Quiz 2

Problem 1
An important concept of cryptographic design is *cryptographic combination*—the process of creating a strong encryption function by combining several component functions, each of which contributes some cryptographic strength. In this problem, you will analyze how this concept applies when the component functions are substitution and transposition ciphers.

Consider a new cipher f that applies substitution and transposition n times, in strict alternation (first substitution, then transposition, and so on), under keys independently and randomly chosen for each substitution and for each transposition. Thus, the function f can be viewed as the composition

$$f = T_{h_n} \circ S_{k_n} \circ \cdots \circ T_{h_2} \circ S_{k_2} \circ T_{h_1} \circ S_{k_1}, \qquad (1)$$

where, for $1 \leq i \leq n$, S_{k_i} denotes substitution under substitution key k_i, and T_{h_i} denotes transposition under transposition key h_i. Assume that each message is a sequence of exactly 100 characters, where the characters are drawn from the 126-symbol ASCII alphabet.

- Does using $n > 1$ increase the cryptographic strength of f over using $n = 1$? What value of n do you recommend using? Carefully explain and justify your answers.