# Quelques méthodes de cryptographie symétrique à clé secrète

**Niveau** : terminale générale maths expertes.
**Lien avec le programme** : matrices, congruences. Théorèmes de Bézout et de Fermat.
**Lien avec *Les maths au quotidien*** : **Codages**.

## A- Le chiffre de César

Lorsque l'on code un message en remplaçant chaque lettre par celle située *n* rangs plus loin dans l'alphabet, on établit ce que l'on appelle un cryptage monoalphabétique (une lettre est codée par une même lettre et deux lettres différentes sont codées par deux lettres différentes). Le nombre choisi pour le décalage est la clé de cryptage du code.

Cette méthode de décalage, appelée « chiffre de César », est un chiffrement simple et très facile à casser. Elle a été utilisée par l'empereur Jules César.

On cherche à crypter le message suivant : J ADORE LES MATHS
Le message crypté devient : U LOZCP WPD XLESD.

**1.** Quelle est la clé de cryptage ? la clé de décryptage ?

Dans un cryptage monoalphabétique, en général, il est possible de retrouver le message initial en utilisant les statistiques. En effet, dans la langue française, on a un ordre d'idée de la fréquence des lettres dans un texte donné, ceci en ayant analysé un grand nombre de textes d'écrivains. Néanmoins, pour que cela reste acceptable, il faut que le message soit suffisamment long.
Si par exemple le codage est un chiffre de César, on peut, à l'aide des statistiques, révéler la clé du code !
Le tableau suivant donne un ordre d'idée des fréquences d'apparition, en pourcentages, des lettres de l'alphabet concernant des textes suffisamment longs écrits en français :

| A | B | C | D | E | F | G | H | I | J | K | L | M |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 7,8 % | 1,1 % | 3,5 % | 3,9 % | 15 % | 1,2 % | 0,9 % | 0,7 % | 7,7 % | 0,5 % | 0,1 % | 5,7 % | 3,2 % |
| N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| 7,2 % | 5,6 % | 3 % | 1,5 % | 6,8 % | 8,1 % | 7,4 % | 6,5 % | 1,7 % | 0,1 % | 0,4 % | 0,3 % | 0,1 % |

**2.** Décoder le message suivant :

« *psvwuyi p sr gshi yr qiwweki ir viqtpegerx yri pixxvi tev yri eyxvi, mp iwx tswwmfpi hi pi higvctxiv ir yxmpmwerx piw wxexmwxmuyiw* »

*Remarque* :

Dans un codage monoalphabétique en général, la lettre E est souvent décodable de façon significative, mais les lettres ayant des fréquences proches (I et S par exemple) ne le sont pas immédiatement : il faut s'intéresser en plus des fréquences à d'autres éléments, comme aux lettres isolées (s'il y a des espaces), aux lettres doublées, au caractère consonne-voyelle…

**B. Chiffrement à l'aide d'une matrice**

**1.** Calculer les produits matriciels :

$$\begin{pmatrix} -3 & 5 & 6 \\ -1 & 2 & 2 \\ 1 & -1 & -1 \end{pmatrix}\begin{pmatrix} 0 & 1 & 2 \\ -1 & 3 & 0 \\ 1 & -2 & 1 \end{pmatrix} \text{ et } \begin{pmatrix} 0 & 1 & 2 \\ -1 & 3 & 0 \\ 1 & -2 & 1 \end{pmatrix}\begin{pmatrix} -3 & 5 & 6 \\ -1 & 2 & 2 \\ 1 & -1 & -1 \end{pmatrix}$$

Qu'en conclure ?

On cherche à coder J ADORE LES MATHS.

La matrice de codage qu'on va utiliser est la matrice M = $\begin{pmatrix} -3 & 5 & 6 \\ -1 & 2 & 2 \\ 1 & -1 & -1 \end{pmatrix}$. C'est la clé de cryptage.

Assignons un nombre à chaque lettre de l'alphabet : une méthode simple est d'associer chaque lettre à sa position dans l'alphabet : A est 1, B est 2, …, Z est 26.

De plus on va ici aussi assigner un nombre à un espace entre deux mots. Un espace sera noté ␣. Donnons-lui la valeur 27.

Le message devient alors :

| J | ␣ | A | D | O | R | E | ␣ | L | E | S | ␣ | M | A | T | H | S |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 10 | 27 | 1 | 4 | 15 | 18 | 5 | 27 | 12 | 5 | 19 | 27 | 13 | 1 | 20 | 8 | 19 |

Puisque nous employons une matrice 3×3, nous décomposons le message à coder en une suite de vecteurs colonnes 3×1 : $\begin{pmatrix} 10 \\ 27 \\ 1 \end{pmatrix}, \begin{pmatrix} 4 \\ 15 \\ 18 \end{pmatrix}, \begin{pmatrix} 5 \\ 27 \\ 12 \end{pmatrix}, \begin{pmatrix} 5 \\ 19 \\ 27 \end{pmatrix}, \begin{pmatrix} 13 \\ 1 \\ 20 \end{pmatrix}, \begin{pmatrix} 8 \\ 19 \\ 27 \end{pmatrix}$.

Remarquez qu'il était nécessaire d'ajouter un espace à la fin du message pour compléter le dernier vecteur. Nous codons maintenant le message en multipliant chacun des vecteurs ci-dessus par la matrice de codage. Nous obtiendrons des vecteurs codés. Faisons l'opération matriciellement en voyant ces six vecteurs comme les vecteurs colonnes d'une matrice B : $\begin{pmatrix} 10 & 4 & 5 & 5 & 13 & 8 \\ 27 & 15 & 27 & 19 & 1 & 19 \\ 1 & 18 & 12 & 27 & 20 & 27 \end{pmatrix}$.

**2.** Coder le message J ADORE LES MATHS.

**3.** Expliquer comment décoder le message codé.

### C. Un cryptage affine

Un cryptage affine consiste à chiffrer chaque lettre de l'alphabet, puis à remplacer le nombre initial $x$ par le nombre $y \equiv ax + b$ (26) avec $0 \leqslant y \leqslant 25$.
Les nombres $a$ et $b$ sont des entiers naturels qui forment la clé du cryptage.

On rappelle que $u \equiv v$ ($n$) signifie que $u$ est congru à $v$ modulo $n$, c'est-à-dire que $u$ et $v$ ont le même reste dans la division euclidienne par $n$.

Exemple avec la clé ($a$ ; $b$) = (3 ; 7).

| En clair | 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Rang $x$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |
| Rang $y$ | | | | | | | | | | | | | | | | | | | | | | | | | | |
| En crypté | | | | | | | | | | | | | | | | | | | | | | | | | | |

**1.** Recopier et compléter les deux dernières lignes du tableau précédent et coder le message : J ADORE LES MATHS.

**2.** Décrypter la phrase RXF HPJJF.

**3.** <u>Attention au choix de la clé</u> : avec la clé précédente, le tableau complété montre que deux lettres distinctes sont cryptées par deux lettres distinctes.
Avec la clé (2 ; 7), montrer que les lettres A ($x$ = 0) et N ($x$ = 13) donnent le même rang $y$ et donc qu'elles sont cryptées par la même lettre.

**4.** Démontrer que $a$ est premier avec 26 si et seulement si deux lettres distinctes sont cryptées par deux lettres distinctes.

### D. Un codage exponentiel

Les codages affines ne résistent pas longtemps aux spécialistes du cassage de codes. Voici un exemple plus ardu :
On affecte à chaque entier compris entre 0 et 28 une lettre de l'alphabet ou un autre symbole (par exemple on affecte A à 0, B à 1…, Z à 25, α à 26, β à 27, γ à 28) puis on fait subir à chacun de ces entiers $x$ la transformation $f$ suivante : $x \longmapsto y$, où $y$ est le reste de la division euclidienne par 29 de $x^3$.
On note $\mathfrak{E} = \{0, 1, 2\ldots, 28\}$.

*Questions* :

**1.** Coder la phrase J ADORE LES MATHS.

**2.** Calculer $3\times19 - 28\times2$. Qu'en déduit-on pour 3 et 28 ?

**3.** Soit $x$ et $x' \in \mathfrak{E}$ tels que $f(x) = f(x')$. Montrer que $x^{2\times28+1} \equiv (x')^{2\times28+1}$ (29).

En déduire avec le petit théorème de Fermat que $x = x'$ et donc que deux éléments distincts de $\mathfrak{E}$ ont deux images différentes par $f$.

**4.** Soit $x$ et $y$ éléments de $\mathfrak{E}$ tels que $y \equiv x^3$ (29). Montrer que $y^{19} \equiv x$ (29).

**5.** Décoder alors le mot RST AZDDT.

*Remarque* : ici, 3 est la clé de codage et 19 la clé de décodage.

*Réponses* :

*A-*

**1.** La clé de cryptage est 11. En effet, chaque lettre du message à crypter est remplacée par la troisième lettre qui la suit dans l'alphabet. La clé de décryptage est alors −11.

**2.** Voici le tableau représentant les fréquences des lettres utilisées dans le message codé :

| A | B | C | D | E | F | G | H | **I** | J | K | L | M |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 % | 0 % | 0,9 % | 0 % | 6,5 % | 0,9 % | 2,8 % | 2,8 % | **18,7 %** | 0 % | 0,9 % | 0 % | 5,6 % |
| N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| 0 % | 0 % | 8,4 % | 1,9 % | 7,5 % | 3,7 % | 3,7 % | 1,9 % | 6,5 % | 10,3 % | 10,3 % | 6,5 % | 0 % |

On constate que la lettre ayant la fréquence la plus élevée est la lettre I avec une fréquence de 18,7 %. On peut dès lors, penser que la lettre I code la lettre E du message initial. Si le codage est un chiffre de César, la clé de cryptage du code serait alors 4.
Voyons cela en essayant de décoder le texte à l'aide d'une clé de décryptage égale à –4 : on remplace les D par A, les E par B, etc. On trouve alors :

« *lorsque l on code un message en remplacant une lettre par une autre, il est possible de le decrypter en utilisant les statistiques* »

Le message est décodé…

*B-*

**1.** $\begin{pmatrix}-3 & 5 & 6\\ -1 & 2 & 2\\ 1 & -1 & -1\end{pmatrix}\begin{pmatrix}0 & 1 & 2\\ -1 & 3 & 0\\ 1 & -2 & 1\end{pmatrix}=\begin{pmatrix}0 & 1 & 2\\ -1 & 3 & 0\\ 1 & -2 & 1\end{pmatrix}\begin{pmatrix}-3 & 5 & 6\\ -1 & 2 & 2\\ 1 & -1 & -1\end{pmatrix}=\begin{pmatrix}1 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & 1\end{pmatrix}$.

La matrice $\begin{pmatrix}0 & 1 & 2\\ -1 & 3 & 0\\ 1 & -2 & 1\end{pmatrix}$ est donc la matrice inverse de la matrice $\begin{pmatrix}-3 & 5 & 6\\ -1 & 2 & 2\\ 1 & -1 & -1\end{pmatrix}$.

**2.** On trouve $\begin{pmatrix}-3 & 5 & 6\\ -1 & 2 & 2\\ 1 & -1 & -1\end{pmatrix}\begin{pmatrix}10 & 4 & 5 & 5 & 13 & 8\\ 27 & 15 & 27 & 19 & 1 & 19\\ 1 & 18 & 12 & 27 & 20 & 27\end{pmatrix}=\begin{pmatrix}111 & 171 & 192 & 242 & 86 & 233\\ 46 & 62 & 73 & 87 & 29 & 84\\ -18 & -29 & -34 & -41 & -8 & -38\end{pmatrix}$

Les colonnes de cette matrice, notée C, donnent le message codé. Celui-ci est transmis de la manière suivante : 111 46 −18 171 62 −29 192 73 −34 242 87 −41 86 29 −8 233 84 −38.

**3.** Pour décoder le message, le correspondant regroupe les valeurs par 3 et réécrit la matrice C trouvée à la question **1.**. Il calcule ensuite la matrice $M^{-1}\times C$ où $M^{-1}$ est l'inverse de la matrice M. Comme $C = M\times B$, on a $M^{-1}\times C = M^{-1}\times M\times B = B$ et on retrouve bien la matrice B. Il suffit alors de transformer les nombres en lettres et le tour est joué. La matrice $M^{-1}$ est la clé de décryptage.

*C-*

*Réponses* :

**1.**

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

J ADORE LES MATHS est codé en I HQXGT OTJ RHMCJ.

**2.** MOI AUSSI.

**3.** $2\times0 + 7 \equiv 7\ (26)$ donc A est codé par H.
$2\times13 + 7 \equiv 7\ (26)$ donc N est aussi codé par H.

**4.** Supposons que $a$ soit premier avec 26 : soient $x$ et $x$' les nombres associés aux deux lettres distinctes. On a donc $x \neq x$'. Montrons alors que $y \neq y$'. De manière logique, cela revient à montrer que si $y = y$' alors $x = x$'. Allons-y.
$y = y' \Leftrightarrow ax + b \equiv ax' + b\ (26) \Leftrightarrow a(x - x') \equiv 0\ (26) \Leftrightarrow 26$ divise $a(x - x')$.
Or 26 et $a$ sont premiers entre eux, donc par le théorème de Gauss, 26 divise $(x - x')$ **(1)**. Comme $0 \leqslant x < 26$ et $0 \leqslant x' < 26$, on a $-26 < x - x' < 26$ **(2)**.
Les conditions **(1)** et **(2)** impliquent que $x = x'$.
« $a$ premier avec 26 » est donc bien une condition suffisante pour qu'à deux lettres distinctes correspondent deux lettres codées distinctes.

Réciproquement, supposons que $a$ ne soit pas premier avec 26.
Soit $d$ le PGCD de $a$ et 26. On a $d > 1$. $d$ divise 26 donc il existe $k$ entier tel que $26 = kd$. De même $d$ divise $a$ donc il existe $k$' tel que : $a = k'd$.
$k$ est un entier non nul et strictement inférieur à 26. Soit Φ la lettre dont l'équivalent numérique est $k$.
Montrons alors que A et Φ, qui sont deux lettres distinctes, sont codées par la même lettre : comme le numéro de A est 0, il suffit de montrer que $ak + b \equiv a\times0 + b \equiv b\ (26)$.
Or $ak + b \equiv k'dk + b \equiv 26\,k' + b \equiv b\ (26)$. OK !
« $a$ premier avec 26 » est donc bien une condition nécessaire pour qu'à deux lettres distinctes correspondent deux lettres codées distinctes.

*D-*

**1.** J a pour rang 9. $9^3 = 729$ et $729 = 25\times29 + 4$. La lettre de rang 4 est E donc J est codé par E.
En faisant de même avec toutes les lettres on trouve E AβSMG αGD RAPYD.
(À la calculatrice, pour avoir le reste de la division euclidienne de $x^3$ par 29, on tape $x^3 - 29\times\text{Partie entière}\left(\frac{x^3}{29}\right)$).

**2.** $3\times19 - 28\times2 = 1$. On en déduit par le théorème de Bézout que 3 et 28 sont premiers entre eux.

**3.** $f(x) = f(x') \Leftrightarrow x^3 \equiv x'^3\ (29) \Rightarrow (x^3)^{19} \equiv (x'^3)^{19}\ (29)$
$\Rightarrow x^{3\times19} \equiv x'^{3\times19}\ (29)$
$\Rightarrow x^{2\times28+1} \equiv (x')^{2\times28+1}\ (29)$ car $3\times19 - 28\times2 = 1$
$\Rightarrow x\,(x^{28})^2 \equiv x'\,(x'^{28})^2\ (29)$
Or 29 est premier et $x$ et $x$' sont premiers avec 29 donc par le petit théorème de Fermat, $x^{28} \equiv 1\ (29)$, $x'^{28} \equiv 1\ (29)$. On a donc :
$f(x) = f(x') \Rightarrow x\,(1)^2 \equiv x'\,(1)^2\ (29)$
$\Rightarrow x \equiv x'\ (29)$
$\Rightarrow x = x'$ car $x$ et $x$' sont deux entiers naturels inférieurs à 29.

**4.** $y \equiv x^3\ (29)$ donc $y^{19} \equiv (x^3)^{19} \equiv x\ (29)$ (voir question précédente).

**5.** Le rang de R est 17. On trouve $\left(17^{19} - 29\times\text{Partie entière}\left(\frac{17^{19}}{29}\right)\right) = 12$ avec une bonne calculatrice. La lettre de rang 12 est M. En procédant de même pour les autres lettres on trouve MOI AUSSI.