2022 부채널정보분석 경진대회

8번 문제 : ECDSA-SPA

- 문제 요약
  - $P = kG$ 연산을 수행중이다. 해당 파형을 참고해 k를 찾아라.
- 제공 파일
  - CTF-8-SPA-trace.bin : $P = kG$ 과정의 소비 전력 신호
  - CTF-9-ECDSA-SPA-code.txt : 해당 연산을 수행하는 코드

- 참고 사항
  - CTF-9-ECDSA-SPA-code.txt 내부 ECC_Point_mul 함수가 $P = kG$ 과정을 담고 있음
  - $result = P$, $point = G$, $scalar = k$
  - G: ECC SECR256R1 타원 곡선의 base point
  - k는 255 비트 수이다.
  - G: (0x6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296, 0x4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5)
  - P: (0xa658dad47af5955da32c5bedcfb6ed68f777ef5c2af9d2822ea80b3e6daebbd0, 0x69d5c5bcc656a88977fd6c14908634191d9b7cbef66e2295df4491fc9dee1c80)
- 플래그
  - 복구한 k를 MSB 부터 차례로 8비트씩 묶어 ASCII 코드 변환해 a 생성
  - a를 4글자 단위로 reverse 하면 Flag
  - 각 ASCII 코드에 대응하는 문자를 연접하여 플래그 생성.

- 참고 문헌

  - ref1 : Courrege, et al. "Simple power analysis on exponentiation revisited."
  - ref2 : Johnson, Don, et al. "The elliptic curve digital signature algorithm (ECDSA)."
  - ref3 : Koblitz, Neal, et al. "Guide to elliptic curve cryptography."