Assignment 1

Daniel is a security engineer, and he has a got a project for side-channel analysis of an AES hardware implementation. He has already collected power traces for that AES implementation with a 128-bit key 'K' and have stored the traces in "traces_AES.csv" file. The first column in the csv file indicates the plaintext, the second column indicates the ciphertext and rest of the columns indicates the sample points. Now Daniel has to analyse the power traces and will have to find the AES key using Correlation Power Analysis (CPA). Help Daniel to perform the CPA attack.

Note: There are 9 groups and each group have to find a particular key byte of the AES key "K" of 128-bits (16) bytes. We have attached a pdf file that provides the group information and the key byte that the group has to recover.

Each group has to prepare a document with the detailed procedure of the CPA attack on the particular key byte and have to submit the code also. Please make a zip file with name "Assignment1_ Group_Number.zip", for e.g. Group 1 will have to submit the zip file renaming it as "Assignment1_ Group_1.zip".