2.13 #11

The ciphertext is:

ABCBABBBAC

If we shift the ciphertext by 1, 2, and 3 places, we find that the most likely key length is 2.

ABCBABBBAC
ABCBA  (shift 1)  2 coincidences
ABCBBABBBAC (shift 2)  3 coincidences
ABCBBABBBAC (shift 3)  1 coincidence

We then examine the 1st, 3rd, … letter frequencies:
A = 3  B = 1  C = 1

This gives us V = (3, 1, 1). Thus W = (0.3, 0.1, 0.1)

In this language, \(A_0 = (0.7, 0.2, 0.1)\) \(A_1 = (0.1, 0.7, 0.2)\) \(A_2 = (0.2, 0.1, 0.7)\)

\[W \cdot A_0 = 0.24 \quad W \cdot A_1 = 0.12 \quad W \cdot A_2 = 0.14\]

Thus, for the first shift, a shift of 0 is most likely, which corresponds to the key letter a.

Examining the 2nd, 4th, … letter frequencies:
A = 0  B = 4  C = 1

This gives us V = (0, 4, 1) and W = (0, 0.4, 0.1)

\[W \cdot A_0 = 0.09 \quad W \cdot A_1 = 0.30 \quad W \cdot A_2 = 0.11\]

Thus, for the second shift, a shift of 1 is most likely, which corresponds to the key letter b.

Thus, the most likely key is ab.