CST8265 - Lab 11

PURPOSE:

The purpose of this lab is to calculate **MD5** hash of a given zip file and to develop **Advanced Encryption Standard (AES)** of some data say user name and password.

You need to download the Lab-11_package.zip from BS to complete this lab work.

EVALUATION:

This lab is worth 3 **marks:**

Activities:

1. Calculate the MD5 hash of a given zip file. (1.5 marks)
2. Write a java application to encrypt information using advanced encryption standard. (1.5 marks)

NB: you are allow to use any other programming language. It's up to you.

DELIVERABLE:

This lab must be completed and demonstrated to your lab teacher and then submit all codes via BS.

DUE DATE:

Friday, April 19, 2019

LAB ACTIVITY

You need to demo your work during lab hours. Then you will submit all codes through BS.

1. Calculate the MD5 hash of a given zip file.
   a. Develop a java application so that you are allow to create a MD5 hash for a given zip file. You can get the MD5.zip file from the downloaded package.
   b. Put all files, MD5.java and test.zip into a folder say C:\Lab-11\MD5.
   c. Now compile your code: C:\Lab-11\MD5\javac MD5.java
   d. Run your application: C:\Lab-11\MD5\java MD5
      Here you will get a 32-character hexadecimal number i.e. 128 bit hash code.

   e. Now extract the test.zip and rename the text files and again create a test.zip file and run your application (follow step d).
      Here you will also get a 32-character hexadecimal number.

   f. Now extract the test.zip file again and change the contents of the text files and create a test.zip file again. Now run again your application for this new test.zip.
      Here you will get also a 32-character hexadecimal number.
   g. In your lab presentation, just mention why those MD5 hash of test.zip files are not same. Why does message digest algorithm is so significant in information security?

2. Write a java application to encrypt information using advanced encryption standard.
   a. You can download AES.zip file (as part of provided zip package) from BS to complete this task.
   b. Extract and put all java files into a folder.
   c. Now compile all java files by using (of course from a terminal):
      javac *.java
   d. Run the application (from terminal):
      java myApplication

You will get a java GUI. Put user name and password and click on the **click me** button.

You will get a message regarding encryption and decryption in a text area.

e. Now your job to complete the two methods: encrypt() and decrypt() which are in AES.java file.
f. Now compile the java codes and run your application again.
g. In demo you must need to mention: How does AES work and without knowing key, is it possible to decrypt a cipher text which is encrypted by AES? Demonstrate by yourself.