Homework Assignment 3
Total Points 25 Due Tuesday 2/7/2016 on BLACKBOARD.

1. Read the attached article "CryptographywithInternationalCharactersets.pdf"
   - Discuss why the authors proposed the following two rules (2 points):
     Rule 1: "Work with bytes not text strings"
     Rule 2: "Do not put ciphertext bytes directly into a string type"
   - What is Byte Order Mark and why is it needed? (1 point)
   - What do the authors recommend regarding store or transmission of ciphertext bytes? (2 points)

1. Answer the following question based on the attached article "BlockCipherModesofOperation.pdf"
   Let's assume, we have a simple XOR block cipher that takes 4 bit blocks as input, XOR a 4 bit key with the block and produce a 4 bit ciphertext for the block. What will be the output of this block cipher with 32 bit input of 0101 1111 0101 1110 1010 1100 0011 1010 with key 1010 in each of the following modes of operation: ECB and CBC? Do you see any problem with either of the outputs? If yes, identify and explain it. For CBC, use a random 4 bit IV of your choice. (5 points)

2. Based on the attached file Padding.pdf and answer the following questions: (5 points)
   - Why do we need padding in encryption process?
   - What are the five methods of padding?
   - When do we NOT need to use padding?

3. Using `Java Cryptography Extension(JCE)` library, implement a Java program that will do the following:
   - Read the contents of a text file (`plaintext.txt`)
   - Encrypt it using AES (you can use default mode and padding)
   - Write the ciphertext to a text file (`ciphertext.txt`)
   - Read the content of `ciphertext.txt`
   - Decrypt it using AES
   - Write the decrypted text to a text file (`decryptedtext.txt`)

   A `JCE` tutorial from IBM is attached (JCETutorial.pdf) for your reference which contains a few examples. (10 points)
   Note: The Java compiler on the department Linux system (login.cpp.edu) automatically provides support for SunJCE. Therefore, it is advised that you use the department system for these programming tasks to avoid compatibility issue.

   Submission guideline: Submit an electronic copy of your answers on Blackboard including the program source code (.java file), a readme.txt and sample output for Q4.

The readme.txt should explain how to interact with your Java program and show sample output.