Digraph transformations. We now suppose that our plaintext and ciphertext message units are *two*-letter blocks, called *digraphs*. This means that the plaintext is split up into two-letter segments. If the entire plaintext has an odd number of letters, then in order to obtain a whole number of digraphs we add on an extra letter at the end; we choose a letter which is not likely to cause confusion, such as a blank if our alphabet contains a blank, or else "X" or "Q" if we are using just the 26-letter alphabet.

Each digraph is then assigned a numerical equivalent. The simplest way to do this is to take $xN + y$, where x is the numerical equivalent of the first letter in the digraph, y is the numerical equivalent of the second letter in the digraph, and N is the number of letters in the alphabet. Equivalently, we think of a digraph as a 2-digit base-N integer. This gives a 1-to-1 correspondence between the set of all digraphs in the N-letter alphabet and the set of all nonnegative integers less than N^2. We described this "labeling" of digraphs before in the special case when $N = 27$.

Next, we decide upon an enciphering transformation, i.e., a rearrangement of the integers $\{0, 1, 2, \ldots, N^2 - 1\}$. Among the simplest enciphering transformations are the *affine* ones, where we view this set of integers as $\mathbf{Z}/N^2\mathbf{Z}$, and define the encryption of P to be the nonnegative integer less than N^2 satisfying the congruence $C \equiv aP + b \ mod \ N^2$. Here, as before, a must have no common factor with N (which means it has no common factor with N^2), in order that we have an inverse transformation telling us how to decipher: $P \equiv a'C + b' \ mod \ N^2$, where $a' \equiv a^{-1} \ mod \ N^2$, $b' \equiv -a^{-1}b \ mod \ N^2$. We translate C into a two-letter block of ciphertext by writing it in the form $C = x'N + y'$, and then looking up the letters with numerical equivalents x' and y'.

Example 5. Suppose we are working in the 26-letter alphabet and using the digraph enciphering transformation $C \equiv 159P + 580 \ mod \ 676$. Then the digraph "NO" has numerical equivalent $13 \cdot 26 + 14 = 352$ and is taken to the ciphertext digraph $159 \cdot 352 + 580 \equiv 440 \ mod \ 676$, which is "QY". The digraph "ON" has numerical equivalent 377, and is taken to 359="NV". Notice that the digraphs change as a unit, and there is no relation between the encryption of one digraph and that of another one that has a letter in common with it or even consists of the same letters in the reverse order.

To break a digraphic encryption system which uses an affine transformation $C \equiv aP + b \ mod \ N^2$, we need to know the ciphertext corresponding to two different plaintext message units. Since the message units are digraphs, a frequency analysis means counting which two-letter blocks occur most often in a long string of ciphertext (of course, counting only those occurrences where the first letter begins a message unit, ignoring the occurrences of the two letters which straddle two message units), and comparing with the known frequency of digraphs in English language texts (written in the same alphabet). For example, if we use the 26-letter alphabet, statistical analyses seem to show that "TH" and "HE" are the two most frequently occurring digraphs, in that order. Knowing two plaintext–ciphertext pairs