2022 부채널정보분석 경진대회

3번 문제 : LEA-128

- 문제 요약
  블록 암호 LEA-128의 마스터 키를 찾으시오.

- 제공 파일
  - CTF-3-LEA-trace.bin : LEA-128 암호화 과정의 소비 전력 신호.
  - CTF-3-LEA-plain.bin : LEA-128의 평문

- 참고 사항
  - 모든 암호화 과정은 동일한 마스터 키를 사용해 수행되었음.
  - 확인용 평문 및 암호문
    - 평문(HEX) : 1f 31 22 39 28 56 14 37 8d d9 fa db c1 a5 5e 7a
    - 암호문(HEX) : 05 e4 eb 4a aa 11 18 84 38 68 ff 24 fe a2 bb da

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

- 참고문헌
  - ref1 : Deukjo Hong et al., LEA: A 128-Bit Block Cipher for Fast Encryption on Common Processors.