Introduction to mathematical cryptography
Homework problems
Week 4

7. Prove that the Caesar cipher is vulnerable against the chosen plaintext attack. How many pairs $(m, e_k(m))$ are needed to reveal k?

8. Let k be a key coming from the Caesar cipher. Prove that if we apply e_k to the message an appropriate number of times, we get back the original message, i.e. for some $N \in \mathbf{N}$,

$$\underbrace{e_k(e_k(e_k(\ldots e_k(m))))}_{e_k \text{ is applied } N \text{ times}} = m$$

for any possible message m. Give an N which works for all possible k's.

Note: Please provide complete arguments everywhere.