of ciphertext. Or perhaps we know from some outside source that a certain 4-letter plaintext segment corresponds to a certain 4-letter ciphertext. In that case we can proceed as follows to determine A and A^{-1}. We put the two columns P_1 and P_2 together into a 2×2–matrix P, and similarly for the ciphertext columns. We obtain an equation of 2×2–matrices: $C = AP$, in which C and P are known to us, and A is the unknown. We can solve for A by multiplying both sides by P^{-1}:

$$A = APP^{-1} = CP^{-1}.$$

Similarly, from the equation $P = A^{-1}C$ we can solve for A^{-1}:

$$A^{-1} = PC^{-1}.$$

Example 6. Suppose that we know that our adversary is using a 2×2 enciphering matrix with a 29-letter alphabet, where A—Z have the usual numerical equivalents, blank=26, ?=27, !=28. We receive the message

"GFPYJP X?UYXSTLADPLW,"

and we suppose that we know that the last five letters of plaintext are our adversary's signature "KARLA." Since we don't know the sixth letter from the end of the plaintext, we can only use the last four letters to make two digraphs of plaintext. Thus, the ciphertext digraphs DP and LW correspond to the plaintext digraphs AR and LA, respectively. That is, the matrix P made up from AR and LA is the result of applying the unknown deciphering matrix A^{-1} to the matrix C made up from DP and LW:

$$\begin{pmatrix} 0 & 11 \\ 17 & 0 \end{pmatrix} = A^{-1} \begin{pmatrix} 3 & 11 \\ 15 & 22 \end{pmatrix}.$$

Thus,

$$A^{-1} = \begin{pmatrix} 0 & 11 \\ 17 & 0 \end{pmatrix} \begin{pmatrix} 3 & 11 \\ 15 & 22 \end{pmatrix}^{-1} = \begin{pmatrix} 0 & 11 \\ 17 & 0 \end{pmatrix} \begin{pmatrix} 3 & 13 \\ 23 & 7 \end{pmatrix} = \begin{pmatrix} 21 & 19 \\ 22 & 18 \end{pmatrix},$$

and the full plaintext message is

$$\begin{aligned} &\begin{pmatrix} 21 & 19 \\ 22 & 18 \end{pmatrix} \begin{pmatrix} 6 & 15 & 9 & 26 & 27 & 24 & 18 & 11 & 3 & 11 \\ 5 & 24 & 15 & 23 & 20 & 23 & 19 & 0 & 15 & 22 \end{pmatrix} \\ &= \begin{pmatrix} 18 & 17 & 10 & 26 & 19 & 13 & 14 & 28 & 0 & 11 \\ 19 & 8 & 4 & 0 & 26 & 14 & 13 & 10 & 17 & 0 \end{pmatrix} \\ &= \text{"STRIKE AT NOON! KARLA."} \end{aligned}$$

Remark. In order for this to work, notice that the matrix P formed by the two known plaintext digraphs must be invertible, i.e., its determinant D must have no common factor with the number of letters N. What if we are not so fortunate? If we happen to know another ciphertext-plaintext pair,