Web Security
Homework Assignment 2
COSC 4371
2019 Spring

In this homework assignment, you will use the `javax.crypto` package. To get familiar with the most important classes and interfaces, read the "*Java security: Java security, Part 1: Crypto basics*" article at http://www.ibm.com/developerworks/java/tutorials/j-sec1/j-sec1.html, focusing on sections "*Keeping a message confidential*" and "*Ensuring the integrity of a message*."

Please solve the following problems by completing the attached Java source file. For each problem, replace the code between `// BEGIN SOLUTION` and `// END SOLUTION` with your solution (you can also import any standard Java library). The submission uploaded to Blackboard should include the completed Java source file. Please make sure that the uploaded source file can be compiled and executed without unhandled exceptions and that you have not used any non-standard libraries.

In each problem, your goal is to obtain a plaintext (or message), most of which are image files. Please note that you will need a working Internet connection to solve this assignment. Each problem builds on the preceding one, so you have to solve them in order.

Problem 1 (2 points): The Game is Afoot

You are at 221B Baker Street in the company of Dr. Watson, when the following e-mail arrives:

"*Dear Mr. Sherlock Holmes,*

I must once again ask you to help us as a consulting detective. Three days ago, the invaluable Koh-i-Noor diamond was stolen from the Tower of London. We fear that the thieves are planning to sell the diamond on the black market, where it may be lost forever. Fortunately, the thieves acted hastily and they accidentally left a disk drive at the scene of the crime. We recovered two files from this drive (please find them attached), but our detectives at Scotland Yard were not able to make sense of them. We believe that the infamous Professor Moriarty is behind this spiteful act, but our detectives have no leads to follow. Sherlock, you are our only hope!

Sincerely,
Inspector Lestrade"

The two files (`cipher1.bmp` and `msg1.txt`) are attached to the homework assignment. See the solution template for help.

Problem 2 (2 points): The Plot Thickens

Thousands of messages, what a puzzle! Dr. Watson immediately starts visiting the links one by one, trying to figure out which one is the real message. His effort is admirable but obviously futile. You know that finding the diamond is urgent, so you must quickly compute the hash value of each message.

Problem 3 (2 points): Looking for a Clue

You look at Dr. Watson… he has fallen asleep checking all those messages. You suspect that he would not be much help anyway, so you decide not to wake him up. Instead, you look at the ciphertext: it is a bitmap image (BMP file) that has been encrypted using ECB mode, so you should be able to see the patterns of the plaintext. However, you cannot open the image since the header of the file is encrypted, so no image-viewer program will be able to figure out how to display it (e.g., without the header, a program will not know what the image width and height are). Suddenly, you get an idea: what if this image has the same format as the first one? You could restore the header by copying the first few thousand bytes of the first plaintext (`plain1.bmp`) to overwrite the first few thousand bytes of the ciphertext (`cipher3.bmp`), and then open the modified ciphertext in an image viewer!

Problem 4 (2 points): End of the Line

Dr. Watson wakes up, looks at the ciphertext, and scratches his head. Not a good sign, obviously. To be honest, you do not have a clue about those three numbers either. However, there are not that many combinations, so you could brute-force the key. But how will you know which key is the correct one? Well, the plaintext is a PNG file, which means that the value of the second byte is 80 (character ‘P’ in ASCII), the value of the third byte is 78 (character ‘N’), and the value of the fourth byte is 71 (character ‘G’).