# Thème : Avant les congruences

## Support de correction de l’activité 2. Chiffrement affine

1. **Exemple 1**  et
   1. On fait le tableau des rangs des 26 lettres de l’alphabet :

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Lettre | A | B | C | D | E | F | G | H | I | J | K | L | M |
| Rang | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|  | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

* 1. On remplit le tableau en utilisant la calculatrice :

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Clé |  |  |  |  |  |  |  |  |  |  |  |  |
| Lettre en clair | A | B | C | D | E | F | G | H | I | J | K | L |
| Rang | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
| Rang |  |  |  |  |  |  |  |  |  |  |  |  |
| Lettre chiffrée |  |  |  |  |  |  |  |  |  |  |  |  |

3) On réalise avec un tableur le tableau proposé dans l’énoncé.

* On peut fixer la largeur des colonnes assez petite (largeur 2 ou 3) pour les colonnes B à AM.
* On saisit les lignes 1 et 2 et la colonne A avec les valeurs présentes dans le tableau de l’énoncé.
* Dans la cellule B3, on entre la formule =CODE(B2) puis on recopie B3 automatiquement, à l’aide de la poignée de recopie située en bas à droite de la cellule B3, jusqu’en AA3.
* Dans la cellule B4, on entre la formule =$C1\*B3+$F1 puis on recopie B4 automatiquement jusqu’en AA4.  
  Le symbole $ placé devant les lettres de colonnes C et F permet de fixer ces références de colonnes afin qu’elles restent inchangées dans la recopie automatique.
* Dans la cellule B5 on entre la formule =MOD(B4 ;26) puis on recopie B5 automatiquement jusqu’en AA5.
* Dans la cellule B6, on entre la formule =CAR(B5+65) puis on recopie B6 automatiquement jusqu’en AA6.

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Lettre** | **Effectif** | **Fréquence** |  | A | 8 | 0,051 |  | M | 2 | 0,013 |
| V | 27 | 0,171 |  | N | 7 | 0,044 |  | D | 2 | 0,013 |
| Z | 16 | 0,101 |  | J | 6 | 0,038 |  | R | 1 | 0,006 |
| F | 15 | 0,095 |  | B | 5 | 0,032 |  | X | 1 | 0,006 |
| S | 13 | 0,082 |  | Y | 5 | 0,032 |  | **TOTAL** | **158** | **1** |
| L | 10 | 0,063 |  | K | 5 | 0,032 |  |  |  |  |
| Q | 10 | 0,063 |  | E | 3 | 0,019 |  |  |  |  |
| I | 10 | 0,063 |  | O | 2 | 0,013 |  |  |  |  |
| H | 8 | 0,051 |  | U | 2 | 0,013 |  |  |  |  |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **M** | **A** | **I** | **N** | **T** | **E** | **N** | **A** | **N** | **T** |  | **V** | **O** | **U** | **S** |  | **E** | **N** |  | **S** | **A** | **V** | **E** | **Z** |  | **A** | **S** | **S** | **E** | **Z** |  | **P** | **O** | **U** | **R** |  |
| **V** | **O** | **U** | **S** |  | **C** | **O** | **N** | **V** | **A** | **I** | **N** | **C** | **R** | **E** |  | **Q** | **U** | **E** |  | **L** | **E** | **S** |  | **C** | **H** | **I** | **F** | **F** | **R** | **E** | **S** |  | **D** | **E** |  |
| **C** | **E** | **T** | **T** | **E** |  | **N** | **A** | **T** | **U** | **R** | **E** |  | **S** | **O** | **N** | **T** |  | **A** | **I** | **S** | **E** | **S** |  | **A** |  | **D** | **E** | **V** | **I** | **N** | **E** | **R** |  |  |  |
| **M** | **A** | **I** | **S** |  | **A** | **S** | **S** | **U** | **R** | **E** | **M** | **E** | **N** | **T** |  | **C** | **E** |  | **S** | **P** | **E** | **C** | **I** | **M** | **E** | **N** |  |  |  |  |  |  |  |  |  |
| **A** | **P** | **P** | **A** | **R** | **T** | **I** | **E** | **N** | **T** |  | **A** | **U** |  | **G** | **E** | **N** | **R** | **E** |  | **L** | **E** |  | **P** | **L** | **U** | **S** |  | **S** | **I** | **M** | **P** | **L** | **E** |  |  |
| **D** | **E** |  | **L** | **A** |  | **C** | **R** | **Y** | **P** | **T** | **O** | **G** | **R** | **A** | **P** | **H** | **I** | **E** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |