2022 부채널정보분석 경진대회

1번 문제 : AES-128

- 문제 요약
  블록 암호 AES-128의 마스터 키를 찾으시오.

- 제공 파일
  - CTF-1-AES-trace.bin : AES-128 암호화 과정의 소비 전력 신호.
  - CTF-1-AES-plain.bin : AES-128의 평문

- 참고 사항
  - 모든 암호화 과정은 동일한 마스터 키를 사용해 수행되었음.

- 알려진 평문-암호문 쌍
  - 평문(B6B6BEB07EA7A79F1472BF8D1BE3D3AE) - 암호문(962D9AE276A53452F8C406ACC67D52B4)
  - 평문(99D56B4A2BB2FA1548499C2CAE8C9650) - 암호문(12E938E3611E9C09895C063D81C5D4D9)
  - 평문(2A5626431DDAC9A2E34050F0E3DE1974) - 암호문(3F561C87AC1182D9B28FCE37B3DD1BF1)

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

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