**TP Décryptage**



**La feuille blanche retrouvée dans l’agenda de Mr.Boidest contenait un message incompréhensible. Dans les indices, les enquêteurs ont aussi trouvé un CD protégé par un mot de passe et une grille de Sudoku un peu particulière : ses cases contiennent des énigmes mathématiques et quatre d’entre elles sont entourées ou coloriées.**

**Principe du TP :**

**Il s’agit ici de décoder le message, puis de résoudre la grille de Sudoku afin de retrouver les quatre chiffres du code. Une des 24 combinaisons de ces chiffres correspond au mot de passe du CD. Les dossiers stockés contiennent des éléments qui feront avancer l’enquête.**

**Résultat : Décodage du message**

**Le message est le suivant : « Vous ne trouverez jamais mon code japonais. »**

**Quelle que soit la méthode utilisée, les élèves sont toujours parvenus à décoder le message, en ayant parfois besoin d’un indice méthodologique. La méthode qui a été la plus souvent utilisée est celle de la correspondance avec un décalage de n lettres, n étant égal au rang de la lettre dans le mot.**

**Méthodes de codage**

**Correspondance d’une lettre avec une autre lettre**

**On attribue à chaque lettre de l’alphabet un autre caractère, soit par décalage de p lettres soit arbitrairement.**

**Par décalage :**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **A** |  | **B** |  | **C** | **D** | **E** | **F** |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **A** | **B** | **C** | **D** |  | **E** |  | **F** |

**Le message devient :**

**ZRYV PH XURYZHUHC MDPDLV PRQ FRGH MDSRQDLV**

**La méthode est connue des élèves de seconde et le décryptage du message ne prend que quelques minutes. Elle ne nécessite pas de donner d’apport méthodologique.**

**Décalage des lettres en fonction de leur rang n dans le mot**

**La première lettre est décalée d’un rang, la deuxième de deux rangs etc. Ainsi dans le message la même lettre n’a pas la même signification.**

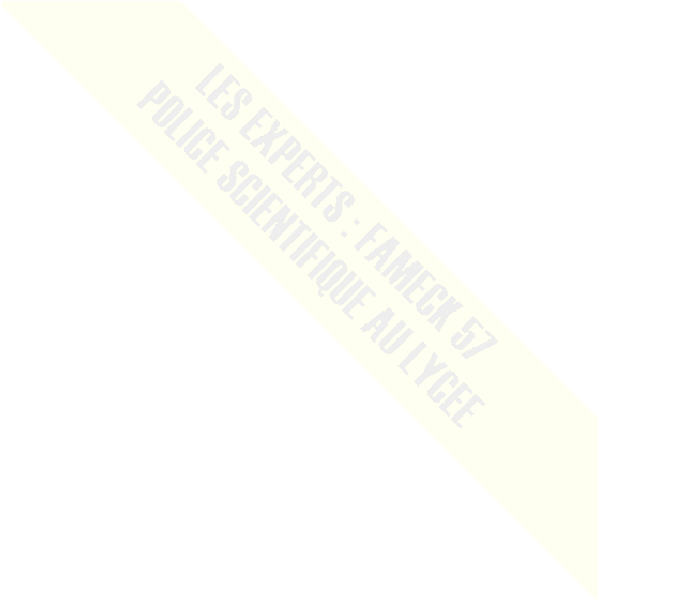
**Le message devient :**

**XQYX OG UTRZBKZMI KCPENZ NQQ DQGI KCSSSGPB**

**Indice méthodologique :**

**Est-il possible d’avoir trois lettres identiques qui se suivent ? La même lettre peut représenter deux lettres différentes.**

**Attribution arbitraire d’un caractère spécial**



|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **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** |
|  |  |  | ∫ |  |  | **?** |  |  | |  |  |  |  |

**Le message codé devient :**

**! ?** 

**Cette méthode est plus difficile, l’étude des fréquences des caractères ne fonctionnent pas dans ce message, il y a plus de o que de e. Les élèves ont besoin d’aide.**

**Indice méthodologique : analyse grammaticale de la phrase**

**Une phrase simple commence par un sujet suivi d’un verbe. Le nombre de lettres indique qu’il s’agit d’un sujet pronominal et non d’un sujet constitué d’un article et d’un substantif.**

**Une autre indication possible consiste à signer le message par le prénom de la victime : « Claude ». Cela permet d’identifier les voyelles a , u et e.**

**! ?** 



**Code utilisant le numéro atomique**

**Chaque lettre est remplacée par un numéro atomique de l’élément chimique commençant par la même lettre. Aucun élément ne commençant par J, on prend le numéro atomique de l’iode.**

**Le message devient :**

**23-8-92-16 7-68 43-37-8-92-23-68-37-68-30 53-89-25-89-53-16 25-8-7 6-8-105-68**

**53-89-15-8-7-89-53-16**

**Indice méthodologique :**

**Quelle est la profession de la victime ? Combien de chiffres représentent une lettre ?**

**La présence d’une classification périodique dans la salle est nécessaire.**

**Carré de Polybe**

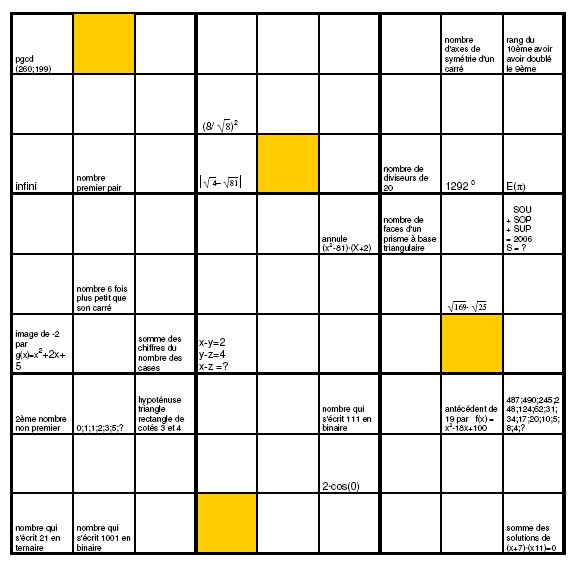
**Premier procédé de cryptage connu (150 av J-C)**

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

**Chaque lettre est remplacée par ses coordonnées dans le tableau : Le message devient :**

**52355144 3415 454335515215431555 251133112444 333534 13351415 511143534112444**

**Utilisation du message décodé**



**Il s’agit ensuite de trouver à quoi sert l’indication donnée par le message décodé. Quelle est la pièce à conviction susceptible d’être concernée ?**

**La grille de Sudoku, c’est évident pour nous, mais les élèves ont en général besoin d’être mis sur la voie.**

**Grille de Sudoku (Valeurs Mutualistes 2006 ( MGEN))**

**Solution du Sudoku**



**Les chiffres noirs ont été obtenus en résolvant les énigmes mathématiques. Les chiffres en rouge correspondent à la résolution de la grille.**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 5 | 7 | 2 3 6  8 4 1 | | | 8 4 9  2 7 5  6 1 3 | | |
| 9 3 6  8 2 4 | | |
| 7 | 9 | 5 |
| 4 7 8  2 6 3  5 1 9 | | | 1 2 9  5 7 4  6 8 3 | | | 5 3 6  9 8 1 | | |
| 4 | 2 | 7 |
| 6 8 5  3 4 1  7 9 2 | | | 4 1 7  9 5 2 | | | 3 9 2  7 6 8  1 5 4 | | |
| 3 | 6 8 | |

**Le mot de passe du CD est constitué des chiffres 5, 9, 2 et 3. Il ne reste plus qu’à trouver les 24 combinaisons et à les essayer tour à tour : chaque groupe se charge d’une série de combinaisons.**