Le chiffre de Hill : correction

Partie A

Le mot « SI » est assimilé à la matrice $X = \begin{pmatrix} 18 \\ 8 \end{pmatrix}$

$U = AX = \begin{pmatrix} 4 & 1 \\ 3 & 2 \end{pmatrix} \times \begin{pmatrix} 18 \\ 8 \end{pmatrix} = \begin{pmatrix} 80 \\ 70 \end{pmatrix}$

$C = \begin{pmatrix} 2 \\ 18 \end{pmatrix}$

Le mot « SI » est donc codé « CS »

Partie B : deux résultats mathématiques

1. $5 \times 21 = 105 = 4 \times 26 + 1$
   D'où $5 \times 21 \equiv 1$ modulo 26.
2. a. $B \times A = \begin{pmatrix} 2 & -1 \\ -3 & 4 \end{pmatrix} \times \begin{pmatrix} 4 & 1 \\ 3 & 2 \end{pmatrix} = \begin{pmatrix} 5 & 0 \\ 0 & 5 \end{pmatrix} = 5I$

   b. On sait que $B \times A = 5I$.
   Donc si on a $AX = U$, alors
   $BAX = BU$
   $5IX = BU$
   $5X = BU$

Partie C : décodage d'un *mot*

1. On sait d'après la question **B. 2.** que $5X = BU$, autrement dit que :
   $5\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 2 & -1 \\ -3 & 4 \end{pmatrix} \times \begin{pmatrix} u \\ v \end{pmatrix}$
   soit
   $\begin{pmatrix} 5x \\ 5y \end{pmatrix} = \begin{pmatrix} 2u - v \\ -3u + 4v \end{pmatrix}$
   que l'on peut écrire : $\left\{\begin{array}{lcl} 5x & = & 2u - v \\ 5y & = & -3u + 4v \end{array}\right.$.
   Or $\left\{\begin{array}{lcl} u & \equiv & 1 \text{ modulo } 26 \\ v & \equiv & 4 \text{ modulo } 26 \end{array}\right.$
   Donc $\left\{\begin{array}{lcl} 5x & \equiv & 2 \times 1 - 4 \text{ modulo } 26 \\ 5y & \equiv & -3 \times 1 + 4 \times 4 \text{ modulo } 26 \end{array}\right.$.
   On a bien $\left\{\begin{array}{lcl} 5x & \equiv & -2 \text{ modulo } 26 \\ 5y & \equiv & 13 \text{ modulo } 26 \end{array}\right.$.

2. On a montré à la question **B. 1** que $5 \times 21 \equiv 1$ modulo 26. Donc en multipliant à gauche et à droite par 21 dans les équations précédentes :
   $\left\{\begin{array}{lcl} 21 \times 5x & \equiv & -2 \times 21 \text{ modulo } 26 \\ 21 \times 5y & \equiv & 13 \times 21 \text{ modulo } 26 \end{array}\right.$.
   ce qui donne :
   $\left\{\begin{array}{lcl} x & \equiv & -42 \text{ modulo } 26 \\ y & \equiv & 273 \text{ modulo } 26 \end{array}\right.$.
   et on a bien :
   $\left\{\begin{array}{lcl} x & \equiv & 10 \text{ modulo } 26 \\ y & \equiv & 13 \text{ modulo } 26 \end{array}\right.$.
   Le *mot* « BE » se décode donc « KN ».