Thus, $a' \equiv 362 \cdot 142 \equiv 374 \ mod\ 729$, and then $b' \equiv 134 - 675 \cdot 374 \equiv 647 \ mod\ 729$. Now applying the deciphering transformation to the digraphs "ND", "XB" and "HO" of our message — they correspond to the integers 354, 622 and 203, respectively — we obtain the integers 365, 724 and 24. Writing $365 = 13 \cdot 27 + 14$, $724 = 26 \cdot 27 + 22$, $24 = 0 \cdot 27 + 24$, we put together the plaintext digraphs into the message "NO WAY". Finally, to find the enciphering key we compute $a \equiv a'^{-1} \equiv 374^{-1} \equiv 614 \ mod\ 729$ (again using the Euclidean algorithm) and $b \equiv -a'^{-1}b' \equiv -614 \cdot 647 \equiv 47 \ mod\ 729$.

Remark. Although affine cryptosystems with digraphs (i.e., modulo N^2) are better than the ones using single letters (i.e., modulo N), they also have drawbacks. Notice that the second letter of each ciphertext digraph depends only on the second letter of the plaintext digraph. This is because that second letter depends on the mod-N value of $C \equiv aP + b \ mod\ N^2$, which depends only on P modulo N, i.e., only on the second letter of the plaintext digraph. Thus, one could obtain a lot of information (namely, a and b modulo N) from a frequency analysis of the even-numbered letters of the ciphertext message. A similar remark applies to mod-N^k affine transformations of k-letter blocks.

Exercises

1. In certain computer bulletin-board systems it is customary, if you want to post a message that may offend some people (e.g., a dirty joke), to encipher the letters (but not the blanks or punctuation) by a translation $C \equiv P + b \ mod\ 26$. It is then easy to decipher the text if one wants to, but no one is forced to see a message that jars on the nerves. Decipher the punchline of the following story (use frequency analysis to find b): At an international convention of surgeons, representatives of different countries were comparing notes on recent advances in reattaching severed parts of the body. The French, Americans and Russians were being especially boastful. The French surgeon said, "We sewed a leg on an injured runner, and a year later he placed in a national 1000-meter race." "Using the most advanced surgical procedures," the Russian surgeon chimed in, "we were able to put back an athlete's entire arm, and a year later with the same arm he established a new world record for the shot put." But they all fell silent when the American, not to be outdone, announced that "Jr frjrq n fzvyr ba n ubefr'f nff, naq n lrne yngre vg jnf ryrpgrq Cerfvqrag!" (Note: We are using a 26-letter alphabet, but we have inserted blanks and punctuation for ease of reading.)
2. Using frequency analysis, cryptanalyze and decipher the following message, which you know was enciphered using a shift transformation of single-letter plaintext message units in the 26-letter alphabet:

   PXPXKXENVDRUXVTNLXHYMXGMAXYKXJN