ASSIGNMENT 1
DUE DATE: Tuesday 5 April, 2011 11:59 PM

The purpose of this assignment is to familiarize you with the `MessageDigest` and `DigestInputStream` classes available as part of the `java.security` package. You will be required to learn more about the classes and then write a program using them.

Description

For this assignment, you will create a Java program called `Hash.java` that has at least two methods – `calculateTextHash` and `calculateFileHash`.

`calculateTextHash` has two arguments – a `MessageDigest` object and a `String` object, and returns another `String` object

```java
public static String calculateTextHash(MessageDigest algorithm, String text) {
    // returns the hash value of a string
}
```

`calculateFileHash` also has two arguments – a `MessageDigest` object and a `String` object and returns another `String` object

```java
public static String calculateFileHash(MessageDigest algorithm, String fileName) {
    // returns the hash value of a file
}
```

Both of these functions compute a hash value for either a line of text or for the contents of a file. It uses the passed `MessageDigest` object to do so.

The main method of your program should perform the following actions in order.

1. Ask the user to input a string of text.

2. Compute and display the SHA1 and MD5 hash values for the entered line of text using your `calculateTextHash` method. In order to do this, you will have to create two `MessageDigest` objects – one for the SHA1 algorithm and one for the MD5 algorithm. You are required to find out how these objects are to be created.

3. Ask the user for the name of a file in the current directory.

4. Compute and display the SHA1 and MD5 hash values for the specified file using your `calculateFileHash` method. You should use the `DigestInputStream` class in this...
part to stream the contents of the file through the MessageDigest object. Again, you will have to find out how!

You must fully comment your program. Put comments in the beginning of the program specifying your name and the purpose of the program. The format of your output should match the one shown in the sample below.

Guidelines

The Internet is a good resource for you to complete this assignment. First find out more about the two classes, what methods they provide and then how the methods are to be used. An example template for the program is given at the end.

Sample output

Assuming that the file test.txt contains the text:

This program computes the SHA1 and MD5 checksums.

>javac Hash.java
>java Hash
Enter a line of text: This program computes the SHA1 and MD5 checksums
SHA1: d571ae7d478bf7d37ffd5aa71ac7109ea17aac2b
MD5: e659779132b480b34e5e228d080770a3

Enter a file name in the current directory: test.txt
SHA1: fc5003fa51b3f31f99ec3f9842d757416690c8ed
MD5: 989b441cf8d684f059ee4c375e263c6c
>

Notice how the computed hash values are so different just for missing the period at the end of the line of text. You should experiment with your program to see how a minor change in the data change the digests.

Submission

Upload the Hash.java file to Blackboard.

Grading

The assignment is worth **10 points**. A program that **does not compile** is a program that you did not submit at all. Remember the GTA is not required to debug your program to give you partial points.

The late policy is available at [http://cs.du.edu/2555/assignments.html](http://cs.du.edu/2555/assignments.html). **You must work alone on this assignment.**
import java.security.MessageDigest;
import java.security.DigestInputStream;
import java.io.*;

// other imports

public class Hash {

    public static String calculateTextHash(MessageDigest algorithm, String text) {
    }

    public static String calculateFileHash(MessageDigest algorithm, String fileName) {
        // you will use DigestInputStream here
    }

    // other methods; e.g. a method that converts a byte array to a hex array

    public static void main(String[] args) throws Exception {
        // perform the actions asked for in the description
    }

}