Homework 4

1. (22 points) Many network applications are written in Java. In the rest of this assignment, you will try to use the javax.crypto package. A good (although kind of old) tutorial is “Java security: Java security, Part 1: Crypto basics” article. (You can focus on the sections “Ensuring the integrity of a message” and “Keeping a message confidential”.) Another source that may be helpful is “Java Cryptography Architecture (JCA) Reference Guide”.

   Please solve the following problems by completing the Java source file, filling out the parts between // BEGIN SOLUTION and // END SOLUTION. The solution uploaded to Brightspace should include the completed source file. Please make sure that the uploaded source file can be compiled and executed without unhandled exceptions.

   A. (4 points): Decrypt the ciphertext from the file P1_cipher.txt.
      - Plaintext was encrypted using AES in CBC mode with ISO10126Padding padding.
      - Use the 16-byte key from the file P1_key and 16 zero bytes as the IV (see the source skeleton).
      - Use the class SecretKeySpec to set the key for the cipher (no offset)
      - Use the class IvParameterSpec to set the IV for the cipher (no offset)

      The correct plaintext is an English sentence.

   B. (4 points): Compute the MD5 hash of the plaintext from the first problem.
      - Use the MessageDigest class with MD5

      The correct hash is 16-bytes long, and the signed value of the first byte is -28.

   C. (4 points): Decrypt the ciphertext from the file P3_cipher.bmp.
      - Plaintext was encrypted using AES in ECB with ISO10126Padding padding
      - Use the MD5 hash of the plaintext from the first problem as the key

      The correct plaintext is an ordinary BMP file.

   D. (10 points): The bitmap file P4_cipher.bmp (which has the same size as the P3_cipher.bmp) was encrypted in ECB mode. Consequently, patterns in the image are not hidden and you should be able to view them easily. (Well, you may try to directly open it, but I guarantee you it will not succeed… bummer!) Can you guess what the possible plaintext message is? (although you do not know the key to decrypt it).
      - Emm… think of the main reason why you can’t open it directly?
      - A hint on how to solve it is in the first sentence of this question!

      You need to think about this by yourself. Do not ask others why and how.