



of the real number line, is now a copy of $\mathbf{Z}/N\mathbf{Z}$. Just as the real xy -plane is often denoted \mathbf{R}^2 , this $N \times N$ array is denoted $(\mathbf{Z}/N\mathbf{Z})^2$.

Once we visualize digraphs as vectors (points in the plane), we then interpret an “enciphering transformation” as a rearrangement of the $N \times N$ array of points. More precisely, an enciphering map is a 1-to-1 function from $(\mathbf{Z}/N\mathbf{Z})^2$ to itself.

Remark. For several centuries one of the most popular methods of encryption was the so-called “Vigenère cipher.” This can be described as follows. For some fixed k , regard blocks of k letters as vectors in $(\mathbf{Z}/N\mathbf{Z})^k$. Choose some fixed vector $b \in (\mathbf{Z}/N\mathbf{Z})^k$ (usually b was the vector corresponding to some easily remembered “key-word”), and encipher by means of the vector translation $C = P + b$ (where the ciphertext message unit C and the plaintext message unit P are k -tuples of integers modulo N). This cryptosystem, unfortunately, is almost as easy to break as a single-letter translation (see Example 1 of the last section). Namely, if one knows (or can guess) N and k , then one simply breaks up the ciphertext in blocks of k letters and performs a frequency analysis on the first letter in each block to determine the first component of b , then the same for the second letter in each block, and so on.

Review of linear algebra. We now review how one works with vectors in the real xy -plane and with 2×2 -matrices with real entries. Recall that, given a 2×2 array of numbers

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad \text{and a vector in the plane} \quad \begin{pmatrix} x \\ y \end{pmatrix}$$

(we shall write vectors as columns), one can *apply the matrix to the vector* to obtain a new vector, as follows: