EXAMPLE 2. (Similar to example 1, but with a plaintext leading to a not-invertible matrix.)

We know that the first four letters of the ciphertext starting with WKNCCHSSJH decipher as “give” and that a block code (mod 26) is being used. We try to find the NxN deciphering matrix \( \mathbf{D} \) starting with \( N=2, N=3, \) etc.

The information that WKNC deciphers to give leads to the matrix equation:

\[
\begin{pmatrix} 22 & 10 \\ 13 & 2 \end{pmatrix} \mathbf{D} \equiv \begin{pmatrix} 6 & 8 \\ 21 & 4 \end{pmatrix} \pmod{26}.
\]

Now \( \det \begin{pmatrix} 22 & 10 \\ 13 & 2 \end{pmatrix} = -86 \equiv 18 \pmod{26}, \) so \( \begin{pmatrix} 22 & 10 \\ 13 & 2 \end{pmatrix} \) is not invertible (mod 26). We therefore view this matrix equation (mod 13) and use \( \mathbf{A} \) to denote a matrix \( \mathbf{A} \) reduced (mod 13). We get

\[
\begin{pmatrix} 22 & 10 \\ 13 & 2 \end{pmatrix} \mathbf{D} \equiv \begin{pmatrix} 6 & 8 \\ 21 & 4 \end{pmatrix} \pmod{13}, \text{ or } \begin{pmatrix} 9 & 10 \\ 0 & 2 \end{pmatrix} \mathbf{D} \equiv \begin{pmatrix} 6 & 8 \\ 8 & 4 \end{pmatrix} \pmod{13}.
\]

Now

\[
\det \begin{pmatrix} 9 & 10 \\ 0 & 2 \end{pmatrix} = 5 \pmod{13}, \text{ so } \begin{pmatrix} 9 & 10 \\ 0 & 2 \end{pmatrix} \text{ is invertible (mod 13) with inverse matrix}
\]

\[
5^{-1} \begin{pmatrix} 2 & -10 \\ 0 & 9 \end{pmatrix} = \begin{pmatrix} 2 & 3 \\ 0 & 7 \end{pmatrix} \equiv \begin{pmatrix} 3 & 11 \\ 0 & 7 \end{pmatrix} \pmod{13}, \text{ and}
\]

\[
\mathbf{D} = \begin{pmatrix} 22 & 10 \\ 13 & 2 \end{pmatrix} \begin{pmatrix} 3 & 11 \\ 0 & 7 \end{pmatrix} \equiv \begin{pmatrix} 2 & 3 \\ 4 & 2 \end{pmatrix} \pmod{13}.
\]

Since the entries of \( \mathbf{D} \) (mod 26) must reduce to the entries of \( \mathbf{D} \) (mod 13) (e.g., the (1,1)-entry of \( \mathbf{D} \) can be either 2 or 15 (mod 26), etc.), we have 8 possible values for \( \mathbf{D} \) and we can write \( \mathbf{D} \) in the form

\[
\mathbf{D} = \begin{pmatrix} 2 & 3 \\ 4 & 2 \end{pmatrix} + 13\mathbf{C}
\]

where \( \mathbf{C} \) is a matrix whose entries are 0s and 1s. There are 16 possibilities for \( \mathbf{C} \). However, we can reduce the number of possibilities by using the fact that a block code (normally) has an invertible enciphering matrix; i.e., the determinant of \( \mathbf{D} \) must be relatively prime to 26, and in particular is odd.

Of the 16 possible choices for \( \mathbf{C} \), only four lead to an odd determinant for \( \mathbf{D} \), namely

\[
\mathbf{C} = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \text{ or } \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \text{ or } \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \text{ or } \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}.
\]

By trial and error, we see that the choice

\[
\mathbf{C} = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}
\]

appears to work since

\[
\mathbf{D} = \begin{pmatrix} 2 & 3 \\ 4 & 2 \end{pmatrix} + 13\mathbf{C} \equiv \begin{pmatrix} 15 & 16 \\ 17 & 15 \end{pmatrix} \pmod{26}
\]

translates

\[
\begin{pmatrix} 22 & 10 \\ 13 & 2 \end{pmatrix} \equiv \begin{pmatrix} 6 & 8 \\ 21 & 4 \end{pmatrix}, \text{ and}
\]

WKNCCHSSJH as “givethemup” since

\[
\begin{pmatrix} 18 & 18 \\ 9 & 7 \end{pmatrix} \mathbf{D} \equiv \begin{pmatrix} 19 & 7 \\ 12 & 4 \end{pmatrix}.
\]