

**Partie A : préliminaires**

1. (a)  $n^2 \equiv N - 1 \pmod{N} \Rightarrow (n^2)^2 \equiv (N - 1)^2 \pmod{N}$   
 Or  $(N - 1)^2 = N^2 - 2N + 1$  et  $N^2 \equiv 0 \pmod{N}$  et  $-2N \equiv 0 \pmod{N}$ , donc  
 $(N - 1)^2 \equiv 1 \pmod{N}$  et finalement car  $n^4 = n \times n^3$ ,  
 $n \times n^3 \equiv 1 \pmod{N}$ .
- (b) On a  $5^2 = 25 = 26 - 1$ , donc  $5^2 \equiv -1 \pmod{26}$ .  
 La question précédente montre que  $5 \times 5^3 \equiv 1 \pmod{26}$ .  
 Donc  $k_1 = 5^3 = 125$ .
2. (a)  $6A = \begin{pmatrix} 24 & 6 \\ 18 & 12 \end{pmatrix}$  et  $A^2 = \begin{pmatrix} 19 & 6 \\ 18 & 7 \end{pmatrix}$ , donc  $6A - A^2 = \begin{pmatrix} 5 & 0 \\ 0 & 5 \end{pmatrix} = 5I$  ( $I$  matrice unité).
- (b) On a  $6A - A^2 = A(6I - A) = 5I$  ou encore  $A \times \frac{1}{5}(6I - A) = I$  : cette égalité montre que la matrice  $A$  est inversible et que son inverse est  
 $A^{-1} = \frac{1}{5}(6I - A) = \frac{6}{5}I - \frac{1}{5}A$ .
- (c)  $A^{-1} = \frac{6}{5}I - \frac{1}{5}A \iff 5A^{-1} = 6I - A = \begin{pmatrix} 2 & -1 \\ -3 & 4 \end{pmatrix} = B$ .  
 Conclusion  $B = 5A^{-1}$ .
- (d) En partant de l'égalité précédente :  
 $B = 5A^{-1} \iff BA = 5A^{-1}A \iff BA = 5I \iff BAX = 5IX \iff$   
 $BY = 5X$ .

**Partie B : procédure de codage**

Coder le mot ET , en utilisant la procédure de codage décrite ci-dessous.

ET est codé par la matrice  $X = \begin{pmatrix} 4 \\ 19 \end{pmatrix}$ .

Puis  $Y = AX = \begin{pmatrix} 35 \\ 50 \end{pmatrix}$ , puis  $R = \begin{pmatrix} 9 \\ 24 \end{pmatrix}$  et d'après le tableau ET est codé JY

**Partie C : procédure de décodage**

Lors du codage, la matrice  $X$  a été transformée en la matrice  $Y = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$  telle que :  
 $Y = AX$ .

1. On a  $Y = AX \iff A^{-1}Y = X \iff 5A^{-1}Y = 5X = BY$  soit  $Y = AX \iff$   

$$\begin{cases} 5x_1 = 2y_1 - y_2 \\ 5x_2 = -3y_1 + 4y_2 \end{cases}$$

2. La question 1. b. de la **partie A** a montré que  $5 \times 21 \equiv 1$  modulo 26. Donc en reprenant le système de la question précédente et en multipliant par 21, on obtient :

$$\begin{cases} 21 \times 5x_1 = 21 \times (2y_1 - y_2) \\ 21 \times 5x_2 = 21 \times (-3y_1 + 4y_2) \end{cases} \iff \begin{cases} 21 \times 5x_1 = 42y_1 - 21y_2 \\ 21 \times 5x_2 = -63y_1 + 84y_2 \end{cases} \iff \begin{cases} x_1 \equiv 16y_1 \\ x_2 \equiv 15y_1 \end{cases}$$

3. QP est associé à la matrice  $\begin{pmatrix} 16 \\ 15 \end{pmatrix}$ .

En utilisant le résultat précédent :

$$\begin{cases} x_1 \equiv 16y_1 + 5y_2 \pmod{26} \\ x_2 \equiv 15y_1 + 6y_2 \pmod{26} \\ x_1 = 19 \\ x_2 = 18 \end{cases} \iff \begin{cases} x_1 \equiv 256 + 75 \pmod{26} \\ x_2 \equiv 240 + 90 \pmod{26} \end{cases} \iff \begin{cases} x_1 \equiv 331 \\ x_2 \equiv 330 \end{cases}$$

Le mot décodé est donc TS