of digraphs is often (but not always) enough to determine a and b.

Example 6. You know that your adversary is using a cryptosystem with a 27-letter alphabet, in which the letters A—Z have numerical equivalents 0—25, and blank=26. Each digraph then corresponds to an integer between 0 and $728 = 27^2 - 1$ according to the rule that, if the two letters in the digraph have numerical equivalents x and y, then the digraph has numerical equivalent $27x + y$, as explained earlier. Suppose that a study of a large sample of ciphertext reveals that the most frequently occurring digraphs are (in order) "ZA", "IA", and "IW". Suppose that the most common digraphs in the English language (for text written in our 27-letter alphabet) are "E " (i.e., "E blank"), "S ", " T". You know that the cryptosystem uses an affine enciphering transformation modulo 729. Find the deciphering key, and read the message "NDXBHO". Also find the enciphering key.

Solution. We know that plaintexts are enciphered by means of the rule $C \equiv aP + b \ mod\ 729$, and that ciphertexts can be deciphered by means of the rule $P \equiv a'C + b' \ mod\ 729$; here a, b form the enciphering key, and a', b' form the deciphering key. We first want to find a' and b'. We know how three digraphs are deciphered, and, after we replace the digraphs by their numerical equivalents, this gives us the three congruences:

$$675a' + b' \equiv 134 \ mod\ 729,$$
$$216a' + b' \equiv 512 \ mod\ 729,$$
$$238a' + b' \equiv 721 \ mod\ 729.$$

If we try to eliminate b' by subtracting the first two congruences, we arrive at $459a' \equiv 351 \ mod\ 729$, which does not have a unique solution $a' \ mod\ 729$ (there are 27 solutions). We do better if we subtract the third congruence from the first, obtaining $437a' \equiv 142 \ mod\ 729$. To solve this, we must find the inverse of 437 modulo 729. By way of review of the Euclidean algorithm, let's go through that in detail:

$$729 = 437 + 292$$
$$437 = 292 + 145$$
$$292 = 2 \cdot 145 + 2$$
$$145 = 72 \cdot 2 + 1$$

and then

$$\begin{aligned} 1 &= 145 - 72 \cdot 2 \\ &= 145 - 72(292 - 2 \cdot 145) \\ &= 145 \cdot 145 - 72 \cdot 292 \\ &= 145(437 - 292) - 72 \cdot 292 \\ &= 145 \cdot 437 - 217 \cdot 292 \\ &= 145 \cdot 437 - 217(729 - 437) \\ &\equiv 362 \cdot 437 \ mod\ 729. \end{aligned}$$