour tous les mots de la première phrase.
A ce stade de l'activité, j'ai senti la nécessité de faire un retour oral pour toute la classe : exposé de la situation par les élèves et exposé des méthodes appliquées. C'est à ce moment là que l'organisation même de leur travail est apparue. Les élèves ont été conscients que coder en comptant 3 lettres de plus pour chaque lettre de chaque mot de chaque phrase du texte clair allait prendre du temps pour ce poème. Le choix d'un texte assez long aux yeux des élèves est donc important pour cette activité. L'intérêt ne réside pas dans le fait de coder l'intégralité du texte mais la longueur de ce dernier oblige les élèves à se poser la question de la méthode de travail, de la démarche à appliquer. Quel serait l'avantage de trouver une méthode pour un texte de deux lignes et comment alors convaincre les élèves de la lourdeur de leur procédé ? Cette activité, dans sa nature de tâches réitératives, est intéressante dans le fait même qu'elle oblige à automatiser le processus (à ce propos, même si cela n'a pas été fait, on peut tout à fait envisager une présentation à la classe d'une possible résolution de l'activité avec le tableur, outil pertinent dans cette fonction d'automatisation).
Ce moment a donc été l'occasion d'une discussion autour de la question : « Comment procéder pour coder efficacement ? »
Les élèves ont rapidement remarqué qu'une fois la lettre claire codée, la substitution pour cette lettre reste la même tout au long du texte ; cette remarque étant vraie pour toutes les lettres de l'alphabet. A partir de cette réflexion, certains élèves ont eu l'idée de construire un tableau avec deux lignes : une pour les lettres du texte clair, l'autre pour ce que deviennent les lettres dans le texte codé.
Les élèves ont alors été invités à retravailler de façon individuelle pour réaliser le tableau et tester la rapidité de ce nouvel outil mis à leur disposition. La construction du tableau a été riche d'enseignements sur l'organisation même du travail.
En effet, un nombre important d'entre eux n'a pas inscrit dans la première ligne les lettres dans l'ordre alphabétique, mais a commencé à remplir le tableau avec les lettres dans l'ordre d'apparition du poème. Cette méthode est bien évidemment correcte pour coder le texte « un peu plus rapidement » que leur méthode initiale (pour les lettres n'apparaissant pas dans le texte clair, il est vrai qu'il n'est pas nécessaire de connaître leur substitution) mais n'est pas très pratique dès que l'on cherche une lettre. Cette remarque montre à quel point la notion d'ordre pour beaucoup d'élèves n'est pas acquise (difficultés pour comparer des nombres entiers, des fractions, des décimaux mais aussi en français pour chercher dans un dictionnaire).

Pour les élèves ayant rempli la première ligne avec apparition des lettres dans l'ordre alphabétique, beaucoup d'entre eux ont compté le décalage de 3 pour toutes les lettres. L'idée d'un décalage immédiat de l'alphabet après avoir effectué le décalage d'une lettre n'a été mis en œuvre par aucun élève de la classe.
Une fois le tableau réalisé par tous les élèves, ils n'ont décodé que deux phrases.
Comme expliqué précédemment, l'intérêt n'était pas dans le codage même du texte, mais dans la prise de conscience par les élèves d'une organisation automatisée du travail.
Les élèves sont ensuite passés à la suite de l'activité, qui leur demandait de décoder un texte. Cette partie a été faite en fin de séance. Même si pour la majorité d'entre eux, la mise au travail dans le décodage a été rapide, comprise et utilisant le tableau précédent, certains élèves n'ont pas su utiliser le tableau correctement. Ils ont recommencé comme dans la première partie de l'activité : lire les lettres du texte chiffré dans la première ligne pour trouver la lettre correspondante dans la deuxième ligne. Et naturellement les mots codés devenaient des mots qui n'avaient toujours aucun sens dans la langue française, d'où leur interrogation et leur prise de conscience d'une erreur de méthode. Une aide a alors été donnée, soit par moi, soit par les autres élèves qui avaient trouvé la solution.
La fin du décodage a été donnée en travail à la maison. La correction (texte obtenu compréhensible) a eu lieu en cours de français. La collègue a utilisé ce prétexte pour leur faire jouer la scène avec les textes qu'ils venaient de découvrir.
En cours de mathématiques, je suis revenu sur le texte en leur montrant deux adaptations : version théâtre et version opéra. Nous avons alors discuté sur le fond de ce texte faisant référence à la notion de fractions : polysémie des mots, différence entre l'usage du contexte mathématique et celui du quotidien.

Prolongement possible : on peut demander aux élèves le nombre de clés de déchiffrement que l'on peut trouver avec cette méthode du code de César.

Variante du code de César : 2 séances

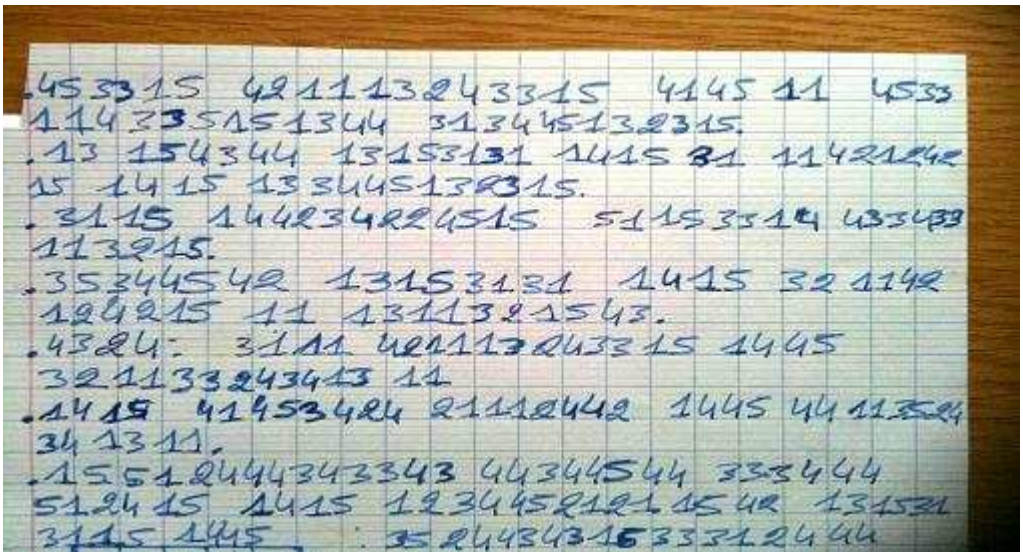
Au début de la séance, chaque élève reçoit les documents et en prend connaissance de façon individuelle. Puis, pour la suite de la séance, les élèves travaillent par groupe de 4. Je pense que ce mode de fonctionnement convient pour cette activité. Il permet la discussion autour des méthodes de chacun. Je choisis de faire moi-même les groupes, de façon à mettre ensemble filles et garçons (les élèves, d'eux-mêmes, font très rarement des groupes mixtes !) et de niveaux hétérogènes (pour essayer d'obtenir le plus d'autonomie !).
Les élèves rentrent très rapidement dans l'activité, curieux de découvrir ce qui se cache derrière ce poème codé.
Dans les groupes, l'idée de compter la lettre E dans le texte chiffré apparaît. Mais après cette première idée, une première discussion surgit. Certains ne comprennent pas pourquoi le nombre trouvé ne correspond pas à l'effectif de la lettre E donné par le graphique. Même si l'élève n'a pas lu correctement le titre du graphique ou même s'il n'a pas compris l'enjeu de l'activité, sa remarque nous indique que, non seulement il est capable de « lire » un diagramme en bâtons, mais qu'il est aussi capable de remettre en question son début de démarche, d'avoir un sens critique sur son résultat. Dans tous les groupes, un ou plusieurs élèves sont capables de comprendre l'information donnée par le diagramme en bâtons et d'expliquer la différence entre le nombre trouvé et la barre du E dans le diagramme.
Après un certain temps, tous les groupes se lancent dans le décompte des différentes lettres présentes dans le texte. A ma grande surprise, ce moment de l'activité est très long. Tous les élèves font leur propre compte, de façon plus ou moins rigoureuse et souvent retranscrit de façon très désordonnée sur la copie. Le résultat est que, à l'intérieur du groupe, les données différent ! Chaque élève est donc obligé de recompter ! C'est à ce moment là que

j'interviens auprès des groupes pour une aide à la démarche de résolution, pour faire naître un questionnement sur l'organisation des données : comment s'organiser pour dénombrer les lettres, comment s'y prendre de façon efficace au sein d'un groupe, comment résumer ce que l'on obtient.
A la fin de la séance, presque tous les groupes sont enfin d'accord sur le nombre d'apparition de chaque lettre.
Ils trouvent donc quelle lettre code le E. Et si le principe avait été compris, ils auraient eu le temps de terminer l'activité. Mais aucun groupe n'a pensé à chercher la clé ni à décaler l'alphabet. Ils ont pour la plupart cherché les lettres qui revenaient le plus après le E (pour le I pas de problème, mais souci ensuite : R et N apparaissent le même nombre de fois). Cette démarche, même si elle n'est pas la plus rapide, fonctionne très bien. A condition d'être un minimum organisé et rigoureux, ce qui est loin d'être acquis pour cette classe de sixième !
Je décide donc de reprendre l'activité lors d'une prochaine séance.
Au début de la deuxième séance, les élèves expliquent à l'oral ce qu'ils ont fait dans la première séance. Et à ce moment là encore, ils sont tous convaincus qu'il faut s'occuper de chaque lettre. Je leur laisse une demi-heure pour essayer de décoder le texte.
Dans les groupes, c'est un peu la panique : l'idée d'un tableau est rarement reprise, le blocage est important quand au fait qu'une lettre pourrait en coder deux autres, et l'idée de remplacer les lettres dans le texte codé au fur et à mesure se fait rarement. Au final, personne n'a de réponse satisfaisante à proposer.
Pour terminer la séance, on reprend ensemble les étapes de la recherche, on réalise un tableau, et on souligne les mots importants (Code de César, décalage, clé) pour qu'un élève trouve enfin la méthode rapide.
Les élèves doivent donc décoder le texte à la maison et apprendre la poésie par cœur. Le travail sera alors vérifié lors d'une récitation orale pendant le cours de français.

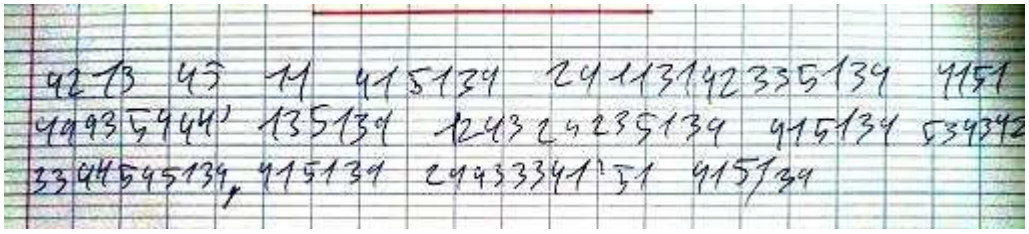
Carré de Polybe : devoir à la maison

Cette activité a été donnée en travail à la maison.

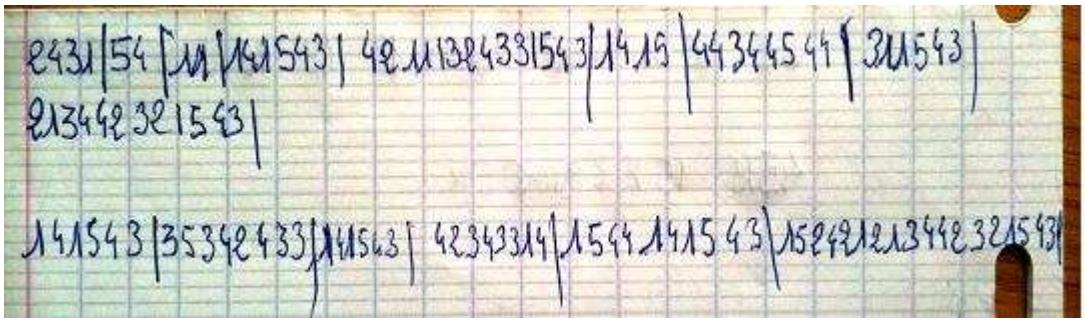
Il y a des élèves qui donnent une suite de chiffres sans que l'on comprenne la logique de leur résultat et qui ne sont pas capables, à l'oral, de donner une explication claire.



Certains élèves confondent le sens de lecture du tableau : ils ne respectent pas la consigne et commencent par donner la colonne.



Enfin certains élèves savent correctement lire le tableau donné.



Le retour en classe avec la correction a permis de travailler autour de la notion de cordonnées avec l'exemple particulier d'un tableau à double entrée (définition des lignes, des colonnes, des cases).

Prolongement possible : on peut travailler en lien avec le professeur de musique.
Pour faire référence au morse, on peut coder musicalement la chanson de Vian : chaque ligne correspond à une hauteur de note, et chaque colonne correspond à une durée de la note. Ainsi, après leur avoir fait écouter la version originale de la chanson, ils découvriront la version codée.

Substitution mono-alphabétique : 3 séances + séance d'écriture expliquant leur recherche

La recherche commence par une prise de connaissance individuelle des documents. Puis les élèves travaillent par groupe de quatre (pour la constitution, même remarque que l'activité sur la variante du code de César) sur une seule séance. La recherche est individuelle sur les 2 autres séances (beaucoup de passivité et de bavardages lors de la première séance, et au final peu de travail intéressant).
Cette activité étant assez difficile pour les élèves, je dois faire de nombreux moments de synthèse-bilan (en début et en fin de séance), mes interventions sont assez nombreuses (avec des aides à la démarche de résolution) et au final, très peu d'autonomie.

Pour le compte-rendu de cette activité, je propose de retranscrire des extraits des textes d'élèves (qui ont raconté leur recherche lors d'une séance d'écriture), auxquels j'ajouterai quelques commentaires.
Présentation des documents et compréhension de la consigne

- Il y a ceux qui analysent correctement les documents :

  « *Sur le document, il y avait un texte codé et en dessous, il y avait un graphique à barre où il y avait combien chaque lettre était dans le texte clair »*

- Il y a encore des élèves qui, après trois séances de travail sur cette recherche, n'ont pas acquis une bonne compréhension de la situation :

  « *Sur la feuille, il y a avait un graphique où il y avait des barres grandes, petites et moyennes et en dessous de ces barres, il y avait des lettres par ordre alphabétique, et il y a avait un texte qui correspondait à ce graphique »*
  « Nous avions un graphique à barres pour savoir combien de fois il y avait les lettres dans le texte clair »

Démarche de résolution

1. **Extraire d'un document papier les informations utiles : entreprendre le comptage des lettres.**

   « *On a eu du mal à commencer mais après les idées sont venues »*
   « Ma camarade m'a donné une idée, mais cela n'allait pas »
   « *On a essayé de trouver les méthodes plus rapides pour ne pas compter. Mais on avait rien trouvé. Alors on a essayé de comprendre le graphique et le texte codé. Et après on a compris. Il fallait compter les lettres qui apparaissent le plus dans le texte codé.»*
   « *Chaque groupe eu ses idées et compta les lettres du texte codé pour voir grâce au graphique quelle lettre est remplacée par quelle lettre. »*

2. **Suivre un protocole : compter le nombre d'apparition de toutes les lettres sans oubli**

   - Non Acquis

« Pour compter les lettres, il y avait des pairs (ex N-Y et T-Y) : cela voulait dire que le N est crypté par le T »

- Acquis

« *On était quatre à compter les lettres dans le texte codé. Mais, il y avait un problème, on oubliait des lettres. Alors, on a eu une idée : partager le texte codé en quatre paragraphes. Pour compter les lettres, notre organisation était de barrer les lettres quand on les avait comptées »*
« On a compté une par une les lettres, mais c'est trop long, alors on a pris chacun un paragraphe »
« Toutes les lettres qui ont été comptées, on les a coloriées. Chaque lettre avait sa couleur, donc normalement toutes les lettres doivent être coloriées »
« Nous étions quatre pour compter les lettres. Chaque élève prend une lettre à compter. Et quand on termine, il faut faire un tableau pour décompter les lettres avec leurs nombres. »
« Nous avons fini et alors nous avons rassemblé nos lettres, nous avons fait les comptes, nous avons fait un tableau pour chaque lettre »
« Nous avions bien avancé mais nous n'avions pas réussi à finir »

Cette dernière remarque d'élève montre à quel point le comptage des lettres a été long et mal organisé. C'est la raison pour laquelle, pour avancer dans la recherche, j'ai donné un tableau bilan pour toute la classe.

« Quelques jours plus tard, M.Mayenson nous redonna une feuille avec le même texte, le même graphique mais en plus il y avait un tableau avec le nombre de lettres qui apparaît dans le texte codé. Il nous a mis un par un pour décoder le texte ».

3. **Proposer une procédure : mettre en œuvre une stratégie pour associer les lettres du texte codé à celles du texte clair.**

- Non acquis

« Le lien avec le graphique : les lettres qui apparaissent sont le double des autres »

Même si les élèves n'en parlent pas dans leur récit, certains ont eu un problème avec la lecture de consigne : confusion avec l'activité 1 et le Code de César. Les élèves ont alors appliqué la méthode du décalage, mais après un essai (texte codé toujours incompréhensible), ils ont vu leur erreur.

- Acquis

« Nous avons fait un tableau avec les lettres rangées dans l'ordre décroissant du nombre de fois où elles apparaissent dans le texte codé. »
« Il fallait décoder le texte en commençant par faire un tableau qui se compose de trois lignes. Dans la première, il fallait mettre le nombre de lettres qui apparaît le plus de fois. Dans la deuxième ligne, il fallait mettre la lettre correspondante au nombre. Ensuite, on s'occupe de la dernière ligne qui a un rapport avec le graphique : on regarde la graduation la plus grande jusqu'à la plus petite, on regarde les lettres qui correspondent et on classe. »
« On a fait un tableau où on a comparé les nombres des lettres du texte codé et les nombres des barres »

En circulant dans les rangs, j'ai rencontré différents procédés concernant la lecture du graphique :

- les élèves classent du plus grand au plus petit avec l'utilisation de l'équerre :

« On fait la correspondance grâce au graphique : les barres des plus grandes au plus petites correspondent à l'ordre décroissant des lettres du texte codé : la lettre qui apparaît le plus est remplacée par la lettre de la barre la plus grande, … »

- certains, du fait des ordonnées de 20 en 20, veulent connaître le nombre exact donné par les barres du graphique : soit par une approximation du nombre de chaque lettre, soit par proportionnalité (nombre de cm pour 20 ramené à l'unité)…mais tout cela est incohérent avec le tableau des lettres du texte codé

« *Grâce au graphique et au tableau nous regardions quel nombre était pareil qu'un autre, mais plein de nombre ne correspondait avec aucun autre »*

4. Rendre compte de la démarche : expliquer les choix pour remplacer les lettres.

« Quand on voulait décoder, on a eu un problème, il y avait des lettres qui avaient le même nombre. »
« Avec le tableau enfin rempli, nous avons commencé à décoder le texte, mais il y avait des lettres qui avaient le même nombre. Alors, on les a mis dans les mots pour voir si cela correspondait à un mot français. »

Pour conclure, je pense que l'activité a été un peu longue et donc décourageante alors qu'elle suscitait curiosité et intérêt lors de la première séance.

« *J'ai bien aimé mas c'était trop long et énervant à force » ;*
« *C'était dur mais assez rigolo à faire » ;*
« J'ai trouvé cela dur et compliqué » ;
« C'était assez bien car il y a avait un peu de français avec le texte et un peu de maths avec le graphique ».

En quatrième

LES FINS DE SEANCES

Ce travail aurait pu être fait sur une seule séance, mais il m'a semblé plus intéressant de l'exploiter ainsi, sans transformer ma progression, et créant une certaine attente chez les élèves. Et surtout cela a généré un moment récréatif de fin de séance, apprécié des élèves qui en sont devenus demandeurs !

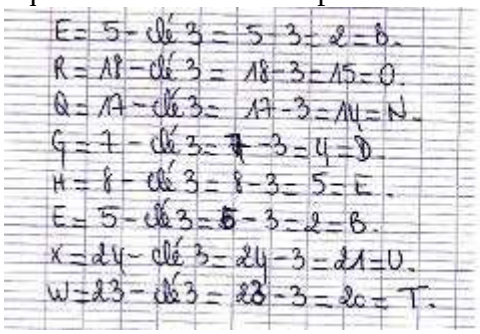
Présentation du travail qui va être effectué sur la cryptographie et de l'objectif en cours de français.

Petite histoire du codage.

Présentation des trois types de codages : les élèves prennent connaissance individuellement de chaque document et cherchent à répondre aux premières questions. Mise en commun des questions/ réponses sur chaque méthode. Correction des premiers exercices. Codages et/ou décodages à faire pour la séance suivante. Seuls les textes codés pour d'autres sont à faire pour la séance des deux heures consécutives (la semaine suivante).

Document 1 : Code de César

Pas de problème pour le codage, le décodage a pris un peu plus de temps (le reflexe de soustraire au lieu d'ajouter n'est pas systématique même en quatrième). Rapidement est apparu la nécessité de l'utilisation d'un tableau pour les textes plus longs, même si ce recours ne s'est pas fait naturellement. Pour remplir le tableau, de même qu'en sixième, le décalage n'est pas fait automatiquement. Même si l'algorithme est compris, les élèves refont les calculs pour chaque lettre et n'utilisent pas le tableau.



Cependant, d'emblée, les élèves des deux classes de quatrième ont été réceptifs et le lendemain, tous avaient fait les exercices et étaient demandeurs d'autres codages : d'où l'exercice facultatif des textes donnés à coder.

Document 2 : Variante

Les élèves se sont immédiatement mis dans l'activité. Beaucoup ont compté le nombre total de lettres (inutile ici mais je leur ai demandé de le noter car ce résultat sera utilisé par la suite pour le calcul de fréquence d'apparition de lettre dans un texte)…Malgré la donnée du tableau, certains élèves ont calculé la fréquence de plusieurs lettres avant de penser à avoir recours au décalage à partir de la première lettre trouvée. Décodage fait à la maison.

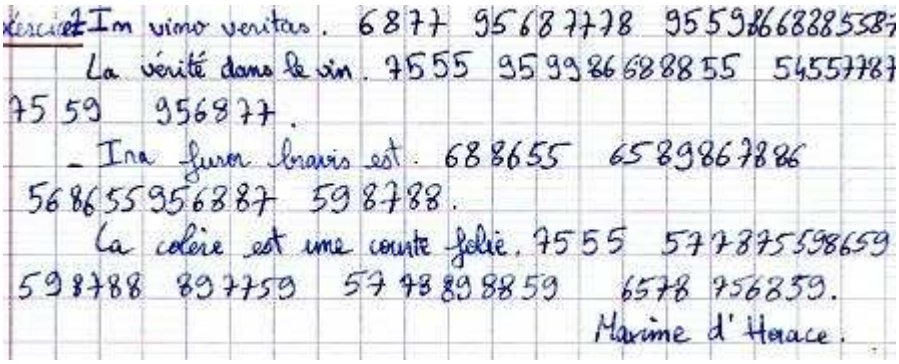
Rappel : fréquence et calcul d'une fréquence en pourcentage.

Document 3 : Carré de Polybe

Les élèves sont maintenant « rodés », le décodage de la première citation a été faite par tous lors de cette séance. Certains ont transformé le carré de Polybe en tableau à deux lignes et 25 colonnes (plus facile ?...).

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
11	12	13	14	15	21	22	23	24	25	31	32	33	34	35	41	42	43	44	45	51	52	53	54	55

Pour le plaisir …

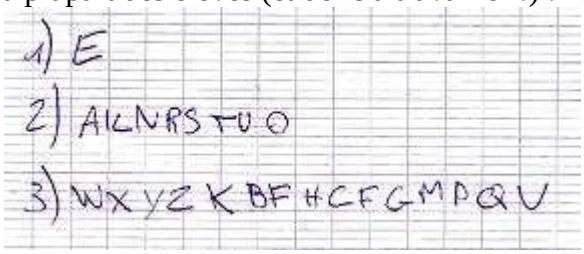


SEANCE EN SALLE INFORMATIQUE : 2 heures consécutives

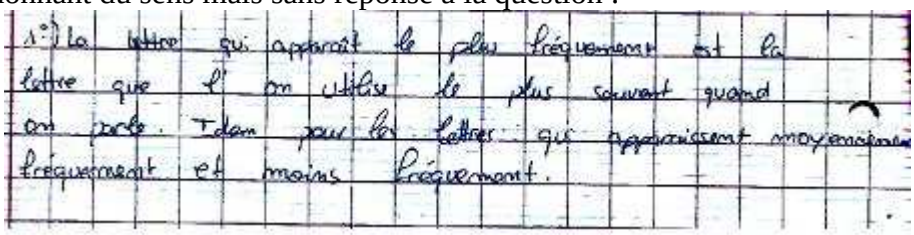
Document 4 : Substitution mono-alphabétique

Au groupe classe : présentation de la méthode. Même 'rituel' que pour les autres méthodes.

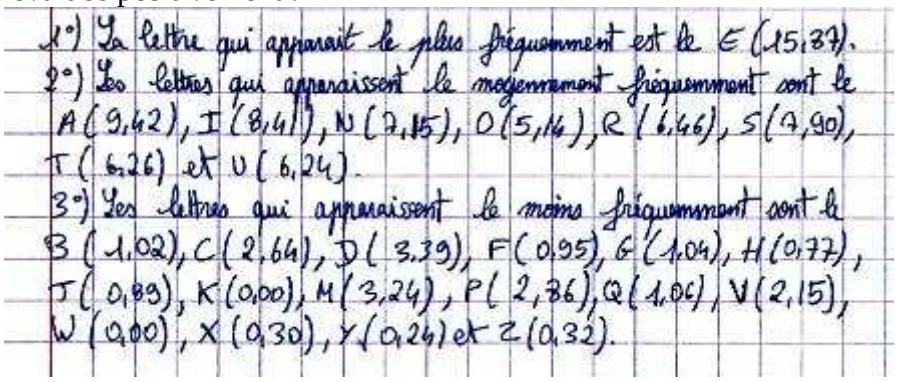
Exercice 1.
Réponse non rédigée par la plupart des élèves (et donc à travailler !) :



Ou réponse donnant du sens mais sans réponse à la question :



Compétence évaluée positivement :


1°) La lettre qui apparait le plus fréquemment est le E (15,37).
2°) Les lettres qui apparaissent le moyennement fréquemment sont le A (9,42), I (8,41), N (7,15), O (5,14), R (6,46), S (7,90), T (6,26) et U (6,24).
3°) Les lettres qui apparaissent le moins fréquemment sont le B (1,02), C (2,64), D (3,39), F (0,95), G (1,04), H (0,77), J (0,89), K (0,00), M (3,24), P (2,36), Q (1,06), V (2,15), W (0,00), X (0,30), Y (0,24) et Z (0,32).

La classe est alors « séparée » en deux : les élèves travaillent en alternance :
– soit par petits groupes pour échanger et corriger les codages et décodages ;
– soit individuellement sur le tableur (Document 5).

Document 5 : Fréquence d'apparition des voyelles

Activités extraites du document « SCÉRÉN/CRDP Nord – Pas de Calais – *Mathématiques et Socle commun au collège* - Juin 2010. »
Un texte de référence est donné à chacun ainsi qu'une recherche à faire (ou finir) à la maison. Les trois premiers poèmes ont été étudiés en français.
Groupe 1 : Dans l'onglet « Exercice 1 », relire le poème *Après trois ans* - Comparaison avec « *Booz assoupi* »
Groupe 2 : Dans l'onglet « Exercice 2 », relire le poème *L'Ennemi* de Charles Baudelaire - Comparaison avec « *La disparition* » avec *L'ennemi*
Groupe 3 : Dans l'onglet « Exercice 3 », relire le poème *Le ciel est, par-dessus les toits* de Paul Verlaine - Comparaison avec « *les Revenentes* »
Groupe 4 : Dans l'onglet « Exercice 4 », lire le poème *Booz endormi* - Comparaison avec « *Booz assoupi* ».

Le but de cette activité est d'avoir le plus grand nombre de données à comparer sans avoir trop de calculs à effectuer. Expliquer les différences observées par rapport à la norme. Les résultats de ces observations sur les voyelles doivent servir de lien, de support à l'introduction du travail sur les contraintes d'écritures en français.

Dans les petits groupes, les échanges ont été fructueux, les exercices tous corrigés, et les textes décodés. Les élèves ont réussi à se gérer avec beaucoup d'autonomie. Très peu m'ont sollicité.

En revanche, la partie « travail à l'aide du tableur » m'a demandé beaucoup plus de présence et d'interventions. Les automatismes du tableur ne sont pas acquis et l'entrée de formule devient parfois un travail fastidieux... Quant à la lecture, compréhension et application de consignes, ces compétences s'avèrent moins mobilisées et maîtrisées que lors du travail sur la cryptographie sur papier ou à l'oral !
Cependant, le travail a été mené à bien dans les deux classes.
Les élèves ont accès à tous les textes et peuvent calculer les fréquences d'apparition des voyelles dans tous les textes s'ils le souhaitent (à la maison ou au CDI, à l'aide du tableur ou manuellement). La plupart ont eu le temps de faire le calcul sur les deux textes qui leur étaient attribués. Le copier/coller a été vite maîtrisé !

Mais pour l'insertion du graphique j'ai dû leur rappeler la démarche. Très peu d'élèves ont utilisé la formule SOMME.
Pour les élèves qui le souhaitaient, une version papier de chaque texte est mise à disposition (ces versions étaient prévues au départ pour les élèves ne respectant pas les règles d'utilisation de l'ordinateur !).

SYNTHESE (deux semaines plus tard)

Recueil et comparaison des résultats

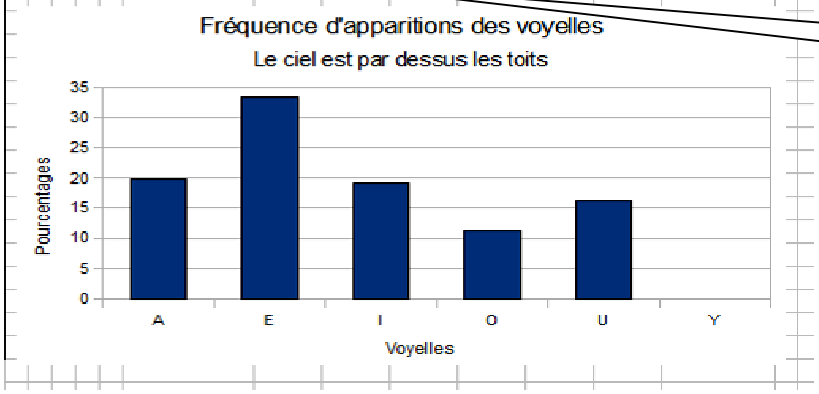
Document 6 : L'objectif de cette activité est d'élargir le calcul des fréquences au nombre total de lettres du texte pour comparer les résultats lors de la synthèse au tableau du document 4. L'objectif mathématique est d'établir les limites de la méthode de l'analyse de fréquence en tant que méthode de cryptage et de servir de support au calcul de pourcentages relatifs à la réunion de deux groupes.

La plupart des élèves ont effectué le travail demandé sur papier, mais un tiers a réutilisé le tableur en précisant qu'ils l'avaient fait parce que « c'était plus rapide pour le calcul ! »

Dans la classe qui a travaillé sur les contraintes d'écriture en français, certains élèves ont calculé les fréquences d'apparitions des lettres dans les textes en prose étudiés en français : des extraits de *Lettre à Acilius* de Pline le Jeune, et d'*Oscar et la dame rose* d'Eric-Emmanuel Schmitt. Dans l'autre classe de 4ème, deux élèves se sont proposés pour présenter une démarche similaire avec des textes d'anglais (l'exposé est prévu pour la dernière semaine de cours).

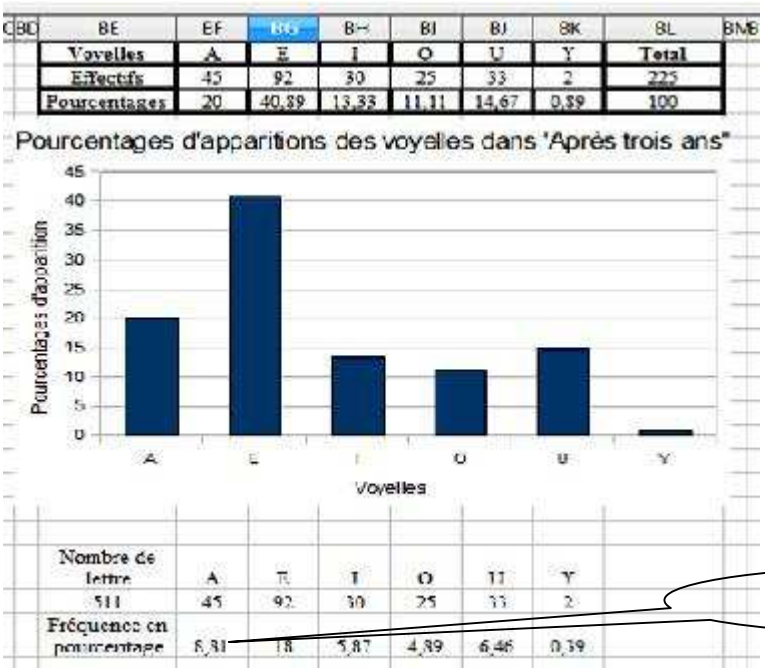
Le ciel est, par-dessus les toits : Colline

	Voyelles	A	E	I	O	U	Y	Total
	Effectifs	28	47	27	16	23	0	141
	Pourcentages	19,86	33,33	19,15	11,35	16,31	0	100
	Total Lettres							328
	Pourcentages	8,54	14,33	8,23	4,88	7,01	0	



=BF2/BL4*100

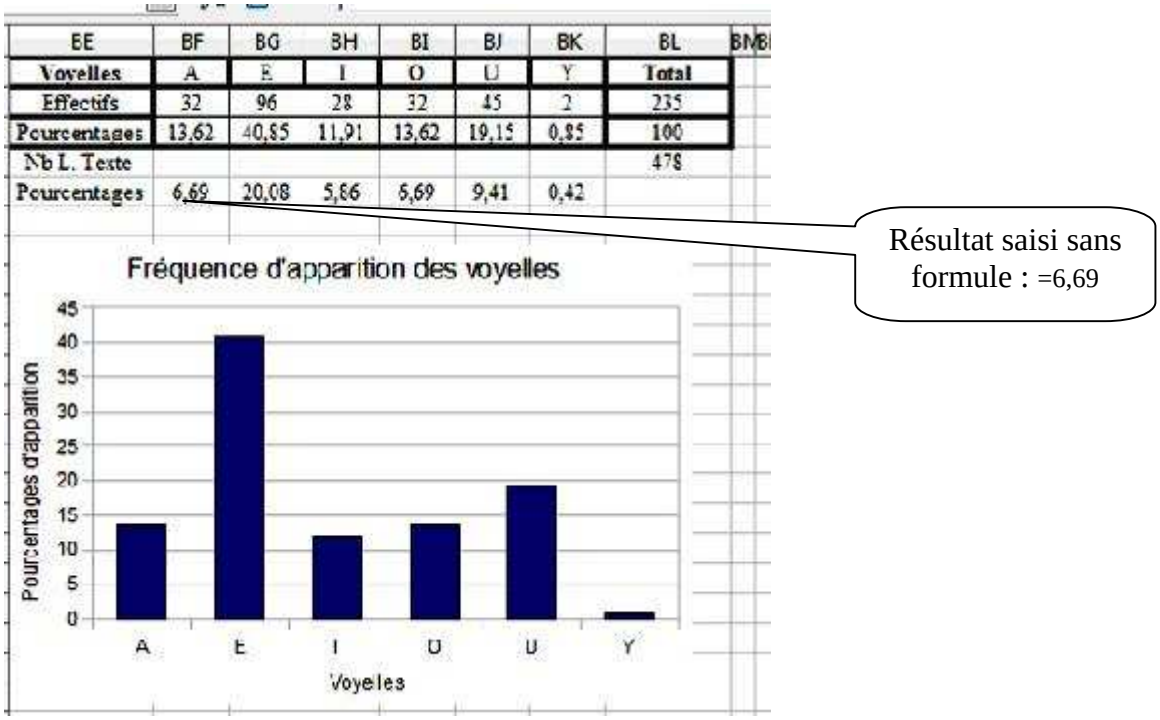
Après trois ans : Adèle « si on met des $ on peut recopier la formule sans que ça change le numéro de la cellule »



Voyelles	A	E	I	O	U	Y	Total
Effectifs	45	92	30	25	33	2	225
Pourcentages	20	40,89	13,33	11,11	14,67	0,89	100

Nombre de lettre	A	E	I	O	U	Y
511	45	92	30	25	33	2
Fréquence en pourcentage	8,81	18	5,87	4,89	6,46	0,39

Ennemi : Alexandre, plus rapide avec le tableur ?



Voyelles	A	E	I	O	U	Y	Total
Effectifs	32	96	28	32	45	2	235
Pourcentages	13,62	40,85	11,91	13,62	19,15	0,85	100
Nb L. Texte							478
Pourcentages	6,69	20,08	5,86	6,69	9,41	0,42	

Les compétences qui restent en cours d'acquisition concernent l'utilisation du tableur et la communication des résultats à l'écrit.

En troisième

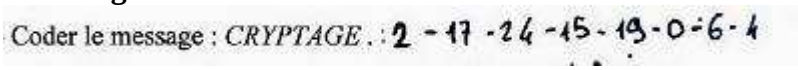
Code de César : **séance de deux heures consécutives (testée avec deux classes de 3ème)**

Consignes orales sur l'objectif et le déroulé de la séance ; Document à rendre ou à sauvegarder. Lecture individuelle des documents, échange collectif sur la méthode. Après la réussite des exercices 1 et 2, travail individuel (exercice 5) sur l'ordinateur (15 postes) en alternance, pendant que les autres poursuivent en groupe ou individuellement les exercices 3 et 4. Les plus intéressés ont eu le temps de travailler sur la variante du Code de César et le Carré de Polybe (documents de 4ème).

Comme en quatrième, le travail sur tableur a été moins autonome que celui sur papier : les élèves ne lisent pas attentivement les consignes écrites. Cependant, le travail a été fait sérieusement pour la première partie (étude des fonctions CAR, MOD et RECHERCHE) mais un quart seulement des élèves a créé son propre outil de codage. La moitié a créé une feuille de calcul en entrant les données manuellement, certains n'utilisant que la fonction RECHERCHE pour le codage ; Les autres ont surtout utilisé le fichier *code de César* pour créer leur tableau de codage en changeant la clé et pour vérifier les textes chiffrés. (« Ah oui, ça marche !!! ») .

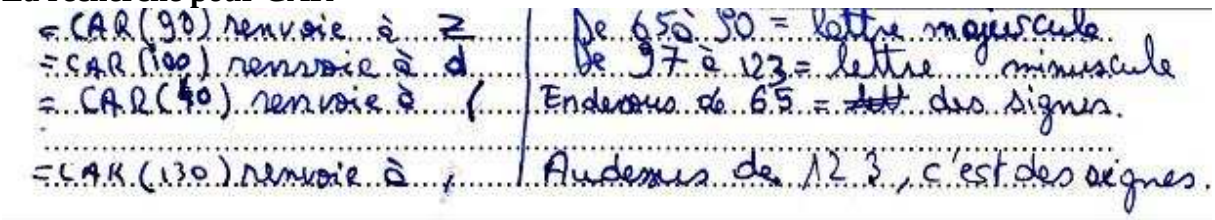
NB : Les fonctions affines et linéaires n'avaient pas encore été étudiées à cette période de l'année.

Le codage de César

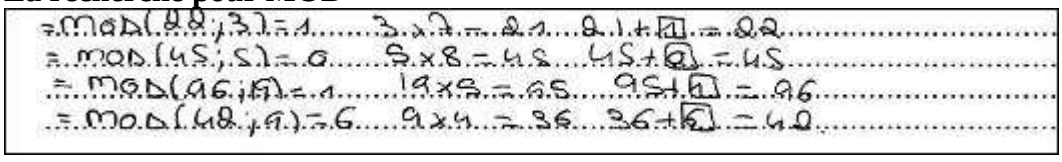


Erreur non rencontrée en quatrième ! Par la suite, les messages seront bien décodés.

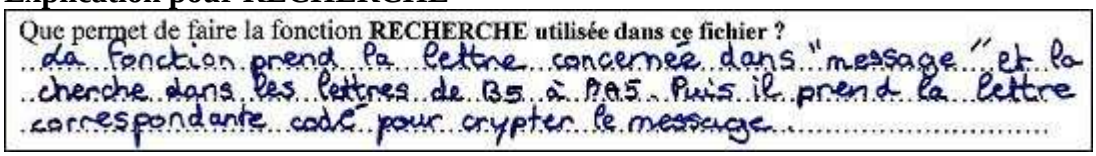
La recherche pour CAR



La recherche pour MOD



Explication pour RECHERCHE



La plupart des élèves ont compris le rôle des fonctions en les appliquant, en les testant sur différentes valeurs. Ils ont passé plus de temps à vérifier les valeurs données par les fonctions du tableur qu'à essayer de programmer un outil d'aide au cryptage.

Les outils de cryptage :

Bastien et le copier/coller qui n'est pas drôle !

	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
1	BASTIEN																										
2																											
3	Clé	3																									
4																											
5	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
6		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
7		3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
8		3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	0	1	2
9	Code	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
10																											
11	Message	C	E		N	'	E	S	T		P	A	S		D	R	Ô	L	E								
12	cryptage	F	H	###	Q	###	H	V	W	###	S	D	V		G	U	R	O	H								
13																											

Le décodage de Médéric : utilisation de la fonction RECHERCHE

B13 : =RECHERCHE(B12;B8:AA8;B5:AA5)

	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
1	Médéric 3ème 4																											
2																												
3	Clé	3																										
4																												
5	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	
6		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	
7		3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	
8		3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	0	1	2	
9	Code	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	
10																												
11	Message	J	U	L	E	S		C	E	S	A	R		E	T		S	O	N		F	I	L	S				
12	cryptage	M	X	O	H	V		F	H	V	D	U		H	W		V	R	Q		I	L	O	V				
13	décodage	J	U	L	E	S		C	E	S	A	R		E	T		S	O	N		F	I	L	S				
14																												

La méthode d'Anthony

C6 : =R6+1

	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
1	Méthode d'Anthony																												
2																													
3	Clé:	19																											
4																													
5	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			
6		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			
7		19	20	21	22	23	24	25	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18			
8	Code	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			
9																														
10	Message:	J	E	***	R	A	S	E	***	L	A	***	T	E	T	E	***	D	E	***	L	'	E	S	C	L	A	V	E
11	Cryptage	C	X	***	K	T	L	X	***	E	T	***	V	X	M	X	***	W	X	***	E	###	X	L	V	E	T	N	X	
12																														

B7 : =B6+19

J7 : =I6+19-26

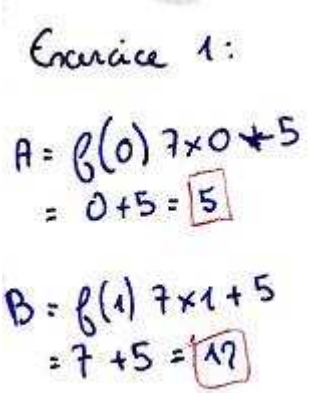
B8 : =CAR(65+B7)

B11 : =RECHERCHE(B10;B5:AA5;B8:AA8)

Code affine : séance de deux heures consécutives (avec une seule classe de 3e)

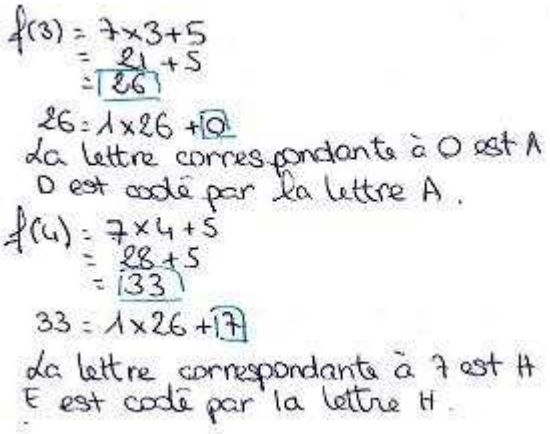
Rappels : synthèse du TP « Code de César », fonction affine et arithmétique (division euclidienne, nombres premiers entre eux).
Consignes orales sur l'objectif de la séance et son déroulé. Distribution des documents. Les élèves ont travaillé en groupe pour les exercices de compréhension de la méthode et se sont répartis plus rapidement sur les ordinateurs que lors du premier TP de cryptographie.

Le va et vient entre le tableur et la table de travail a été plus fréquent et plus efficace que lors du premier TP. J'ai donc donné, au cours de la deuxième heure, l'accès au fichier tableur *Code affine* pour permettre aux élèves de vérifier leurs cryptages. Les élèves n'ayant pas créé leur outil de codage pour le code de César lors de la première séance ont souhaité le faire, ce dernier leur semblant plus facile que pour le code affine généralisé.
Exercice 1 : calculer la valeur d'une expression, acquis par tous malgré des présentations manquant de rigueur.


Exercice 1 :

A = f(0) 7×0+5
= 0+5 = 5

B = f(1) 7×1+5
= 7+5 = 12


f(3) = 7×3+5
= 21+5
= 26

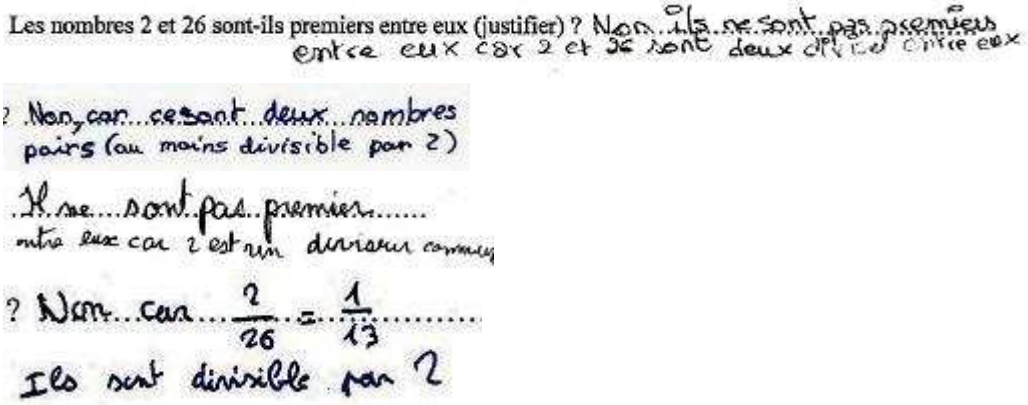
26 = 1×26 +0
La lettre correspondante à 0 est A
D est codé par la lettre A.

f(4) = 7×4+5
= 28+5
= 33

33 = 1×26 +7
La lettre correspondante à 7 est H
E est codé par la lettre H.

Exercice 2
Tous les élèves ont trouvé la fonction correspondant au code de César, et déduit que la fonction affine $2x + 3$ ne permettait pas de définir une fonction de codage.

Plusieurs réponses pour montrer que 2 et 26 ne sont pas premiers entre eux :


Les nombres 2 et 26 sont-ils premiers entre eux (justifier) ? Non ils ne sont pas premiers entre eux car 2 et 26 sont deux diviseurs entre eux

? Non, car ce sont deux nombres pairs (au moins divisible par 2)

Il ne sont pas premier
entre eux car 2 est un diviseur commun

? Non car $\frac{2}{26} = \frac{1}{13}$

Ils sont divisible par 2

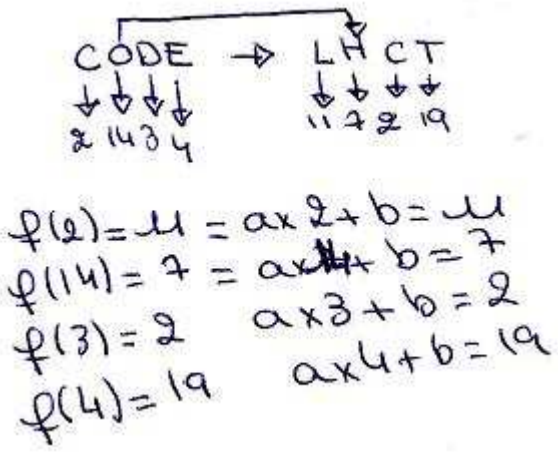
Trois quart des élèves ont trouvé le nombre de fonctions affines possibles.

12×26 = 312

Pour la recherche d'une fonction affine (3°) de l'exercice 2) : 6 élèves sur 28 ont élaboré un raisonnement basé sur la résolution de systèmes d'équations avec utilisation des contraintes et des multiples de 26 pour obtenir une valeur positive pour a et b. 10 élèves ont trouvé par

essai erreur à partir des 12 valeurs possibles de *a* dont 6 à l'aide du fichier *Code affine.* Quatre élèves ont trouvés des valeurs négatives pour *a* et *b* et n'ont pas traité la question (« Trop compliqué ! »).

Une recherche non aboutie, mais un bon départ ….des compétences même hors socle peuvent être évaluées positivement.



Une égalité qui apparaît …fruit d'un travail colaboratif ?

Aucun élève n'a eu le temps de programmer son propre outil de codage mais ils ont tous sauvegardé leur travail de test et de recherches effectuées à partir de la donnée du fichier *Code affine.* Cette donnée a bien sûr réduit l'intérêt de fabriquer son propre outil, mais ce n'était pas l'objectif principal de cette séance…. Il aurait fallu pour cela disposer de plus de temps. De plus, je n'ai pas souhaité freiner l'enthousiasme des élèves qui préféraient inventer des fonctions affines et calculer manuellement!

Lors de cette séance les échanges ont été très riches entre les élèves et je n'ai eu à gérer aucun conflit ni manque d'implication ! Une élève a même prétendu avoir enfin compris les fonctions affines grâce à ce travail… peut-être parce qu'elle s'est un peu plus impliquée.

Conclusion : La cryptographie est un thème riche en source d'activités adaptables à tous les niveaux de classes, et motivant pour les élèves. Elle permet de travailler le raisonnement et la démarche de résolution de problème ainsi qu'un certain nombre de connaissances et savoir-faire mathématiques du programme.