digraphs in the Russian language are “HO” and “ET”. Find the deciphering key, and write out the plaintext message.

13. Recall from Exercise 8 that a *fixed* plaintext message unit is one that the given enciphering transformation keeps the same. Find all fixed digraphs for the enciphering transformation in Exercise 11.

14. By the *product* (or *composition*) of two cryptosystems, we mean the cryptosystem that results from enciphering a plaintext using the first cryptosystem and then treating the resulting ciphertext as plaintext for the second cryptosystem, i.e., encrypting a second time using the second system. More precisely, we must assume that the set $\mathcal{C}_1$ of ciphertext message units for the first cryptosystem is contained in the set of plaintext message units for the second system. Let f_1 and f_2 be the enciphering functions; then the product cryptosystem is given by the enciphering function $f = f_2 \circ f_1$. If we let I (for “intermediate text”) denote a ciphertext message unit for the first system, and let $\mathcal{I} = \mathcal{C}_1$ denote the set of intermediate texts, then the product cryptosystem can be represented schematically by the composite diagram:

$$\mathcal{P} \xrightarrow{f_1} \mathcal{I} \xrightarrow{f_2} \mathcal{C}.$$

Prove that:

(a) The product of two shift enciphering transformations is also a shift enciphering transformation.

(b) The product of two linear enciphering transformations is a linear enciphering transformation.

(c) The product of two affine enciphering transformations is an affine enciphering transformation.

15. Here is a slightly more complicated cryptosystem, in which the plaintexts and ciphertexts are written in different alphabets. We choose an N-letter alphabet for plaintexts and an M-letter alphabet for ciphertexts, where $M > N$. As usual, we regard digraphs in the N-letter alphabet as two-digit integers written to the base N, i.e., as integers between 0 and $N^2 - 1$; and we similarly regard digraphs in the M-letter alphabet as integers between 0 and $M^2 - 1$. Now choose any integer L between N^2 and M^2: $N^2 \leq L \leq M^2$. Also choose integers a and b with $g.c.d.(a, L) = 1$. We encipher a plaintext digraph P using the rule $C \equiv aP + b \; mod \; L$ (in which C is taken to be the least nonnegative residue modulo L which satisfies the congruence). (Here the set $\mathcal{P}$ of all possible digraphs P consists of all integers from 0 to $N^2 - 1$; but the set $\mathcal{C}$ of all possible ciphertext digraphs C in the larger alphabet is only part of the integers from 0 to $M^2 - 1$, in fact, it is the subset of the integers less than L that arises from applying the enciphering rule to all possible plaintext digraphs.) Suppose that the plaintext alphabet is the 27-letter alphabet (as in Exercise 3), and the ciphertext alphabet is the 30-letter alphabet in Exercise 11. Suppose