# 2024 암호분석경진대회

## 2번 문제

암호가 이론적으로 안전하게 설계되더라도 실제 환경에서 구현되어 운용될 때 소모전력, 실행시간 등의 정보가 발생한다. 부채널 공격은 이러한 정보를 이용하여 암호를 분석하는 기법이다.

**문제**

AES-128 암호화 연산기에 내장된 마스터키를 복구하기 위해 암호화시 소모전력을 측정하였다. 그런데 1천개의 입출력 및 파형이 저장되었으나, 소모전력 측정 중에 문제가 발생하여 파형의 일부분만 저장되었다. 이 파형은 1, 2 라운드 연산 중 일부분의 파형으로 추정된다. 주어진 정보만을 가지고 마스터키를 찾아내시오.

**데이터셋 설명**

■ 2024-contest-sca-tr.bin
(4 Byte, unsigned int) : 파형 개수 N = 1,000
(4 Byte, unsigned int) : 파형 길이 L
(4 Byte * L, float) : 파형1
…
(4 Byte * L, float) : 파형N

■ 2024-contest-sca-tr-reference.bin : AES 전체 파형
(4 Byte, unsigned int) : 파형 개수 N
(4 Byte, unsigned int) : 파형 길이 L
(4 Byte * L, float) : 파형1

■ 2024-contest-sca-pt.txt : 평문
■ 2024-contest-sca-ct.txt : 암호문
각 줄마다 16 Byte Hex 표기 되어 있으며, 평문 암호문 파일의 같은 라인 줄은 AES 암호화의 입출력에 대응