Secure and Dependable Systems
Jacobs University Bremen
Taha Zia

Course: CO21-320203
8th May, 2017

Homework 6

Problem 6.3

Solution:

a) Block cipher steps 1,2,3, and the IV step have negligible probabilities. Due to this all sub-steps are comp-ind. And finally, the combination of all sub-steps will in turn be comp-ind as well.

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.