2022 부채널정보분석 경진대회

2번 문제 : AES-128 정렬

- 문제 요약
  - 정렬되지 않은 파형으로부터 블록 암호 AES-128의 마스터 키를 찾으시오.

- 제공 파일
  - CTF-tracealign-traces.bin : AES-128 암호화 과정의 소비 전력 신호 (정렬 X)
  - CTF-tracealign-plains.bin : AES-128의 평문
  - CTF-tracealign-ciphers.bin : AES-128의 암호문

- 참고 사항
  - 모든 암호화 과정은 동일한 마스터 키를 사용해 수행되었음.
  - AES-128 암호화 과정의 소비 전력 신호는 기존 암호화 과정의 신호에 비해 기준 점으로부터 랜덤으로 50pt 내외로 흔들려있음.

- 알려진 평문-암호문 쌍
  - 평문(C1F2A2B9B8843389A56FDEEBD94FF16C - 암호문(B4FF90D50B9C625B6C09696266256C04)
  - 평문(D8C2867D639F02F2BB86893A1648A01E - 암호문(B296F2394B11D80CD810B48A3F126B6C)
  - 평문(81E5E250AE2A1A8C0FBAC765F3C0B3F7 - 암호문(F1B15FC0FFF65BD76091409C0F4795FC)

- 플래그
  - 복구한 마스터 키 128비트를 MSB 부터 차례로 8비트씩 묶은 것이 Flag의 ASCII 코드임.
  - 각 ASCII 코드에 대응하는 문자를 연접하여 플래그 생성.

- 참고 문헌
  - ref1 : NIST, FIPS-192: ADVANCED ENCRYPTION STANDARD (AES).
  - ref2 : Eric Brier et al., Correlation Power Analysis with a Leakage Model.