Assignment 1: Trace Identification

Due Date: 25. October 2023, 11:00

Important: Please submit your individual solution before the above-specified due date (and time) digitally in the Moodle course.

- You received two files "Traces_X.dat" for $X \in \{A, B\}$ which each contain five power measurement of a part of an AES encryption.
- The binary format of each power trace is:
  nr_of_points(uint32) | point1(int8) | . . . | pointX(int8)
  Each point represents the power consumption at a specific point in time.
- The binary format of each file is:
  trace1 | trace2 | trace3 | trace4 | trace5
- Plot the contents of each file in a separate coordinate system. Label your axis properly.
  (Deliverables: 2 .png files, 1 plotting script)
- For each trace make an educated guess about the underlying architecture of AES. (hint: You learned four different architectures of AES in the lecture). You are also expected to provide an explanation (1 sentence each) for your answer. Refer to the plot in your answer and describe what part (e.g. how many rounds) of an AES encryption it depicts.
  (Deliverable: 1 .txt file)
- Please write your program in any environment that you like.
- Include all your files in an archive and name it properly:
  <lastname>_Assignment1.zip