can represent the situation schematically by the diagram

$$\mathcal{P} \xrightarrow{f} \mathcal{C} \xrightarrow{f^{-1}} \mathcal{P}.$$

Any such set-up is called a *cryptosystem.*

The first step in inventing a cryptosystem is to "label" all possible plaintext message units and all possible ciphertext message units by means of mathematical objects from which functions can be easily constructed. These objects are often simply the integers in some range. For example, if our plaintext and ciphertext message units are single letters from the 26-letter alphabet A—Z, then we can label the letters using the integers 0, 1, 2, . . . , 25, which we call their "numerical equivalents." Thus, in place of A we write 0, in place of S we write 18, in place of X we write 23, and so on. As another example, if our message units are digraphs in the 27-letter alphabet consisting of A—Z and a blank, we might first let the blank have numerical equivalent 26 (one beyond Z), and then label the digraph whose two letters correspond to $x,\ y \in \{0,\ 1,\ 2, \ldots, 26\}$ by the integer

$$27x + y \in \{0,\ 1, \ldots, 728\}.$$

Thus, we view the individual letters as digits to the base 27 and we view the digraph as a 2-digit integer to that base. For example, the digraph "NO" corresponds to the integer $27 \cdot 13 + 14 = 365$. Analogously, if we were using trigraphs as our message units, we could label them by integers $729x+27y+z \in \{0, 1, \ldots, 19682\}$. In general, we can label blocks of k letters in an N-letter alphabet by integers between 0 and $N^k - 1$ by regarding each such block as a k-digit integer to the base N.

In some situations, one might want to label message units using other mathematical objects besides integers — for example, vectors or points on some curve. But for the duration of this section we shall use integers.

Examples. Let us start with the case when we take a message unit (of plaintext or of ciphertext) to be a single letter in an N-letter alphabet labeled by the integers $0, 1, 2, \ldots, N-1$. Then, by definition, an enciphering transformation is a rearrangement of these N integers.

To facilitate rapid enciphering and deciphering, it is convenient to have a relatively simple rule for performing such a rearrangement. One way is to think of the set of integers $\{0,\ 1,\ 2, \ldots, N-1\}$ as $\mathbf{Z}/N\mathbf{Z}$, and make use of the operations of addition and multiplication modulo N.

Example 1. Suppose we are using the 26-letter alphabet A—Z with numerical equivalents 0—25. Let the letter $P \in \{0,\ 1, \ldots, 25\}$ stand for a plaintext message unit. Define a function f from the set $\{0,\ 1, \ldots, 25\}$ to itself by the rule

$$f(P) = \begin{cases} P+3, & \text{if } x < 23, \\ P-23, & \text{if } x \geq 23. \end{cases}$$

In other words, f simply adds 3 modulo 26: $f(P) \equiv P + 3 \ mod\ 26$. The definition using modular arithmetic is easier to write down and work with.