ciphertext. That means that the shift takes "E"=4 to "U"=20, i.e., $20 \equiv 4+b \; mod \; 26$, so that $b=16$. To decipher the message, then, it remains for us to subtract 16 (working modulo 26) from the numerical equivalents of "FQOCUDEM":

$$\text{"FQOCUDEM"} = 5\;16\;14\;2\;20\;3\;4\;12 \;\mapsto\; 15\;0\;24\;12\;4\;13\;14\;22 = \text{"PAYMENOW"}.$$

In the case of a shift encryption of single letters of a 26-letter alphabet, it is not even necessary to have a long string of ciphertext to find the most frequently occurring letter. After all, there are only 26 possibilities for b, and one can simply run through all of them. Most likely, only one will give a message that makes any sense, and that b is the enciphering key.

Thus, this type of cryptosystem is too simple to be much good. It is too easy to break. An improvement is to use a more general type of transformation of $\mathbf{Z}/N\mathbf{Z}$, called an **affine** map: $C \equiv aP+b \; mod \; N$, where a and b are fixed integers (together they form the enciphering key). For example, working again in the 26-letter alphabet, if we want to encipher our message "PAYMENOW" using the affine transformation with enciphering key $a=7$, $b=12$, we obtain: 15 0 24 12 4 13 14 22 $\mapsto$ 13 12 24 18 14 25 6 10 = "NMYSOZGK".

To decipher a message that was enciphered by means of the affine map $C \equiv aP+b \; mod \; N$, one simply solves for P in terms of C, obtaining $P \equiv a'C+b' \; mod \; N$, where a' is the inverse of a modulo N and b' is equal to $-a^{-1}b$. Note that this works only if $g.c.d.(a,N)=1$; otherwise, we cannot solve for P in terms of C. If $g.c.d.(a,N)>1$, then it is easy to see that more than one plaintext letter will give the same ciphertext letter, so we cannot uniquely recover the plaintext from the ciphertext. By definition, that is not an enciphering transformation: we always require that the map be 1-to-1, i.e., that the plaintext be uniquely determined from the ciphertext. To summarize, an affine cryptosystem in an N-letter alphabet with parameters $a \in (\mathbf{Z}/N\mathbf{Z})^*$ and $b \in \mathbf{Z}/N\mathbf{Z}$ consists of the rules:

$$C \equiv aP+b \; mod \; N, \qquad P \equiv a'C+b' \; mod \; N,$$

where

$$a' = a^{-1} \text{ in } (\mathbf{Z}/N\mathbf{Z})^*, \;\; b' = -a^{-1}b.$$

As a special case of the affine cryptosystems we can set $a=1$, thereby obtaining the shift transformations. Another special case is when $b=0$: $P \equiv aC \; mod \; N$, $C \equiv a^{-1}P \; mod \; N$. The case $b=0$ is called a *linear* transformation, meaning that the map takes a sum to a sum, i.e., if C_1 is the encryption of P_1 and C_2 is the encryption of P_2, then C_1+C_2 is the encryption of P_1+P_2 (where, of course, we are adding modulo N).

Now suppose that we know that an intercepted message was enciphered using an affine map of single letters in an N-letter alphabet. We would like to determine the enciphering key a, b so that we can read the message. We need two bits of information to do this.