Indian Institute of Technology (IIT-Kharagpur)

SPRING Semester, 2022
COMPUTER SCIENCE AND ENGINEERING

CS60004: Hardware Security

Coding Exam

Full Marks: 40

Time allowed: 1 hour

1. In this assignment, you need to implement the Correlation Power Analysis (CPA) attack on real power traces of AES. To keep it simple, we target only the first key byte. Here we assume the Hamming Distance (HD) power model. The target architecture uses a register to store the output of every round including the ciphertext. The HD is to be computed between the contents of the register of two consecutive clock cycles. You are provided with a code snippet in Python where a part of the code is missing. Use the comments mentioned in the file to complete the code and compute the first key byte. NOTE: The code may take some time to run. Please be patient while it is running.

Answer the following question based on the output of your CPA code.

(a) What is the value of the first key byte?

(40 marks)