Sean Poston
MA 464 Quiz 3

# Quiz 3

Assume that our substitution cipher is as follows:

$\{a \to b, b \to c, c \to d \ldots z \to a\}$

This is also a shift cipher with $[K = +1]$

As we know, shift ciphers are idempotent.

Thus, by encrypting affine(substitution(e)), it's not any more secure because it just switches the key, rather than makes it more secure.