$$C = AP, \qquad \text{i.e.,} \qquad \begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}.$$

To decipher a message, we simply apply the inverse matrix:

$$P = A^{-1}AP = A^{-1}C, \qquad \text{i.e.,} \qquad \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} D^{-1}d & -D^{-1}b \\ -D^{-1}c & D^{-1}a \end{pmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix}.$$

Example 3. Working in the 26-letter alphabet, use the matrix A in Example 1 to encipher the message unit "NO."

Solution. We have:

$$AP = \begin{pmatrix} 2 & 3 \\ 7 & 8 \end{pmatrix} \begin{pmatrix} 13 \\ 14 \end{pmatrix} = \begin{pmatrix} 68 \\ 203 \end{pmatrix} = \begin{pmatrix} 16 \\ 21 \end{pmatrix},$$

and so $C = AP$ is "QV."

Remark. To encipher a plaintext sequence of k digraphs $P = P_1P_2P_3 \cdots P_k$, we can write the k vectors as columns of a $2 \times k$–matrix, which we also denote P, and then multiply the 2×2–matrix A by the $2 \times k$-matrix P to get a $2 \times k$–matrix $C = AP$ of coded digraph-vectors.

Example 4. Continue as in Example 3 to encipher the plaintext "NOANSWER."

Solution. The numerical equivalent of "NOANSWER" is the sequence of vectors $\binom{13}{14}\binom{0}{13}\binom{18}{22}\binom{4}{17}$. We have

$$C = AP = \begin{pmatrix} 2 & 3 \\ 7 & 8 \end{pmatrix} \begin{pmatrix} 13 & 0 & 18 & 4 \\ 14 & 13 & 22 & 17 \end{pmatrix} = \begin{pmatrix} 68 & 39 & 102 & 59 \\ 203 & 104 & 302 & 164 \end{pmatrix}$$
$$= \begin{pmatrix} 16 & 13 & 24 & 7 \\ 21 & 0 & 16 & 8 \end{pmatrix},$$

i.e., the coded message is "QVNAYQHI."

Example 5. In the situation of Examples 3–4, decipher the ciphertext "FWMDIQ."

Solution. We have:

$$P = A^{-1}C = \begin{pmatrix} 14 & 11 \\ 17 & 10 \end{pmatrix} \begin{pmatrix} 5 & 12 & 8 \\ 22 & 3 & 16 \end{pmatrix}$$
$$= \begin{pmatrix} 0 & 19 & 2 \\ 19 & 0 & 10 \end{pmatrix} = \text{"ATTACK."}$$

As in §1, suppose that we have some limited information from which we want to analyze how to decipher a string of ciphertext. We know that the "enemy" is using digraph-vectors in an N-letter alphabet and a linear enciphering transformation $C = AP$. However, we do not have the enciphering "key" — the matrix A — or the deciphering "key" — the matrix A^{-1}. But suppose we are able to determine two pairs of plaintext and ciphertext digraphs: $C_1 = AP_1$ and $C_2 = AP_2$. Perhaps we learned this information from an analysis of the frequency of occurrence of digraphs in a long string