Secure and Dependable Systems Jacobs University Bremen Taha Zia

## Homework 6

Course: CO21-320203

8th May, 2017

## Problem 6.3 Solution:

a)

b) Theoretically, it is possible to try out all possibilities and hence, figure out the combination. As in Example 15.20:

PRG can be used to iterate on the output a couple of times. A key can then be generated from these outputs. Then every bit can be xor-ed with the corresponding bits in the encryption steps. Decryption can be found the same way.

So, E is then not CPA-ind secure.