Chapter 2 Exercise 14

solved → GEZXDS using a Hill cipher with a 2x2 matrix M. So, first break the word solved into 2-vectors that can be multiplied by M.

solved = (18,14),(11,21),(4,3)

Say M = $\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}$

So, for example $\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \begin{bmatrix} 18 \\ 14 \end{bmatrix} = \begin{bmatrix} 6 \\ 4 \end{bmatrix}$

Then, using 2 systems of equations we can solve for M.

$11\alpha + 21\beta \equiv 25 \pmod{26}$

$\underline{4\alpha + 3\beta \equiv 3 \pmod{26}}$

$17\alpha \equiv -4 \pmod{26}$

$\alpha \equiv 12 \pmod{26}$

Thus,

$\beta \equiv 11 \pmod{26}$

$18\gamma + 14\delta \equiv 4 \pmod{26}$

$\underline{11\gamma + 21\delta \equiv 23 \pmod{26}}$

$-20\gamma \equiv -8 \pmod{26}$

$\gamma \equiv 3 \pmod{26}$

$\delta \equiv 2 \pmod{26}$

So, M = $\begin{bmatrix} 12 & 11 \\ 3 & 2 \end{bmatrix}$.

AN EASIER APPROACH: USE MATRICES AS A SUBSTITUTE FOR THE ABOVE CALCULATION WITH LINEAR EQUATIONS.

$\begin{pmatrix} 18 & 14 \\ 11 & 21 \\ 4 & 3 \end{pmatrix} \boldsymbol{M} \equiv \begin{pmatrix} 6 & 4 \\ 25 & 23 \\ 3 & 18 \end{pmatrix}$ (mod 26). We want to cut $\begin{pmatrix} 18 & 14 \\ 11 & 21 \\ 4 & 3 \end{pmatrix}$ down to an invertible 2 x 2 matrix (i.e., one with determinant invertible (mod 26)). Now $\begin{pmatrix} 18 & 14 \\ 11 & 21 \end{pmatrix}$ is not invertible because its determinant is not relatively prime to 26. However we can compute

$\begin{pmatrix} 11 & 21 \\ 4 & 3 \end{pmatrix}^{-1} \equiv (1)^{-1} \begin{pmatrix} 3 & -21 \\ -4 & 11 \end{pmatrix} \equiv \begin{pmatrix} 3 & 5 \\ 22 & 11 \end{pmatrix}$ (mod 26), and so solving the matrix equation

$\begin{pmatrix} 11 & 21 \\ 4 & 3 \end{pmatrix} \boldsymbol{M} \equiv \begin{pmatrix} 25 & 23 \\ 3 & 18 \end{pmatrix}$ (mod 26) we have $\boldsymbol{M} \equiv \begin{pmatrix} 11 & 21 \\ 4 & 3 \end{pmatrix}^{-1} \begin{pmatrix} 25 & 23 \\ 3 & 18 \end{pmatrix} \equiv \begin{pmatrix} 3 & 5 \\ 22 & 11 \end{pmatrix} \begin{pmatrix} 25 & 23 \\ 3 & 18 \end{pmatrix} \equiv \begin{pmatrix} 12 & 3 \\ 11 & 2 \end{pmatrix}$ (mod 26).

[This is the transpose of the matrix found above because we used <u>row</u> vectors for plaintext.]