# Thème : Avant les congruences

## Corrigé de l’activité 2. Chiffrement affine

Voir le fichier tableur [pf5372a02.chiffrement\_affine.xls](http://www.astrovirtuel.fr/pf5372/avant_congruences/pf5372a02.chiffrement_affine.xls) ou [pf5372a02.chiffrement\_affine.ods](http://www.astrovirtuel.fr/pf5372/avant_congruences/pf5372a02.chiffrement_affine.ods)

Remarque préalable sur le vocabulaire :

Conformément au programme, on définit :

* Le **codage** comme une association simple d’un objet avec un nombre. Par exemple le sexe masculin est codé 1 dans le numéro INSEE, la lettre A est codée 65 sur un ordinateur.
* Le **chiffrement** comme cryptage par un processus plus complexe. Par exemple le chiffrement affine, de Vigenère ou de Hill.

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 |

* a pour rang

.

Le reste de la division de par est

Donc est chiffré par .

* a pour rang

.

Le reste de la division de par est

Donc est chiffré par .

* a pour rang

.

Le reste de la division de par est

Donc est chiffré par .

* a pour rang

.

Le reste de la division de par est

Donc est chiffré par .

* a pour rang

.

Le reste de la division de par est

Donc est chiffré par .

* a pour rang

.

Le reste de la division de par est

Donc est chiffré par .

Donc **EUCLIDE** est chiffré en **RNLMDOR**

* 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 |
|  | 5 | 8 | 11 | 14 | 17 | 20 | 23 | 26 | 29 | 32 | 35 | 38 |
| Rang | 5 | 8 | 11 | 14 | 17 | 20 | 23 | 0 | 3 | 6 | 9 | 12 |
| Lettre chiffrée | F | I | L | O | R | U | X | A | D | G | J | M |

Par lecture du tableau depuis la ligne « lettre chiffrée », on déchiffre :

* U est déchiffré en F
* F est déchiffré en A
* L est déchiffré en C
* D est déchiffré en I
* M est déchiffré en L
* R est déchiffré en E

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)-65 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.

1. **Exemple 2**

* a pour rang

.

Le reste de la division de par est

Donc est chiffré par .

* a pour rang

.

Le reste de la division de par est

Donc est chiffré par .

* a pour rang

.

Le reste de la division de par est

Donc est chiffré par .

* a pour rang

.

Le reste de la division de par est

Donc est chiffré .

Donc **RAGE** est chiffré en **REEE**.

On constate que des lettres distinctes sont chiffrées en une même lettre.

Ceci provient du fait que :

, et ont le même reste dans la division par 26.

Une même lettre chiffrée correspond à des « lettres en clair » différentes. Le déchiffrement est donc impossible. La clé ne peut donc pas être utilisée.

*Remarque :*

On peut se demander quelle condition nécessaire et suffisante il y a sur la clé pour qu’elle soit utilisable.

Soit et les rangs de deux lettres en clair. Soit et les rangs des lettres chiffrées correspondantes.

On a avec et

* A quelle condition sur a-t-on  ?

D’après le théorème de Gauss,

Autrement dit, puisque ,

On voit qu’une condition suffisante sur la clé est que soit premier avec 26.

* Est-elle nécessaire ?

Si n’est pas premier avec 26 alors est divisible par 2 ou 13. Dans ce cas, le produit peut-être un multiple de 26 tout en ayant non nul. C’est le cas lorsque est un multiple de 2 ou de 13.

Donc elle est nécessaire.

Conclusion : Pour que, quels que soient les rangs et , il faut et il suffit que soit premier avec 26.

1. **Exemple 3**

Comme le suggère l’énoncé, ce chiffrement peut être cassé par une analyse fréquentielle.

On relève donc l’effectif de chaque lettre présente et l’effectif total.

On calcule les fréquences.

Pour plus de facilité, on trie la liste par ordre décroissant de fréquences.

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **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 |  |  |  |  |

* Le V a une fréquence nettement plus élevée. On suppose donc qu’il chiffre le E.
* Le Z a la deuxième fréquence la plus élevée. Donc il chiffre probablement le A ou le S. Si c’est le A alors le cinquième mot comporte deux A à suivre ce qui est très improbable. On suppose donc que Z chiffre le S.
* Le F a la troisième fréquence la plus élevée. On suppose donc qu’il chiffre le A.
* Le quatrième mot est très probablement ASSEZ, ce qui montre que O chiffre le Z.

Et ainsi de suite, on procède en s’aidant des fréquences et en regardant la vraisemblance des conjectures.

Après quelques minutes, on obtient le texte en clair :

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **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** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |