Thus, with this system, to encipher the word "YES" we first convert to numbers: 24 4 18, then add 3 modulo 26: 1 7 21, then translate back to letters: "BHV." To decipher a message, one subtracts 3 modulo 26. For example, the ciphertext "ZKB" yields the plaintext "WHY." This cryptosystem was apparently used in ancient Rome by Julius Caesar, who supposedly invented it himself.

Example 1 can be generalized as follows. Suppose we are using an N-letter alphabet with numerical equivalents $0, 1, \ldots, N-1$. Let b be a fixed integer. By a *shift* transformation we mean the enciphering function f defined by the rule $C = f(P) \equiv P + b \bmod N$. Julius Caesar's cryptosystem was the case $N = 26$, $b = 3$. To decipher a ciphertext message unit $C \in \{0, 1, \ldots, N-1\}$, we simply compute $P = f^{-1}(C) \equiv C - b \bmod N$.

Now suppose that you are not privy to the enciphering and deciphering information, but you would nevertheless like to be able to read the coded messages. This is called *breaking* the code, and the science of breaking codes is called *cryptanalysis*.

In order to break a cryptosystem, one needs two types of information. The first is the general nature (the *structure*) of the system. For example, suppose we know that the cryptosystem uses a shift transformation on single letters of the 26-letter alphabet A—Z with numerical equivalents 0—25, respectively. The second type of information is knowledge of a specific choice of certain parameters connected with the given type of cryptosystem. In our example, the second type of information one needs to know is the choice of the shift parameter b. Once one has that information, one can encipher and decipher by the formulas $C \equiv P + b \bmod N$ and $P \equiv C - b \bmod N$.

We shall always assume that the general structural information is already known. In practice, users of cryptography often have equipment for enciphering and deciphering which is constructed to implement only one type of cryptosystem. Over a period of time the information about what type of system they're using might leak out. To increase their security, therefore, they frequently change the choice of parameters used with the system. For example, suppose that two users of the shift cryptosystem are able to meet once a year. At that time they agree on a list of 52 choices of the parameter b, one for each week of the coming year.

The parameter b (more complicated cryptosystems usually have several parameters) is called a *key*, or, more precisely, the *enciphering key*.

Example 2. So suppose that we intercept the message "FQOCUDEM", which we know was enciphered using a shift transformation on single letters of the 26-letter alphabet, as in the example above. It remains for us to find the b. One way to do this is by *frequency analysis*. This works as follows. Suppose that we have already intercepted a long string of ciphertext, say several hundred letters. We know that "E" is the most frequently occurring letter in the English language. So it is reasonable to assume that the most frequently occurring letter in the ciphertext is the encryption of E. Suppose that we find that "U" is the most frequently occurring character in the