**Georgia Gwinnett College**

**School of Science and Technology**

**ITEC 3300: Information Security**

**Homework Assignment 2**

**Problem 1 [20 Points]**

Draw a diagram, in the style of the one on Slide 32 of the presentation Private-Key Encryption Part 3, that illustrates the decryption of three ciphertext blocks produced by Cipher Block Chaining (CBC) as shown in the diagram on Slide 32. The input for the decryption algorithm should be , and the output should be . Note that the CBC decryption algorithm should use the block decryption function .

**Problem 2 [30 Points]**

In the style of the pseudocode on Slide 33 of the presentation Private-Key Encryption Part 3 and with the ideas from the diagram in Problem 1, describe the CBC decryption algorithm , where is the key that has been chosen and fixed. In the pseudocode, the header of the decryption algorithm should be , where is the same IV that was used for encryption in , and are the ciphertext blocks to decrypt. The decryption algorithm should compute and return the plaintext blocks , using the block decryption function and the XOR operator. Note that it is assumed implicitly that the decryption algorithm has the key , and therefore can efficiently compute the block decryption function .