DM07 (2nde E et C)

Le but de l'activité est le cryptage et le décryptage d'un message à l'aide d'une fonction affine.

Partie I : Application affine

La personne qui souhaite coder le message donne des nombres à trois personnes. A James Bond elle donne 0,5 et 7, à Bruce Willis elle donne -0,5 et -1 et à Sherlock Holmes elle donne -1 et -5.

Déterminer l'équation $y=mx+p$ de la droite définie par ces nombres.

L'intérêt d'avoir trois personnes ou plus, est soit de pouvoir vérifier avec un troisième point que c'est la bonne équation de droite, soit de pouvoir quand même décrypter si un des agents meurt en mission ! Il faut au moins deux agents pour pouvoir déterminer l'équation de la droite qui permet de décrypter le message.

Partie II : Cryptage affine

Nous allons coder la phrase suivante :

La musique est une mathématique sonore, la mathématique une musique silencieuse. (Edouard Herriot)

Compléter sur une feuille le tableau suivant qui permet de crypter le message :

Lettres	L	a		m	u	s	…..
Rang x	12	1		13	21	19	
y							

Ecrire le message crypté obtenu :

Partie IV : Décryptage

1. Déterminer x en fonction de y et donner une méthode qui permet de décrypter un message codé.

2. Décrypter le message suivant :

99 43/163/21/35/43 35/43/155 107/11/163/67/43/107/11/163/75/139/171/43/155 43/155/163 27/123/107/107/43 99/43 115/75/99 139/171/75 27/123/107/107/43/115/27/43 43/115 107/123/35/43/155/163/75/43 43/163 51/75/115/75/163 43/115 107/11/59/115/75/51/75/27/43/115/27/43 (27/123/99/163/123/115)

Evaluation

Thème 12			
AA	A	EA	NA
SEI06			
AA	A	EA	NA

Histoire

Le premier document chiffré remonte à l'Antiquité au XVI ième siècle avant JC

Le code de César

(1er siècle av JC)

Le chiffrement de Vigenère

(1586) qui a été cassé en 1854

Avec les deux grandes guerres mondiales, la cryptographie s'est considérablement développée.

Machine Enigma

(1919)

Le code RSA

Rivest **S**hamir **A**dleman