Introduction to mathematical cryptography
Homework problems
Week 7

13. Assume N is the product of two different prime numbers. Prove that if N and $\varphi(N)$ are given, then you can compute the prime factors of N in polynomial time.

14. ('multiplication without modulus' cipher) Now the cryptosystem is the following: $\mathcal{M}, \mathcal{C}, \mathcal{K} = \mathbf{N}$, and for $m \in \mathcal{M}, k \in \mathcal{K}$, $e_k(m) = km$. Alice and Bob agree on a large number $k \in \mathcal{K}$, and start to communicate. Eve intercepts the messages

$$c_1 = 10302619, \qquad c_2 = 5277099287.$$

How can Eve decrypt the messages? (Recall that Eve has the ability that if she reads a message, she recognizes it.)

Note: Please, provide complete arguments everywhere, and explain how you arrived at your answer/solution. Giving the result without explanation leads to score deduction.