Web Security
Homework Assignment 2
COSC 4371
2018 Fall

Problem 0:

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 and the correct plaintexts. 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). All plaintexts are plain English texts. Please note that you will need a working Internet connection to solve this assignment. Each problem builds on the preceding one, you have to solve in order.

Problem 1 (2.5 points): The Game is Afoot

You are in your study room 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.txt` 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 reading them one by one, trying to figure out which one is the real message. His effort is admirable but futile. You know that finding the diamond is urgent, so you must quickly compute the hash value of each message.

Problem 3 (2 points): Out of Order

You look at Dr. Watson… he has fallen asleep reading 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 and see that it is 48 bytes (384 bits) long, which means that it comprises only three AES blocks, each being 16 bytes (128 bits) long. You can just try to rearrange the three blocks in different ways (there are only 5 possibilities) to restore the ciphertext.

Problem 4 (2.5 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 two 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 simple English language text, so all the bytes of the correct plaintext have to be between 0 and 127. Note that when you decrypt the ciphertext with an incorrect key, you **might** encounter a `BadPaddingException` exception. You can ignore these by simply catching them and then continuing with the next key candidate.[1]

[1] You should surround the decryption with try-catch, e.g.,

```
for (key in possible_keys) {
  …
  try {
    … // test key
  }
  catch (BadPaddingException e) {
    // decryption with wrong key, ignore this
  }
}
```