Assignment 8 – 2019.11.19

Submission deadline: 2019.11.26

1. Show that the RSA trapdoor function when used directly as the encryption is not semantically secure. Provide a game between an adversary A and a challenger B.

2. Theorem 11.2 states that when H is modeled as a random oracle, and if T is one-way and E_S is semantically secure, then E_{TDF} is semantically secure as follows:

$$SS^{ro}adv[A, E_{TDF}] \leq 2 \cdot OWadv[B_{ow}, T\ ] + SSadv[B_s, E_s]$$

   Please read the proof (PP.432 - 434) on the textbook carefully and describe how the adversary B_{ow} and B_s can be constructed by using A's help. Please draw the figure along with the explanation.