Cette fiche a été réalisée par des enseignantes et des enseignants des lycées et des universités de l'Académie de Créteil.
Titre : Chiffrement.
Disciplines mises en jeu : Mathématiques niveau terminale S spécialité.

Objectifs :découvrir et travailler sur les chiffrements de messages.
Mise en place : une séance de TD.

Contenu : après avoir découvert un exemple de décodage, on examine un deuxième exemple de chiffrement en utilisant les matrices et la notion de modulo.

Exercice n°1 : chiffrement de Polybe

Polybe (200-125 av J.C) a proposé le mécanisme de cryptage suivant : on considère les lettres de l'alphabet privé de W soit 25 lettres. On les range dans un tableau 5*5 en commençant par le mot clé (et en supprimant les doublons) puis on continue avec les lettres restantes de l'alphabet dans l'ordre. Par exemple si le mot-clé est MATHS, on a le tableau suivant :

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

Le chiffrement s'effectue en remplaçant chaque lettre par les deux chiffres: celui de la ligne d'abord puis celui de la colonne qui définissent la position de la lettre dans la grille.
Par exemple dans ce codage 31 correspond à G.

Raoul envoie le message suivant à Anna. Déchiffrez le message. (Le mot clé n'est pas maths)

1232225122 15424215 512242242255 53435211 15 24225254 322252512211 515222 5322511422 5115435221

indication : la lettre la plus utilisée habituellement est le E ; on peut supposer que Z est codé par 55 et on remarquera que Anna est un prénom symétrique.

Exercice n°2 :

Dans le chiffrement de Hill, chaque lettre de l'alphabet est représentée par un entier naturel compris entre 0 et 25.
L'algorithme est un chiffrement par blocs de m lettres, qui transforme un bloc (x1,x2,……,xm)en un bloc (y1,y2,….,ym) défini par la relation :

(y1,y2,….,ym)=(x1,x2,….,xm).A
avec A une matrice d'ordre m dont les coefficients sont des entiers compris entre 0 et 25.
Tous les calculs se font donc modulo 26.
On supposera dans la suite que m=2

1) Quelles particularités doit posséder la matrice A pour déchiffrer un message. Quelle est la formule utilisée alors ? A est appelée la matrice clé.

2) On a le message FRIDAY codé par PQCFKU. Trouver la matrice clé de taille 2*2 . On vérifiera soigneusement les résultats obtenus