| *Année 2010-2011* | **Enseignements d'exploration : Secondes** |
|---|---|
| **Investigation Policière** | **Thème : cryptographie : approche mathématique** |
| **FICHE N°5** | **Objectif : établir une méthode de décodage** |

**Problématique** : on considère un message crypté dont on sait que le principe de cryptage est celui du décalage circulaire des lettres, dans un sens donné, d'un nombre donné de lettres.

**Première expérimentation**

Réaliser "à la main" le codage du mot POLICIER puis de son décodage :

- avec un décalage de 3 lettres
- avec un décalage de 17 lettres

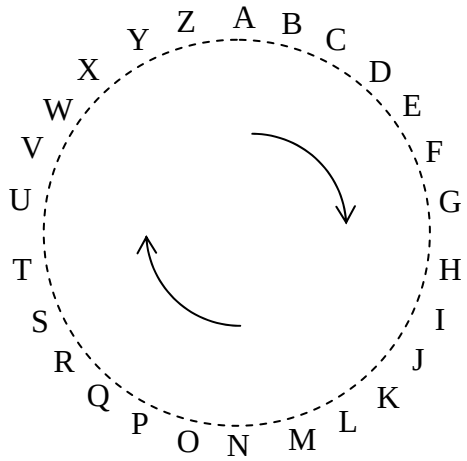
**Découvrir le codage ASCII des lettres**

Rechercher sur Internet la signification du *codage ASCII* et proposer le codage du mot POLICIER :

| P | O | L | I | C | I | E | R |
|---|---|---|---|---|---|---|---|
| | | | | | | | |

**Principe de la permutation circulaire**

Il consiste ici à tourner dans l'ordre alphabétique et lorsqu'on arrive à Z on repart à A.




Ecrire à l'intérieur du cercle en pointillé le code ASCII de chaque lettre.

Si on décale le T de 9 rangs, on obtient C ; on passe donc du code ….. au code …..

On a donc : CODE(T) + 9 = CODE(C) + …..

Soit : CODE(T) + 9 - ….. = CODE(C)

**Découverte des fonctions Excel**

- Trouver la fonction Excel permettant de traduire une lettre en son code ASCII.
- Trouver la fonction Excel permettant de traduire un nombre en la lettre dont il est le code ASCII.
- Etudier, toujours sur Excel, la fonction MODE.

**Première application**

Monter une feuille Excel permettant de coder le mot POLICIER par un décalage circulaire de 17 lettres.
Décoder le mot SRKVRL qui a été codé selon le même principe

**Ecriture d'une phrase**

Le code ASCII du *blanc* est ….. On souhaite qu'il ne soit pas soumis au codage mais qu'il reste un blanc.
On se propose d'utiliser la fonction SI d'Excel pour compléter la formule trouvée ci-dessus. Etudier la syntaxe de cette fonction et proposer une formule complète.

**Codage d'un message secret**

Le message suivant a été retrouvé sur le lieu du crime :

**XM RXQOTQFFQ QEF XQ EUSZMX UX QZ HQGF M YM HUQ XM HQDUFQ QEF PMZE XQ OARRDQ XQ OAPQ QEF AUEQMG QZ MEOUU**

La seule certitude que l'on a est que le message a été écrit par décalage circulaire mais on ignore l'ampleur du décalage. Proposer une méthode pour résoudre ce problème.