**CS 177**

**Homework 1**

**Task 1:**

The semantic security does not hide the length of the plaintext. An attacker can figure out this information by subtracting the length of the cipher text by the length of the IV. The attacker would know about the length of the IV because the length of an IV is just the block size which should be publicly known.

**Task2:**