1. On trouve : EIROGAYDGWOY.
2. L'impératif premier d'une quelconque méthode de chiffrement est que ce chiffrement soit réversible, c'est-à-dire au moins que deux messages ne peuvent donner le même message codé. Avec la première matrice, tout message devient une succession de A : impossible de retrouver le message initial. Avec la seconde matrice, les messages AA et CZ sont codés tous les deux par AA : même conclusion!
3. On trouve : $AB = (\det A)I_2$, où I_2 est la matrice unité 2×2.
4. Si $\det A$ est inversible dans $\mathbb{Z}|26\mathbb{Z}$, alors l'inverse de B est donné par $(\det A)^{-1}B$, où B est la matrice précédente.
   Réciproquement, si A est inversible, on a $AC = I_2$ pour une certaine matrice C. Mais alors, $\det A \det C = 1$, et $\det A$ est inversible dans $\mathbb{Z}|26\mathbb{Z}$.
   Si cette condition est réalisée, le chiffrement de Hill est alors inversible : en effet, l'égalité
   $$\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = A \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$$
   s'inverse en
   $$\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = A^{-1} \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}.$$
5. Le déterminant de la matrice est 43. Ce nombre est premier avec 26, et est donc inversible dans $\mathbb{Z}|26\mathbb{Z}$. On calcule son inverse par n'importe quelle méthode, comme par exemple l'algorithme d'Euclide. On trouve que son inverse est 23 dans $\mathbb{Z}|26\mathbb{Z}$, et la matrice inverse de A est :
   $$A^{-1} = \begin{pmatrix} 5 & 12 \\ 15 & 25 \end{pmatrix}.$$
   Il suffit de réappliquer la formule de la question précédente. Le message clair est ASSAUTDEMAIN.
6. (a) Le premier bloc du texte clair est $\begin{pmatrix} 12 \\ 14 \end{pmatrix}$, et il codé par la matrice A en $\begin{pmatrix} 24 \\ 10 \end{pmatrix}$. De même pour le deuxième bloc. Les règles du produit matriciel donnent le résultat.
   (b) Il suffirait que la matrice $\begin{pmatrix} 12 & 13 \\ 14 & 6 \end{pmatrix}$ soit inversible, pour déterminer complètement A. Mais son déterminant est -110, qui est un nombre pair et n'est donc pas premier avec 26.
   (c) On a aussi, en exploitant le deuxième et le troisième bloc :
   $$\begin{pmatrix} 19 & 25 \\ 25 & 20 \end{pmatrix} = A \begin{pmatrix} 13 & 4 \\ 6 & 13 \end{pmatrix}.$$
   Le déterminant de la matrice de droite est 145, qui est inversible dans $\mathbb{Z}|26\mathbb{Z}$. On calcule l'inverse de cette matrice, et on trouve :
   $$A = \begin{pmatrix} 19 & 25 \\ 25 & 20 \end{pmatrix} \begin{pmatrix} 13 & 24 \\ 10 & 13 \end{pmatrix} = \begin{pmatrix} 3 & 1 \\ 5 & 2 \end{pmatrix}.$$
   (d) MONGENERALSOUSMARINENNEMIREPEREZ (le Z n'est pas une faute d'orthographe, mais un moyen de compléter le message pour qu'il y ait un nombre pair de lettres!).