Exercise on AES cache-timing attack

The goal of this exercise is to code, using the MATLAB/Python environment[1], a cache-based timing attack on a Tbox-based AES implementation.

- The provided file (`aes_cache_attack.zip`) contains skeleton code that hints how to attack ciphers AES in file `main.m`.
- The provided file (`aes_cache_attack.zip`) contains 50k time measurements while AES performs table lookups. Every time measurement is labeled by the value of the plaintext byte that is input.

- ▶ Load the time measurements, plaintext labels and server key during the profiling phase (`profile_measurement_and_plaintext_and_key.mat`).
- ▶ Load the time measurements and plaintext labels during the attack phase (`attack_measurement_and_plaintext.mat`).
- ▶ Write code in `main.m` that recovers a key byte used in AES, by utilizing the timing differences
- ▶ **Deliverables:** The MATLAB code and all related files that you used to perform the timing attack.

[1] check https://datanose.nl/#byod to use the UvA MATLAB licence