

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
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

I. Version bigraphique : regroupement par blocs de 2

A. Première clé

a) $A = \begin{pmatrix} 2 & 5 \\ 1 & 3 \end{pmatrix}$. On pose $B = \begin{pmatrix} 8 \\ 13 \end{pmatrix}$, $C = \begin{pmatrix} 3 \\ 8 \end{pmatrix}$ et $D = \begin{pmatrix} 2 \\ 4 \end{pmatrix}$.

$$AB = \begin{pmatrix} 81 \\ 47 \end{pmatrix} \quad AC = \begin{pmatrix} 46 \\ 27 \end{pmatrix} \quad AD = \begin{pmatrix} 24 \\ 14 \end{pmatrix}$$

$$81 = 26 \times 3 + 3 \quad 46 = 26 \times 1 + 20$$

$$47 = 26 \times 1 + 21 \quad 27 = 26 \times 1 + 1$$

Donc $\begin{pmatrix} I \\ N \end{pmatrix}$, $\begin{pmatrix} D \\ I \end{pmatrix}$, $\begin{pmatrix} C \\ E \end{pmatrix}$ donne $\begin{pmatrix} 3 \\ 21 \end{pmatrix}$, $\begin{pmatrix} 20 \\ 1 \end{pmatrix}$, $\begin{pmatrix} 24 \\ 14 \end{pmatrix}$.

b) INDICE est chiffré en **DVUBYO**.

c) $A^{-1} = \begin{pmatrix} 3 & -5 \\ -1 & 2 \end{pmatrix}$.

On pose $E = \begin{pmatrix} 3 \\ 21 \end{pmatrix}$, $F = \begin{pmatrix} 20 \\ 1 \end{pmatrix}$ et $G = \begin{pmatrix} 24 \\ 14 \end{pmatrix}$.

$$A^{-1} \times E = \begin{pmatrix} -96 \\ 39 \end{pmatrix} \equiv \begin{pmatrix} 8 \\ 13 \end{pmatrix} [26] \quad (\text{exemple de calcul : } -96 = 26 \times (-4) + 8)$$

$$\text{De même } A^{-1} \times F = \begin{pmatrix} 55 \\ -18 \end{pmatrix} \equiv \begin{pmatrix} 3 \\ 8 \end{pmatrix} [26] \quad \text{et } A^{-1} \times G = \begin{pmatrix} 2 \\ 4 \end{pmatrix}.$$

On retrouve bien le mot **INDICE**.

B. Deuxième clé

1. a) $9 \times 7 - 5 \times 4 = 43$ et $43 \neq 0$ donc **A est inversible**.

$$A = \begin{pmatrix} 9 & 5 \\ 4 & 7 \end{pmatrix} \quad A^{-1} = \begin{pmatrix} \frac{7}{43} & -\frac{5}{43} \\ -\frac{4}{43} & \frac{9}{43} \end{pmatrix} = \frac{1}{43} \begin{pmatrix} 7 & -5 \\ -4 & 9 \end{pmatrix} \quad \text{d'après la calculatrice.}$$

On pose donc $B = \begin{pmatrix} 7 & -5 \\ -4 & 9 \end{pmatrix}$.

b) $\frac{1}{43}$ apparaît dans la matrice A^{-1} , donc en calculant $A^{-1}Y$, **on n'obtiendra pas des entiers...**

2. Recherche de l'inverse de 43 modulo 26

a) $X = \frac{1}{43} BY$ donc $43mX = 43m \frac{1}{43} BY$ ie $43mX = mBY$.

Or, $43m \equiv 1 [26]$ donc $43mX \equiv X [26]$ ie $mBY \equiv X [26]$.

Ce qui nous permet donc de **décoder Y en calculant mBY**.

b) $43 = 26 \times 1 + 17$

$$26 = 17 \times 1 + 9$$

$$17 = 9 \times 1 + 8$$

$$9 = 8 \times 1 + 1$$

$$8 = 1 \times 8 + 0$$

donc d'après l'algorithme d'Euclide : $\text{PGCD}(43; 26) = 1$.

43 et 26 sont premiers entre eux, donc d'après le théorème de Bézout : **(E) admet au moins une solution**.

c) Existence

D'après la question précédente, on sait qu'il existe un entier relatif x tel que $43x \equiv 1 [26]$.

• Si $x > 25$ ou $x < 0$, alors $x = 26k + r$ (division euclidienne) avec $0 \leq r \leq 25$.

On pose $m = r$ et on a donc $43m \equiv 1 [26]$.

• Si $0 \leq x \leq 25$, il suffit de poser $m = x$.

Donc il existe un entier m tel que $0 \leq m \leq 25$ et $43m \equiv 1 [26]$.

Unicité

S'il existe deux entiers distincts m et m' tels que $0 \leq m \leq 25$, $43m \equiv 1 [26]$, $0 \leq m' \leq 25$ et $43m' \equiv 1 [26]$, alors :

$43(m - m') \equiv 0 [26]$ ie $26 \mid 43(m - m')$. Or 26 et 43 sont premiers entre eux, donc d'après le théorème de Gauss, $26 \mid m - m'$. Or $-25 \leq m - m' \leq 25$ donc ceci est impossible...

Conclusion : **il existe un unique entier m tel que $0 \leq m \leq 25$ et $43m \equiv 1 [26]$.**

On pose $a = 43$ et $b = 26$:

$$43 = 26 \times 1 + 17 \quad 17 = a - b$$

$$26 = 17 \times 1 + 9 \quad 9 = -a + 2b$$

$$17 = 9 \times 1 + 8 \quad 8 = 2a - 3b$$

$$9 = 8 \times 1 + 1 \quad 1 = -3a + 5b$$

$$8 = 1 \times 8 + 0$$

On a donc (coefficients de Bézout) : $-3 \times 43 + 5 \times 26 = 1$.

$x = -3$ et $-3 = 26 \times (-1) + 23$ donc on trouve **$m = 23$** .

d) $\begin{pmatrix} H \\ T \end{pmatrix}$, $\begin{pmatrix} P \\ Q \end{pmatrix}$ et $\begin{pmatrix} M \\ K \end{pmatrix}$ correspondent à $\begin{pmatrix} 7 \\ 19 \end{pmatrix}$, $\begin{pmatrix} 15 \\ 16 \end{pmatrix}$ et $\begin{pmatrix} 12 \\ 10 \end{pmatrix}$.

Remarque : on peut vérifier facilement que INDICE était bien codé en HTPQMK

$$K = \begin{pmatrix} 8 \\ 13 \end{pmatrix} \quad L = \begin{pmatrix} 3 \\ 8 \end{pmatrix} \quad M = \begin{pmatrix} 2 \\ 4 \end{pmatrix} \quad A = \begin{pmatrix} 9 & 5 \\ 4 & 7 \end{pmatrix}$$

$$AK = \begin{pmatrix} 137 \\ 123 \end{pmatrix} \equiv \begin{pmatrix} 7 \\ 19 \end{pmatrix} [26] \text{ car } 137 = 26 \times 5 + 7 \text{ et } 123 = 26 \times 4 + 19$$

$$\text{De la même manière : } AL = \begin{pmatrix} 67 \\ 68 \end{pmatrix} \equiv \begin{pmatrix} 15 \\ 16 \end{pmatrix} [26] \text{ et } AM = \begin{pmatrix} 38 \\ 36 \end{pmatrix} \equiv \begin{pmatrix} 12 \\ 10 \end{pmatrix} [26]$$

INDICE est donc bien codé en HTPQMK.

$$B = \begin{pmatrix} 7 & -5 \\ -4 & 9 \end{pmatrix}$$

• Si $Y = \begin{pmatrix} 7 \\ 19 \end{pmatrix}$ alors $BY = \begin{pmatrix} -46 \\ 143 \end{pmatrix}$ (à faire)

$$23BY = \begin{pmatrix} -1058 \\ 3289 \end{pmatrix} \equiv \begin{pmatrix} 8 \\ 13 \end{pmatrix} [26] \text{ car } -1058 = 26 \times (-41) + 8 \text{ et } 3289 = 26 \times 126 + 13$$

• Si $Y = \begin{pmatrix} 15 \\ 16 \end{pmatrix}$ alors $BY = \begin{pmatrix} 25 \\ 84 \end{pmatrix}$ (à faire)

$$23BY = \begin{pmatrix} 575 \\ 1932 \end{pmatrix} \equiv \begin{pmatrix} 3 \\ 8 \end{pmatrix} [26] \text{ car } 575 = 26 \times 22 + 3 \text{ et } 1932 = 26 \times 74 + 8$$

• Si $Y = \begin{pmatrix} 12 \\ 10 \end{pmatrix}$ alors $BY = \begin{pmatrix} 84 \\ -48 \end{pmatrix}$ (à faire)

$$23BY = \begin{pmatrix} 782 \\ 966 \end{pmatrix} \equiv \begin{pmatrix} 2 \\ 4 \end{pmatrix} [26] \text{ car } 782 = 26 \times 30 + 2 \text{ et } 966 = 26 \times 37 + 4$$

En décodant HTPQMK, on retrouve bien le mot INDICE.

C. Cas général : clés possibles

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

1. Condition nécessaire

À un couple Y ne doit correspondre qu'un seul couple X , afin de déchiffrer le message sans ambiguïté.

Or, $AX = Y$ admet une unique solution si, et seulement si, A est inversible.

Il est donc nécessaire que la matrice A soit inversible, c'est-à-dire que :

$$ad - bc \neq 0$$

2. Condition suffisante

a) 43 et 26 étaient premiers entre eux. Cela a permis le déchiffrement.

b) (on va reprendre ici la question B.2. en changeant 43 par $ad - bc$...)

Si $ad - bc$ et 26 sont premiers entre eux :

Existence

D'après la question précédente, on sait qu'il existe un entier relatif x tel que $ad - bc x \equiv 1 [26]$.

• Si $x > 25$ ou $x < 0$, alors $x = 26k + r$ (division euclidienne) avec $0 \leq r \leq 25$.

On pose $m = r$ et on a donc $(ad - bc)m \equiv 1 [26]$.

• Si $0 \leq x \leq 25$, il suffit de poser $m = x$.

Donc il existe un entier m tel que $0 \leq m \leq 25$ et $(ad - bc)m \equiv 1 [26]$.

Unicité

S'il existe deux entiers distincts m et m' tels que $0 \leq m \leq 25$, $(ad - bc)m \equiv 1 [26]$, $0 \leq m' \leq 25$ et $(ad - bc)m' \equiv 1 [26]$, alors :

$(ad - bc)(m - m') \equiv 0 [26]$ ie $26 \mid (ad - bc)(m - m')$. Or 26 et $ad - bc$ sont premiers entre eux, donc d'après le théorème de Gauss, $26 \mid m - m'$. Or $-25 \leq m - m' \leq 25$ donc ceci est impossible...

Conclusion : il existe un unique entier m tel que $0 \leq m \leq 25$ et $(ad - bc)m \equiv 1 [26]$.

Rappel : $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ donc $A^{-1} = \frac{1}{ad-bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$ (cours)

II. Version trigraphique : regroupement par blocs de 3

On souhaite coder la phrase « codage de hill ».

Le texte à coder est découpé en blocs successifs de trois lettres :

$$\begin{pmatrix} C \\ O \\ D \end{pmatrix}, \begin{pmatrix} A \\ G \\ E \end{pmatrix}, \begin{pmatrix} D \\ E \\ H \end{pmatrix}, \begin{pmatrix} I \\ L \\ L \end{pmatrix}$$

soit

$$\begin{pmatrix} 2 \\ 14 \\ 3 \end{pmatrix}, \begin{pmatrix} 0 \\ 6 \\ 4 \end{pmatrix}, \begin{pmatrix} 3 \\ 4 \\ 6 \end{pmatrix}, \begin{pmatrix} 8 \\ 11 \\ 11 \end{pmatrix}.$$

On se donne pour clé de chiffrement la matrice $A = \begin{pmatrix} 1 & 2 & 3 \\ 9 & 7 & 4 \\ 8 & 6 & 5 \end{pmatrix}$.

$$1. A = \begin{pmatrix} 1 & 2 & 3 \\ 9 & 7 & 4 \\ 8 & 6 & 5 \end{pmatrix}$$

$$B = \begin{pmatrix} 2 \\ 14 \\ 3 \end{pmatrix} \quad AB = \begin{pmatrix} 39 \\ 128 \\ 115 \end{pmatrix} \equiv \begin{pmatrix} 13 \\ 24 \\ 11 \end{pmatrix} \quad [26]$$

$$C = \begin{pmatrix} 0 \\ 6 \\ 4 \end{pmatrix} \quad AC = \begin{pmatrix} 24 \\ 58 \\ 56 \end{pmatrix} \equiv \begin{pmatrix} 24 \\ 6 \\ 4 \end{pmatrix} \quad [26]$$

$$D = \begin{pmatrix} 3 \\ 4 \\ 6 \end{pmatrix} \quad AD = \begin{pmatrix} 29 \\ 79 \\ 78 \end{pmatrix} \equiv \begin{pmatrix} 3 \\ 1 \\ 0 \end{pmatrix} \quad [26]$$

$$E = \begin{pmatrix} 8 \\ 11 \\ 11 \end{pmatrix} \quad AE = \begin{pmatrix} 63 \\ 193 \\ 185 \end{pmatrix} \equiv \begin{pmatrix} 11 \\ 11 \\ 3 \end{pmatrix} \quad [26]$$

CODAGEDEHILL est donc codé en NYLYGEDBALLD.

2. a) Déterminer l'inverse de la matrice A, sous la forme $\frac{1}{21} B$.

$$A^{-1} = \begin{pmatrix} -\frac{11}{21} & -\frac{8}{21} & \frac{13}{21} \\ \frac{13}{21} & \frac{19}{21} & -\frac{23}{21} \\ \frac{2}{21} & -\frac{10}{21} & \frac{11}{21} \end{pmatrix} = \frac{1}{21} \begin{pmatrix} -11 & -8 & 13 \\ 13 & 19 & -23 \\ 2 & -10 & 11 \end{pmatrix}.$$

b) On cherche m tel que $21m \equiv 1 \pmod{26}$.

On peut tester quelques nombres avec la calculatrice, on trouve rapidement $m=5$.

En effet, $21 \times 5 = 105$ et $105 = 26 \times 4 + 1$.

Autre méthode, si on ne trouve pas rapidement ou si on n'a pas d'algorithme qui fait « le job » :

$$26 = 21 \times 1 + 5$$

$$21 = 5 \times 4 + 1 \quad (\text{algorithme d'Euclide})$$

$$5 = 1 \times 5 + 0$$

Coefficients de Bézout :

$$5 = 26 - 21 \times 1$$

$$1 = 21 - 5 \times 4$$

$$1 = 21 - (26 - 21) \times 4$$

$$1 = 26 \times (-4) + 21 \times 5$$

Donc $21 \times 5 \equiv 1 \pmod{26}$: l'inverse de 21 modulo 26 est 5.

c) La clé de déchiffrement est $5A^{-1}$.

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 9 & 7 & 4 \\ 8 & 6 & 5 \end{pmatrix} \quad A^{-1} = \begin{pmatrix} -\frac{11}{21} & -\frac{8}{21} & \frac{13}{21} \\ \frac{13}{21} & \frac{19}{21} & -\frac{23}{21} \\ \frac{2}{21} & -\frac{10}{21} & \frac{11}{21} \end{pmatrix} \quad 5A^{-1} = \begin{pmatrix} -\frac{55}{21} & -\frac{40}{21} & \frac{65}{21} \\ \frac{65}{21} & \frac{95}{21} & -\frac{115}{21} \\ \frac{10}{21} & -\frac{50}{21} & \frac{55}{21} \end{pmatrix}$$

$$A^{-1} = \begin{pmatrix} -\frac{11}{21} & -\frac{8}{21} & \frac{13}{21} \\ \frac{13}{21} & \frac{19}{21} & -\frac{23}{21} \\ \frac{2}{21} & -\frac{10}{21} & \frac{11}{21} \end{pmatrix} = \frac{1}{21} \begin{pmatrix} -11 & -8 & 13 \\ 13 & 19 & -23 \\ 2 & -10 & 11 \end{pmatrix}$$

$$B = 21A^{-1} = \begin{pmatrix} -11 & -8 & 13 \\ 13 & 19 & -23 \\ 2 & -10 & 11 \end{pmatrix}$$

En déchiffrant RCJZJKHFTYYG, on trouve **MATHEMATHIEU**.

Exemple de calcul pour RCJ :

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 9 & 7 & 4 \\ 8 & 6 & 5 \end{pmatrix} \quad C = \begin{pmatrix} 17 \\ 2 \\ 9 \end{pmatrix} \quad 5 \times 21A^{-1}C = \begin{pmatrix} -430 \\ 260 \\ 565 \end{pmatrix} \equiv \begin{pmatrix} 12 \\ 0 \\ 19 \end{pmatrix} \pmod{26} \rightarrow \begin{pmatrix} M \\ A \\ T \end{pmatrix}.$$

Ps : j'espère que vous avez eu l'intelligence de faire un algorithme pour faire tous ces calculs, sinon vous avez dû y passer du temps :-)