**Objective- DOM attack:**

In this assignment, you will be provided with the power traces of AES. The power traces are stored in a CSV file, where each row indicates the power consumption of one AES execution. For every row, the first entry is plaintext, the second entry is ciphertext, and all the subsequent entries are power consumption values. Your task is to write a code for Difference of Mean Attack, and use that code on the given power traces to recover the 4th and 5th bytes of the secret key used in the AES execution. The demo code is for finding out the 0th byte of the secret key.

**Note**: You will be provided with 10 CSV files, you have to use one according to your group number.  
(e.g., if your group number is 1, then use HW power trace 1.csv)

**Deliverables:**

1. Even though you are working in group, you need to submit solutions individually.  
2. The solution for the assignment should be submitted as a zip file. The file should be named as  
StudentNameRollNumber.zip.  
3. The submission should contain the following:  
• A python file.  
• The report (as pdf).