**CSCI 5531 – Summer 2019**

**Assignment 4**

**Due: Monday 07/29/2019 by 11:59pm.**

In this assignment you are to modify the algorithm presented in figure 11.9 (TEA) to use Cypher Block Chaining as described in figure 11.5. Your algorithm will use the encryption and decryption algorithms within a chain of blocks according the specifications of CBC (64 bit block size). Your output is supposed to be able to show the entire message or even portions of the message both encrypted and then later decrypted.

Basically, read a string from input, simulate CBC encryption on it. Output the encrypted results and then decrypt it and produce the decrypted result.

How you build that user interface to show how the algorithm works is entirely up to you as long as you show the required results.

Best of Luck