Compte rendu MPS au lycée Vauvenargues

Claude Daviet, Arnaud Lathelize(*) & Hervé Roux

I. Organisation générale et thèmes choisis

Au lycée Vauvenargues (Aix en Provence), l'organisation en MPS est la suivante : 5 groupes de 18 élèves provenant de 3 classes de seconde soit 2,5 classes sur 13 classes de seconde que comporte le lycée.

L'emploi du temps initial de 1h30 sur 36 semaines a été annualisé, d'une part pour des raisons de commodité organisationnelle d'emploi du temps, mais aussi pour être sûr d'avoir le temps de traiter la notion choisie. Ainsi avons-nous donc effectué 27 séances de 2 heures, en commençant mi-octobre.

Au premier semestre c'est-à-dire les 13 premières séances, nous avons choisi de travailler sur le thème « Sciences et Vision du monde » » pour quatre groupes et « Sciences et Œuvres d'Art » pour un groupe, et au deuxième semestre sur le thème « Sciences et Investigations policières ».

Lors du premier semestre, l'organisation de travail fut proche de celle des TPE, à savoir des groupes de 2 à 3 élèves travaillant sur des sujets différents se rapportant au thème sciences et vision du monde, alors qu'au deuxième semestre nous avons construit une suite de TP (3 TP de Mathématiques, 3 TP de Sciences-Physiques et 3 TP de SVT) que tous les élèves effectuaient pour répondre à une question précise.

Nous avons eu la chance d'avoir des moyens importants pour la mise en place des MPS, en effet nous étions trois enseignants (un dans chaque discipline) attribués à chaque groupe, et pour chaque séance deux professeurs intervenaient en même temps. Le chef d'établissement a accepté de nous laisser un tel volant d'heures pour laisser toutes ses chances à cette dynamique de travail par projet. Au vu de l'engouement des élèves et de la qualité du travail produit, il nous a été permis pour la rentrée prochaine de continuer sur la même organisation.

Le travail du premier semestre fut globalement décevant, le principal échec fut le manque d'autonomie des élèves.

II. Le deuxième semestre

Lors de ce deuxième semestre, nous avons choisi le thème « Sciences et investigations policières » et, devant le semi-échec du premier semestre, nous avons radicalement changé notre manière de fonctionner. Nous avons mis chacun nos compétences au service de la réussite de ce thème dont le seul intitulé déclenchait

(*) arnoooo.lath@gmail.com

l'enthousiasme des élèves.

1. Organisation et travail demandé

Nous avons écrit un scénario de crime, nous permettant de construire 9 TP (3 en SVT, 3 en Sciences-Physiques et 3 en mathématiques) ; à la fin de chaque TP, les élèves obtiennent des informations sur un des indices découverts sur le lieu du crime et se rapprochent donc de la solution de l'enquête.

Les élèves ont constitué des binômes, et tous les binômes ont effectué le même travail.

Nous avons commencé notre première séance en visionnant deux documentaires extraits de l'émission « C'est pas sorcier » (« Les sorciers mènent l'enquête » et « Les sorciers jouent les experts » en streaming sur le site de France 3) afin d'introduire quelques idées sur le travail de la police scientifique. Ensuite nous avons présenté notre scène de crime avec la liste des indices.

Lors de chaque TP, les binômes ont dû produire un compte rendu qui fut noté.

Voici la liste des 9 TP (dans un ordre quelconque) correspondant aux indices retrouvés sur la scène du crime :

Entomologie : Datation du décès de la victime par entomologie médico-légale.

Chromatologie : Analyse chimique d'une poudre blanche retrouvée sur la scène de crime.

Balistique : Étude du mouvement d'une pierre, afin de déterminer l'origine du lancer de la pierre ayant cassé la vitre.

Dosage KCl : Analyse du sang afin de déterminer la dose de KCl retrouvée dans le sang de la victime.

Analyse du sol : comparaison de deux types de terre par recherche d'ions.

Cryptographie 1 et 2 : Formation à la cryptographie et cryptanalyse (Chiffrement de César et Affine puis Analyse fréquentielle). Déchiffrement d'un texte retrouvé sur l'ordinateur de la victime.

Palynologie : Comparaison de pollens.

ADN : Comparaison d'ADN.

Dominique BARBOLOSI est venu faire une conférence sur la démarche scientifique car lors de ce travail, les élèves ont eu une tendance à faire trop de conclusions hâtives.

La production finale demandée fut un bilan complet de l'enquête une fois l'ensemble des TP effectués. Les élèves devaient remplir un tableau reprenant chaque indice avec leur conclusion et devaient enfin rédiger leur propre solution de l'enquête. Cette production finale fut aussi notée. Le groupe ayant fait initialement « Sciences et œuvres d'art » a choisi de ne pas noter tous les TP préférant évaluer l'engagement des binômes (notation par compétences) et imposer un oral de fin de présentation

d'enquête où chaque binôme présenterait le travail réalisé et les conclusions du groupe.

2. Bilan du deuxième semestre

L'implication des élèves sur ce deuxième semestre fut sans comparaison avec le premier. On peut expliquer cela par le choix du thème mais aussi par le fait d'avoir noté chaque TP et surtout d'avoir opéré avec un mode plus directif. Mais c'est aussi grâce à une implication de toute une équipe, avec des travaux exceptionnels de certains collègues en particulier (travail d'entomologie légale à partir d'une thèse, palynologie à partir d'un document ministériel, cryptographie à partir d'un travail réalisé par l'IREM notamment). C'est la première fois que le travail en équipe interdisciplinaire s'est fait aussi naturellement sans compter les heures. Certes c'est du temps de passé, mais celui-ci sera réinvesti les années futures, et cela donne du souffle à l'enseignement traditionnel.

Sur certains sujets la présence conjointe d'enseignants de deux disciplines a pu illustrer à petite échelle le travail qui est fait dans la recherche où chacun apporte sa contribution à la résolution d'un problème.

Il nous a été demandé de présenter nos travaux en Corse auprès de collègues désirant s'impliquer dans cet enseignement d'exploration. Ce fut une journée riche de débats et de volonté de mutualiser les pratiques.

3. TP impliquant des mathématiques

Sur plusieurs TP orientés Sciences-Physique ou SVT, nous avons eu besoin de construire des courbes d'étalonnage (en fait des droites) et d'en connaître leurs équations, nous avons donc utilisé des modèles de régressions linéaires à l'aide d'un tableur, principalement le modèle de régression par les moindre carrés.

Le TP de balistique

Nous avons présenté un plan en trois dimensions de la scène de crime (cf ci-dessous).

À l'aide du logiciel Géogébra, l'élève devait reproduire le plan et les trajectoires possibles de la pierre afin de déterminer le lieu éventuel de l'origine du lancer. Pour cela, les élèves avaient à leur disposition deux points de la trajectoire de la pierre, le lieu de l'impact dans la vitre ainsi que l'endroit où la pierre a été retrouvée. Il a été supposé pour simplifier que la trajectoire de la pierre n'a pas été modifiée lors de l'impact dans la vitre et de plus que la pierre n'a pas roulé sur le sol.
En pièce jointe, l'énoncé du TP et le fichier Géogébra correspondant.

Les TP de cryptographie et cryptanalyse

Lors de la première séance, nous avons présenté le concept de chiffrement mono-alphabétique à l'aide du chiffrement de César. Les élèves ont dû construire une feuille de calcul sur tableur permettant de passer d'un message clair à un message chiffré (avec la possibilité de modifier la clé de chiffrement) et réciproquement.

Nous avons dû, au passage, expliquer comment étaient codés les caractères sur un ordinateur (Code ASCII).

Nous avons ensuite étudié le chiffrement affine et construit sur le même modèle une feuille de calcul tableur permettant de passer d'un message clair à un message chiffré avec la possibilité de modifier la clé de chiffrement.

Enfin, nous avons exposé une méthode d'attaque des chiffrements affines par analyse fréquentielle.

En pièce jointe, l'énoncé du TP et le fichier Excel correspondant.

III. Les perspectives

Nous, l'équipe pédagogique, avons pris du plaisir lors de ces séances de MPS. Nous avons travaillé en équipe interdisciplinaire et ce fut très enrichissant. La dynamique créée a eu pour effet de donner une image positive des enseignements d'exploration. Certains collègues frileux l'année dernière commencent à vouloir participer à la MPS.

L'enseignement commencera dès le début de l'année afin que les élèves rentrent directement dans la dynamique de la MPS. En effet, il y a parfois des journées banalisées ou des élèves en voyage, ou d'autres raisons d'absence. Cela nous permettra d'être sûr d'avoir le temps de traiter tout ce qui est prévu.

Après cette première année, nous avons eu de nouvelles idées pour enrichir les TP existants, pour créer de nouveaux TP, sur la façon d'organiser le travail et d'évaluer les élèves.

Nous sommes tous partants pour une nouvelle année, curieux de chercher de nouvelles idées.

Nous pensons qu'il faudrait créer une dynamique de sites académique de mutualisation.

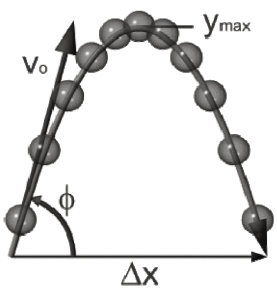
En commençant par « sciences et investigations policières » nous espérons donner aux élèves des méthodes de travail. Nous comptons faire intervenir la police scientifique de Marseille qui semble être habituée à intervenir auprès des établissements. Dans un deuxième temps, le thème sera laissé plus libre pour voir si les élèves ont gagné en autonomie et ainsi voir dans quelle mesure les compétences sont acquises. De plus, il pourra être fait un travail de préparation aux TPE de première.

Nous avons hâte de continuer l'aventure…

TP : travail sur les indices 1 et 2
Dossiers 56 BCXX991|1 et 56 BCXX991|2

Les enquêteurs arrivés sur les lieux où le corps de la victime a été retrouvé, ont constaté qu'une vitre de la porte-fenêtre du salon avait été cassée à l'aide d'une pierre que l'on a par ailleurs retrouvée dans le salon.
En utilisant le plan de la maison, la trace d'impact de la pierre dans la vitre ainsi que le point de chute de la pierre dans le salon, nous allons étudier les lieux possibles du lancer de cette pierre

On admettra que la trajectoire d'un objet soumis à un champ de pesanteur uniforme (en l'absence de frottements) est une parabole « tournée vers le bas » (voir figure ci-dessous) :



Vous trouverez, en annexe1, le plan en 3 dimensions de la maison et en annexe 2, une vue latérale de la maison à l'échelle 1/100.

1. Sur le plan fourni en annexe 2, construire un repère orthonormé. Vous prendrez comme axe des abscisses le sol du jardin, comme axe des ordonnées le mur de la maison comportant la baie vitrée fracturée et comme unité graphique 1cm. En vous aidant de l'annexe 1, construire sur ce plan la haie délimitant le terrain entourant la maison.
2. Déterminer les coordonnées de l'impact de la pierre dans la vitre et du point de chute de la pierre sur le sol du salon. Placer ces points sur le plan.
3. On rappelle qu'une parabole d'axe vertical est la représentation graphique d'une fonction f définie sur $\mathbb{R}$ par :
$$f(x) = ax^2 + bx + c$$
où a, b et c sont des réels fixés.
   a. Combien de paramètres faut-il déterminer pour obtenir l'équation d'une telle parabole ?
   b. Combien de points faut-il déterminer sur la parabole pour obtenir son équation?
   c. Combien de points connaissez-vous sur cette parabole ? Combien d'équations pouvez-vous obtenir ?

d. Écrire ces équations. Exprimer alors b en fonction de a.

4. Sur le plan fourni en annexe 2, hachurer la zone probable de l'origine du lancer, puis donner un encadrement des abscisses et des ordonnées des points de cette zone.

5. À l'aide de Géogébra, reproduire le plan de la maison avec la haie de lauriers, puis construire les paraboles possibles (on pourra utiliser des curseurs). Combien de paraboles peut-on construire ?

6. Faire le bilan sur l'endroit où a été lancée la pierre.

Conclusion :

Quelles conséquences pouvez-vous en tirer pour l'enquête que vous cherchez à résoudre ?

Annexe 1

Rapport de l'expert géomètre :

Vous trouverez ci-dessous un plan simplifié des lieux en rapport avec le dossier 56BXX991

Les longueurs sont exprimées en mètre.

Vous ne me l'aviez pas demandé expressément, mais il m'a semblé judicieux de vous informer que la haie de lauriers est située à 4 mètres de la face IBCJ, *mesure 2,5 mètres de haut et fait environ 1 mètre de large.*

Par ailleurs, un chemin de 2,5 mètres de large longe la haie

Sur le plan ci-dessous, I1 *correspond à l'impact de la pierre sur la vitre et* P1 *à l'emplacement de la pierre trouvée.*

Je reste à votre entière disposition pour tout renseignement complémentaire.

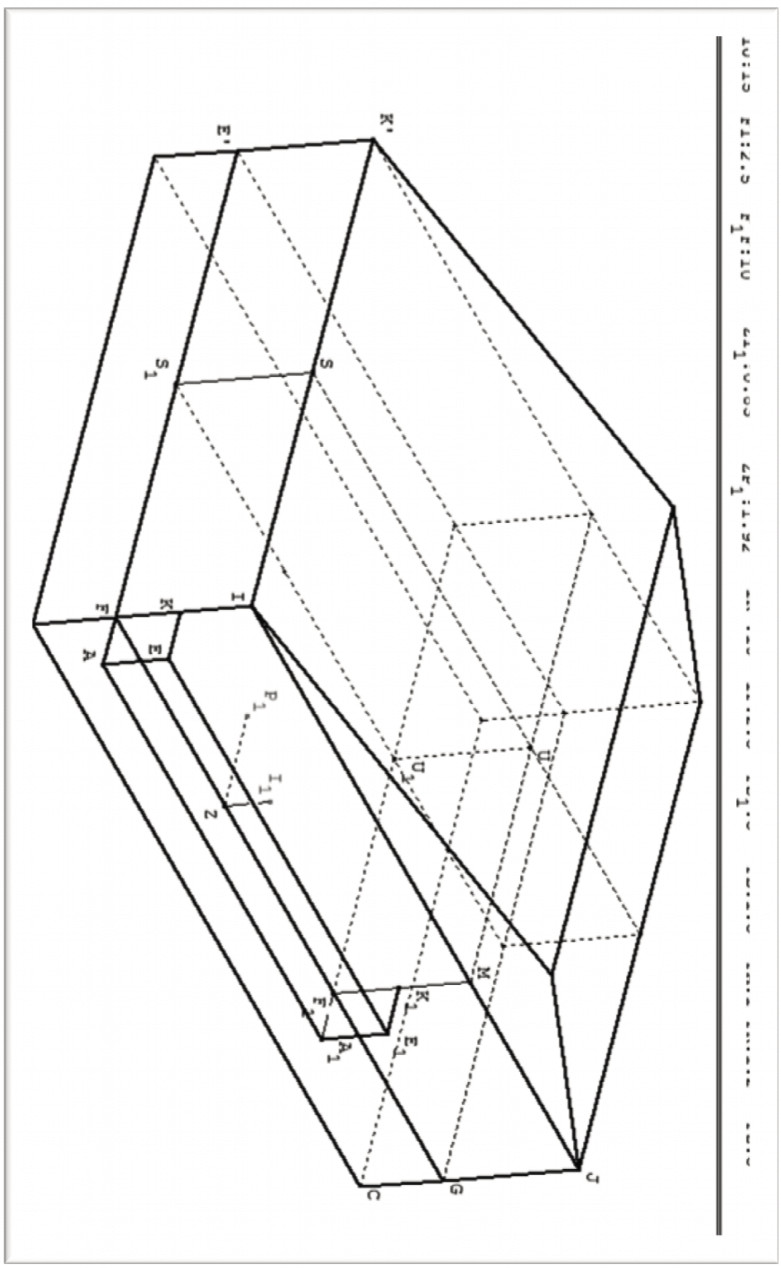
Je vous prie de croire en mon sincère dévouement,

Pour le cabinet d'expertise VERITAS,

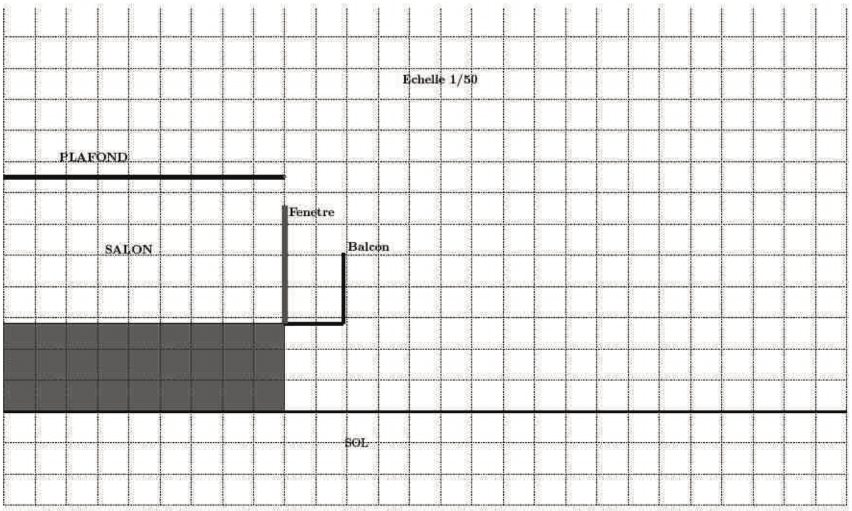
A.G. Expert Géomètre auprès du tribunal d'Aix en Provence

Plan de la maison en 3 dimensions

$P_1Z = 2\ mètres$ et $I_1Z = 0{,}83\ mètres$



Annexe 2 : vue latérale de la maison à l'échelle 1/50



Cryptographie

1. Introduction

Depuis l'invention de l'écriture et les premières guerres, il a toujours été important de pouvoir transmettre des messages protégés, c'est-à-dire des messages qui ne puissent être compris par l'ennemi même en cas d'interception.

Le chiffrement est la capacité à rendre un message illisible et le déchiffrement, la capacité à transformer le message illisible en un message clair.

Ne pas confondre le mot chiffrement et le mot codage. Le codage est une méthode permettant de passer d'une représentation des données vers une autre. Par exemple, dans un ordinateur chaque lettre est représentée par un nombre (code ASCII).

2. Les premières méthodes de chiffrement

Le plus vieux document chiffré

Le premier « document » chiffré connu remonte à l'Antiquité. Il s'agit d'une tablette d'argile, retrouvée en Irak, et datant du XVI^{e} siècle av. J.-C. Un potier y avait gravé sa recette secrète en supprimant des consonnes et en modifiant l'orthographe des mots.

La technique grecque

La première grande compilation des procédés cryptographiques et stéganographique (la stéganographie est l'art de la dissimulation : l'objet de la stéganographie est de

faire passer inaperçu un message dans un autre message) pratiqués durant l'Antiquité est celle du chapitre 31 de la Poliorcétique d'Énée le Tacticien, datant du IVe siècle av. J.-C.

Entre le Xe et le VIIe siècle av. J.-C. semble attestée une technique de chiffrement par transposition, c'est-à-dire reposant sur le changement de position des lettres dans le message, en utilisant un bâton de diamètre déterminé appelée scytale. On enroulait en hélice une bande de cuir autour de la scytale avant d'y inscrire un message. Une fois déroulé, le message était envoyé au destinataire qui possédait un bâton identique, nécessaire au déchiffrement. Cependant, l'utilisation de la scytale lacédémonienne comme procédé cryptographique n'est explicitement affirmée que par Plutarque et Aulu-Gelle, auteurs de la fin de l'Antiquité, et n'est pas mentionnée par Énée le Tacticien : dès lors, la scytale a-t-elle véritablement été un procédé cryptographique ?

La technique des Hébreux

À partir du Ve siècle av. J.-C., l'une des premières techniques de chiffrement est utilisée dans les textes religieux par les Hébreux qui connaissent plusieurs procédés.

Le plus connu appelé *Atbash* est une méthode de substitution alphabétique inversée. Son nom est formé par les initiales des premières et dernières lettres de l'alphabet hébreux aleph, tav, beth, shin.

Elle consiste à remplacer chaque lettre du texte en clair par une autre lettre de l'alphabet choisie de la manière suivante : A devient Z, B devient Y, etc.

Nabuchodonosor

Aux alentours de –600, Nabuchodonosor, roi de Babylone, employait une méthode originale : il écrivait sur le crâne rasé de ses esclaves, attendait que leurs cheveux aient repoussé, et il les envoyait à ses généraux. Il suffisait ensuite de raser à nouveau le messager pour lire le texte. Il s'agit toutefois de stéganographie à proprement parler et non pas de cryptographie : l'information est cachée et non pas chiffrée.

3. La substitution mono-alphabétique

Définition : La substitution mono-alphabétique consiste à remplacer dans un message chaque lettre de l'alphabet par une autre. C'est une permutation des lettres de l'alphabet. On dit alphabet désordonné.

Exemple : Chiffrement Atbash

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
Chiffré : z y x w v u t s r q p o n m l k j i h g f e d c b a

Texte clair : MON MESSAGE
Texte chiffré : nlm nvhhztv

a. Chiffrement de César

En cryptographie, le chiffrement de César est une méthode de chiffrement par substitution mono-alphabétique très simple utilisée par Jules César dans ses correspondances secrètes. Le chiffrement de César est un chiffrement par décalage.

Exemple : Décalage de 3 vers la droite
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
Chiffré : 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

Texte clair : ALEA JACTA EST
Texte chiffré : dohd mdfwd hvw

Le décalage de 3 vers la droite s'appelle la clé du chiffrement. Donc on a une clé égale à +3.
À un décalage de 3 vers la gauche correspondra une clé égale à −3.
Pour éviter de retrouver facilement les mots simples comme les lettres esseulées « à » ou les déterminants « le, la,… », on regroupe les lettres du message chiffré par groupe de 5 ou 6 lettres ou plus, au choix.

Question 1 : Combien existe-t-il de clés dans le chiffrement de César ?
Question 2 : Déchiffrer le message suivant sachant que la clé de chiffrement est égale à +10.

Message : pkmsv onono mrspp bobkf omvkm vo

Quel décalage vers la gauche utilisez-vous pour déchiffrer ?

À quel décalage vers la droite le déchiffrement correspond-il ?

Quelle clé positive utilisez-vous pour déchiffrer lors d'un chiffrement de clé égale à +10 ?

Cette méthode était utilisée dans l'armée romaine et bien qu'elle soit beaucoup moins robuste que la technique Atbash, la faible alphabétisation de la population la rendait suffisamment efficace.

Un système connu et pourtant

Le chiffrement de César a été utilisé sur des forums internet sous le nom de ROT13 (rotation ou décalage de 13 lettres). Le ROT13 n'a pas pour but de rendre du texte confidentiel, mais plutôt d'empêcher la lecture involontaire (d'une réponse à une devinette, ou de l'intrigue d'un film, etc.).

Question 3 : Choisir un mot de 5 ou 6 lettres, le chiffrer à l'aide du ROT13, puis chiffrer de nouveau le message obtenu avec ROT13. Qu'obtenez-vous ?

Question 4 : Expliquer pourquoi si l'on applique deux fois de suite le chiffrement ROT13, on obtient de nouveau le message en clair.

b. Utilisation d'un tableur pour chiffrer et déchiffrer en César

Sur un ordinateur les caractères sont représentés par des nombre, on dit qu'ils sont codés. Le code le plus utilisé est le code ASCII (American Standard Code for Information Interchange c'est à dire Code Américain Normalisé pour l'Echange d'Information).

Table ASCII

Dec	Hex	Char	Dec	Hex	Char	Dec	Hex	Char	Dec	Hex	Char
0	00	Null	32	20	Space	64	40	@	96	60	`
1	01	Start of heading	33	21	!	65	41	A	97	61	a
2	02	Start of text	34	22	"	66	42	B	98	62	b
3	03	End of text	35	23	#	67	43	C	99	63	c
4	04	End of transmit	36	24	$	68	44	D	100	64	d
5	05	Enquiry	37	25	%	69	45	E	101	65	e
6	06	Acknowledge	38	26	&	70	46	F	102	66	f
7	07	Audible bell	39	27	'	71	47	G	103	67	g
8	08	Backspace	40	28	(	72	48	H	104	68	h
9	09	Horizontal tab	41	29	)	73	49	I	105	69	i
10	0A	Line feed	42	2A	*	74	4A	J	106	6A	j
11	0B	Vertical tab	43	2B	+	75	4B	K	107	6B	k
12	0C	Form feed	44	2C	,	76	4C	L	108	6C	l
13	0D	Carriage return	45	2D	-	77	4D	M	109	6D	m
14	0E	Shift out	46	2E	.	78	4E	N	110	6E	n
15	0F	Shift in	47	2F	/	79	4F	O	111	6F	o
16	10	Data link escape	48	30	0	80	50	P	112	70	p
17	11	Device control 1	49	31	1	81	51	Q	113	71	q
18	12	Device control 2	50	32	2	82	52	R	114	72	r
19	13	Device control 3	51	33	3	83	53	S	115	73	s
20	14	Device control 4	52	34	4	84	54	T	116	74	t
21	15	Neg. acknowledge	53	35	5	85	55	U	117	75	u
22	16	Synchronous idle	54	36	6	86	56	V	118	76	v
23	17	End trans. block	55	37	7	87	57	W	119	77	w
24	18	Cancel	56	38	8	88	58	X	120	78	x
25	19	End of medium	57	39	9	89	59	Y	121	79	y
26	1A	Substitution	58	3A	:	90	5A	Z	122	7A	z
27	1B	Escape	59	3B	;	91	5B	[	123	7B	{
28	1C	File separator	60	3C	<	92	5C	\	124	7C	|
29	1D	Group separator	61	3D	=	93	5D	]	125	7D	}
30	1E	Record separator	62	3E	>	94	5E	^	126	7E	~
31	1F	Unit separator	63	3F	?	95	5F	_	127	7F	□

Sur Excel, l'instruction =CODE(''caractère'') renvoie le code ASCII du caractère et l'instruction =CAR(nombre) renvoie le caractère ayant pour code ASCII nombre.

Question 5 : Déterminer le code ASCII de « à ».

Question 6 : Déterminer le caractère dont le code ASCII est 233.

Pour simplifier, dans la suite nous n'utiliserons que *les lettres minuscules sans accents* de code ASCII compris entre 97 et 122. On appelle rang d'une lettre sa position dans l'alphabet en comptant à partir de zéro. On a :

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

Question 7 : Si on note x le code ASCII, d'une lettre, quelle formule permet d'obtenir son rang ? Si on note y le rang d'une lettre, quelle formule permet d'obtenir son code ASCII ?

Question 8 : En quels nombres sont transformés les rangs des caractères « a », « r » et « v » lors d'un chiffrement de César de clé égale à +12 ?
En quels nombres sont transformés les codes ASCII des caractères « a », « r » et « v » lors d'un chiffrement de César de clé égale à +12 ?

Pour les questions 9 et 11, on suppose la clé égale à +12

Question 9 : On note $\text{MOD}_{26}(n)$ le reste de la division euclidienne d'un entier n par 26.
Calculer $\text{MOD}_{26}(15)$, $\text{MOD2}_{26}(37)$ et $\text{MOD}_{26}(75)$

Si on appelle x le rang du caractère à chiffrer, vérifier à l'aide des caractères « a », « r » et « v » que la fonction définie par $f(x) = \text{MOD}_{26}(x + 12)$ détermine le rang du caractère chiffré.
On nommera cette fonction, la fonction de chiffrement.

Question 10 : Déterminer la fonction de chiffrement lors d'un chiffrement de César de clé égale à +17, puis de clé égale à +13.

Question 11 : Si on appelle x le rang du caractère à déchiffrer, vérifier à l'aide des caractères « m », « d » et « h » que la fonction définie par $f(x) = \text{MOD}_{26}(x + 14)$ détermine le rang du caractère déchiffré.
On nommera cette fonction, la fonction de déchiffrement.

Question 12 : Déterminer la fonction de déchiffrement lors d'un chiffrement de César de clé égale à +17, puis de clé égale à +13.

Sur Excel, la formule =MOD(nombre ; 26) correspond à la fonction MOD*26*(nombre).
Sur Excel, on peut à l'aide des fonctions GAUCHE() et DROITE() extraire les lettres d'un message, puis appliquer à chacune de ces lettres la fonction de chiffrement et enfin reformer le message chiffré à l'aide de la fonction CONCATENER() (cf. ci-dessous)

Message=	lacryptographieestuneactivitepassionnante							clé= 9		
position	extraction	lettre	ASCII	rang	rang chiffré	ASCII	chiffré			
1	l	l	108	11	20	117	u	u		
2	la	a	97	0	9	106	j	uj		
3	lac	c	99	2	11	108	l	ujl		
4	lacr	r	114	17	0	97	a	ujla		
5	lacry	y	121	24	7	104	h	ujlah		
6	lacryp	p	112	15	24	121	y	ujlahy		
7	lacrypt	t	116	19	2	99	c	ujlahyc		
8	lacrypto	o	111	14	23	120	x	ujlahycx		
9	lacryptog	g	103	6	15	112	p	ujlahycxp		
10	lacryptogr	r	114	17	0	97	a	ujlahycxpa		
11	lacryptogra	a	97	0	9	106	j	ujlahycxpaj		
12	lacryptograp	p	112	15	24	121	y	ujlahycxpajy		
13	lacryptograp	h	104	7	16	113	q	ujlahycxpajyq		
14	lacryptograp	i	105	8	17	114	r	ujlahycxpajyqr		

La deuxième colonne utilise la fonction GAUCHE(texte ; position_caractère) qui extrait tous les caractères d'une chaîne de caractères du début jusqu'à une position donné. On utilisera la position donnée par la première colonne.
La troisième colonne utilise la fonction DROITE(texte) qui extrait le caractère le plus à droite d'une chaîne de caractères.
La quatrième colonne utilise la fonction CODE() déjà vu.
La cinquième colonne calcule le rang d'une lettre dans l'alphabet à partir de son code ASCII.
La sixième colonne utilise la fonction de chiffrement à l'aide de la clé en haut à droite.
La septième colonne calcule le code ASCII de la lettre chiffrée à partir de la sixième colonne.
La huitième colonne utilise la fonction CAR() déjà vu.
La neuvième colonne reconstitue le message à l'aide de la fonction CONCATENER(Texte1 ;Texte2) qui renvoie la chaîne de caractères formée de Texte1 suivi de Texte2 .

Question 13 : Construire sur le modèle précédent une feuille de calcul permettant le chiffrement d'un message enregistré en case B1. La feuille doit être interactive c'est-à-dire que l'on peut modifier la valeur de la clé.

Question 14 : Peut-on utiliser cette feuille de calcul pour déchiffrer ? Si oui, expliquer comment.

Question 15 : A l'aide de votre feuille Excel, déchiffrer le message suivant sachant qu'il a été chiffré par un chiffrement de César de clé inconnue.

Message : pktrjc dgsxcp itjgrt hiqtpj rdjeea jhuprx at

c. Chiffrement affine

Le chiffrement affine est une méthode de chiffrement par substitution mono-alphabétique. Le principe est le suivant :

On choisit deux entiers a et b, une lettre de rang x est chiffrée par la lettre de rang le

reste de la division euclidienne de $ax + b$ par 26, c'est-à-dire $\text{MOD}_{26}(ax + b)$. Le couple (a,b) s'appelle la clé de chiffrement.

Exemple : Avec la clé (3,7) code est chiffré en nxqt

Question 16 : Chiffrer le mot « code » avec la clé (7,10) puis avec (33,10. Que constatez-vous ?

Question 17 : Que se passe-t-il si on choisit une clé avec $a = 1$?

Question 18 : Deux lettres consécutives sont-elles chiffrées par deux lettres consécutives par chiffrement de César ? et par chiffrement affine ?

Question 19 : Chiffrer « magique » avec la clé (13,5). Que pouvez-vous en déduire ?

On admet que pour obtenir un chiffrement affine qui respecte le principe de substitution mono-alphabétique, il faut et il suffit de choisir l'entier a premier avec 26.
Rappel : Deux nombres distincts a et b sont premiers entre eux si et seulement si $\text{PGCD}(a,b) = 1$.

Question 20 : Quels sont les entiers entre 1 et 25 premiers avec 26 ? En déduire le nombre de clés possibles dans un chiffrement affine qui ne soit pas un chiffrement de César.

d. Déchiffrement affine

On admet la méthode suivante :
Soit un message chiffré à l'aide d'un chiffrement affine de clé (a,b). Le déchiffrement affine s'effectue avec un chiffrement affine de clé (a',b') vérifiant :

$$\text{MOD}_{26}(aa') = 1 \text{ et } b' = \text{MOD}_{26}(a\,(26 - b)).$$

Exemple : Quel mot est chiffré par « ec» lorsque la clé est égale à (7,10) ?

On cherche un entier a' tel que $\text{MOD}_{26}(7a') = 1$ (remarque : a' est aussi premier avec 26).

Utilisons Excel et la fonction MOD(entier ; 26). On a :

a = 7

a'	3	5	7	9	11	15	17	19	21	23	25
$\text{MOD}_{26}(aa')$	21	9	23	11	25	1	15	3	17	5	19

On trouve ici, $a' = 15$. Calculons alors $b' = \text{MOD}_{26}(15\,(26 - b)) = 6$.

La fonction de déchiffrement est donc $f(x) = \text{MOD}_{26}(15x + 6)$

$e \rightarrow \text{MOD}_{26}(15 \times 4 + 6) = 14 \rightarrow o$ et $c \rightarrow \text{MOD}_{26}(15 \times 2 + 6) = 10 \rightarrow k$
Ainsi « ec » signifie « ok ».

Question 21 : Écrire la fonction de déchiffrement lorsque la clé est égale à (5,17). Déterminer le mot chiffré par « jnf »

e. Utilisation du tableur pour chiffrer et déchiffrer en affine

On construit de la même manière que pour le chiffrement de César une feuille Excel sur le modèle suivant :

message =	lechiffrementaffinemelangebienlalphabet								a = 7	
Position	Extraction	lettre	ASCII	rang	rang chiffré	ASCII	chiffrée		b = 10	
1	l	l	108	11	9	106	j			
2	le	e	101	4	12	109	m	jm		
3	lec	c	99	2	24	121	y	jmy		
4	lech	h	104	7	7	104	h	jmyh		
5	lechi	i	105	8	14	111	o	jmyho		
6	lechif	f	102	5	19	116	t	jmyhot		
7	lechiff	f	102	5	19	116	t	jmyhott		
8	lechiffr	r	114	17	25	122	z	jmyhottz		
9	lechiffre	e	101	4	12	109	m	jmyhottzm		
10	lechiffrem	m	109	12	16	113	q	jmyhottzmq		

Question 22 : Construire sur le modèle précédent une feuille de calcul permettant le chiffrement d'un message enregistré en case B1. La feuille doit être interactive c'est-à-dire que l'on peut modifier les valeurs de la clé. Peut-on utiliser cette feuille pour déchiffrer ?

Question 23 : Utiliser votre feuille de calcul pour déchiffrer le message suivant chiffré selon la méthode du chiffrement affine avec la clé .

Message : ofvvpi fbpwxz rxbfmx mxbepi ikxk

Question 24 : Si on intercepte un message chiffrée en affine, combien doit-on essayer de clés au maximum ?