Resources on Differential Cryptanalysis and Timing Attacks

Preparation Lecture 5:

- Read the core idea of Differential Cryptanalysis in Section 6.1:
  Differential Cryptanalysis: The Idea, Chapter 6 on the Block Cipher Companion by L. Knudsen
  https://tinyurl.com/3v2ufhj6

- Make sure to understand the AES T-box implementation:
  Read the post here:
  https://blog.tclaverie.eu/posts/understanding-golangs-aes-implementation-t-tables/
  Read the *AES Proposal: Rijndael by J. Daemen, V. Rijmen*, emphasizing on section 5.2.1

- Practice your Matlab coding by following the 1-hour course on matrix, vector and statistical calculations https://matlabacademy.mathworks.com/details/calculations-with-vectors-and-matrices/otmlcvm

Literature Lecture 5:

- Read the rest of of Differential Cryptanalysis in Sections 6.2, 6.3:
  Differential Cryptanalysis: The Idea, Chapter 6 on the Block Cipher Companion by L. Knudsen
  https://tinyurl.com/3v2ufhj6

- Read the early cache attack on AES:
  Cache-timing attacks on AES by D. Bernstein
  https://cr.yp.to/antiforgery/cachetiming-20050414.pdf
  Emphasize on sections 1 until 7