2022 부채널정보분석 경진대회

4번 문제 : ARIA-128

- 문제 요약

  일부 라운드의 전력 신호만을 이용해 블록 암호 ARIA-128의 마스터 키를 찾아으시오.

- 제공 파일

  - CTF-4-ARIA-trace.bin : ARIA-128 암호화 과정 중에서 2라운드 Diffusion layer ~ 5라운드 Diffusion layer의 소비 전력 신호
  - CTF-4-ARIA-plain.bin : ARIA-128의 평문

- 참고 사항

  - 모든 암호화 과정은 동일한 마스터 키를 사용해 수행되었음. 2(D3) 7(4D) 12(76) 13(CE)번째가 빔
  - 1라운드 키의 일부: CB * 16 A7 91 AA * 47 4D A2 D8 * * 2B C8 83 (*는 제공되지 않음)

- 알려진 평문-암호문 쌍

  - 평문(98A5F86BD2D44502E04C717379AA1882) - 암호문(6F905F30DB9A19D6B6F409CA66230069)
  - 평문(C5FC660BA7E7B4438A991BCDE10E3512) - 암호문(CEFFBC1667B82CFD1AEC0FFDC3F66354)
  - 평문(D59BC361E3BFC15FC0EFC6DC70B3E843) - 암호문(E32A539CC2D4A3E5884AD676EBD30E4C)

- 플래그

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

- 참고문헌

  - Ref.-1 : KISA, 민관겸용 블록 암호 알고리즘 ARIA.
  - Ref.-2 : 서정갑 et al., 블럭 암호 ARIA에 대한 차분전력분석공격.