1. **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)

2. **CPA:** In this assignment, you will be provided with the power consumption of the last round of AES. The power traces are obtained from SAKURA-G platform that runs an implementation of AES-128 on a Spartan-6 FPGA. The power trace is 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 Correlation Power Attack, and use that code on the given power trace to recover the target byte assigned to your group. The target byte assignment for the groups are given below:

•    Group 1: 1st byte  
•    Group 2: 2nd byte  
•    Group 3: 3rd byte  
•    Group 4: 5th byte  
•    Group 5: 6th byte  
•    Group 6: 7th byte  
•    Group 7: 9th byte  
•    Group 8: 10th byte  
•    Group 9: 11th byte  
•    Group 10: 13th byte

An example code that obtains the 0th byte of the key is provided for your reference. We would like to thank Prof. Debdeep Mukhopadhyay of IIT Kharagpur for kindly providing us the power traces of FPGA based AES implementation.